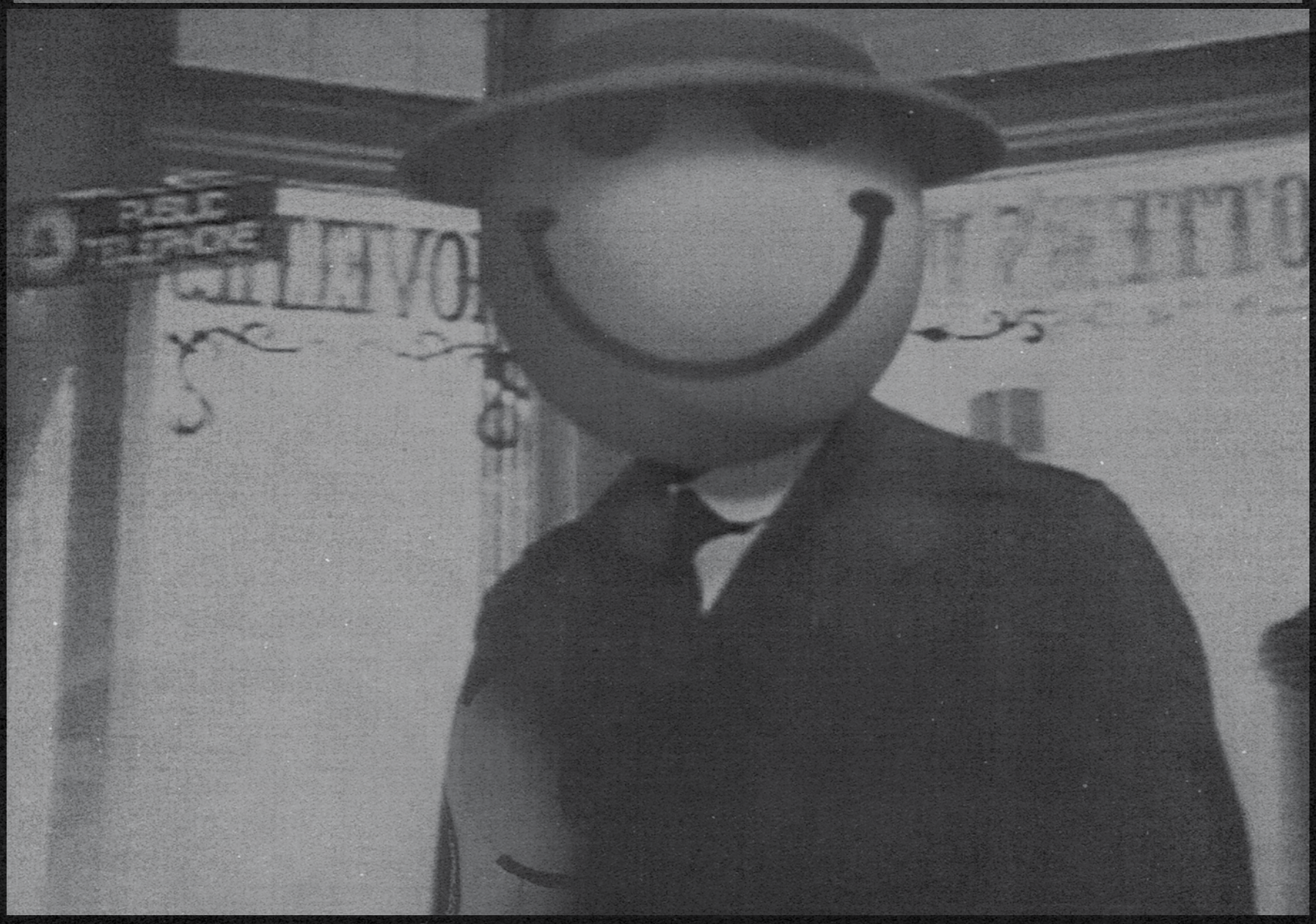
DEF CON TIMES

NO. 203 VOL. 23 LAS VEGAS, NEVADA AUGUST 6-9, 2015 SPECIAL EDITION $FREE

A Chilling Hacker Noir:

THE 23 ENIGMA!



THE SECRET OVERLORDS ARE ALREADY AMONG US. YOU WILL LEARN TO COWER BEFORE THEM SOONER THAN YOU MAY KNOW...

ONCE YOU SEE THE PATTERN
YOU'LL NEVER STOP SEEING IT.

If you're reading this, it's probably too late for me. I spotted the tail days ago. Late-model American sedan, cop shades, Flowbee haircut. Ever since I went down this crazy rabbithole, I knew someone like Mr. Flowbee was eventually going to pay me a visit.

The only thing I can tell you is to keep your eyes open - but not too open. If you let it in all at once you could come untethered in a serious and lasting way.

You'll see it around the edges first. The numbers on receipts, currency, license plates. If you keep digging, maybe you'll notice the odd facts. Like the first telegraph message being a quote from the Book of Numbers. Verse 23. Chapter 23. "What hath God wrought" indeed.

But if you're diligent, and you look past the disaster anniversaries and the easily provable internet falsehoods (it's easy enough to look up the number of vertebrae in the human spine) - you'll notice the scary bit. It's not what the coincidences mean 'out there', in history books and almanacs. Window dressing, the lot of it.

The real kick in the head is how the anomalies are coming for you, personally. How many times a day the 23s and the holy Fives and the fnords are right there in your own datastream, daring you to see them.

That's when you realize the hard bit. The numbers, they aren't part of a conspiracy. The reason they fit so neatly into all the cracks is that everything is made of numbers. The sea, the sky, the fidgety waitress way down the bar. Even you, friend. Even you. The lie is that anything was ever organic, or human or rough to the touch. It's all pixels and probabilities. From inside the machine, it's impossible to tell what kind of simulation this is, but it doesn't matter. Because once you see it, you see it forever. And you'll want to tell someone.

And that's when they send along Lieutennant Flowbee.

For followers of Discordianism, 23 is a holy number. Discordianism is described as "a joke disguised as a religion disguised as a joke".

It takes 23 seconds for blood to flow through the body.

FROM THE EDITOR'S DESK

WELCOME TO DEF CON 23!

Welcome to DEF CON 23! We now are in two hotels, and spreading like a virus. We've tried to set it up such that the Paris side holds all the speaking tracks, and the Ballys side has all the contests, villages, events, and chill out space with close access to the elevators that will take you to the top of Ballys. That is where you'll find Sky Talks, suites, evening parties, and live music.

We have the most space we have ever had, the most contests and villages, and more ways than ever for you to hack the shit out of something. Take advantage of it.

If DEF CON 21 was the year we realized how completely Offense has dominated Defense then DEF CON 23 is the rise of legislation, regulation, activism and a global awareness of the importance of information security. Companies and governments have been wrecked by information breaches. These are very dangerous times for us as a community and a society. The decisions that are made in the next five years will be with us for the next twenty five. We are at the intersection now of politics and tech, and your ability to explain tech to power will be critical in avoiding bad decisions that will hurt us all. All that stuff we were saying about the importance of protecting your networks the last two decades? We weren't lying. Now companies and governments are paying attention, trying the "manage" the problem with insurance, regulation, and legislation. Without addressing the root cause of liability - something the large software makers won't allow - don't expect the needle to move much. Why does Adobe ship their products in the least secure configuration? There is no downside for them and the incentives are all backwards.

I don't think this can last, and I hope the changes will come from within the industry, even if it is for competitive reasons. For example, do you think Boeing, Tesla, and Google like the fact that they have software liability if someone gets injured by their moving data centers, while Oracle has none for their stationary data centers? It is not sustainable in the long run and the sooner we accept this the sooner we can trash the shrink wrap license liability waiver and deal with the real issues: Vendors have few reasons to "ship secure" and uninformed consumers are helpless to defend themselves. Hackers, academics, and researchers are the last line of defense and anything that prevents their work will harm us all.

Next year at DEF CON 24 I expect will be largely influenced by our new robotic overlords, led by the DARPA Cyber Grand Challenge super computer bake off, and the hope that we can somehow automate our way out of the current mess. The thing is, automation is a two way street.

The Dark Tangent

WHAT IS DEF CON?

What is DEF CON? I was recently asked by Russ about my vision of what DEF CON is. First and foremost DEF CON is a hacker conference. I agree with what Vyrus said, DEF CON is our hacker clubhouse.

That means DEF CON is not the IT department, the professional job fair, or the maker fair. DEF CON is about what interests and inspires hackers. We don't seek or accept sponsorships, helping ensure our independence from outside influence.

I believe in giving hackers a chance to show off and prove themselves, and as Jericho once said DEF CON is really a meta-conference - a conference of mini-conferences. We set the tone, direction, and the main content but all the blanks get filled in by the community. The more we can enable that the stronger the conference will become.

-The Dark Tangent

CALL FOR SUITES

ON THE TOP FLOOR OF BALLYS ARE FOUR PENTHOUSE SUITES, AND THESE PEOPLE OR GROUPS ANSWERED THE CALL TO THROW SOMETHING COOL FOR THE HACKING COMMUNITY.

DC801DERLAND

Shenanigans! Count on it. DC801derland is a space for folks to come together and geek out while… Playing classic arcade games on a number of our full size cabinets. Fly drones through an obstacle course for the chance to win prizes worth up to… dollars! Get into the bath tub ball pit to make a new friend. Play one of the many table games we'll be bringing. Get in a robot fight. Watch corny hacker movies. Or just sit and chat at the bar, and talk tech. It's like Chuck E. Cheese … for hackers!

w us at @dc801 on the twitter place for updates.

MSTEDHAXZORS

Come play and create with IoT devices, Kinect sensors, and cloud services at a 3 day hackathon. There will be regular workshops to take you from n00b to ninja, demos, and plenty of opportunity to join in with people doing crazy projects (or for you to pitch, recruit, and build your own).

WHISKEY PIRATES

Need a chill space for hacking hardware/software? Want to play games on full sized arcade machines? Have a cool project that you want to show people? Need to call home form a real life payphone, Feel like watching a robot play Mario? Want to look at silicon wafers under a big ol' microscope? Well stop by, have a drink and hang out.

Follow us @WhiskeyHackers and check whiskeypirates dot com for updates.

WHAT'S NEW?

Every year we make changes to the con, and this year we have made some pretty visible ones .

If you are old school enough you'll remember a time when all Goons wore red shirts, and I've brought that back. I wanted everyone to see how many people it takes to run a con of this size, and to remind everyone that all staff are Goons. If someone is wearing a red shirt than they are on duty and can help answer any questions you may have. If they can't, they'll point you in the right direction.

We've made the 101 track on Thursday an Official track of content, and it will be recorded for later release. As a matter of fact with some of our best content happening in the villages many of them will now be recorded!

With more space we've added more villages and contests, as well as grown the size of the speaking rooms. We're going to be learning as we go along with what works for the new hotel spaces, and any feedback you have is welcome. Please visit https://forum.defcon.org/ and post your thoughts in the "How to make DEF CON 24 better" thread.

Finally the pool party is back! Queer Con is hosting on Friday night, and IOActive and friends are doing one Saturday night. The pool is all the way in the back - quite a walk, but the good news is we can stay open longer with more music. Get some fresh 102 degree air at midnight!

DEF CON MEDIA SERVER

The DEF CON Media server is back!

https://10.0.0.16/ or https://dc23-media.defcon.org/

Browse and leech files from all the past DEF CON conferences as well as a large collection of other hacking cons. About 5TB of data, and more being added all the time up to the last minute! We expect you to leech at full speed, and the server is warmed up and ready to go.

Want to access the files faster? Want to share your own files? Come to the Data Village and use the faster WiFi or plug into a network port.

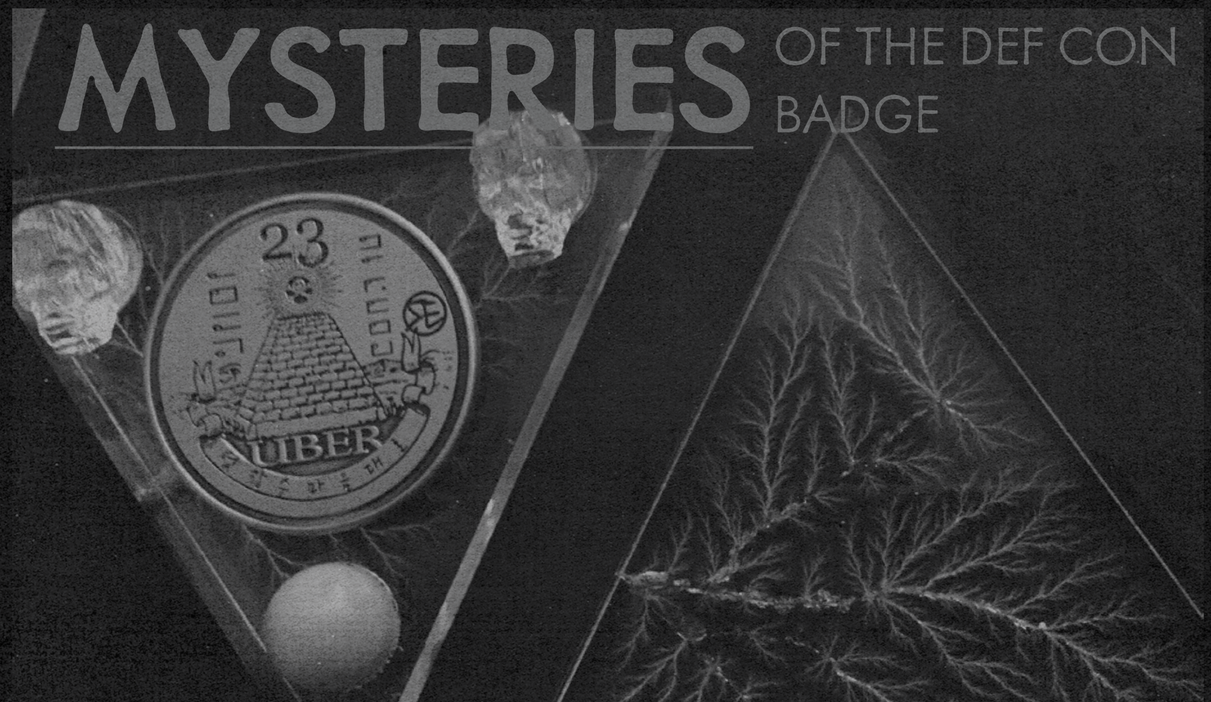
THE HIROSHIMA BOMB WAS DROPPED AT 8:15AM. 8 + 15 = 23. THE DATE WAS 08/06/45. 8 + 6 + 4 + 5 = 23.

CONTENTS OF THIS ISSUE

VgjbhyqagorQrspbajvgubhgbhetbbqsevraqPnrfne (fbzrgenqvgvbafjvyyarireqvr) Hjvyyxabjjung2qbjuraHhafpenzoyr "Ubjqnqqlvfqbvat"

WFST HDXE HGY BNK BAWH QJG PSOR WNFATG IDDW OQUHVNKINGCY GOG CTUK.

MYSTERIES OF THE DEF CON BADGE



The general attendance badge this year is a 7" vinyl record. They are fully mastered and playable, not simply cosmetic. There, you came to DEF CON, and now you have a record. You can quote me on that. ;)

As is par for the course, I had to do something special for the über badges this year. My personal studies this year have brought me to feel a close kinship with Richard Feynman- who was a great hacker. This year's über was inspired by him.

The base of the über badges this year are Lichtenberg sculptures- essentially lightning "fossils" preserved in time. Originally discovered by Georg Christoph Lichtenberg (1742-1799), the physical principles involved in forming Lichtenberg figures evolved into what is now modern-day plasma physics. The über bases are polymethyl methacrylae(PMMA) that have been put through a Dynamitron, a 5 million volt, 150 kW particle accelerator. This irradiates the PMMA with electrons traveling at somewhere between 98.5% and 99.6% of the speed of light. Charging to just below the point of dielectric breakdown, after which an insulated metal spike is used to force focus a discharge. The result is an avalanche breakdown that takes place within approximately 120 nanoseconds. (It is believed that dielectric avalanche breakdown inside a charge- injected solid is the most energetic chemical reaction known, including high explosives.) The resulting patterns left in the PMMA are fossil patterns left by these miniature lightning bolts. These patterns are self-similar, or fractals. I got some great stories from the retired physicists I interviewed about these processes, some of which I'll be sharing in the opening ceremonies presentation, including how the U.S. Air Force holds a patient on the process for fabricating these sculptures...

Speaking of the Air Force, (because chemical reactions that have more kick than high explosives just weren't enough) I decided to also go nuclear- as each of the points on the über badge houses a different form radioactive material.

The first corner holds a glass, Uranium doped marble. These were made by adding Uranium to glass while it was still in a molten state. Each marble contains 3% Uranium 238 (by weight). Just for fun, I put coarse granular Europium phosphorescent powder underneath each piece of glass, which can be seen from the underside of the badge. This powder should glow for approximately 30 hours after 10 minutes of exposure to light.

The second corner holds a small vial of tritium, housed inside a small crystal skull. Tritium is a weak beta emitter, and these vials will glow (without exposure to light) for approximately 20 years. Tritium is commonly found in exit signs and on watch faces or gun sights. Tritium vials are not approved for sale in the United States (ownership is ok- and you CAN buy them in the UK), so be sure to stop by opening ceremonies if you want to hear more about the sourcing story here...

And just for fun under the tritium skulls are Uranium ore samples (consisting of Carnotite, Uraninite, Gummite, Pitchblende, and Uranophane).

The third corner holds a Trinitite sample, underneath a second crystal skull. These samples are collected from the Trinity test site in New Mexico, where on July 16, 1945, the first atomic bomb was detonated. The blast was the equivalent of 18,000 tons of TNT, producing a half- mile diameter fireball. Temperatures at the site exceeded 10 million degrees Fahrenheit (hotter than the Sun). Feynman, Fermi, and Oppenheimer were among those present that day. Feynman is believe to be the only person to witness the explosion without protective goggles. The samples on these badges have been tested and are from approximately 76 meters from ground zero of the Trinity explosion.

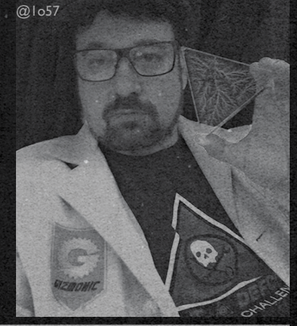
All of the sources of radiation are safe to handle and to be in contact with. The Trinitite has measured gamma activity of 1183.29 CPM ± 5.43 CPM (thanks to Hunter Scott for independent testing). This is two orders of magnitude less than normal background dose radiation, for perspective, if you kept the Uber badge 1 cm away from you for a year. (Radiation exposure from eating a banana is about 0.1 µSv, if you care to calculate the equivalent banana dose...)

Finally, for those unaware, the contest surrounding the badges every year is fierce, and one of the most difficult to complete at DEF CON. It is structured to be solved in groups, so I encourage you to introduce yourself to someone new, and try your hand at the contest.

Have a great DEF CON everyone.

Ryan "1o57" Clarke

@1o57



DEF CON NETWORK LOUSY WITH HACKERS

HERE'S HOW YOU CAN JOIN IN :)

DEF CON WIFI NETWORK | 2.4 & 5 GHZ

DEFCON-OPEN : TYPE: OPEN
DEFCON : TYPE: WPA2/ 802.1X

Once again the DEF CON NOC worked hard to provide you the internetz via WiFi access throughout the Paris & Bally's convention centers.

There are two official ESSIDs to access the conference network: the encrypted and cert/user-based authentication (DefCon) and the unencrypted free-for-all one (DefCon-Open): choose wisely.

Most of the devices these days should are 802.1x compatible, despite the corks some of them still present without an MDM solution behind it, and no one really want your devices managed by us.

http://wifireg.defcon.org is where you can create your credentials, download the digital certificates and fingerprints, and read our awesome support documentation. Remember, practice safe internets: make sure you pick a credential that is not used anywhere else (aka: your Windows domain) and double check your fingerprints. As always, this is a hacker conference.

http://www.defconnetworking.org is your stop for stats, data, and important updates about the network during and post-con.

And, believe it or not, we want your feedback: noc@defconnetworking.org

DEF CON TV TO BROADCAST LIVE!

Nurse your hangover comfortably watching the presentations in your hotel room.

DC TV brings the DEF CON talks to you. Turn on the TV, grab your favorite beverage of choice and aspirin and don't forget to shower.

http://dctv.defcon.org is the spot for all your channel info needs.

Presentations

Thursday Talks

Introduction to SDR and the Wireless Village

DaKahuna

satanklawz

Thursday - 10:00 - 101 Track

In many circumstances, we all have to wear different hats when pursuing hobbies, jobs and research. This session will discuss the exploration and use of software defined radio from two perspectives; that of a security researcher and Ham Radio operator. We will cover common uses and abuses of hardware to make them work like transceivers that the Ham crowed is use too, as well as extending the same hardware for other research applications. Additionally we will highlight some of the application of this knowledge for use at The Wireless Village! Come and join this interactive session; audience participation is encouraged.

Guests N' Goblins: Exposing Wi-Fi Exfiltration Risks and Mitigation Techniques

Peter Desfigies
Cyber Security Investigations Unit, TELUS Security Solutions

Joshua Brierton
Sr. Security Analyst, TELUS Communications

Naveed Ul Islam
Managing Consultant, TELUS

Thursday - 16:00 - 101 Track

Wi-Fi is a pervasive part of everyone's everyday life. Whether it be home networks, open hotspots at cafés, corporate networks or corporate guest networks they can be found virtually everywhere. Fortunately, for the security minded, some steps are taken to secure these weak points in one's infrastructure. Usually this is done through some form of registration page which is common in the case of guest networks. But is this enough? And what new threats could be unleashed from even the most isolated of Wi-Fi networks?

In the most paranoid of cases, companies will generally attempt to isolate Wi-Fi networks from their official networks in order to protect their own assets from attacks, while still ensuring that Wi-Fi is convenient for end users. But there is another way to attack a company that could be damaging to the host company and harmful to other targets. This presentation will go over the utilization of various techniques of getting onto and getting out through publicly accessible Wi-Fi networks for nefarious purposes, termed Wi-Fi Exfiltration. Through this technique one is able to obfuscate their identity by using the host of the Wi-Fi's identity, thus implicating the host in the attack.

During the presentation we will cover the findings through our tests along with a list of recommendations for what can be done to mitigate this risk. This is a must attend session to all security professionals and high level management.

Dark Side of the ELF - Leveraging Dynamic Loading to Pwn Noobs

Alessandro Di Federico
PhD Student, Politecnico di Milano

Yan Shoshitaishvili
PhD Student, UC Santa Barbara

Thursday - 17:00 - 101 Track

The ELF format is ancient, and much mystery lurks in its dark depths. For 16 years, it has safely encompassed our software, providing support for binary loading, symbol resolution, and lots of very useful binary stuff. In that time, security has become a key concern, resulting in binary defenses like NX and ASLR, which have made exploiting vulnerabilities quite difficult. ASLR, for example, randomizes the location of the stack, the heap, libraries, and (optionally), the binary itself at every execution of an application.

There is no easy way to say this: ELF has let us down. In this talk, we'll explore the dark side of ELF. Specifically, we'll show how ELF, by design, implicitly trusts data structures in the ELF headers. Even in the presence of ASLR, an attacker able to corrupt these headers can trick the ELF loader into calling any function in any linked-in library, providing nothing but the name of the binary. In essence, this technique allows an attacker to call arbitrary library functions (such as system()!) without leaking memory addresses. We call this technique Leakless.

While developing Leakless, we checked many different implementations of the standard C library and found that Leakless can be adapted to attack the ELF loader implementations in all of the common ones (i.e., GNU libc, the libc of the major BSDs, and uClibc). In this talk, we'll describe the internals of the ELF format, show how Leakless works to subvert library function resolution, and demonstrate how it can be use to carry out attacks without information disclosures. And, of course, we'll open-source the tool that we developed to make carrying out this attack easier.

Secure Messaging for Normal People

Justin Engler
Senior Security Engineer, iSEC Partners

Thursday - 18:00 - Track 4

"Secure" messaging programs and protocols continue to proliferate, and crypto experts can debate their minutiae, but there is very little information available to help the rest of the world differentiate between the different programs and their features. This talk will discuss the types of attacks various secure messaging features can defend against so those who are tech-savvy but not crypto-experts can make informed decisions on which crypto applications to use.

This talk is intended for people with no preexisting cryptography knowledge. There will be no math or programming knowledge required. The goal is to explain secure messaging concepts such as PKI, PFS, and key validation without diving into heavier crypto, math, or programming content.

Medical Devices: Pwnage and Honeypots

Scott Erven
Associate Director, Protiviti

Mark Collao
Security Consultant, Protiviti

Thursday - 18:00 - 101 Track

We know medical devices are exposed to the Internet both directly and indirectly, so just how hard is it to take it to the next step in an attack and gain remote administrative access to these critical life saving devices? We will discuss over 20 CVEis Scott has reported over the last year that will demonstrate how an attacker can gain remote administrative access to medical devices and supporting systems. Over 100 remote service and support credentials for medical devices will be presented.

So is an attack against medical devices a reality or just a myth? Now that we know these devices have Internet facing exposure and are vulnerable to exploit, are they being targeted? We will release and present six months of medical device honeypot research showing the implications of these patient care devices increasing their connectivity.

Seeing Through the Fog

Zack Fasel
Urbane Security

Thursday - 12:00 - Track 4

Yes. "The Cloud" (drink). Even though many of us would much like to see use of public clouds decline, they're not going away any time soon. And with such, a plethora of companies now have revolutionary new solutions to solve your "cloud problems". From crypto to single sign on with two step auth, proxies to monitoring and DLP, every vendor has a solution, even cloud based for the cloud!

What we haven't seen is much of an open source or community lead solution to these problems. So let's change that.

Zack will review the laundry list of security problems with various cloud providers (and their pluthera of APIs), provide some easy fixes to the common issues seen, and introduce a few new open source tools to help monitor and defend the data and access in the wild.

Alice and Bob are Really Confused

David Huerta
Cryptoparty Organizer

Thursday - 13:00 - Track 4

There have been over 20 cryptoparties in New York City, in which people are introduced to open source cryptography software. This doesn't always go smoothly. Usability experts have only recently being included in the design process for encryption tools, but by and large what we have to work with were designed by cryptography experts in the 90s. I'll be going over some pain points between real-world users and their real-life encounters with open source cryptography tools.

Forensic Artifacts from a Pass the Hash Attack

Gerard Laygui
Security Researcher

Thursday - 15:00 - Track 4

A pass the hash (PtH) attack is one of the most devastating attacks to execute on the systems in a Windows domain. Many system admins are unaware about this type of attack and the amount of damage it can do. This presentation is for the system admins that don't have a full time forensics person working with them. This presentation will help identify key windows events and explain why these events are important. The presentation will also show various free tools that can assist in examining some of the common evidence left behind. The presentation will explain and demonstrate a pass the hash attack against common windows systems in an example domain. In the end, the presentation may offer some insight into what an attacker wants and needs to use PtH to pivot in a network.

Responsible Incident: Covert Keys Against Subverted Technology Latencies, Especially Yubikey

LosT

Thursday - 15:00 - 101 Track

We're no strangers to love
You know the rules and so do I
A full commitment's what I'm thinking of
You wouldn't get this from any other guy
I just wanna tell you how I'm feeling
Gotta make you understand
Never gonna give you up
Never gonna let you down
Never gonna run around and desert you
Never gonna make you cry
Never gonna say goodbye
Never gonna tell a lie and hurt you

Sorry, Wrong Number: Mysteries of the Phone System - Past and Present

"Unregistered436" Patrick McNeil
Security Architect

"Snide" Owen
Security Researcher

Thursday - 16:00 - Track 4

Exploring the phone system was once the new and exciting realm of "phone phreaks," an ancestor of today's computer "hackers." The first phreaks "owned" and explored the vague mysteries of the telephone network for a time until their activities drew too much attention from the phone companies and law enforcement. The phone system evolved, somewhat, in an attempt to shut them out, and phreaking became both difficult and legally dangerous. Such events paralleled a new personal computer "revolution" wherein phone phreaks made the transition from the secret subtleties of telephony to the new and mystical frontier of personal computing. Private BBS(s) and, eventually, the Internet was not only the next logical step forward, but also provided "safer" alternatives that still allowed for the thrill of exploring the mysteries of a new modern age. Telephony, and voice security in general, became, as the years passed, something of a lost art to all but those who remember...

In this presentation we begin our adventure with a journey back in time, starting in the post-war Film Noir era of the 40's and 50's, when users required an operator at the switchboard to make a call, investigating some of the early roots of phreaking that many have forgotten. We will briefly take a look at the weaknesses of early telephone systems and the emergence of the original phreaks in the 50's and 60's who found and exploited them. Our journey will also allow us to demonstrate how some of the same basic phreaking approaches are still applicable to today's "advanced" VoIP systems.

Certainly the initial creation and emergence of VoIP opened a variety of attack vectors that were covered at security conferences at the time. Commercial VoIP adoption, however, remained stagnant until standards and carriers caught up. Some VoIP hacking tools were left unmaintained, and VoIP wasn't the sexy and mysterious attack vector it once was with the exception of tricksters who found old or insecure systems to be easy targets. Due to increased VoIP adoption over the last few years, however, telephony attacks are provocative once again.

As hardboiled VoIP detectives, we'll unravel the mysteries of the curious, shadowy, and secretive world of phreaks, tricksters, and VoIP hackers. We'll compare and contrast old school phreaking with new advances in VoIP hacking. We'll explain how voice systems are targeted, how they are attacked using old and new methods, and how to secure them - with demonstrations along with practical and actionable tips along the way. We may even drop a new VoIP telephony phishing tool to fuse the past and the present..

Backdooring Git

John Menerick
Security @ NetSuite

Thursday - 17:00 - Track 4

Join us for a fun-filled tour of source control management and services to talk about how to backdoor software. We will focus on one of the most popular, trendy SCM tools and related services out there -- Git. Nothing is sacred. Along the way, we will expose the risks and liabilities one is exposed to by faulty usage and deployments. When we are finished, you will be able to use the same tools and techniques to protect or backdoor popular open source projects or your hobby project.

There are exactly 23 characters, numbers, and letters on the face of all U.S. coins.

Hacker in the Wires

Dr. Phil Polstra
Professor, Bloomsburg University

Thursday - 14:00 - Track 4

This talk will show attendees how to use a small ARM-based computer that is connected inline to a wired network for penetration testing. The computer is running a full-featured penetration testing Linux distro. Data may be exfiltrated using the network or via a ZigBee mesh network or GSM modem.

The device discussed in this talk is easily integrated into a powerful penetration test that is performed with an army of ARM-based small computer systems connected by XBee or ZigBee mesh networking.

Some familiarity with Linux and penetration testing would be helpful, but not required.

DEF CON 101: The Panel.

Mike Petruzzi (WiseAcre)
Senior Cyber Security Penetration Tester

Nikita Kronenberg
Not a Security Researcher, DEF CON

PushPin

Plug

Russ Rogers
Chief of Operations, DEF CON

Thursday - 12:00 - 101 Track

DEF CON has changed for the better since the days at the Alexis Park. It has evolved from a few speaking tracks to an event that still offers the speakers, but also Villages, where you can get hands-on experience and Demo Labs where you can see tools in action. Of course, there is still the entertainment and Contest Area, as well as, Capture The Flag. There is so much more to DEF CON than there was in the past and it is our goal to help you get the best experience possible. In addition to introducing each of the different aspects and areas of DEF CON, we have a panel of speakers that will talk about how they came to be part of DEF CON and their personal experiences over the years.

Hardware and Trust Security: Explain It Like I'm 5

Teddy Reed
Security Engineer Facebook

Nick Anderson
Research Scientist

Thursday - 10:00 Track Four

There are a lot of presentations and suggestions that indicate HSMs, TrustZone, AMT, TrEE, SecureBoot, Attestation, TPMs, IOMMU, DRTM, etc. are silver bullets. What does it all mean, should we be afraid, excited, hopeful? Hardware-based security features are not the end of the world, nor its savior, but they can be fun and useful. Although these technologies are vulnerability research targets, their trust concepts can be used to build secure software and devices.

This primer covers practical defensive uses of existing and upcoming hardware security and mobile trust technologies. We will overview the strengths, pitfalls, gotchas of these esoteric acronyms; and explain the capabilities of related features built into consumer and enterprise laptops, mobile, and embedded devices. Let's take a tour around the wild world of hardware and trust security!

Teddy is a Security Engineer at Facebook developing production security tools. He is very passionate about trustworthy, safe, and secure code development. He loves open source and collaborative engineering when scale, resiliency, and performance enable defensive and protective software design. Teddy has published at security conferences on trusted computing, hardware trusted systems, UAVs, botnet development, human performance engineering, competition game theory, biometric vulnerabilities, and PaaS API vulnerabilities.

Nick Anderson is a research scientist at a US super serious secret laboratory. When Nick is not fighting cyber warriors in the cyber threatscape in his cyber career, he is actively engaged in malware research and enjoys failing at web development. Nick received his masters degree from NYU Polytechnic School of Engineering after completing his bachelors degree in Mathematics from the University of Wyoming.

Beyond the Scan: The Value Proposition of Vulnerability Assessment

Damon Small
Security Researcher

Thursday - 14:00 - 101 Track

Vulnerability Assessment is, by some, regarded as one of the least "sexy" capabilities in information security. However, it is the presenter's view that it is also a key component of any successful infosec program, and one that is often overlooked. Doing so serves an injustice to the organization and results in many missed opportunities to help ensure success in protecting critical information assets. The presenter will explore how Vulnerability Assessment can be leveraged "Beyond the Scan" and provide tangible value to not only the security team, but the entire business that it supports.

Hackers Hiring Hackers - How to Do Things Better

Tottenkoph
Security Consultant, Rapid7

IrishMasms
Hacker

Thursday - 11:00 - 101 Track

There are a lot of talks about how to be a better pen tester and workshops that show you how to use all of the cool new tools that are available to make our jobs easier, but there are only a few talks that address what some of us consider to be the hardest part of getting a job in security: the hiring process. The information security field is in desperate need of people with the technical skills hackers have to fill a myriad of roles within organizations across the world. However, both sides of the table are doing horribly when it comes to hiring and interviewing for work.

Organizations are doing poorly trying to communicate expectations for a job, there are people going to interviews without knowing how to showcase their (limited or vast) experience, and some people posture themselves so poorly that the hiring managers don't think the candidates are really interested in the job. This talk takes the experiences of the speakers as both interviewers and interviewees as well as from others within the scene in order to help better prepare hackers to enter (or move within) "the industry" as well as let the people making hiring decisions know what they can do to get the people and experience they need for their teams.

Hacking Web Apps

Brent White
Security Consultant, Solutionary, Inc.

Thursday - 11:00 - Track Four

Assessing the security posture of a web application is a common project for a penetration tester and a good skill for developers to know. In this talk, I'll go over the different stages of a web application pen test, from start to finish. We'll start with the discovery phase to utilize OSINT sources such as search engines, sub-domain brute-forcing and other methods to help you get a good idea of targets "footprint", all the way to fuzzing parameters to find potential SQL injection vulnerabilities. I'll also discuss several of the tools and some techniques that I use to conduct a full application penetration assessment. After this talk, you should have a good understanding of what is needed as well as where to start on your journey to hacking web apps.

Julius Caesar was stabbed 23 times.

Presentations

FRIDAY TALKS

MALWARE IN THE GAMING MICRO-ECONOMY

Zack Allen
Lead Research Engineer, ZeroFOX

Rusty Bower
Information Security Engineer - Riot Games

Friday - 12:00 - Track One

Microeconomics focuses on how patterns of supply and demand determine price and output in individual markets [1]. Within recent years, micro-economies have flourished within the video game industry. Companies like Valve rely heavily on a business model that depends on gamers making purchases for in-game items. Players can trade these items in bulk for a rare item, make bets on a competitive gaming match or gift the item for a charity event.

While originally well-intentioned, creating these micro-economies also created an incentive for criminals to scam and even steal from unsuspecting victims. Traditional scams date as far back to games like Diablo or Runescape where players were duped in trade windows and in game messaging systems were used to steal items. These low-tech strategies are effective, but recently a new, high-tech scam strategy has emerged relying upon malware specifically targeting the Steam micro-economy.

Over the last year, we have collected and reversed dozens of samples of malware that target Steam users. Pieces of malware can be sophisticated RAM scrapers that pilfer an item in memory and send trade requests through the Steam trading API, or as simple as a remote login service. The end result is the same - the hacker loots the victim's backpack of in game items to sell them on the market for profit. This talk focuses on the techniques we have found in these samples, surveys of victims of these scams and the distribution of money lost from them (up to the $1000s of dollars for users in some cases) and the defenses Steam has put in place to combat this hacker underground.

HOW TO SECURE THE KEYBOARD CHAIN

Paul Amicelli
Student from IT Engineering School - ESIEA in Laval, France

Baptiste David
Engineer from IT Engineer School - ESIEA in Laval, France

Friday - 16:30 - Track One

Keyloggers are hardware or software tools that record keystrokes. They are an overlooked threat to the computer security and user's privacy. As they are able to retrieve all sensitive information typed on a keyboard in an almost invisibly way , they need to be seriously considered both for companies and individuals. Almost all the security measures against keyloggers are post-active and static.

*So what if the solution were to be proactive, and use the same technology as keyloggers do, in order to fool them ? This is all about this presentation, a way of fooling all known and unknown keyloggers (physicals, kernel-mode and user-mode) through a kernel mode driver developed under Windows. The technical details will be presented during the presentation, as well as the results and propositions.

Basically, the idea is to use a kernel mode driver which encrypts each keyboard key hit, at a very low level in the system (near the driver port). The encryption is made according to a common key, exchanged with a client application which needs to ensure that the entered text is secured and not recorded. After the driver has encrypted a key, it spreads it to the entire system. Thus, only the client application, holding the encryption key, can decrypt the keyboard key. In this way, the whole system is fooled.

HOW TO HACK YOUR WAY OUT OF HOME DETENTION

AmmonRa
Security Researcher

Friday - 15:00 - Track One

Home detention and criminal tracking systems are used in hostile environments, and because of this, the designers of these trackers incorporate a range of anti-removal and tamper detection features. Software security, however, is an area on which less focus is placed.

This talk will cover practical attacks against home detention tracking systems, with a focus on software security. Intercepting and modifying tracking information sent from the device in order to spoof the tracker's location will be demonstrated.

General information about how home detention tracking systems operate will be discussed, including the differences between older proximity based systems which used landlines, and newer models which use GPS and cellular networks. Topics will include how to (legally) get hold of and test a real world device, and how to use cheap software defined radios to spoof GSM cell towers. Focus will be on the details of how one particular device is constructed, how it operates and the vulnerabilities it was found to contain. How these vulnerabilities can be exploited and the challenges of doing so in the wild will also be covered.

WHEN THE SECRETARY OF STATE SAYS: "PLEASE STOP HACKING US..."

David An
Former U.S. State Department

Friday - 16:00 - Track Three

Senior American officials routinely hold dialogues with foreign officials to discuss cyber espionage. However, if a cyber attack can be performed through proxy servers jumping several countries before reaching the U.S., then can anyone ever be sure of who is really behind the attack? Yet we often see newspaper headlines clearly identifying that one country is hacking another country through state-sponsored, cyber criminal, or hacktivist means. Even if government cyber analysts with TS/SCI security clearances have high confidence in the identity of an attacker based on forensics and human intelligence, what are the challenges in effectively addressing the topic in a diplomatic or military dialogue with the attacker country?

Two major roadblocks in cyber diplomacy are the "attribution problem," and the related "disclosure dilemma." If there is indeed an attribution problem—when a country cannot be sure which other state is hacking it because a third country could be using it as a proxy—then a country could never accuse another countries of state-sponsored cyber attacks. Yet, countries routinely accuse others of cyber attacks, the public sees this in newspapers almost every day, and it is often an important topic in bilateral dialogues. Furthermore, the disclosure dilemma occurs when a country has both incentives and disincentives to disclose details on how it was hacked. On one hand, evidence will prove its case, but on another hand, evidence will make the attacker more savvy and careful not to repeat the same mistakes next time. Disclosure could create a stronger adversary. These are major concerns in the practice of cyber diplomacy today.

My presentation identifies how government-to-government cyber diplomacy works, examines the attribution problem and disclosure dilemma more fully, and shows how the U.S. approaches this topic differently with partners versus potential adversaries. This is not a technical presentation, but rather it is a policy presentation on cyber diplomacy drawing from political science and my diplomatic experience.

FUN WITH SYMBOLIKS

ATLAS
dude at Grimm

Friday - 17:00 - Track Two

Asking the hard questions... and getting answer! Oh binary, where art thine vulns?

Symbolic analysis has been a "thing" for 20 years, and yet it's still left largely to the obscure and the academic researchers (and NASA). several years ago, Invisigoth incorporated the Symboliks subsystem into the Vivisect binary analysis framework. due to that inclusion, the very nature of binary analysis has been broken down, rethought, and arisen out of the ashes. this talk will give an introduction into Symboliks, Graph Theory, and the path forward for reverse engineering and vulnerability research, all from an interactive Python session or scripts.

QUANTUM COMPUTERS VS. COMPUTERS SECURITY

Jean-Philippe Aumasson
Principal Cryptographer, Kudelski Security, Switzerland

Friday - 15:00 - Track Four

We've heard about hypothetical quantum computers breaking most of the public-key crypto in use—RSA, elliptic curves, etc.—and we've heard about "post-quantum" systems that resist quantum computers. We also heard about quantum computers' potential to solve other problems considerably faster than classical computers, such as discrete optimization, machine learning, or code verification problems. And we heard about a commercial quantum computer, and we heard vendors of quantum key distribution or quantum random number generators promise us security as solid as the laws of physics. Still, most of us are clueless regarding:

- How quantum computers work and why they could solve certain problems faster than classical computers?
- What are the actual facts and what is FUD, hype, or journalistic exaggeration?
- Could quantum computers help in defending classical computers and networks against intrusions?
- Is it worth spending money in post-quantum systems, quantum key distribution, or in purchasing or developing of a quantum computer?
- Will usable quantum computers be built in the foreseeable future?

This talk gives honest answers to those questions, based on the latest research, on analyses of the researchers' and vendors' claims, and on a cost-benefit-risk analyses. We'll expose the fundamental principles of quantum computing in a way comprehensible by anyone, and we'll skip the technical details that require math and physics knowledge. Yet after this talk you'll best be able to assess the risk of quantum computers, to debunk misleading claims, and to ask the right questions.

CRACKING CRYPTOCURRENCY BRAINWALLETS

Ryan Castellucci
Security Researcher, White Ops

Friday - 14:00 - Track Four

Imagine a bank that, by design, made everyone's password hashes and balances public. No two-factor authentication, no backsies on transfers. Welcome to "brainwallets", a way for truly paranoid cryptocurrency users to wager their fortunes on their ability to choose a good password or passphrase.

Over the last decade, we've seen the same story play out dozens of times - a website is broken into, the user database is posted online, and most of the password hashes are cracked. Computers are now able make millions, billions or even trillions of guesses per second. Every eight character password you can type on a standard keyboard and every combination of five common english words could be tried in less than a day by today's botnets. Can people come up with passphrases able to stand up to that when money is on the line? Let's find out.

For this talk, I will be releasing my high speed brainwallet cracker, "Brainflayer". I'll cover a history of brainwallets, safer passphrase-based wallet generation, passphrase security, in-the-wild cracking activity, and how I accidently stole 250 Bitcoins (and tracked down the owner to give them back).

BUGGED FILES: IS YOUR DOCUMENT TELLING ON YOU?

Daniel "unicornFurnace" Crowley
Security Consultant, NCC Group

Damon Smith
Associate Security Consultant, NCC Group

Friday - 10:00 - Track 4

Certain file formats, like Microsoft Word and PDF, are known to have features that allow for outbound requests to be made when the file opens. Other file formats allow for similar interactions but are not well-known for allowing such functionality. In this talk, we explore various file formats and their ability to make outbound requests, as well as what that means from a security and privacy perspective. Most interestingly, these techniques are not built on mistakes, but intentional design decisions, meaning that they will not be fixed as bugs. From data loss prevention to de-anonymization to request forgery to NTLM credential capture, this presentation will explore what it means to have files that communicate to various endpoints when opened.

REVISITING RE:DOS

Eric (XlogicX) Davisson
Not a security researcher

Friday - 15:00 - Track Three

Regular Expression Denial of Service has existed for well over a decade, but has not received the love it deserves lately. There are some proof of concept attacks out there currently, most of which are ineffective due to implementation optimizations. Regardless of the effectiveness most of these PoC's are geared only to NFA engines.

This talk will demonstrate working PoC's that bypass optimizations. Both NFA and DFA engines will get love. Tools will be released (with demonstration) that benchmark NFA/DFA engines and automate creation of 'evil strings' given an arbitrary regular expression. Attendees can expect a review of regex and a deep under the hood explanation of both regex engines before abuses ensue.

LICENSED TO PWN: THE WEAPONIZATION AND REGULATION OF SECURITY RESEARCH

Jim Denaro
Dave Aitel
Matt Blaze
Nate Cardozo
Mara Tam
Special Guest – TBA

Friday - 11:00 - Track Two

Security research is under attack. Updates to the Wassenaar Arrangement in 2013 established among its 41 member nations an agreement to place a variety of previously undesignated "cybersecurity items" under export control. After 18 months and a half-dozen open advisory meetings, the U.S. has taken the entire security research community by surprise with its proposed rule; we are confronted by a sweeping implementation with profound consequences for academia, independent research, commercial cybersecurity, human rights, and national security.

While the outcome of this round of regulatory intervention is still uncertain, the fact that there will be more is not. This panel of experts will discuss the context, history, and general process of regulation, as well the related question of "weaponized" research in regulatory discourse.

There is significant daylight between the relatively lax text of the Wassenaar Arrangement itself and the extraordinarily broad implementation proposed in the U.S. What will the practical effects of those differences be, and why did the U.S. diverge from the Wassenaar text? Regulators are, even now, still struggling to comprehend what the consequences of this new "cyber rule" might be. So, how are we to understand this regulatory process? What are its objectives? Its impacts? Its limits? How can we influence its outcomes?

Eleventh-hour interventions are quickly becoming a hallmark of regulatory activities with implications for the wider world of information security; the fight here is almost exclusively a rearguard action. Without resorting to the usual polemics, what failures of analysis and advice are contributing to these missteps – on both sides? What interests might encourage them? How are security researchers being caught so off-balance? Come victory or despair in the present case, this panel aims to answer the question of whether there is a solution that prevents technology transfer to hostile nations while still enabling free markets, freedom of expression, and freedom of research.

FIGHTING BACK IN THE WAR ON GENERAL PURPOSE COMPUTERS

Cory Doctorow
Author & Activist, Electronic Frontier Foundation

Friday - 11:00 - Track Three

EFF's Apollo 1201 project is a 10-year mission to abolish all DRM, everywhere in the world, within a decade. We're working with security researchers to challenge the viability of the dread DMCA, a law that threatens you with jail time and fines when you do your job: discover and disclosing defects in systems that we rely on for life and limb.

USB ATTACK TO DECRYPT WI-FI COMMUNICATIONS

Jeremy Dorrough
Senior Network Security Architect / Genworth Financial

Friday - 12:00 - Track Three

The term "Bad USB" has gotten some much needed press in last few months. There have been talks that have identified the risks that are caused by the inherent trust between the OS and any device attached by USB. I found in my research that most of the available payloads for the USB rubber ducky would be stopped by common enterprise security solutions. I then set out to create a new exploit that would force the victim to trust my Man-In-The-Middle access point. After my payload is deployed, all Wi-Fi communications will be readable, including usernames, passwords and authentication cookies. The attack will work without the need of elevating privileges, which makes it ideal for corporate environments.

STAGEFRIGHT: SCARY CODE IN THE HEART OF ANDROID

Joshua J. Drake
Sr. Director of Platform Research and Exploitation, Zimperium

Friday - 11:00 - Track One

With over a billion activated devices, Android holds strong as the market leading smartphone operating system. Underneath the hood, it is primarily built on the tens of gigabytes of source code from the Android Open Source Project (AOSP). Thoroughly reviewing a code base of this size is arduous at best — arguably impossible. Several approaches exist to combat this problem. One such approach is identifying and focusing on a particularly dangerous area of code.

This presentation centers around the speaker's experience researching a particularly scary area of Android, the Stagefright multimedia framework. By limiting his focus to a relatively small area of code that's critically exposed on 95% of devices, Joshua discovered a multitude of implementation issues with impacts ranging from unassisted remote code execution down to simple denial of service. Apart from a full explanation of these vulnerabilities, this presentation also discusses; techniques used for discovery, Android OS internals, and the disclosure process. Finally, proof-of-concept code will be demonstrated.

After attending this presentation, you will understand how to discover vulnerabilities in Android more effectively. Joshua will show you why this particular code is so scary, what has been done to help improve the overall security of the Android operating system, and what challenges lie ahead.

CRYPTO FOR HACKERS

Eijah
Founder, Demonsaw

Friday - 11:00 - 101 Track

Hacking is hard. It takes passion, dedication, and an unwavering attention to detail. Hacking requires a breadth of knowledge spread across many domains. We need to have experience with different platforms, operating systems, software packages, tools, programming languages, and technology trends. Being overly deficient in any one of these areas can add hours to our hack, or even worse, bring us total failure.

And while all of these things are important for a well-rounded hacker, one of the key areas that is often overlooked is cryptography. In an era dominated by security breaches, an understanding of encryption and hashing algorithms provides a tremendous advantage. We can better hone our attack vectors, especially when looking for security holes. A few years ago I released the first Blu-Ray device key, AA856A1BA814AB99FFDEBA6AEFBE1C04, by exploiting a vulnerability in an implementation of the AACS protocol. As hacks go, it was a simple one. But it was the knowledge of crypto that made it all possible.

This presentation is an overview of the most common crypto routines helpful to hackers. We'll review the strengths and weaknesses of each algorithm, which ones to embrace, and which ones to avoid. You'll get C++ code examples, high-level wrapper classes, and an open-source library that implements all the algorithms. We'll even talk about creative ways to merge algorithms to further increase entropy and key strength. If you've ever wanted to learn how crypto can give you an advantage as a hacker, then this talk is for you. With this information you'll be able to maximize your hacks and better protect your personal data.

UNBOOTABLE: EXPLOITING THE PAYLOCK SMARTBOOT VEHICLE IMMOBILIZER

FLUXIST
Hacker, Entrepreneur

Friday - 16:00 - Track One

Many of us have seen the big yellow "boot" on the wheel of a parked car, marking like a scarlet letter some poor sap who hasn't paid his parking tickets. Since 2005 many US municipalities have switched from a manual boot to the PayLock SmartBoot. With just a phone call and a credit card you can pay your fines and extortionate fees and fill the county coffers — and in return they'll give you the secret code to type in and unlock the electronic vehicle immobilizer. But what if there were another way to remove the boot, quicker than a phone call and a credit card payment? Join me in a thorough reverse engineering of the PayLock SmartBoot as we disassemble one, recover and analyze the firmware from the embedded controller, and find the secrets to thoroughly pwn the device. This talk will reveal a backdoor that can be used to disarm every SmartBoot in over 50 municipalities.

HOOKED BROWSER MESHED-NETWORKS WITH WEBRTC AND BEEF

Christian (@xntrik) Frichot
Principal Security Consultant at Asterisk Information Security

Friday - 18:00 - Track Three

One of the biggest issues with BeEF is that each hooked browser has to talk to your BeEF server. To try and avoid detection, you often want to try and obfuscate or hide your browsers, particularly if you're heavily targeting a single organization. Don't worry Internet-friends, those crazy pioneers at Google, Mozilla and Opera have solved this problem for you with the introduction of Web Real-Time Communications (WebRTC). Initially designed to allow browsers to stream multimedia to each other, the spec has made its way into most Chrome and Firefox browsers, not to mention it's enabled by default.

Using this bleeding-edge web technology, we can now mesh all those hooked browsers, funnelling all your BeEF comms through a single sacrificial beach-head. Leveraging WebRTC technologies (such as STUN/TURN and even the fact the RTC-enabled browsers on local subnets can simply UDP each other), meshing browsers together can really throw a spanner into an incident-responders work. The possibilities for a browser-attacker are fairly endless, channeling comms through a single browser, or, making all the browsers communicate with each other in round-robin. This is just another tool tucked into your belt to try and initiate and maintain control over browsers.

This presentation will present a background into WebRTC, and then demonstrate the WebRTC BeEF extension. (Bloody JavaScript...)

GOODBYE MEMORY SCRAPING MALWARE: HOLD OUT TILL "CHIP AND PIN"

Weston Hecker
SR Pentester, Sr Systems Security Analyst at "KLJ Security"

Friday - 11:00 - Track Four

Proof of concept for stopping credit card theft in memory skimming operations .Alternative methods of stopping credit card skimming

I am leading project on Free Open Source software that attacks POS skimming malware. Launching platform and concept for stores to not be low hanging fruit In effect making it no longer possible to sell credit card numbers from skim breaches. Better collection of forensic data with cannery features (such as putting flagged card into memory so if it is skimmed it will be flagged at processor and catch the breaches much faster)Injects 1-500 false random CC numbers for every one legitimate CC number that is entered. In effect making stolen credit card batches harder to sell. I will go in detail of how criminals Steal and sell credit cards at this time. This is a software for making credit cards numbers harder to steal in the methods that have been happening in larger breaches Target, Home Depot.

LOW-COST GPS SIMULATOR – GPS SPOOFING BY SDR

Lin Huang
Senior wireless security researcher, Qihoo 360 Technology Co. Ltd.

Qing Yang
Team Leader of Unicorn Team, Qihoo 360 Technology Co. Ltd.

Friday - 15:00 - Track Two

It is known that GPS L1 signal is unencrypted so that someone can produce or replay the fake GPS signal to make GPS receivers get wrong positioning results. There are many companies provide commercial GPS emulators, which can be used for the GPS spoofing, but the commercial emulators are quite expensive, or at least not free. Now we found by integrating some open source projects related to GPS we can produce GPS signal through SDR tools, e.g. USRP / bladeRF. This makes the attack cost very low. It may influence all the civilian use GPS chipset. In this presentation, the basic GPS system principle, signal structure, mathematical models of pseudo-range and Doppler effect will be introduced. The useful open source projects on Internet will be shared with attendees.

DRIVE IT LIKE YOU HACKED IT: NEW ATTACKS AND TOOLS TO WIRELESSLY STEAL CARS

Samy Kamkar

Friday - 13:00 - Track Two

Gary Numan said it best. Cars. They're everywhere. You can hardly drive down a busy freeway without seeing one. But what about their security?

In this talk I'll reveal new research and real attacks in the area of wirelessly controlled gates, garages, and cars. Many cars are now controlled from mobile devices over GSM, while even more can be unlocked and ignitions started from wireless keyfobs over RF. All of these are subject to attack with low-cost tools (such as RTL-SDR, GNU Radio, HackRF, Arduino, and even a Mattel toy).

We will investigate how these features work, and of course, how they can be exploited. I will be releasing new tools and vulnerabilities in this area, such as key-space reduction attacks on fixed-codes, advanced "code grabbers" using RF attacks on encrypted and rolling codes, and how to protect yourself against such issues.

By the end of this talk you'll understand not only how vehicles and the wirelessly-controlled physical access protecting them can be exploited, but also learn about various tools for car and RF research, as well as how to use and build your own inexpensive devices for such investigation.

Ladies and gentlemen, start your engines. And other people's engines.

HARNESS: POWERSHELL WEAPONIZATION MADE EASY (OR AT LEAST EASIER)

Rich Kelley
security researcher & co-founder of Gray Tier Technologies

Friday - 16:00 - Track Two

The Harness toolset aims to give penetration testers and red teams the ability to pull a remote powershell interface with all the same features of the native Powershell CLI and more. Several tools and utilities have been released to solve the powershell weaponization problem, but no freely available tool give operators the full capabilities of powershell through a remote interface. We'll start the talk with a quick survey of the previous methods of weaponizing powershell, and then move into the capabilities of the Harness toolset which includes a fully interactive powershell CLI, and remote importing of modules across the wire without staging. We'll conclude with taking a look at the underlying code that makes the toolset work, and briefly discuss planned features. The Harness toolset will be released open source in conjunction with this talk.

LTE RECON AND TRACKING WITH RTLSDR

Ian Kline
Wolf Den Associates

Friday - 16:00 - 101 Track

Since RTLSDR became a consumer grade RX device, numerous talks and open source tools enabled the community to monitor airplanes, ships, and cars... but come on, what we really want to track are cell phones. If you know how to run cmake and have $50 to pick up an RTLSDR-E4000, I'll make sure you walk out of here with the power to monitor LTE devices around you on a slick Kibana4 dashboard. You'll also get a primer on geolocating the devices if you've got a second E4000 and some basic soldering skills.

ROCKING THE POCKET BOOK: HACKING CHEMICAL PLANT FOR COMPETITION AND EXTORTION

Marina Krotofil
Senior Security Consultant. European Network for Cyber Security

Jason Larsen
Principal Security Consultant, IOActive

Friday - 18:00 - 101 Track

The appeal of hacking a physical process is dreaming about physical damage attacks lighting up the sky in a shower of goodness. Let's face it, after such elite hacking action nobody is going to let one present it even at a conference like DEF CON. As a poor substitute, this presentation will get as close as using a simulated plant for Vinyl Acetate production for demonstrating a complete attack, from start to end, directed at persistent economic damage to a production site while avoiding attribution of production loss to a cyber-event. Such an attack scenario could be useful to a manufacturer aiming at putting competitors out of business or as a strong argument in an extortion attack.

Picking up a paper these days it's easy to find an article on all the "SCADA insecurity" out there associated with an unstoppable attacker with unsophisticated goal of kicking up another apocalypse. Sorry to disappoint excited crowd but formula "Your wish is my command" does not work for control systems. The target plant is not designed in a hacker friendly way. Hopefully by the end of the presentation, the audience will understand the difference between breaking into the system and breaking the system, obtaining control and being in control. An attacker targeting a remote process is not immediately gifted with complete knowledge of the process and the means to manipulate it. In general, an attacker follows a series of stages before getting to the final attack. Designing an attack scenario is a matter of art as much as economic consideration. The cost of attack can quickly exceed damage worth. Also, the attacker has to find the way to compare between competing attack scenarios.

In traditional IT hacking, a goal is to go undetected. In OT (operational technologies) hacking this is not an option. An attack will change things in the real world that cannot be removed by simply erasing the log files. If a piece of equipment is damaged or if a plant suddenly becomes less profitable, it will be investigated. The attacker has to create forensic footprint for investigators by manipulating the process and the logs in such a way that the analysts draw the wrong conclusions.

Exploiting physical process is an exotic and hard to develop skill which have so far kept a high barrier to entry. Therefore real-world control system exploitation has remained in the hands of a few. To help the community mastering new skills we have developed „Damn Vulnerable Chemical Process" – first open source framework for cyber-physical experimentation based on two realistic models of chemical plants. Come to the session and take your first master class on complex physical hacking.

HACK THE LEGACY! IBM I (AKA AS/400) REVEALED.

Bart Kulach (Bartlomiej Jakub Kulach)
Security Researcher

Friday - 17:00 - Track Four

Have you ever heard about the famous "green screen"? No, it's not a screensaver... Believe me, it still does exist!

In many industries, although the front-end systems are all new and shiny, in the back-end they still rely on well-known, proven IBM i (aka AS/400) technology for their back-office, core systems. Surprisingly, nobody truly seems to care about the security. Even if these nice IBM heavy black boxes are directly connected to the Internet...

The aim of the talk is to give you more insight in a number of techniques for performing a security test of / securing an IBM i system from perspective of

an external and internal intruder. Methods like privilege escalation by nested user switching, getting full system access via JDBC or bypassing the "green screen" (5250) limitations will be presented.

Last but not least: I will also show a undocumented output format of the built-in password transfer API, giving you direct access to all password hashes. Even IBM engineers may wonder...

TELL ME WHO YOU ARE AND I WILL TELL YOU YOUR LOCK PATTERN

Marte Løge
Security Researcher

Friday - 16:00 - Track Four

You are predictable. Your passwords are predictable, and so are your PINs. This fact is being used by the hackers, as well as the agencies watching you. But what about your Android lock patterns? Can who you are reveal what patterns you create?

This presentation will present the result from an analysis of 3400 user-selected patterns. The interesting part is that we collected additional information about the respondents, not just the patterns themselves.

Will being left-handed and having experience with security affect the way you create your lock patterns? There are 389,112 possible patterns. Your full device encryption won't save you if your lock pattern is L - as in "looser".

REMOTE ACCESS, THE APT

Ian Latter
Midnight Code

Friday - 14:00 - Track Three

ThruGlassXfer (TGXf) is a new and exciting technique to steal files from a computer through the screen.

Any user that has screen and keyboard access to a shell (CLI, GUI or browser) in an enterprise IT environment has the ability to transfer arbitrary data, code and executables in and out of that environment without raising alarms, today. This includes staff, partners and suppliers, both on and off-shore. And implementation of best practice Data Center (Jump hosts), Perimeter / Remote Access (VPN, VDI, ..) and End Point Security (DLP, AV, ..) architectures have no effect on the outcome.

In this session I will take you from first principles to a full exploitation framework. At the end of the session you'll learn how build on this unidirectional file transfer and augment the solution into a full duplex communications channel (a virtual serial link) and then a native PPP link, from an user owned device, through the remote enterprise-controlled screen and keyboard, to the most sensitive infrastructure in the enterprise. In this special DEF CON presentation I will also be releasing the new high-speed data exfiltration tool, hsTGXf.

This is an exciting and cross-discipline presentation that picks up the story in the DEC VT220 terminal era and will take you on a journey to exploiting modern enterprise security architectures. So join me, whatever your knowledge or skill-set and learn something interesting!

INFORMATION ACCESS AND INFORMATION SHARING: WHERE WE ARE AND WHERE WE ARE GOING

Alejandro Mayorkas
Department of Homeland Security

Friday: 10:00 - Track 2

The underbelly of the Internet has been in a precarious condition for a while now. Even with all the knowledge about it's weaknesses, we only make slow progress in implementing technology to secure it. We see BGP routing leaks on a regular basis. It almost feels like we take it for granted but at the same time it undermines our trust in the Internet. In this talk, we'll review the current situation for BGP, a foundational piece of the network we all rely on, and focus on the practical implementation of available countermeasures through live demos and examples. In and of itself, we launch a call to action for private organizations, government entities, and academia alike to roll up the sleeves and get cracking at fixing our Internet. If we want to keep trust in "The Internet of Things," we first have to build trust in the network that powers it.

PUT ON YOUR TINFO_T HAT IF YOU'RE MY TYPE

MIAUBIZ
Senior Dr. at Azimuth Security

Friday - 16:30 - Track Three

The IDA Pro APIs for interacting with type information are full of opportunities (horrible problems). I will show you how to create unparseable types, how to apply these types to functions and variables and how to transfer these types from one IDB to another.

SEPARATING BOTS FROM THE HUMANS

Ryan Mitchell
Software Engineer, LinkeDrive Inc

Friday - 16:30 - Track Four

There's an escalating arms race between bots and the people who protect sites from them. Bots, or web scrapers, can be used to gather valuable data, probe large collections of sites for vulnerabilities, exploit found weaknesses, and are often unfazed by traditional solutions like robots.txt files, Ajax loading, and even CAPTCHAs. I'll give an overview of both sides of the battle and explain what what really separates the bots from the humans. I'll also demonstrate and easy new tool that can be used to crack CAPTCHAs with high rates of success, some creative approaches to honeypots, and demonstrate how to scrape many "bot-proof" sites.

RED VS. BLUE: MODERN ACTIVE DIRECTORY ATTACKS & DEFENSE

Sean Metcalf
CTO, DAn Solutions, Inc.

Friday - 13:00 - Track Three

Kerberos "Golden Tickets" were unveiled by Alva "Skip" Duckwall & Benjamin Delpy in 2014 during their Black Hat USA presentation. Around this time, Active Directory (AD) admins all over the world felt a great disturbance in the Force. Golden Tickets are the ultimate method for persistent, forever AD admin rights to a network since they are valid Kerberos tickets and can't be detected, right?

This talk explores the latest Active Directory attack vectors and describes how Golden Ticket usage can be detected. When forged Kerberos tickets are used in AD, there are some interesting artifacts that can be identified. Yes, despite what you may have read on the internet, there are ways to detect Golden & Silver Ticket usage.

Skip the fluff and dive right into the technical detail describing the latest methods for gaining and maintaining administrative access in Active Directory, including some sneaky AD persistence methods. Also covered are traditional security measures that work (and ones that don't) as well as the mitigation strategies that disrupts the attacker's preferred game-plan. Prepare to go beyond "Pass-the-Hash" and down the rabbit hole.

Some of the topics covered:

- Sneaky persistence methods attackers use to maintain admin rights.
- How attackers go from zero to (Domain) Admin
- MS14-068: the vulnerability, the exploit, and the danger.
- "SPN Scanning" with PowerShell to identify potential targets without network scans (SQL, Exchange, FIM, webservers, etc.).
- Exploiting weak service account passwords as a regular AD user.
- Mimikatz, the attacker's multi-tool.
- Using Silver Tickets for stealthy persistence that won't be detected (until now).
- Identifying forged Kerberos tickets (Golden & Silver Tickets) on your network.
- Detecting offensive PowerShell tools like Invoke-Mimikatz.
- Active Directory attack mitigation.

Kerberos expertise is not required since the presentation covers how Active Directory leverages Kerberos for authentication identifying the areas useful for attack. Information presented is useful for both Red Team & Blue Team members.

DETECTING RANDOMLY GENERATED STRINGS; A LANGUAGE BASED APPROACH

Mahdi Namazifar
Senior Data Scientist, Talos Team, Cisco Systems

Friday - 16:30 - 101 Track

Numerous botnets employ domain generation algorithms (DGA) to dynamically generate a large number of random domain names from which a small subset is selected for their command and control. A vast majority of DGA algorithms create random sequences of characters. In this work we present a novel language-based technique for detecting strings that are generate by chaining random characters. To evaluate randomness of a given string (domain name in this context) we lookup substrings of the string in the dictionary that we've built for this technique, and then we calculate a randomness score for the string based on several different factors including length of the string, number of languages that cover the substrings, etc. This score is used for determining whether the given string is a random sequence of characters. In order to evaluate the performance of this technique, on the one hand we use 9 known DGA algorithms to create random domain names as DGA domains, and on the other hand we use domain names from the Alexa 10,000 as likely non-DGA domains. The results show that our technique is more than 99% accurate in detecting random and non-random domain names.

HACKING SQL INJECTION FOR REMOTE CODE EXECUTION ON A LAMP STACK

Nemus
Software Engineer

Friday - 14:00 - 101 Track

Remember that web application you wrote when you where first learning PHP? Ever wonder how vulnerable that code base is? Through the perspective of an attacker you will see how SQL injection can lead to data loss and system compromise. This presentation will take you through the techniques and tools used to take control of a PHP web application starting from an injection point moving to PHP web shells, and ending with a Linux wildcard attack.

DON'T WHISPER MY CHIPS: SIDECHANNEL AND GLITCHING FOR FUN AND PROFIT

Colin O'Flynn
Dalhousie University

Friday - 13:00 - Track Four

If you thought the security practices of regular software was bad, just wait until you start learning about the security of embedded hardware systems. Recent open-source hardware tools have made this field accessible to a wider range of researchers, and this presentation will show you how to perform these attacks for equipment costing $200.

Attacks against a variety of real systems will be presented: AES-256 bootloaders, internet of things devices, hardware crypto tokens, and more. All of the attacks can be replicated by the attendees, using either their own tools if such equipped (such as oscilloscopes and pulse generators), the open-hardware ChipWhisperer-Lite, or an FPGA board of their own design.

The hands-on nature of this talk is designed to introduce you to the field, and give you the confidence to pick up some online tutorials or books and work through them. Even if you've never tried hardware hacking before, the availability of open-source hardware makes it possible to follow published tutorials and learn all about side-channel power analysis and glitching attacks for yourself.

ONE DEVICE TO PWN THEM ALL

Dr. Phil Polstra
Professor, Bloomsburg University

Friday - 19:00 - Track One

This talk will present a device that can be used as a dropbox, remote hacking drone, hacking command console, USB writeblocker, USB Mass Storage device impersonator, or scripted USB HID device. The device is based on the BeagleBone Black, can be battery operated for several days, and is easily constructed for under $100.

The dropbox, remote hacking drone, and hacking command console functionality were presented at DEF CON 21. This talk will emphasize the new USB-based attack functionality. Topics will include injecting payloads by emulating an optionally write-protected USB mass storage device, rapidly executing commands on a target using the BeagleBone Black operating as a scripted USB HID device, USB mass storage device impersonation, and other attacks that can be performed with brief physical access to the target.

Some familiarity with Linux and USB devices would be helpful, but not required. All hardware and software to be discussed is 100% open source.

NETRIPPER - SMART TRAFFIC SNIFFING FOR PENETRATION TESTERS

Ionut Popescu
Senior Security Consultant at KPMG Romania

Friday - 17:00 - Track Three

The post-exploitation activities in a penetration test can be challenging if the tester has low-privileges on a fully patched, well configured Windows machine. This work presents a technique for helping the tester to find useful information by sniffing network traffic of the applications on the compromised machine, despite his low-privileged rights. Furthermore, the encrypted traffic is also captured before being sent to the encryption layer, thus all traffic (clear-text and encrypted) can be sniffed. The implementation of this technique is a tool called NetRipper which uses API hooking to do the actions mentioned above and which has been especially designed to be used in penetration tests, but the concept can also be used to monitor network traffic of employees or to analyze a malicious application.

CHELLAM – A WI-FI IDS/FIREWALL FOR WINDOWS

Vivek Ramachandran
Founder, SecurityTube.net and Pentester Academy

Friday - 15:00 - 101 Track

This talk will introduce techniques to detect Wi-Fi attacks such as Honeypots, Evil Twins, Mis-association , Hosted Network based backdoors etc. on a Windows client without the need for custom hardware or drivers. Our attack detection techniques will work for both Encrypted (WPA/WPA2 PSK and Enterprise) and Unencrypted networks.

We will also release a proof of concept tool implementing our detection techniques. Even though the focus of this talk is Windows, the same principles can be used to protect other Operating Systems, both workstation and mobile.

I WILL KILL YOU

Chris Rock
Kustodian Pty Ltd

Friday - 16:30 - Track Two

Have you ever wanted to kill someone? Do you want to get rid of your partner, your boss or your arch nemesis? Perhaps you want to enjoy your life insurance payout whilst you're still alive. Do you have rich elderly parents that just won't die quick enough? Or do you want a "Do Over" new identity.

Then, this presentation is for you! I'll provide you with the insight and techniques on how to "kill" someone and obtain a real death certificate and shutdown their lives. It focuses on the lack of security controls that allow any of us to virtually kill off anyone or any number of people. Forget the Dexter way of killing someone, I'll show you how to avoid the messy clean up and focusing in on the digital aspects. You could be dead right now and not even know it.

The presentation will explain the death process and will highlight the vulnerabilities and its implications world-wide.

You will learn:

- How to fill in a doctor's medical cause of death certificate anonymously.
- How to become a funeral director and dispose of the body.
- How to obtain a Death Certificate.

Once you've wrapped your mind around that concept, I will also show you how to "birth" Virtual identities that obtain real birth certificates. You will learn the birth registration process and the security vulnerabilities associated with this as well.

The third and final step of the presentation is "The baby harvest", a concept that I've developed, which involves creating and raising virtual identities. This technique is similar to a shelf company. Virtuals will be "born", registered with the government complete with birth certificates and social security numbers. They can open up bank accounts, get a virtual job to launder money, pay taxes, obtain home loans and obtain life insurance policies. They can be married to anyone (virtual or not) and be directors of companies…. the list is endless and to complete the circle of life, they can be killed off when they are ready for "harvest" for their life insurance payouts or sold as permanent I.D's. With no victim, this is taking identity theft to the next level.

HOW TO HACK A TESLA MODEL S

Marc Rogers
Principle Security Researcher for CloudFlare

Kevin Mahaffey
CTO of Lookout Inc

Friday - 14:00 - Track Two

The Tesla Model S is the most connected car in the world. It might surprise you to hear that it is also one of the most secure. In this talk we will walk you through the architecture of a Tesla Model S noting things that Tesla got right as well as identifying those that they got wrong. This knowledge will help the industry as a whole build more secure "things".

From this talk you will get an intimate understanding of how the many interconnected systems in a Tesla model S work and most importantly how they can be hacked. You will also get a good understanding of the data that this connected car collects. We will also be releasing a tool that will enable Tesla Model S owners to view and analyze that telemetry. Finally we will also be discussing several unpatched vulnerabilities that will allow you to gain root access to a Tesla Model S with physical access to the car. Note that all of these vulnerabilities have been responsibly disclosed.

Disclaimer: With great access comes great responsibility—In other words we are not responsible for any Tesla Model S bricked by over-enthusiastic attendees of this talk :)

WHEN IOT ATTACKS: HACKING A LINUX-POWERED RIFLE

Runa A. Sandvik

Michael Auger

Friday - 17:00 - Track One

TrackingPoint is an Austin startup known for making precision-guided firearms. These firearms ship with a tightly integrated system coupling a rifle, an ARM-powered scope running a modified version of Linux, and a linked trigger mechanism. The scope can follow targets, calculate ballistics and drastically increase its user's first shot accuracy. The scope can also record video and audio, as well as stream video to other devices using its own wireless network and mobile applications.

In this talk, we will demonstrate how the TrackingPoint long range tactical rifle works. We will discuss how we reverse engineered the scope, the firmware, and three of TrackingPoint's mobile applications. We will discuss different use cases and attack surfaces. We will also discuss the security and privacy implications of network-connected firearms.

BRUCE SCHNEIER Q&A

Bruce Schneier
CTO, Resilient Systems

Friday - 12:00 - 101 Track

Bruce Schneier Talks Security. Come hear about what's new, what's hot, and what's hype in security. NSA surveillance, airports, voting machines, ID cards, cryptography — he'll talk about what's in the news and what matters. Always a lively and interesting talk.

APPLIED INTELLIGENCE: USING INFORMATION THAT'S NOT THERE

Michael Schrenk
Security Researcher

Friday - 13:00 - 101 Track

Organizations continue to unknowingly leak trade secrets on the Internet. To those in the know, these leaks are a valuable source of competitive intelligence. This talk describes how the speaker collects competitive intelligence for his own online retail business. Specifically, you learn how he combines, trends, and analyzes information within specific contexts to manufacture useful data that is real, but technically doesn't exist on it's own. For example, you will learn about the trade secrets that are hidden within sequential numbers, how he uses collected intelligence to procure inventory, and how and why he gauges the ongoing health of his industry and that of his competitors. And on a related note, you'll also learn how the federal government nearly exposed an entire generation to identity fraud.

I AM PACKER AND SO CAN YOU

Mike Sconzo
Security Researcher

Friday - 17:00 - 101 Track

Automating packer and compiler/toolchain detection can be tricky and best and downright frustrating at worst. The majority of existing solutions are old, closed source or aren't cross platform. Originally, a method of packer identification that leveraged some text analysis algorithms was presented. The goal is to create a method to identify compilers and packers based on the structural changes they leave behind in PE files. This iteration builds upon previous work of using assembly mnemonics for packer detection and grouping. New features and analysis are covered for identification and clustering of PE files.

DRINKING FROM LETHE: NEW METHODS OF EXPLOITING AND MITIGATING MEMORY CORRUPTION VULNERABILITIES

Daniel Selifonov
Engineer, Skyport Systems Inc

Friday - 18:00 - Track Two

Memory corruption vulnerabilities have plagued computer systems since we started programming software. Techniques for transforming memory corruption primitives into arbitrary code execution exploits have evolved significantly over the past two decades, from "smashing the stack for fun and profit" to the current apex of "just in time code reuse" while playing a cat and mouse game with similarly evolving defensive mitigations: from PaX/NX-bit to fine-grained ASLR and beyond. By contextualizing this battle between attack and defense, I will demonstrate new defense strategies based on augmenting fine-grained ASLR with memory disclosure mitigations to render existing exploitation techniques unreliable. Modifications to the Xen hypervisor exploiting hardware accelerated virtualization extensions on the modern Intel platform enable realizing these new defense strategies without imposing significant runtime CPU overhead.

BREAKING SSL USING TIME SYNCHRONISATION ATTACKS

Jose Selvi
Senior Security Consultant, NCC Group

Friday - 18:00 - Track Four

What time? When? Who is first? Obviously, Time is strongly present in our daily life. We use time in almost everything we do, and computers are not an exception to this rule. Our computers and devices use time in a wide variety of ways such as cache expiration, scheduling tasks or even security technologies. Some of those technologies completely relies on the local clock, and they can be affected by a clock misconfiguration.

However, since most operating system providers do not offer secure time synchronisation protocols by default, an attacker could manipulate those protocols and control the local clock. In this presentation, we review how different operating systems synchronise their local clocks and how an attacker could exploit some of them in order to bypass different well-known security protections.

INSTEON' FALSE SECURITY AND DECEPTIVE DOCUMENTATION

Peter Shipley
Security Researcher

Ryan Gooler

Friday - 13:00 - Track One

Insteon is a leading home automation solution for controlling lights, locks, alarms, and much more. More than forty percent of homes with automation installed use Insteon.

For the last fifteen years, Insteon has published detailed documentation of their protocols—documentation that is purposely misleading, filled with errors, and at times deliberately obfuscated. As my research over the last year has revealed, this sad state of affairs is the direct result of Insteon papering over the fact that it is trivial to wirelessly take control, reprogram, and monitoring any Insteon installation.

Worse still, the embedded nature of the Insteon protocol coupled with devices that do not support flash updates means that there are no current fixes or workarounds short of ripping out the Insteon products.

I will be presenting my research, and releasing tools demonstrating the vulnerabilities throughout the Insteon home automation system.

NSM 101 FOR ICS

Chris Sistrunk
Sr. ICS Security Consultant, FireEye

Friday - 10:00 - 101 Track

Is your ICS breached? Are you sure? How do you know?

The current state of security in Industrial Control Systems is a widely publicized issue, but fixes to ICS security issues are long cycle, with some systems and devices that will unfortunately never have patches available. In this environment, visibility into security threats to ICS is critical, and almost all of ICS monitoring has been focused on compliance, rather than looking for indicators/evidence of compromise. The non-intrusive nature of Network Security Monitoring (NSM) is a perfect fit for ICS. This presentation will show how NSM should be part of ICS defense and response strategy, various options for implementing NSM, and some of the capabilities that NSM can bring to an ICS security program. Free tools such as Security Onion, Snort IDS, Bro IDS, NetworkMiner, and Wireshark will be used to look at the ICS environment for anomalies. It will be helpful if attendees have read these books (but they aren't required): The Cuckoo's Egg by Cliff Stoll, The Practice of Network Security Monitoring by Richard Bejtlich, and Applied Network Security Monitoring by Chris Sanders and Jason Smith.

SHALL WE PLAY A GAME?

Tamas Szakaly
Lead security researcher @ PR-Audit Ltd., Hungary

Friday - 10:00 - Track One

Everybody plays games, and a whole lot of people plays computer games. Despite this fact, very few of us, security researchers consider them as interesting targets. Granted, you won't likely be able to directly hack into a big corporate network via game exploits, but you could for example target the people running the company via their favorite games. Or their children's favorite games. Another scenario: you should consider that a hacked game could allow Not So Admirable people access to your internal network - which at first does not seem that big of a deal considering it's "just" a home network, but when you realize all your mobile phones, your TV set, your VOIP phones, your security cameras, and even your smart house sensors and controllers are part of that network, it looks much more scary.

Games are also interesting from a technical standpoint too, since they tend to be quite complex. The majority of them have networking, and they process complex data structures (maps, saved games, etc.) which makes them ideal fuzzing targets. But this talk is not about those kind of exploits. Hackers tend to ignore the low hanging fruits in favor of beautiful exploits, but we really shouldn't - bad guys don't care about how sophisticated some exploit is, they only care about the results. This is why I have decided to take a look around and see what's already there in the games that allows access to the gamers' network. Thus this research about how game scripting engines can be abused started.

I'll show in this talk that playing on custom game servers and playing community created maps could easily lead to code execution on our machines - more so, in most cases without the need to bypass the operating system's exploit mitigation techniques. My targets include popular games and game engines like CryEngine 3, Dota 2, Garry's Mod, ARMA3 and Digital Combat Simulator. I'll show a wide range of script abuse from a simple direct command execution in an unrestricted scripting environment through brute forcing a security camera via HTTP requests to complex script sandbox escapes.

WELCOME TO DEF CON

The Dark Tangent
Founder, DEF CON

1057

Friday - 10:00 - Track Three

Defcon 23 opening ceremonies- DarkTangent and LostboY 1o57 officially open Defcon 23 and welcome you to the conference in a 'state of the union' style talk. Come hear the story behind the infamous Defcon Black (Uber) badge and a jump start on the cryptographic challenges. We'll probably have to redact or deny any Defcon lore that may be leaked. On second thought nothing to see here- what are you doing here? Defcon is cancelled… nothing to see here…move along…

CONFESSIONS OF A PROFESSIONAL CYBER STALKER

Ken Westin
Sr. Security Analyst with Tripwire Inc.

Friday - 12:00 - Track Four

For several years I developed and utilized various technologies and methods to track criminals leading to at least two dozen convictions. In the process of recovering stolen devices, larger crimes would be uncovered including drugs, theft rings, stolen cars, even a violent car jacking. Much of the evidence in these cases would be collected by stolen devices themselves, such as network information, photos captured from laptops and cell phones, but often times there was additional data that would need to be gathered for a conviction. In this presentation I will walk through actual real cases and discuss in depth the technologies used and additional processes I went through utilizing open source data and other methods to target criminals. I will also discuss how these same tools and methods can be used against the innocent and steps users and developers can take to better protect privacy.

In this presentation here are a few examples of cases I worked on which I will reveal details of:

- How a theft ring targeting Portland, Oregon schools was unveiled leading to multiple convictions
- How I tracked and recovered $9K worth of stolen camera equipment sold multiple times a year after it was stolen based on data extracted from images online
- How mobile phones stolen from a wireless store were tracked leading to the arrest of a theft ring, leading to the conviction of six people and the recovery of a stolen car
- Embedding of custom designed trojan for thermal imaging devices for theft tracking and export controls
- Tracking of a stolen flash drive to a university computer lab and correlation of security camera and student access ID cards
- Tracking a stolen laptop across state lines and how I gathered mountains of evidence in another theft ring case
- Several other cases….

HOW TO TRAIN YOUR RFID HACKING TOOLS

Craig Young
Security Researcher, Tripwire VERT

Friday - 18:00 - Track One

With insecure low frequency RFID access control badges still in use at businesses around the world and high frequency NFC technology being incorporated into far more consumer products, RFID hacking tools are invaluable for penetration testers and security researchers alike. Software defined radio has revolutionized this field with powerful devices like Proxmark3 and RFIDler available for a modest price. 3D printing has also presented new opportunities for makers to create custom antennas and cases to fit specific tasks. While there is a lot of great information out there about how people use these tools, there is relatively little more than source code available for learning how to develop new firmware to equip these devices with purpose-built logic. This presentation will discuss the overall architecture of the Proxmark3 and RFIDler tools and provide tutorial style examples for enhancing the firmware. Proxmark3 development will be demonstrated by upgrading the stand-alone mode to support NFC operations. For the new kid on the block, RFIDler, we will take a look at how to tweak the system for optimal reliability using 3D printing and enhanced diagnostic tools.

BUILD A FREE CELLULAR TRAFFIC CAPTURE TOOL WITH A VXWORKS BASED FEMOTO

Yuwei Zheng
Senior security researcher, Qihoo 360 Technology Co. Ltd.

Haoqi Shan
Wireless/hardware security researcher, Qihoo 360 Technology Co. Ltd.

Friday - 14:00 - Track One

In recent years, more and more products, are integrated with cellular modem, such as cars of BMW, Tesla, wearable devices, remote meters, i.e. Internet of things. Through this way, manufactories can offer remote service and develop a lot of attractive functions to make their product more valuable. However, many vulnerabilities have also been introduced into these systems.

It puts new questions to black-box penetration testing engineer. How to capture the SMS command between the cellular modem and the remote server? How to intercept the data link?

Some existing solutions, such as USRP based OpenBTS, commercial product nanoBTS can be used to build a fake base station and capture data traffic. However all of them cannot access the real operator's core network so that they cannot capture real SMS and voice traffic.

With the inspiration from social engineering, we got a femto-cell base station from a telecom operator. After a series of hacking and modifications, we built it as a powerful SMS, voice and data link inception tool. Furthermore, not like a fake station, it's a legal base station and authorized to access the operator's core network. By this tool, we can conveniently explore vulnerabilities of cellular modem inside products.

Presentations

SATURDAY TALKS

DIY NUKEPROOFING: A NEW DIG AT "DATA-MINING"

3AlarmLampscooter
enigmatic armored mammal

Saturday - 18:00 - Track Four

Does the thought of nuclear war wiping out your data keep you up at night? Don't trust third party data centers? Few grand burning a hole in your pocket and looking for a new Sunday project to keep you occupied through the fall? If you answered yes to at least two out of three of these questions, then 3AlarmLampscooter's talk on extreme pervasive communications is for you! You'll learn everything from calculating radiation half layer values to approximating soil stability involved in excavating your personal apocalypse-proof underground data fortress.

GAME OF HACKS: PLAY, HACK & TRACK

Amit Ashbel
Product Evangelist Checkmarx

Maty Siman
CTO and Founder Checkmarx

Saturday - 18:00 - 101 Track

Fooling around with some ideas we found ourselves creating a hacker magnet. Game of Hacks, built using the node.js framework, displays a range of vulnerable code snippets challenging the player to locate the vulnerability. A multiplayer option makes the challenge even more attractive and the leaderboard spices up things when players compete for a seat on the iron throne.

Within 24 hours we had 35K players test their hacking skills...we weren't surprised when users started breaking the rules. Join us to:

- Play GoH against the audience in real time and get your claim for fame
- Understand how vulnerabilities were planted within Game of Hacks
- See real attack techniques (some caught us off guard) and how we handled them
- Learn how to avoid vulnerabilities in your code and how to go about designing a secure application
- Hear what to watch out for on the ultra-popular node.js framework.

Check it out at www.Gameofhacks.com

ABUSING XSLT FOR PRACTICAL ATTACKS

Fernando Arnaboldi
Senior Security Consultant at IOActive

Saturday - 14:00 - 101 Track

Over the years, XML has been a rich target for attackers due to flaws in its design as well as implementations. It is a tempting target because it is used by other programming languages to interconnect applications and is supported by web browsers. In this talk, I will demonstrate how to use XSLT to produce documents that are vulnerable to new exploits.

XSLT can be leveraged to affect the integrity of arithmetic operations, lead to code logic failure, or cause random values to use the same initialization vector. Error disclosure has always provided valuable information, but thanks to XSLT, it is possible to partially read system files that could disclose service or system's passwords. Finally, XSLT can be used to compromise end-user confidentiality by abusing the same-origin policy concept present in web browsers.

This presentation includes proof-of-concept attacks demonstrating XSLT's potential to affect production systems, along with recommendations for safe development.

KEY-LOGGER, VIDEO, MOUSE — HOW TO TURN YOUR KVM INTO A RAGING KEY-LOGGING MONSTER

Yaniv Balmas
Security Researcher, Check Point Software Technologies

Lior Oppenheim
Security Researcher, Check Point Software Technologies

Saturday - 11:00 - Track One

Key-Loggers are cool, really cool. It seems, however, that every conceivable aspect of key-logging has already been covered: from physical devices to hooking techniques. What possible innovation could be left in this field?

Well, that's what we used to think too. That is until we noticed that little grey box sitting there underneath a monitor, next to yesterday's dirty coffee cup. The little grey box that is most commonly known as 'KVM'.

The talk will tell the tale of our long journey to transform an innocent KVM into a raging key-logging monster. We will safely guide you through the embedded wastelands, past unknown IC's, to explore uncharted serial protocols and unravel monstrous obfuscation techniques.

Walking along the misty firmware woods of 8051 assembly we will challenge ambiguous functions and confront undebuggable environments.

Finally, we will present a live demo of our POC code and show you that air-gapped networks might not be as segregated as you imagined.

You will witness that malware code could actually reside outside your computer, persisting through reboots, wipes, formats, and even hardware replacements. You might laugh, you might cry, but one thing is certain - you will never look at your KVM the same as before.

EXTRACTING THE PAINFUL (BLUE)TOOTH

Matteo Beccaro

Matteo Collura

Saturday - 14:00 - Track One

Do you know how many Bluetooth-enabled devices are currently present in the world? With the beginning of the IoT (Internet of Things) and Smart Bluetooth (Low energy) we find in our hands almost a zillion of them. Are they secure? What if I tell you I can unlock your Smartphone? What if I tell you I'm able to open the new shiny SmartLock you are using to secure your house's door?

In this talk we will explain briefly how the Bluetooth (BDR/EDR/LE) protocols work, focusing on security aspects. We will show then some known vulnerabilities and finally we will consider deeply undisclosed ones, even with live demonstrations.

IT'S THE ONLY WAY TO BE SURE: OBTAINING AND DETECTING DOMAIN PERSISTENCE

Grant Bugher
Perimeter Grid

Saturday - 13:00 - 101 Track

When a Windows domain is compromised, an attacker has several options to create backdoors, obscure his tracks, and make his access difficult to detect and remove. In this talk, I discuss ways that an attacker who has obtained domain administrator privileges can extend, persist, and maintain control, as well as how a forensic examiner or incident responder could detect these activities and root out an attacker.

802.11 MASSIVE MONITORING

Andres Blanco
Sr Researcher, Core Security

Andres Gazzoli
Sr Developer, Core Security

Saturday - 17:00 - Track Three

Wireless traffic analysis has been commonplace for quite a while now, frequently used in penetration testing and various areas of research. But what happens when channel hopping just doesn't cut it anymore — can we monitor all 802.11 channels?

In this presentation we describe the analysis, different approaches and the development of a system to monitor and inject frames using routers running OpenWRT as wireless workers. At the end of this presentation we will release the tool we used to solve this problem.

EXPLORING LAYER 2 NETWORK SECURITY IN VIRTUALIZED ENVIRONMENTS

Ronny L. Bull
Ph.D. Graduate Student, Clarkson University

Jeanna N. Matthews
Associate Professor, Clarkson University

Saturday - 17:00 - Track One

Cloud service providers offer their customers the ability to deploy virtual machines in a multi-tenant environment. These virtual machines are typically connected to the physical network via a virtualized network configuration. This could be as simple as a bridged interface to each virtual machine or as complicated as a virtual switch providing more robust networking features such as VLANs, QoS, and monitoring. In this paper, we explore whether Layer 2 network attacks that work on physical switches apply to their virtualized counterparts by performing a systematic study across four major hypervisor environments - Open vSwitch, Citrix XenServer, Microsoft Hyper-V Server and VMware vSphere - in seven different virtual networking configurations. First, we use a malicious virtual machine to run a MAC flooding attack and evaluate the impact on co-resident VMs. We find that network performance is degraded on all platforms and that it is possible to eavesdrop on other client traffic passing over the same virtual network for Open vSwitch and Citrix XenServer. Second, we use a malicious virtual machine to run a rogue DHCP server and then run multiple DHCP attack scenarios. On all four platforms, co-resident VMs can be manipulated by providing them with incorrect or malicious network information.

SWITCHES GET STITCHES

Colin Cassidy
Senior Security Consultant at IOActive

Éireann Leverett

Robert M. Lee

Saturday - 16:00 - Track One

This talk will introduce you to Industrial Ethernet Switches and their vulnerabilities. These are switches used in industrial environments, like substations, factories, refineries, ports, or other homes of industrial automation. In other words: DCS, PCS, ICS & SCADA switches.

The researchers focus on attacking the management plane of these switches, because we all know that industrial system protocols lack authentication or cryptographic integrity. Thus, compromising any switch allows the creation of malicious firmwares for further MITM manipulation of a live process. Such MITM manipulation can lead to the plant or process shutting down (think: nuclear reactor SCRAM) or getting into a unknown and hazardous state (think: damaging a blast furnace at a steel mill)

Not only will vulnerabilities be disclosed for the first time, but the methods of finding those vulnerabilities will be shared. All vulnerabilities disclosed will be in the default configuration state of the devices. While these vulnerabilities have been responsibly disclosed to the vendors, SCADA/ICS patching in live environments tends to take 1-3 years. Because of this patching lag, the researchers will also be providing live mitigations that owner/operators can use immediately to protect themselves. At least four vendors switches will be examined: Siemens, GE, Garrettcom and Opengear.

"INTRUSION SOFTWARE" THREATEN VULNERABILITY RESEARCH?

Tom Cross aka Decius
CTO, Drawbridge Networks

Collin Anderson
Independent Researcher

Saturday - 10:00 - Track Three

At the end of 2013, an international export control regime known as the Wassenaar Arrangement was updated to include controls on technology related to "Intrusion Software" and "IP Network Surveillance Systems." Earlier this year, the US Government announced a draft interpretation of these new controls, which has kicked off a firestorm of controversy within the information security community. Questions abound regarding what the exact scope of the proposed rules is, and what impact the rules might have on security researchers. Is it now illegal to share exploit code across borders, or to disclose a vulnerability to a software vendor in another country? Can export controls really keep surveillance technology developed in the west out of the hands of repressive regimes? This presentation will provide a deep dive on the text of the new controls and discuss what they are meant to cover, how the US Government has indicated that it may interpret them, and what those interpretations potentially mean for computer security researchers, and for the Internet as a whole.

BURPKIT - USING WEBKIT TO OWN THE WEB

Nadeem Douba
Founding Principal, Red Canari

Saturday - 14:00 - Track Four

Today's web apps are developed using a mashup of client- and server-side technologies. Everything from sophisticated Javascript libraries to third-party web services are thrown into the mix. Over the years, we've been asked to test these web apps with security tools that haven't evolved at the same pace. A common short-coming in most of these tools is their inability to perform dynamic analysis to identify vulnerabilities such as dynamically rendered XSS or DOM-based XSS. This is where BurpKit comes in - a BurpSuite plugin that integrates the power of WebKit with that of BurpSuite. In this presentation we'll go over how one can leverage WebKit to write their own web pen-testing tools and introduce BurpKit. We'll show you how BurpKit is able to perform a variety of powerful tasks including dynamic analysis, BurpSuite scripting, and more! Best of all, the plugin will be free and open source so you can extended it to your heart's desire!

LET'S ENCRYPT - MINTING FREE CERTIFICATES TO ENCRYPT THE ENTIRE WEB

Peter Eckersley
Electronic Frontier Foundation

James Kasten
Electronic Frontier Foundation

Yan Zhu
Electronic Frontier Foundation

Saturday - 15:00 - Track Four

Let's Encrypt is a new certificate authority that is being launched by EFF in collaboration with Mozilla, Cisco, Akamai, IdenTrust, and a team at the University of Michigan. It will issue certificates for free, using a new automated protocol called ACME for verification of domain control and issuance.

This talk will describe the features of the CA and available clients at launch; explore the security challenges inherent in building such a system; and its effect on the security of the CA marketplace as a whole. We will also update our place on the roadmap to a Web that uses HTTPS by default.

EXTENDING FUZZING GRAMMARS TO EXPLOIT UNEXPLORED CODE PATHS IN MODERN WEB BROWSERS

Saif El-Sherei
Analyst, SensePost

Etienne Stalmans
Analyst, SensePost

Saturday - 15:00 - 101 Track

Fuzzing is a well-established technique for finding bugs, hopefully exploitable ones, by brute forcing inputs to explore code paths in an application. In recent years, fuzzing has become a near mandatory part of any major application's security team efforts. Our work focused on fuzzing web browsers, a particularly difficult challenge given the size and quality of some of their security teams, the existing high-quality fuzzers available for this, and, of late, bug bounty programs.

Despite this, our improved fuzzing approach was able to find four confirmed bugs within Google Chrome and two within Microsoft Internet Explorer 11. The bugs had varying potential exploitability. Interestingly, some had been independently discovered indicating others are active in this field. The work is on going, and we hope to have more before the presentation.

As browsers continue to grow as the new universal interface for devices and applications, they have become high value targets for exploitation. Additionally, with the growth of browser fuzzing since 2004, this is a complex field to get started in. Something we hope to help address.

Our research and presentation will consist of two parts:

The first part is an introduction to fuzzing for the security practitioner. Here we combine the approaches, tool sets and integrations between tools we found to be most effective into a recipe for fuzzing various browsers and various platforms.

The second part is a description of our work and approach used to create, and extend, browser fuzzing grammars based on w3c specifications to discover new and unexplored code paths, and find new browser security bugs. In particular, example of real bugs found in the Chrome and IE browser will be demonstrated.

NSA PLAYSET: JTAG IMPLANTS

Joe FitzPatrick
SecuringHardware.com

Matt King
Security Researcher

Saturday - 16:00 - Track Four

While the NSA ANT team has been busy building the next generation spy toy catalog for the next leak, the NSA Playset team has been busy catching up with more open hardware implementations. GODSURGE is a bit of software that helps to persist malware into a system. It runs on the FLUXBABBIT hardware implant that connects to the depopulated JTAG header of certain models of Dell servers.

This talk will introduce SAVIORBURST, our own implementation of a jtag-based malware delivery firmware that will work hand-in-hand with SOLDERPEEK, our custom hardware design for a standalone JTAG attack device. We will demonstrate how to this pair enables the persistent compromise of an implanted system as well as release all the hardware and software necessary to port SAVIORBURST and SOLDERPEEK to your jtag-equipped target of choice. Anyone curious to know more about JTAG, regardless of previous hardware experience, will learn something from this talk.

WHYMI SO SEXY? WMI ATTACKS, REAL-TIME DEFENSE, AND ADVANCED FORENSIC ANALYSIS

Matt Graeber
Reverse Engineer, FireEye Inc.

Willi Ballenthin
Reverse Engineer, FireEye Inc.

Claudiu Teodorescu
Reverse Engineer, FireEye Inc.

Saturday - 13:00 - Track Three

Windows Management Instrumentation (WMI) is a remote management framework that enables the collection of host information, execution of code, and provides an eventing system that can respond to operating system events in real time. FireEye has recently seen a surge in attacker use of WMI to carry out objectives such as system reconnaissance, remote code execution, persistence, lateral movement, covert data storage, and VM detection. Defenders and forensic analysts have largely remained unaware of the value of WMI due to its relative obscurity and completely undocumented file format. After extensive reverse engineering, our team has documented the WMI repository file format in detail, developed libraries to parse it, and formed a methodology for finding evil in the repository.

In this talk, we will take a deep dive into the architecture of WMI, reveal a case study in attacker use of WMI in the wild, describe WMI attack mitigation strategies, show how to mine its repository for forensic artifacts, and demonstrate how to detect attacker activity in real-time by tapping into the WMI eventing system. By the end of this talk, we will have convinced the audience that WMI is a valuable asset not just for system administrators and attackers, but equally so for defenders and forensic analysts.

LINUX CONTAINERS: FUTURE OR FANTASY?

Aaron Grattafiori
Principal Security Consultant, iSEC Partners/NCC Group

Saturday - 19:00 - 101 Track

Containers, a pinnacle of fast and secure deployment or a panacea of false security? In recent years Linux containers have developed from an insecure and loose collection of Linux kernel namespaces to a production-ready OS virtualization stack. In this talk, the audience will first learn the basics of how containers function, understanding namespaces, capabilities and cgroups in order to see how Linux containers and the supporting kernel features can offer an effective application and system sandboxing solution yet to be widely deployed or adopted. Understanding LXC or Docker use, weaknesses and security for PaaS and application sandboxing is only the beginning.

Leveraging container technologies is rapidly becoming popular within the modern PaaS and devops world but little has been publicly discussed in terms of actual security risks or guarantees. Understanding prior container vulnerabilities or escapes, and current risks or pitfalls in major public platforms will be explored in this talk. I'll cover methods to harden containers against future attacks and common mistakes to avoid when using systems such as LXC and Docker. This will also include an analysis and discussion of techniques such as Linux kernel hardening, reduced capabilities, Mandatory Access Controls (MAC), the User kernel namespace and seccomp-bpf (syscall filtering); all of which help actually contain containers. The talk will end on some methods for creating minimal, highly-secure containers and end on where containers are going and why they might show up where you least expect them.

HOW TO SHOT WEB: WEB AND MOBILE HACKING IN 2015

Jason Haddix
Director of Technical Operations, Bugcrowd

Saturday - 16:00 - 101 Track

2014 was a year of unprecedented participation in crowdsourced and static bug bounty programs, and 2015 looks like a trendmaker. Join Jason as he explores successful tactics and tools used by himself and the best bug hunters. Practical methodologies, tools, and tips make you better at hacking websites and mobile apps to claim those bounties. Convert edge-case vulnerabilities to practical pwnage even on presumably heavily tested sites. These are tips and tricks that the every-tester can take home and use. Jason will focus on philosophy, discovery, mapping, tactical fuzzing (XSS, SQLi, LFI, ++), CSRF, web services, and mobile vulnerabilities. In many cases we will explore these attacks down to the parameter, teaching the tester common places to look when searching for certain bugs. In addition he will cover common evasions to filters and as many time saving techniques he can fit in.

THUNDERSTRIKE 2: SITH STRIKE

Trammel Hudson
Vice President, Two Sigma Investments

Xeno Kovah
Co-founder, LegbaCore, LLC

Corey Kallenberg
Co-Founder, LegbaCore, LLC

Saturday - 10:00 - Track Two

The number of vulnerabilities in firmware disclosed as affecting Wintel PC vendors has been rising over the past few years. Although several attacks have been presented against Mac firmware, unlike their PC counterparts, all of them required physical presence to perform. Interestingly, when contacted with the details of previously disclosed PC firmware attacks, Apple systematically declared themselves not vulnerable.

This talk will provide conclusive evidence that Mac's are in fact vulnerable to many of the software only firmware attacks that also affect PC systems. In addition, to emphasize the consequences of successful exploitation of these attack vectors, we will demonstrate the power of the dark side by showing what Mac firmware malware is capable of.

I'M A NEWBIE YET I CAN HACK ZIGBEE – TAKE UNAUTHORIZED CONTROL OVER ZIGBEE DEVICES

LI Jun
Graduate student from CUIT(Chengdu University of Information Technology , Chengdu ,China), Intern at Qihoo 360 Technology Co. Ltd.

YANG Qing
Team Leader of Unicorn Team, Qihoo 360 Technology Co. Ltd.

Saturday - 19:00 - Track Four

With the advent of the Internet of Things, more and more objects are connected via various communication protocols like Bluetooth, Z-wave, WiFi , ZigBee etc. Among those protocols ZigBee accounts for the largest market share, it has been adapted to various applications like WSN, Wireless Sensor Network, Smart Home . Over the last few years, large amount of research has been conducted on the security of ZigBee. In this presentation we will introduce a new technique to beat the security of ZigBee, we found the "signature" of the location of the security key . We will go through a specific example and share the thinking process along the way. The techniques used throughout this example can be generalized and used by other hardware reverse engineers.

I WANT THESE * BUGS OFF MY * INTERNET

Dan Kaminsky
Chief Scientist, White Ops

Saturday - 16:00 - Track Two

Are you interested in the gory details in fixing ugly bugs? No? Just like watching stuff blow up? Go to some other talk! But if you want to see what it takes to comprehensively end an entire bug class — how you dive into a code base, what performance and usability and maintainability and debuggability constraints it takes to make a web browser more secure — oh do I have some dirt for you.

ARE WE REALLY SAFE? - BYPASSING ACCESS CONTROL SYSTEMS

Dennis Maldonado
Security Consultant - KLC Consulting

Saturday - 12:00 - 101 Track

Access control systems are everywhere. They are used to protect everything from residential communities to commercial offices. People depend on these to work properly, but what if I had complete control over your access control solution just by using my phone? Or perhaps I input a secret keypad combination that unlocks your front door? You may not be as secure as you think.

The world relies on access control systems to ensure that secured areas are only accessible to authorized users. Usually, a keypad is the only thing stopping an unauthorized person from accessing the private space behind it. There are many types of access control systems from stand-alone keypads to telephony access control. In this talk, Dennis will be going over how and where access control systems are used. Dennis will walk through and demonstrate the tips and tricks used in bypassing common access control systems. This presentation will include attack methods of all nature including physical attacks, RFID, wireless, telephony, network, and more.

F*CK THE ATTRIBUTION, SHOW US YOUR .IDB!

Morgan Marquis-Boire
Senior Researcher, Citizen Lab

Marion Marschalek
Malware reverse engineer, Cyphort Inc

Claudio Guarnieri
Creator and lead developer, Cuckoo Sandbox

Saturday - 12:00 - Track Two

Over the past few years state-sponsored hacking has received attention that would make a rockstar jealous. Discussion of malware has shifted in focus from 'cyber crime' to 'cyber weapons', there have been intense public debates on attribution of various high profile attacks, and heated policy discussion surrounding regulation of offensive tools. We've also seen the sale of 'lawful intercept' malware become a global trade.

While a substantial focus has revolved around the activities of China, Russia, and Iran, recent discoveries have revealed the capabilities of Western nations such as WARRIORPRIDE aka. Regin (FVEY) and SNOWGLOBE aka. Babar (France). Many have argued that digital operations are a logical, even desirable part of modern statecraft. The step from digital espionage to political persecution is, however, a small one. Commercially written, offensive software from companies like FinFisher and Hacking Team has been sold to repressive regimes under the guise of 'governmental intrusion' software.

Nation state hacking operations are frequently well-funded, difficult to attribute, and rarely prosecuted even if substantive evidence can be discovered. While efforts have been made to counter this problem, proof is hard to find and even more difficult to correctly interpret. This creates a perfect storm of conditions for lies, vendor lies, and flimsy attribution.

In this talk we will unveil the mess happening backstage when uncovering nation state malware, lead the audience on the track of actor attribution, and cover what happens when you find other players on the hunt. We will present a novel approach to binary stylometry, which helps matching binaries of equal authorship and allows credible linking of binaries into the bigger picture of an attack. After this session the audience will have a better understanding of what happened behind the scenes when the next big APT report surfaces.

I HUNT PENETRATION TESTERS: MORE WEAKNESSES IN TOOLS AND PROCEDURES

Wesley McGrew
Assistant Research Professor Distributed Analytics and Security Institute, Mississippi State University

Saturday - 12:00 - Track Three

When we lack the capability to understand our tools, we operate at the mercy of those that do. Penetration testers make excellent targets for bad actors, as the average tester's awareness and understanding of the potential risks and vulnerabilities in their tools and processes is low, and the value of the information they gather and gain access to among their client base is very high. As demonstrated by Wesley's DEF CON 21 talk on vulnerabilities in penetration testing devices, and last year's compromise of WiFi Pineapple devices, the tools of offensive security professionals often represent a soft target. In this talk, operational security issues facing penetration testers will be discussed, including communication and data security (not just "bugs"), which impact both testers and clients. A classification system for illustrating the risks of various tools is presented, and vulnerabilities in specific hardware and software use cases are presented. Recommendations are made for improving penetration testing practices and training. This talk is intended to be valuable to penetration testers wanting to protect themselves and their clients, and for those who are interesting in profiling weaknesses of opposing forces that may use similar tools and techniques.

REMOTE EXPLOITATION OF AN UNALTERED PASSENGER VEHICLE

Charlie Miller
Security engineer at Twitter

Chris Valasek
Director of Vehicle Security Research at IOActive

Saturday - 14:00 - Track Two

Although the hacking of automobiles is a topic often discussed, details regarding successful attacks, if ever made public, are non-comprehensive at best. The ambiguous nature of automotive security leads to narratives that are polar opposites: either we're all going to die or our cars are perfectly safe. In this talk, we will show the reality of car hacking by demonstrating exactly how a remote attack works against an unaltered, factory vehicle. Starting with remote exploitation, we will show how to pivot through different pieces of the vehicle's hardware in order to be able to send messages on the CAN bus to critical electronic control units. We will conclude by showing several CAN messages that affect physical systems of the vehicle. By chaining these elements together, we will demonstrate the reality and limitations of remote car attacks.

SPREAD SPECTRUM SATCOM HACKING: ATTACKING THE GLOBALSTAR SIMPLEX DATA SERVICE

Colby Moore
Manager of Special Activities, Synack

Saturday - 13:00 - Track One

Recently there have been several highly publicized talks about satellite hacking. However, most only touch on the theoretical rather than demonstrate actual vulnerabilities and real world attack scenarios. This talk will demystify some of the technologies behind satellite communications and do what no one has done before - take the audience step-by-step from reverse engineering to exploitation of the GlobalStar simplex satcom protocol and demonstrate a full blown signals intelligence collection and spoofing capability. I will also demonstrate how an attacker might simulate critical conditions in satellite connected SCADA systems.

In recent years, Globalstar has gained popularity with the introduction of its consumer focused SPOT asset-tracking solutions. During the session, I'll deconstruct the transmitters used in these (and commercial) solutions and reveal design and implementation flaws that result in the ability to intercept,

spoof, falsify, and intelligently jam communications. Due to design tradeoffs these vulnerabilities are realistically unpatchable and put millions of devices, critical infrastructure, emergency services, and high value assets at risk.

ASK THE EFF: THE YEAR IN DIGITAL CIVIL LIBERTIES

Kurt Opsahl
General Counsel, Electronic Frontier Foundation

Nate Cardozo
EFF Staff Attorney

Mark Jaycox
EFF Legislative Analyst

Corynne McSherry
EFF Legal Director

Nadia Kayyali
EFF Activist

Peter Eckersley
EFF Technology Projects Director

Saturday - 18:00 - Track Two

Get the latest information about how the law is racing to catch up with technological change from staffers at the Electronic Frontier Foundation, the nation's premiere digital civil liberties group fighting for freedom and privacy in the computer age. This session will include updates on current EFF issues such as surveillance online and fighting efforts to use intellectual property claims to shut down free speech and halt innovation, discussion of our technology project to protect privacy and speech online, updates on cases and legislation affecting security research, and much more. Half the session will be given over to question-and-answer, so it's your chance to ask EFF questions about the law and technology issues that are important to you.

DEF CON COMEDY INCEPTION: HOW MANY LEVELS DEEP CAN WE GO?

Larry Pesce
Senior Security Analyst, InGuardians

Chris Sistrunk
Mandiant/FireEye

illwill
Co-Founder, NESIT

Chris Blow
Rook Security

Dan Tentler
Carbon Dynamics

Amanda Berlin
Hurricane Labs

Katie Moussouris
HackerOne

Saturday - 18:00 - Track Three

This year at DEF CON a former FAIL PANEL panelist attempts to keep the spirit alive by playing moderator. Less poetry, more roasting. A new cast of characters, more lulz, and no rules. Nothing is sacred, not the industry, not the audience, not even each other. Our cast of characters will bring you all sorts of technical fail, ROFLCOPTER to back it up. No waffles, but we have other tricks up our sleeve to punish, er, um, show love to our audience, all while raising money of the EFF and HFC. The FAIL PANEL may be dead, but the "giving" goes on.

HACKING SMART SAFES: ON THE "BRINK" OF A ROBBERY

Dan "AltF4" Petro
Security Associate, Bishop Fox

Oscar Salazar
Senior Security Associate at Bishop Fox

Saturday - 12:00 - Track One

Have you ever wanted to crack open a safe full of cash with nothing but a USB stick? Now you can!

The Brink's CompuSafe cash management product line provides a "smart safe as a service" solution to major retailers and fast food franchises. They offer end-to-end management of your cash, transporting it safely from your storefront safe to your bank via armored car.

During this talk, we'll uncover a major flaw in the Brink's CompuSafe and demonstrate how to crack one open in seconds flat. All you need is a USB stick and a large bag to hold all of the cash. We'll discuss how to remotely takeover the safe with full administrator privileges, and show how to enumerate a target list of other major Brink's CompuSafe customers (exposed via configuration files stored right on the safe).

At any given time, up to $240,000 can be sitting in each of the 14,000 Brink's CompuSafe smart safes currently deployed across the United States - potentially billions of dollars just waiting to be stolen.

We will also release a USB Rubber Ducky script to automate the whole attack, acting as a skeleton key that can open any Brink's safe. Plug and plunder!

So come ready to engage us as we explore these tools and more in this DEMO rich presentation. And don't forget to call Kenny Loggins… because this presentation is your highway to the Danger Zone…

STAYING PERSISTENT IN SOFTWARE DEFINED NETWORKS

Gregory Pickett
Cybersecurity Operations, Hellfire Security

Saturday - 18:00 - Track One

The Open Network Install Environment, or ONIE, makes commodity or WhiteBox Ethernet possible. By placing a common, Linux-based, install environment onto the firmware of the switch, customers can deploy the Network Operating Systems of their choice onto the switch and do so whenever they like without replacing the hardware. The problem is, if this gets compromised, it also makes it possible for hackers to install malware onto the switch. Malware that can manipulate it and your network, and keep doing it long after a Network Operating System reinstall.

With no secure boot, no encryption, no authentication, predictable HTTP/TFTP waterfalls, and exposed post-installation partition, ONIE is very susceptible to compromise. And with Network Operating Systems such as Switch Light, Cumulus Linux, and Mellanox-OS via their agents Indigo and eSwitchd not exactly putting up a fight with problems like no authentication, no encryption, poor encryption, and insufficient isolation, this is a real possibility.

In this session, we'll cover the weaknesses in ONIE, ways to reach the platform through these Network Operating Systems, and what can happen if we don't properly protect the Control Plane these switches run on. I'll even demonstrate with a drive-by web-attack that is able to pivot through a Windows management station to reach the isolated control plane network, and infect one of these ONIE-based switches with malware, malware that's there even after a refresh. You'll even get the source code to take home with you to see how easily it's done. Finally, we'll talk about how to compensate for these issues so that your network doesn't become infected with and manipulated by this sort of persistent firmware-level malware.

A HACKER'S GUIDE TO RISK

Bruce Potter
The Shmoo Group

Saturday - 10:00 - 101 Track

When the latest and greatest vulnerability is announced, the media and PR frenzy can be dizzying. However, when the dust settles, how do we actually measure the risk represented by a given vulnerability. When pen testers find holes in an organization, is it really "ZOMG, you're SO 0WNED!" or is it something more manageable and controlled? When you're attempting to convince the boss of the necessity of the latest security technology, how do really rank the importance of the technology against the threats facing the organization.

Understanding risk can be tricky, especially in an industry that often works on gut feelings and values quantity over quality. But risk and risk management doesn't need to be complicated. With a few basic formulas and access to some simple models, understanding risk can be a straightforward process. This talk will discuss risk, why its important, and the poor job the hacker community has done when it comes to properly assessing risk. It will also touch on some existing risk assessment and management systems, as well as provide worked examples of real world vulnerabilities and systems and the risks they pose. Finally, this talk will examine some practical guidance on how you, as hackers, security researchers, and security practitioners can better measure risk in your day to day life

CHIGULA — A FRAMEWORK FOR WI-FI INTRUSION DETECTION AND FORENSICS

Vivek Ramachandran
Founder, SecurityTube.net and Pentester Academy

Saturday - 12:00 - Track Four

Most of Wi-Fi Intrusion Detection & Forensics is done today using million dollar products or spending hours applying filters in Wireshark :) Chigula aims to solve this by providing a comprehensive, extensible and scriptable framework for Wi-Fi intrusion detection and forensics.

A non-exhaustive list of attacks which will be detected using this framework include:

- Attack tool detection - Aireplay-NG, Airbase-NG, Mdk3 etc.
- Honeypot, Evil Twin and Multipot attacks
- Rogue devices
- Vulnerable clients based on Probed SSIDs
- Hosted network based backdoors
- MAC spoofing
- Deauthentication attacks
- Disassociation attacks
- Channel Jamming attacks using duration field

HACKING ELECTRIC SKATEBOARDS: VEHICLE RESEARCH FOR MORTALS

Mike Ryan
Red Team, eBay

Richo Healey
Security Engineer, Stripe

Saturday - 15:00 - Track Two

In the last year there's been an explosion of electric skateboards onto the market- seemingly volleyed into popularity by the Boosted Boards kickstarter.

Following on from the success of their original Boosted Board exploit, the team went on to get their hands on the other popular boards on the market, and predictably broke all of them.

Richo and Mike will investigate the security of several popular skateboards, including Boosted's flagship model and demonstrate several vulnerabilities that allow complete control of a an unmodified victim's skateboard, as well as other attacks on the firmware of the board and controller directly.

SCARED POOPLESS – LTE AND *YOUR* LAPTOP

Mickey Shkatov
Security researcher, Intel Advanced Threat Research.

Jesse Michael
Security researcher

Saturday - 10:00 - Track One

With today's advancement in connectivity and internet access using 3G and LTE modems it seems we all can have a device that's always internet capable, including our laptops, tablets, 2 in 1's ultrabook. It becomes easier to be online without using your WiFi at all. In our talk we will demonstrate and discuss the exploitation of an internal LTE modem from Huawei which can be found in a number of devices including laptops by HP.

Mickey Shkatov is a security researcher and a member of the Intel Advanced Threat Research team. His areas of expertise include vulnerability research, hardware and firmware security, and embedded device security. Mickey has presented some of his past research at DEF CON, Black Hat USA, BruCON, and BsidesPDX

ANGRY HACKING - THE NEXT GENERATION OF BINARY ANALYSIS

Yan Shoshitaishvili
PhD Student, UC Santa Barbara

Fish Wang
PhD Student, UC Santa Barbara

Saturday - 13:00 - Track Two

Security has gone from a curiosity to a phenomenon in the last decade. Fortunately for us, despite the rise of memory-safe, interpreted, lame languages, the security of binaries is as relevant as ever. On top of that, (computer security) Capture the Flag competitions have skyrocketed in popularity, with new and exciting binaries on offer for hacking every weekend.

This all sounds great, and it is. Unfortunately, the more time goes by, the older we get, and the more our skills fade. Whereas we were happy to stare at objdump a decade ago, today, we find the menial parts of reversing and pwning more and more tiring and more and more difficult. Worse, while security analysis tools have been evolving to make life easier for us hackers, the core tools that we use (like IDA Pro) have remained mostly stagnant. And on top of that, the term "binaries" have expanded to regularly include ARM, MIPS, PPC, MSP430, and every other crazy architecture you can think of, rather than the nice, comfortable x86 of yesteryear.

New tools are required, and we're here to deliver. Over the last two years, we have been working on a next-generation binary analysis framework in an attempt to turn back the tide and reduce our mounting noobness. The result is called angr.

angr assists in binary analysis by providing extremely powerful, state-of-the-art analyses, and making them as straightforward to use as possible. Ever wanted to know *what freaking value* some variable could take on in a function (say, can the target of a computed write point to the return address)? angr can tell you! Want to know what input you need to trigger a certain code path and export a flag? Ask angr! In the talk, we'll cover three of the analyses that angr provides: a powerful static analysis engine (able to, among other things, automatically identify potential memory corruption in binaries through the use of Value-Set Analysis), its symbolic execution engine, and dynamic emulation of various architectures (*super* useful for debugging shellcode).

On top of that, angr is designed to make the life of a hacker as easy as possible — for example, the whole system is 98% Python, and is designed to be a breeze to interact with through iPython. Plus, it comes with a nifty GUI with nice visualizations for symbolically exploring a program, tracking differences between different program paths, and understanding value ranges of variables and registers. Finally, angr is designed to be easily extensible and embeddable in other applications. We'll show off a semantic-aware ROP gadget finder ("are there any gadgets that write to a positive offset of rax but don't clobber rbx" or "given this program state, what are the gadgets that won't cause a segfault") and a binary diffing engine, both built on angr.

We've used angr to solve CTF binaries, analyze embedded devices, debug shellcode, and even dabble in the DARPA Cyber Grand Challenge. We'll talk about our experiences with all of that and will release angr to the world, hopefully revolutionizing binary analysis and making everyone ANGRY!

DISSECTING THE DESIGN OF SCADA WEB HUMAN MACHINE INTERFACES (HMIS) - HUNTING VULNERABILITIES

Aditya K Sood
Architect - Threat Research Labs, Elastica inc.

Saturday - 10:00 - Track Four

Human Machine Interfaces (HMIs) are the subsets of the Supervisory Control and Data Acquisition (SCADA) systems. HMIs are control panels that provide interfaces for humans to interact with machines and to manage operations of various types of SCADA systems. HMIs have direct access to SCADA databases including critical software programs. The majority of SCADA systems have web-based HMIs that allow the humans to control the SCADA operations remotely through Internet. This talk unveils various flavors of undisclosed vulnerabilities in web-based SCADA HMIs including but not limited to remote or local file inclusions, insecure authentication through clients, weak password hashing mechanisms, firmware discrepancies, hardcoded credentials, insecure web-services, weak cryptographic design, cross-site request forgery, and many others. This talk digs deeper into the design models of various SCADA systems to highlight security deficiencies in the existing SCADA HMI deployments. The research is driven with a motivation to secure SCADA devices and to build more intelligent solutions by hunting vulnerabilities in SCADA HMIs. The vulnerabilities presented in this talk are completely undisclosed and will be revealed for the first time with live demonstrations.

HIGH-DEF FUZZING: EXPLORING VULNERABILITIES IN HDMI-CEC

Joshua Smith
Senior Security Researcher, HP Zero Day Initiative

Saturday - 15:00 - Track Three

The HDMI (High Definition Multimedia Interface) standard has gained extensive market penetration. Nearly every piece of modern home theater equipment has HDMI support and most modern mobile devices actually have HDMI-capable outputs, though it may not be obvious. Lurking inside most modern HDMI-compatible devices is something called HDMI-CEC, or Consumer Electronics Control. This is the functionality that allows a media device to, for example, turn on your TV and change the TV's input. That doesn't sound interesting, but as we'll see in this presentation, there are some very surprising things an attacker can do by exploiting CEC software implementations. Then there's something called HEC or HDMI Ethernet Connection, which allows devices to establish an Ethernet connection of up to 100Mbit/s over their HDMI connections (newer HDMI standards raise the speed to 1Gbit/s).

Don't think your mobile phone implements CEC? You might be wrong. Most modern Android-based phones and tablets have a Slimport(r) connection that supports HDMI-CEC. Ever heard of MHL (Mobile High-Definition Link)? Think Samsung and HTC (among other) mobile devices, and many JVC, Kenwood, Panasonic, and Sony car stereos – as many as 750 million devices in the world so far. Guess what? MHL supports HDMI-CEC as well. Let's explore, and own, this attack space.

THE BIEBER PROJECT: AD TECH 101, FAKE FANS AND ADVENTURES IN BUYING INTERNET TRAFFIC

Mark Ryan Talabis
Chief Security Scientist, zVelo

Saturday - 17:00 - 101 Track

In the past year, I found myself immersed in the multi-billion dollar digital advertising industry. This gave me the opportunity to investigate the unique security challenges and issues facing the industry. It was a shock to me at first how complex the advertising ecosystem was particularly in the advent of programmatic advertising. But I dove in head first and learned a lot which I would like to share with my fellow security professionals. During this time, I got involved with unscrupulous publishers, apathetic ad networks, angry advertisers and activist malware researchers. I encountered self proclaimed experts with fantastic claims, vendors using scare tactics, and a glaring disconnect between the security and ad tech worlds.

In this presentation, I would like to be able to provide the audience with my experience plus a number of things. Among which are:

Provide security professionals a 101 type of introduction to the world of digital advertising ecosystem. Among the things we will tackle is what is programmatic advertising, what the roles are of the different players like ad networks are and how money is made off all this interplay.

Provide the audience a perspective on what security challenges the advertising industry is facing and opportunities for us security professionals to be involved. We all know about malvertising and its a big deal to us security guys but there are bigger, and in an advertisers perspective, more relevant issues that needs to be taken care of first. All of this will be discussed in this talk.

An introduction about the different and creative ways unscrupulous publishers can pad their earnings. We will be talking about hidden ads, ad stacking, intrusive ads, auto-refreshes, popups, popunders, blackhat SEO techniques and dirty inventory.

An in..depth discussion on the problems caused by non-human traffic (NHT). We will talk about what it is, why is it a problem, how it is generated, and more importantly, how do we catch it? In fact, this presentation is named the "Bieber Project" which is the experiment which I leveraged to understand non-human traffic and determine how we can identify it.

HACKING THE HUMAN BODY/BRAIN: IDENTITY SHIFT, THE SHAPE OF A NEW SELF, AND HUMANITY 2.0

Richard Thieme
Author and Professional Speaker, ThiemeWorks

Saturday - 17:00 - Track Four

This presentation is beyond fiction.

Current research in neuroscience and the extension and augmentation of senses is proceeding in directions that might sound to a twentieth century mind like science fiction. Progress is rapid but unevenly distributed: Some is directed by military, intelligence and corporate interests but beyond their concerns, we can discern the future shape of human identity itself in nascent forms.

The human body/brain is being hacked to explore radical applications for helping, healing, and harming this and future generations. Some can be done in garage-hacking style. The presenter, in fact, recently had lenses in both eyes removed and replaced with artificial ones engineered for the vision he wanted, a now-trivial surgery. The reach of new technologies promises an even more radical transformation in what it means to be human.

One area of research is the recovery of memories, the deletion of emotional charges from memories, the removal of specific memories, the alteration of the content of memories, and the implantation of new memories. Another seeks to read the mind at a distance and extract information. Another explores the use of genomes to understand and replicate thinking, feeling, and behavior patterns. Another implements mind-to-mind communication, using neuroscience to understand brains best suited for remote viewing as well as implants and non-invasive technologies that control the electromagnetic energies of the brain to enable psychokinesis, clairvoyance and telepathy.

Augmentation of human abilities is being achieved by splicing information from sensors integrated with existing neurological channels. To feel the magnetic field of the earth, see the infrared and ultraviolet parts of the electromagnetic spectrum, discern the yaw and pitch of airplanes, see and hear by going around our eyes and ears — all this means we will experience the "self" in new ways.

Thieme concludes with quotes from remote viewer Joe McMoneagle, astronaut Edgar Mitchell, and his new novel FOAM to suggest the shape of the mind of the future. If you're 20 years old, you have at least a century of productive life ahead of you, so you had better be on board with the shape of your future selves. :-)

QARK: ANDROID APP EXPLOIT AND SCA TOOL

Tony Trummer
Staff Information Security Engineer/LinkedIn

Tushar Dalvi
Sr. Security Engineer/LinkedIn

Saturday - 11:00 - Track Four

Ever wonder why there isn't a metasploit-style framework for Android apps? We did! Whether you're a developer trying to protect your insecure app from winding up on devices, an Android n00b or a pentester trying to pwn all the things, QARK is just what you've been looking for! This tool combines SCA, teaching and automated exploitation into one, simple to use application!

FROM 0 TO SECURE IN 1 MINUTE — SECURING IAAS

Nir Valtman
CISO – Retail, NCR

Moshe Ferber
Co-chairman of the board, Cloud Security Alliance Israel

Saturday - 13:00 - Track Four

Recent hacks to IaaS platforms reveled that we need to master the attack vectors used: Automation and API attack vector, insecure instances and management dashboard with wide capabilities. Those attack vectors are not unique to Cloud Computing but there are magnified due to the cloud characteristics. The fact is that IaaS instance lifecycle is accelerating, nowadays we can find servers that are installed, launched, process data and terminate - all within a range of minutes. This new accelerated lifecycle makes traditional security processes such as periodic patches, vulnerability scanning, hardening, and forensics impossible. In this accelerated lifecycle, there are no maintenance windows for patches or ability to mitigate vulnerability, so the security infrastructure must adapt to new methods. In this new thinking, we require automation of instance security configuration, hardening, monitoring, and termination. Because there are no maintenance windows, Servers must be patched before they boot up, security configuration and hardening procedures should be integrated with server installation and vulnerability scanning and mitigation processes should be automatic.

In the presentation, we plan to announce the full version of a new open source tool called "Cloudefigo" and explain how it enables accelerated security lifecycle. We demonstrate how to launch a pre-configured, already patched instance into an encrypted storage environment automatically while evaluating their security and mitigating them automatically if a vulnerability is found. In the live demo, we leverage Amazon Web Services EC2 Cloud-Init scripts and object storage for provisioning automated security configuration, integrating encryption, including secure encryption key repositories for secure server's communication. The result of those techniques is cloud servers that are resilient, automatically configured, with the reduced attack surface.

LOOPING SURVEILLANCE CAMERAS THROUGH LIVE EDITING OF NETWORK STREAMS

Eric Van Albert
Independent Security Researcher

Zach Banks
Independent Security Researcher

Saturday - 15:00 - Track One

This project consists of the hardware and software necessary to hijack wired network communications. The hardware allows an attacker to splice into live network cabling without ever breaking the physical connection. This allows the traffic on the line to be passively tapped and examined. Once the attacker has gained enough knowledge about the data being sent, the device switches to an active tap topology, where data in both directions can be modified on the fly. Through our custom implementation of the network stack, we can accurately mimic the two devices across almost all OSI layers.

We have developed several applications for this technology. Most notable is the editing of live video streams to produce a "camera loop," that is, hijacking the feed from an Ethernet surveillance camera so that the same footage repeats over and over again. More advanced video transformations can be applied if necessary. This attack can be executed and activated with practically no interruption in service, and when deactivated, is completely transparent.

MACHINE VS. MACHINE: INSIDE DARPA'S FULLY AUTOMATED CTF

Michael Walker
Program Manager, DARPA/I2O

Jordan Wiens
CTF A(p|nthro)pologist @vector35.com

Saturday - 11:00 - Track Two

For 22 years, the best binary ninjas in the world have gathered at DEF CON to play the world's most competitive Capture-the-Flag. At DEF CON 24, DARPA will challenge machines to play this game for the first time, with the winner taking home a $2 million prize. This talk will include a first public look at the machines, teams, technology, and visualization behind Cyber Grand Challenge. The technology: machines that discover bugs and build patches? We're bringing our qualifier results to show just how real this is. The teams: we'll talk about the finalists who prevailed to make it to the CGC final round. Visualization: the product of CTF players working with game designers, this talk will include a live interactive demo of a graphical debugger for everyone that will let an audience follow along in real time. The machines: we're bringing high performance computing to the DEF CON stage. The event: In 2016, machines will Capture the Flag! Follow DARPA Cyber Grand Challenge on Twitter: #DARPACGC

'DLL HIJACKING' ON OS X? #@%& YEAH!

Patrick Wardle
Director of R&D, Synack

Saturday - 11:00 - Track Three

Remember DLL hijacking on Windows? Well, turns out that OS X is fundamentally vulnerable to a similar attack (independent of the user's environment).

By abusing various 'features' and undocumented aspects of OS X's dynamic loader, this talk will reveal how attackers need only to plant specially-crafted dynamic libraries to have their malicious code automatically loaded into vulnerable applications. Through this attack, adversaries can perform a wide range of malicious actions, including stealthy persistence, process injection, security software circumvention, and even 'remote' infection. So come watch as applications fall, Gatekeeper crumbles (allowing downloaded unsigned code to execute), and 'hijacker malware' arises - capable of bypassing all top security and anti-virus products! And since "sharing is caring" leave with code and tools that can automatically uncover vulnerable binaries, generate compatible hijacker libraries, or detect if you've been hijacked.

INVESTIGATING THE PRACTICALITY AND COST OF ABUSING MEMORY ERRORS WITH DNS

Luke Young
Information Security Engineer, Hydrant Labs LLC

Saturday - 16:00 - Track Three

In a world full of targeted attacks and complex exploits this talk explores an attack that can simplified so even the most non-technical person can understand, yet the potential impact is massive:

Ever wonder what would happen if one of the millions of bits in memory flipped value from a 0 to a 1 or vice versa? This talk will explore abusing that specific memory error, called a bit flip, via DNS.

The talk will cover the various hurdles involved in exploiting these errors, as well as the costs of such exploitation. It will take you through my path to 1.3 million mis-directed queries a day, purchasing hundreds of domain names, wildcard SSL certificates, getting banned from payment processors, getting banned from the entire Comcast network and much more.

SECURITY NECROMANCY: FURTHER ADVENTURES IN MAINFRAME HACKING

Philip Young aka Soldier of Fortran
Chief Mainframe Hacker

Chad "Bigendian Smalls" Rikansrud
President of Mainframe Hacking

Saturday - 17:00 - Track Two

You thought they were dead didn't you? You thought "I haven't seen a mainframe since the 90s, no one uses those anymore." Well you're wrong. Dead wrong. If you flew or drove to DEF CON your information was hitting a mainframe. Did you use credit or cash at the hotel? Doesn't matter, still a mainframe. Did you pay taxes, or perhaps call 911? What about going to the doctor? All using mainframes. At multiple points throughout the day, even if you don't do anything, your data is going through some mainframe, somewhere. 1984? Yeah right, man. That's a typo. Orwell is here now. He's livin' large. So why is no one talking about them?

SoF & Bigendian Smalls, aka 'the insane chown posse', will dazzle and amaze with feats of hackery never before seen on the mainframe. From fully breaking network job entry (NJE) and their concept of trusted nodes, to showing you what happens when you design security in the 80s and never update your frameworks. We'll demonstrate that, yes Charlie Brown, you can in fact overflow a buffer on the mainframe. New tools will be released! Things like SET'n'3270 (SET, but for mainframes!) and VTAM walker (profiling VTAM applications). Updates to current tools will be released (nmap script galore!) everything from accurate version profiling to application ID brute forcing and beyond. You'll also learn how to navigate IBM so you can get access to your very own mainframe and help continue the research that we've started!

All of your paychecks rely on mainframes in one form or another, so maybe we should be talking about it.

AND THAT'S HOW I LOST MY OTHER EYE: FURTHER EXPLORATIONS IN DATA DESTRUCTION

Zoz
Robotics Engineer and Security Researcher

Saturday - 11:00 - 101 Track

How much more paranoid are you now than you were four years ago? Warrantless surveillance and large-scale data confiscation have brought fear of the feds filching your files from black helicopter territory into the mainstream. Recent government snatch-and-grabs have run the gamut from remotely imaging foreign servers to straight up domestic coffeeshop muggings, so if you think you might need to discard a lot of data in hurry you're probably right. In their legendary DEF CON 19 presentation Shane Lawson, Bruce Potter and Deviant Ollam kicked off the discussion, and now it's time for another installment. While purging incriminating material residing on spinning disks remains the focus, the research has been expanded to encompass solid state storage and mobile solutions to your terabyte trashing needs. With best efforts to comply with the original constraints, the 2015 update features more analysis of the efficacy of kinetic projectiles, energetic materials and high voltages for saving your freedom at the potential cost of only a redundant body part... or two.

THE TRAIN TO HOGWARTS WAS NUMBER 5972. 5 + 9 + 7 + 2 = 23.

Presentations

SUNDAY TALKS

SAFE(R)

Rob Bathurst (evilrob)
Security Engineer and Penetration Tester

Jeff Thomas (xaphan)
Senior Cyber Security Penetration Testing Specialist

Sunday - 11:00 - Track Two

The security of SSL/TLS is built on a rickety scaffolding of trust. At the core of this system is an ever growing number of Certificate Authorities that most people (and software) take for granted. Recent attacks have exploited this inherent trust to covertly intercept, monitor and manipulate supposedly secure communications. These types of attack endanger everyone, especially when they remain undetected. Unfortunately, there are few tools that non-technical humans can use to verify that their HTTPS traffic is actually secure.

We will present our research into the technical and political problems underlying SSL/TLS. We will also demonstrate a tool, currently called "Canary", that will allow all types users to validate the digital certificates presented by services on the Internet.

RFIDIGGITY: PENTESTER GUIDE TO HACKING HF/NFC AND UHF RFID

Francis Brown
Partner - Bishop Fox

Shubham Shah
Security Analyst at Bishop Fox

Sunday - 13:00 - 101 Track

Have you ever attended an RFID hacking presentation and walked away with more questions than answers? This talk will finally provide practical guidance for penetration testers on hacking High Frequency (HF - 13.56 MHz) and Ultra-High Frequency (UHF – 840-960 MHz). This includes Near Field Communication (NFC), which also operates at 13.56 MHz and can be found in things like mobile payment technologies, e.g., Apple Pay and Google Wallet. We'll also be releasing a slew of new and free RFID hacking tools using Arduino microcontrollers, Raspberry Pis, phone/tablet apps, and even 3D printing.

This presentation will NOT weigh you down with theoretical details or discussions of radio frequencies and modulation schemes. It WILL serve as a practical guide for penetration testers to better understand the attack tools and techniques available to them for stealing and using RFID tag information, specifically for HF and UHF systems. We will showcase the best-of-breed in hardware and software that you'll need to build an RFID penetration toolkit. Our goal is to eliminate pervasive myths and accurately illustrate RFID risks via live attack DEMOS:

High Frequency / NFC – Attack Demos:

- HF physical access control systems (e.g., iCLASS and MIFARE DESFire 'contactless smart card' product families)
- Credit cards, public transit cards, passports (book), mobile payment systems (e.g., Apple Pay, Google Wallet), NFC loyalty cards (e.g., MyCoke Rewards), new hotel room keys, smart home door locks, and more
- Ultra-High Frequency – Attack Demos:
- Ski passes, enhanced driver's licenses, passports (card), U.S. Permanent Resident Card ('green card'), trusted traveler cards

Schematics and Arduino code will be released, and 100 lucky audience members will receive one of a handful of new flavors of our Tastic RFID Thief custom PCB, which they can insert into almost any commercial RFID reader to steal badge info or use as a MITM backdoor device capable of card replay attacks. New versions include extended control capabilities via Arduino add-on modules such as Bluetooth low energy (BLE) and GSM/GPRS (SMS messaging) modules.

This DEMO-rich presentation will benefit both newcomers to RFID penetration testing as well as seasoned professionals.

ATTACKING HYPERVISORS USING FIRMWARE AND HARDWARE

Yuriy Bulygin
Advanced Threat Research, Intel Security

Mikhail Gorobets
Advanced Threat Research, Intel Security

Alexander Matrosov
Advanced Threat Research, Intel Security

Oleksandr Bazhaniuk
Advanced Threat Research, Intel Security

Andrew Furtak
Security Researcher

Sunday - 13:00 - Track One

In this presentation, we explore the attack surface of modern hypervisors from the perspective of vulnerabilities in system firmware such as BIOS and in hardware emulation. We will demonstrate a number of new attacks on hypervisors based on system firmware vulnerabilities with impacts ranging from VMM DoS to hypervisor privilege escalation to SMM privilege escalation from within the virtual machines.

We will also show how a firmware rootkit based on these vulnerabilities could expose secrets within virtual machines and explain how firmware issues can be used for analysis of hypervisor-protected content such as VMCS structures, EPT tables, host physical addresses (HPA) map, IOMMU page tables etc. To enable further hypervisor security testing, we will also be releasing new modules in the open source CHIPSEC framework to test issues in hypervisors when virtualizing hardware.

WHO WILL RULE THE SKY? THE COMING DRONE POLICY WARS

Matt Cagle
Technology and Civil Liberties Policy Attorney, ACLU of Northern California

Eric Cheng
General Manager, DJI SF and Director of Aerial Imaging, DJI

Sunday - 11:00 - Track One

Your private drone opens up limitless possibilities – how can manufacturers and policymakers ensure you are able to realize them? As private drone ownership becomes the norm, drone makers and lawmakers will need to make important policy decisions that account for the privacy and free speech issues raised by this new technology. What legal and technical rules are being considered right now, and how might they affect your ability to do things like record footage at a city park, monitor police at a protest, or fly near a government building? These decisions will dictate the technical limitations (or lack thereof) placed on drones, and the legal consequences of operating them. Join Eric Cheng, General Manager of DJI SF and DJI's Director of Aerial Imaging, and Matt Cagle, a Technology and Civil Liberties Policy Attorney with the ACLU of Northern California, to discuss the policy issues at this leading edge of law and consumer technologies.

WHY NATION-STATE MALWARES TARGET TELCO NETWORKS: DISSECTING TECHNICAL CAPABILITIES OF REGIN AND ITS COUNTERPARTS

Omer Coskun
Ethical Hacker with KPN REDteam, KPN (Royal Dutch Telecom)

Sunday - 13:00 - Track Two

The recent research in malware analysis suggests state actors allegedly use cyber espionage campaigns against GSM networks. Analysis of state-sponsored malwares such like Flame, Duqu, Uruborus and the Regin revealed that these were designed to sustain long-term intelligence-gathering operations by remaining under the radar. Antivirus companies made a great job in revealing technical details of the attack campaigns, however, it exclusively has almost focused on the executables or the memory dump of the infected systems - the research hasn't been simulated in a real environment.

GSM networks still use ancient protocols; Signaling System 7 (SS7), GPRS Tunneling Protocol (GTP) and the Stream Control Transmission Protocol (SCTP) which contain loads of vulnerable components. Malware authors totally aware of it and weaponing exploits within their campaigns to grab encrypted and unencrypted streams of private communications handled by the Telecom companies. For instance, Regin was developed as a framework that can be customized with a wide range of different capabilities, one of the most interesting ability to monitor GSM networks.

In this talk, we are going to break down the Regin framework stages from a reverse engineering perspective - kernel driver infection scheme, virtual file system and its encryption scheme, kernel mode manager- while analyzing its behaviors on a GSM network and making technical comparison of its counterparts - such as TDL4, Uruborus, Duqu2.

REPSYCH: PSYCHOLOGICAL WARFARE IN REVERSE ENGINEERING

Chris Domas
Security Researcher

Sunday - 11:00 - Track Three

Your precious 0-day? That meticulously crafted exploit? The perfect foothold? At some point, they'll be captured, dissected, and put on display. Reverse engineers. When they begin snooping through your hard work, it pays to have planned out your defense ahead of time. You can take the traditional defensive route - encryption, obfuscation, anti-debugging - or you can go on the offense, and attack the heart and soul of anyone who dare look at your perfect code. With some carefully crafted assembly, we'll show how to break down a reverse engineer by sending them misleading, intimidating, and demoralizing messages through the control flow graphs of their favorite RE tools - turning their beloved IDA (Hopper, BinNavi, Radare, etc) into unwitting weapons for devastating psychological warfare in reverse engineering.

UBIQUITY FORENSICS - YOUR ICLOUD AND YOU

Sarah Edwards
Test Engineer, Parsons Corporation & Author/Instructor, SANS Institute

Sunday - 11:00 - 101 Track

Ubiquity or "Everything, Everywhere" - Apple uses this term describe iCloud related items and its availability across all devices. iCloud enables us to have our data synced with every Mac, iPhone, iPad, PC as well as accessible with your handy web browser. You can access your email, documents, contacts, browsing history, notes, keychains, photos, and more all with just a click of the mouse or a tap of the finger - on any device, all synced within seconds.

Much of this data gets cached on your devices, this presentation will explore the forensic artifacts related to this cached data. Where is the data stored; how to look at it; how is it synced; and what other sensitive information can be found that you may not have known existed!

ABUSING ADOBE READER'S JAVASCRIPT APIS

Brian Gorenc
Manager, HP's Zero Day Initiative

Abdul-Aziz Hariri
Security Researcher, HP's Zero Day Initiative

Jasiel Spelman
Security Researcher, HP's Zero Day Initiative

Sunday - 10:00 - Track One

Adobe Reader's JavaScript APIs offer a rich set of functionality for document authors. These APIs allow for processing forms, controlling multimedia events, and communicating with databases, all of which provide end-users the ability to create complex documents. This complexity provides a perfect avenue for attackers to take advantage of weaknesses that exist in Reader's JavaScript APIs.

In this talk, we will provide insight into both the documented and undocumented APIs available in Adobe Reader. Several code auditing techniques will be shared to aid in vulnerability discovery, along with numerous proofs-of-concept which highlight real-world examples. We'll detail out how to chain several unique issues to obtain execution in a privileged context. Finally, we'll describe how to construct an exploit that achieves remote code execution without the need for memory corruption.

LET'S TALK ABOUT SOAP, BABY. LET'S TALK ABOUT UPNP

Ricky "HeadlessZeke" Lawshae
Security Researcher, HP TippingPoint

Sunday - 14:00 - Track Two

Whether we want it to be or not, the Internet of Things is upon us. Network interfaces are the racing stripes of today's consumer device market. And if you put a network interface on a device, you have to make it do something right? That's where a Simple Object Access Protocol (SOAP) service comes in. SOAP services are designed with ease-of-access in mind, many times at the expense of security. Ludicrous amounts of control over device functionality, just about every category of vulnerability you can think of, and an all-around lack of good security practice about sums it up. In this talk, I will discuss this growing attack surface, demonstrate different methods for attacking/fuzzing it, and provide plenty of examples of the many dangers of insecure SOAP/ UPnP interfaces on embedded and "smart" devices along the way.

INTER-VM DATA EXFILTRATION: THE ART OF CACHE TIMING COVERT CHANNEL ON X86 MULTI-CORE

Etienne Martineau
Software engineer, Cisco Systems

Sunday - 14:00 - Track One

On x86 multi-core covert channels between co-located Virtual Machine (VM) are real and practical thanks to the architecture that has many imperfections in the way shared resources are isolated.

This talk will demonstrate how a non-privileged application from one VM can ex-filtrate data or even establish a reverse shell into a co-located VM using a cache timing covert channel that is totally hidden from the standard access control mechanisms while being able to offer surprisingly high bps at a low error rate.

In this talk you'll learn about the various concepts, techniques and challenges involve in the design of a cache timing covert channel on x86 multi-core such as:

- An overview of some of the X86 shared resources and how we can use / abuse them to carry information across VMs.
- Fundamental concept behind cache line encoding / decoding.
- Getting around the hardware pre-fetching logic (without disabling it from the BIOS!)
- Data persistency and noise. What can be done?
- Guest to host page table de-obfuscation. The easy way.
- Phase Lock Loop and high precision inter-VM synchronization. All about timers.

At the end of this talk we will go over a working VM to VM reverse shell example as well as some surprising bandwidth measurement results. We will also cover the detection aspect and the potential countermeasure to defeat such a communication channel. The source code is going to be release at that time on 'github'

HOW TO HACK GOVERNMENT: TECHNOLOGISTS AS POLICY MAKERS

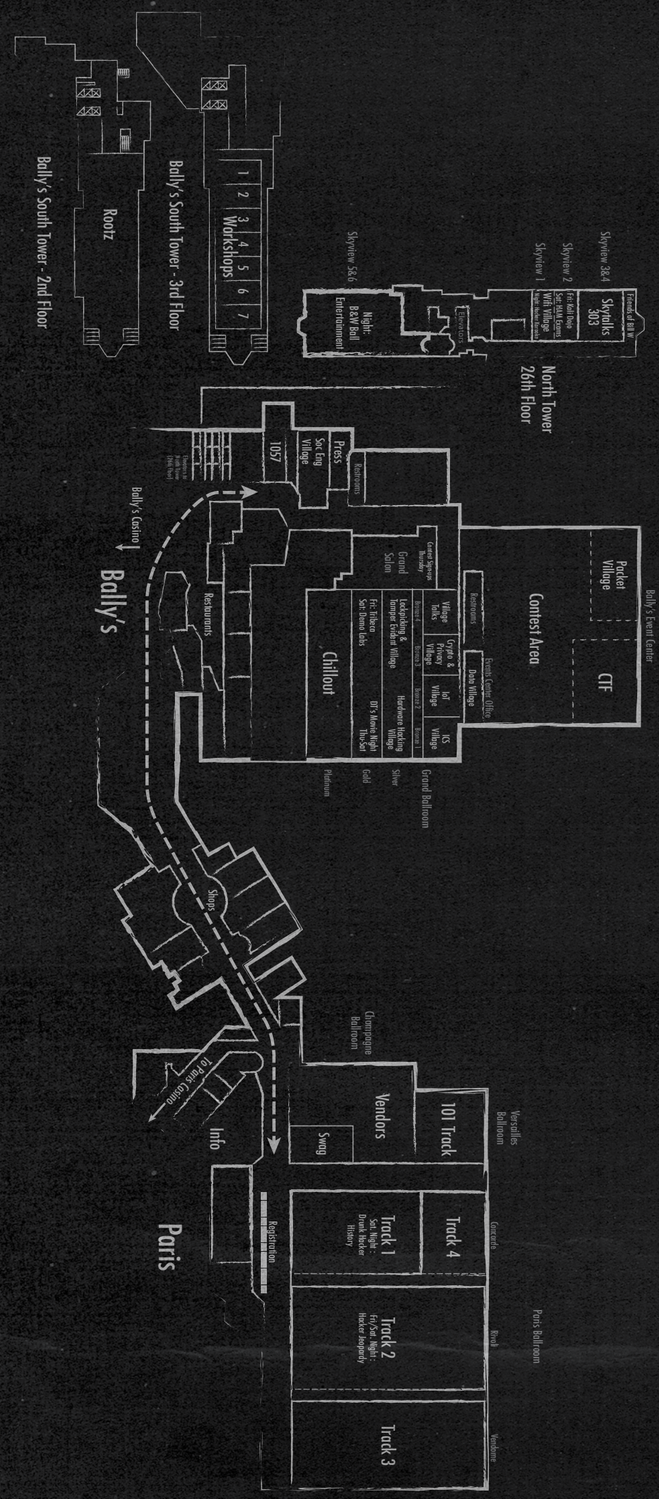
Terrell McSweeny
Commissioner, Federal Trade Commission

Ashkan Soltani
Chief Technologist, Federal Trade Commission

Sunday - 10:00 - Track Three

As the leading federal agency responsible for protecting your privacy rights online, technology is at the core of the Federal Trade Commission's work. You may be familiar with the agency's enforcement actions against some of the world's biggest tech companies for privacy/data security violations - but you may not know how your research skills can inform its investigations

Map & Schedule



Thursday, August 6

	Track Four	DEF CON 101
10:00	HARDWARE AND TRUST SECURITY: EXPLAIN IT LIKE I'M 5 Teddy Reed & Nick Anderson	INTRODUCTION TO SDR AND THE WIRELESS VILLAGE DaKahuna & satanclawz
11:00	HACKING WEB APPS Brent White	HACKERS HIRING HACKERS - HOW TO DO THINGS BETTER Tottenkoph & IrishMASMS
12:00	SEEING THROUGH THE FOG Zack Fasel	
13:00	ALICE AND BOB ARE REALLY CONFUSED David Huerta	DEF CON 101: THE PANEL The DEF CON 101 Panel
14:00	HACKER IN THE WIRES Dr. Phil Polstra	BEYOND THE SCAN: THE VALUE PROPOSITION OF VULNERABILITY ASSESSMENT Damon Small
15:00	FORENSIC ARTIFACTS FROM A PASS THE HASH ATTACK Gerard Laygui	RESPONSIBLE INCIDENT: COVERT KEYS AGAINST SUBVERTED TECHNOLOGY LATENCIES, ESPECIALLY YUBIKEY 1057
16:00	SORRY, WRONG NUMBER: MYSTERIES OF THE PHONE SYSTEM - PAST AND PRESENT Unregistered436 and Snide Owen	GUESTS N' GOBLINS: EXPOSING WIFI EXFILTRATION RISKS AND MITIGATION TECHNIQUES Peter Desfigies, Joshua Brierton & Naveed Ul Islam
17:00	BACKDOORING GIT John Menerick	DARK SIDE OF THE ELF - LEVERAGING DYNAMIC LOADING TO PWN NOOBS Alessandro Di Federico & Yan Shoshi-taishvil
18:00	SECURE MESSAGING FOR NORMAL PEOPLE Justin Engler	MEDICAL DEVICES: PWNAGE AND HONEYPOTS Scott Erven & Mark Collao

Friday, August 7

	Track One	Track Two	Track Three	Track Four	DEF CON 101
10:00	SHALL WE PLAY A GAME? Thomas Szakaly	INFORMATION ACCESS AND INFORMATION SHARING: WHERE WE ARE AND WHERE WE ARE GOING Alejandro Mayorkas	WELCOME TO DEF CON 23 DT & 1o57	BUGGED FILES: IS YOUR DOCUMENT TELLING ON YOU? Daniel 'UnicornFurnace' Crowley & Damon Smith	NSM 101 FOR ICS Chris Sistrunk
11:00	STAGEFRIGHT: SCARY CODE IN THE HEART OF ANDROID Joshua J. Drake		FIGHTING BACK IN THE WAR ON GENERAL PURPOSE COMPUTERS Cory Doctorow	GOODBYE MEMORY SCRAPING MALWARE: HOLD OUT TILL 'CHIP AND PIN' Weston Hecker	CRYPTO FOR HACKERS Eijah
12:00	MALWARE IN THE GAMING MICROECONOMY Zack Allen and Rusty Bower	LICENSED TO PWN: THE WEAPONIZATION AND REGULATION OF SECURITY RESEARCH Panel	USB ATTACK TO DECRYPT WI-FI COMMUNICATIONS Jeremy Dorough	CONFESSIONS OF A PROFESSIONAL CYBER STALKER Ken Westin	BRUCE SCHNEIER Q&A Bruce Schneier
13:00	INSTEON'S FALSE SECURITY AND DECEPTIVE DOCUMENTATION Peter Shipley and Ryan Gooler	DRIVE IT LIKE YOU HACKED IT: NEW ATTACKS AND TOOLS TO WIRELESSLY STEAL CARS Samy Kamkar	RED VS. BLUE: MODERN ACTIVE DIRECTORY ATTACKS AND DEFENSE Sean Metcalf	DON'T WHISPER MY CHIPS: SIDECHANNEL AND GLITCHING FOR FUN AND PROFIT Colin O'Flynn	APPLIED INTELLIGENCE: USING INFORMATION THAT'S NOT THERE Michael Schrenk
14:00	BUILD A FREE CELLULAR TRAFFIC CAPTURE TOOL WITH A VXWORKS FEMOTO Yuwei Zheng & Haoqi Shan	HOW TO HACK A TESLA MODEL S Marc Rogers & Kevin Mahaffey	REMOTE ACCESS, THE APT Ian Latter	CRACKING CRYPTOCURRENCY BRAINWALLETS Ryan Castellucci	HACKING SQL INJECTION FOR REMOTE CODE EXECUTION ON A LAMP STACK nemus
15:00	HOW TO HACK YOUR WAY OUT OF HOME DETENTION AmmonRa	LOW-COST GPS SIMULATOR - GPS SPOOFING BY SDR Lin Huang & Qing Yang	REVISITING RE:DOS Eric 'XlogicX' Davison	QUANTUM COMPUTERS VS. COMPUTER SECURITY Jean-Phillippe Aumasson	CHELLAM: A WI-FI IDS/FIREWALL FOR WINDOWS Vivek Ramachandran
16:00	UNBOOTABLE: EXPLOITING THE PAYLOCK SMARTBOOT VEHICLE IMMOBILIZER Fluxist	HARNESS: POWERSHELL WEAPONIZATION MADE EASY (OR AT LEAST EASIER) Rich Kelley	WHEN THE SECRETARY OF STATE SAYS, "PLEASE STOP HACKING US..." David An	TELL ME WHO YOU ARE AND I WILL TELL YOU YOUR LOCK PATTERN Marte Loge	LTE RECON AND TRACKING WITH RTLS-DR Ian Kline
16:30	HOW TO SECURE THE KEYBOARD CHAIN Paul Amicelli & Baptiste David	I WILL KILL YOU Chris Rock	PUT ON YOUR TINFO_T HAT IF YOU'RE MY TYPE Miaubiz	SEPARATING THE BOTS FROM THE HUMANS Ryan Mitchell	DETECTING RANDOMLY GENERATED STRINGS; A LANGUAGE-BASED APPROACH mahdi manazifar
17:00	WHEN IOT ATTACKS: HACKING A LINUX-POWERED RIFLE Runa A. Sandvik & Michael Auger	FUN WITH SYMBOLIKS Atlas	NETRIPPER: SMART TRAFFIC SNIFFING FOR PENETRATION TESTERS Ionut Popescu	HACK THE LEGACY! IBM I (AKA AS/400) REVEALED Bart Kulach	IAM PACKER AND SO CAN YOU Mike Sconzo
18:00	HOW TO TRAIN YOUR RFID ATTACKING TOOLS Craig Young	DRINKING FROM LETHE: NEW M ETHODS OF EXPLOITING AND MITIGATING MEMORY CORRUPTION VULNS Daniel Selifonov	HOOKED BROWSER MESHED-NETWORKS WITH WEBRTC AND BEEF Christian (@xntrik) Frichot	BREAKING SSL USING TIME SYNCHRONIZATION ATTACKS Jose Selvi	ROCKING THE POCKET BOOK: HACKING CHEMICAL PLANTS FOR COMPETITION AND EXTORTION Marina Krotofil & Jason Larsen
19:00	ONE DEVICE TO PWN THEM ALL Dr. Phil Polstra				

Saturday, August 8

	Track One	Track Two	Track Three	Track Four	DEF CON 101
10:00	SCARED POOPLESS – LTE AND *YOUR* LAPTOP Mickey Shkatov & Jesse Michael	THUNDERSTRIKE 2: SITH STRIKE Trammel Hudson, Xeno Kovah, Corey Kallenberg	DO EXPORT CONTROLS ON "INTRUSION SOFTWARE" THREATEN VULNERABILITY RESEARCH? Tom Cross aka Decius & Collin Anderson	DISSECTING THE DESIGN OF SCADA WEB HUMAN MACHINE INTERFACES (HMIS) - HUNTING VULNERABILITIES Aditya K Sood	A HACKER'S GUIDE TO RISK Bruce Potter
11:00	KEY-LOGGER, VIDEO, MOUSE — HOW TO TURN YOUR KVM INTO A RAGING KEY-LOGGING Yaniv Balmas & Lior Oppenheim	MACHINE VS. MACHINE: INSIDE DARPA'S FULLY AUTOMATED CTF Michael Walker & Jordan Wiens	'DLL HIJACKING' ON OS X? #@%& YEAH! Patrick Wardle	QARK: ANDROID APP EXPLOIT AND SCA TOOL Tony Trummer & Tushar Dalvi	AND THAT'S HOW I LOST MY OTHER EYE: FURTHER EXPLORATIONS IN DATA DESTRUCTION Zoz
12:00	HACKING SMART SAFES: ON THE "BRINK" OF A ROBBERY Dan 'AltF4' Petro & Oscar Salazar	F*CK THE ATTRIBUTION, SHOW US YOUR .IDB! Morgan Marquis-Boire, Marion Marschalek, Claudio Guarnieri	I HUNT PENETRATION TESTERS: MORE WEAKNESSES IN TOOLS AND PROCEDURES Wesley McGrew	CHIGULA : A FRAMEWORK FOR WI-FI INTRUSION DETECTION AND FORENSICS Vivek Ramachandran	ARE WE REALLY SAFE? - BYPASSING ACCESS CONTROL SYSTEMS Dennis Maldonado
13:00	SPREAD SPECTRUM SATCOM HACKING: ATTACKING THE GLOBALSTAR SIMPLEX DATA SERVICE Colby Moore	ANGRY HACKING - THE NEXT GENERATION OF BINARY ANALYSIS Yan Shoshitaishvili & Fish Wang	WHYMI SO SEXY? WMI ATTACKS, REAL-TIME DEFENSE, AND ADVANCED FORENSIC ANALYSIS Matt Graeber, Willi Ballentin, Claudiu Teodorescu	FROM 0 TO SECURE IN 1 MINUTE — SECURING IAAS Nir Valtman & Moshe Ferber	IT'S THE ONLY WAY TO BE SURE: OBTAINING AND DETECTING DOMAIN PERSISTENCE Grant Bugher
14:00	EXTRACTING THE PAINFUL (BLUE)TOOTH Matteo Beccaro & Matteo Collura	REMOTE EXPLOITATION OF AN UNALTERED PASSENGER VEHICLE Charlie Miller and Chris Valasek		BURPKIT – USING WEBKIT TO OWN THE WEB Nadeem Douba	ABUSING XSLT FOR PRACTICAL ATTACKS Fernando Arnaboldi
15:00	LOOPING SURVEILLANCE CAMERAS THROUGH LIVE EDITING OF NETWORK STREAMS Eric Van Albert & Zach Banks	HACKING ELECTRIC SKATEBOARDS: VEHICLE RESEARCH FOR MORTALS Mike Ryan & Richo Healey	HIGH-DEF FUZZING: EXPLORING VULNERABILITIES IN HDMI-CEC Joshua Smith	LET'S ENCRYPT - MINTING FREE CERTIFICATES TO ENCRYPT THE ENTIRE WEB Peter Eckersley, James Kasten, & Yan Zhu	EXTENDING FUZZING GRAMMARS TO EXPLOIT UNEXPLORED CODE PATHS IN MODERN WEB BROWSERSS Saif El-Sherei & Etienne Stalmans
16:00	SWITCHES GET STITCHES Colin Cassidy, Éireann Leverett, Robert M. Lee	I WANT THESE * BUGS OFF MY * INTERNET Dan Kaminsky	INVESTIGATING THE PRACTICALITY AND COST OF ABUSING MEMORY ERRORS WITH DNS Luke Young	NSA PLAYSET: JTAG IMPLANTS Joe FitzPatrick & Matt King	HOW TO SHOT WEB: WEB AND MOBILE HACKING IN 2015 Jason Haddix
17:00	EXPLORING LAYER 2 NETWORK SECURITY IN VIRTUALIZED ENVIRONMENTS Ronny L. Bull & Jeanna N. Matthews	SECURITY NECROMANCY: FURTHER ADVENTURES IN MAINFRAME HACKING Philip Young & Chad "Bigendian Smalls" Rikansrud	802.11 MASSIVE MONITORING Andres Blanco & Andres Gazzoli	HACKING THE HUMAN BODY/BRAIN: IDENTITY SHIFT, THE SHAPE OF A NEW SELF, AND HUMANITY 2.0 Richard Thieme	THE BIEBER PROJECT: AD TECH 101, FAKE FANS AND ADVENTURES IN BUYING INTERNET TRAFFIC Mark Ryan Talabis
18:00	STAYING PERSISTENT IN SOFTWARE DEFINED NETWORKS Gregory Pickett			DIY NUKEPROOFING: A NEW DIG AT "DATA-MINING" 3AlarmLampscooter	GAME OF HACKS: PLAY, HACK & TRACK Amit Ashbel & Maty Siman
19:00	CONTEST: DRUNK HACKER HISTORY Until 20:20	ASK THE EFF: THE YEAR IN DIGITAL CIVIL LIBERTIES Panel	DEF CON COMEDY INCEPTION: HOW MANY LEVELS DEEP CAN WE GO? Panel	I'M A NEWBIE YET I CAN HACK ZIGBEE – TAKE UNAUTHORIZED CONTROL OVER ZIGBEE DEVICES Li Jun & Yang Qing	LINUX CONTAINERS: FUTURE OR FANTASY? Aaron Grattafiori

Sunday, August 9

	Track One	Track Two	Track Three	DEF CON 101
10:00	ABUSING ADOBE READER'S JAVASCRIPT APIS Brian Gorenc, Abdul-Aziz Hariri, Jasiel Spelman	DOCKER, DOCKER, GIVE ME THE NEWS, I GOT A BAD CASE OF SECURING YOU David Mortman	HOW TO HACK GOVERNMENT: TECHNOLOGISTS AS POLICY MAKERS Terrell McSweeny & Ashkan Soltani	ABUSING NATIVE SHIMS FOR POST EXPLOITATION Sean Pierce
11:00	WHO WILL RULE THE SKY? THE COMING DRONE POLICY WARS Matt Cagle & Eric Cheng	CANARY: KEEPING YOUR DICK PICS SAFE(R) Rob Bathurst (evilrob) & Jeff Thomas (xaphan)	REPSYCH: PSYCHOLOGICAL WARFARE IN REVERSE ENGINEERING Chris Domas	UBIQUITY FORENSICS - YOUR ICLOUD AND YOU Sarah Edwards
12:00	KNOCKING MY NEIGHBOR'S KID'S CRUDDY DRONE OFFLINE Michael Robinson & Alan Mitchell	PIVOTING WITHOUT RIGHTS – INTRODUCING PIVOTER Geoff Walton & Dave Kennedy	STICK THAT IN YOUR (ROOT) PIPE & SMOKE IT Patrick Wardle	HIJACKING ARBITRARY .NET APPLICATION CONTROL FLOW Topher Timzen
13:00	ATTACKING HYPERVISORS USING FIRMWARE AND HARDWARE Yuriy Bulygin	WHY NATION-STATE MALWARES TARGET TELCO NETWORKS: DISSECTING TECHNICAL CAPABILITIES OF REGIN AND ITS COUNTERPARTS Omer Coskun	"QUANTUM" CLASSIFICATION OF MALWARE John Seymour	RFIDIGGITY: PENTESTER GUIDE TO HACKING HF/NFC AND UHF RFID Francis Brown & Shubham Shah
14:00	INTER-VM DATA EXFILTRATION: THE ART OF CACHE TIMING COVERT CHANNEL ON X86 MULTI-CORE Etienne Martineau	LET'S TALK ABOUT SOAP, BABY. LET'S TALK ABOUT UPNP Ricky "HeadlessZeke" Lawshae	ADVANCES IN LINUX PROCESS FORENSICS USING ECFS Ryan O'Neill	CONTEST CLOSING CEREMONIES
15:00	CLOSED FOR SETUP			
16:00	CLOSING CEREMONIES Dark Tangent & Friends			CLOSED

and policy. Come hear about some of the Commission's recent tech-related actions, research and reports, plus how its work impacts both consumers and businesses. You'll also learn how you can directly or indirectly help the agency protect consumers, guide businesses to develop better/strong data security, and much more.

DOCKER, DOCKER, GIVE ME THE NEWS, I GOT A BAD CASE OF SECURING YOU

David Mortman
Chief Security, Architect & Distinguished Engineer, Dell Software

Sunday - 10:00 - Track Two

Docker is all the rage these days. Everyone is talking about it and investing in it, from startups to enterprises and everything in between. But is it secure? What are the costs and benefits of using it? Is this just a huge risk or a huge opportunity? There's a while lot of ranting and raving going on, but not nearly enough rational discourse. I'll cover the risks and rewards of using Docker and similar technologies such as AppC as well as discuss the larger implications of using orchestration systems like Mesos or Kubernetes. This talk will cover the deep technical issues to be concerned about as well as the pragmatic realities of the real world.

ADVANCES IN LINUX PROCESS FORENSICS USING ECFS

Ryan O'Neill
Security Consultant, Leviathan Security Group

Sunday - 14:00 - Track Three

Many hackers today are using process memory infections to maintain stealth residence inside of a compromised system. The current state of forensics tools in Linux, lack the sophistication used by the infection methods found in real world hacks. ECFS (Extended core file snapshot) technology, https://github.com/elfmaster/ecfs is an innovative extension to regular ELF core files, designed to be used as forensics-friendly snapshots of process memory. A brief showcasing of the ECFS technology was featured in POC||GTFO 0x7 (Innovations with core files).

However this talk will reveal deeper insight on the many features of this technology, such as full symbol table reconstruction, builtin detection heuristics, and how common binutils such as objdump, and readelf can be used to quickly identify complex infections such as PLT/GOT hooks and shared library injection. We will also cover the libecfs API that was created specifically for malware and forensics analysts who aim to implement support for ECFS snapshots into new or existing malware detection software.

While the ECFS core format was initially designed for runtime malware and forensics purposes, another very neat aspect to this technology was quickly extrapolated on; the ECFS snapshots can also be reloaded into memory and executed. Very similar to VM snapshots, which opens many more doors for research and exploration in a vast array of areas from dynamic analysis to migrating live processes across systems. ECFS is still a work in progress, but for those who understand the arduous nature of dissecting a process and identifying anomalies, will surely acquire a quick respect for the new technology that makes all of this so much easier.

ABUSING NATIVE SHIMS FOR POST EXPLOITATION

Sean Pierce
Technical Intelligence Analyst for iSIGHT Partners

Sunday - 10:00 - 101 Track

Shims offer a powerful rootkit-like framework that is natively implemented in most all modern Windows Operating Systems. This talk will focus on the wide array of post-exploitation options that a novice attacker could utilize to subvert the integrity of virtually any Windows application. I will demonstrate how Shim Database Files (sdb files / shims) are simple to create, easy to install, flexible, and stealthy. I will also show that there are other far more advanced applications such as in-memory patching, malware obfuscation, evasion, and system integrity subversion. For defenders, I am releasing 6 open source tools to prevent, detect, and block malicious shims.

KNOCKING MY NEIGHBOR'S KID'S CRUDDY DRONE OFFLINE

Michael Robinson
Professor, Stevenson University

Sunday - 12:00 - Track One

My neighbor's kid is constantly flying his quad copter outside my windows. I see the copter has a camera and I know the little sexed crazed monster has been snooping around the neighborhood. With all of the hype around geo-fencing and drones, this got me to wondering: Would it be possible to force a commercial quad copter to land by sending a low-level pulse directly to it along the frequencies used by GPS? Of course, radio signal jamming is illegal in the U.S and, frankly, it would disrupt my electronics, too. In this presentation, we'll look at some of the research and issues we encountered, when we attempted to force land two commercial drones (the new DJI Phantom 3 and the Parrot Bepop Drone) by sending GPS signals directly at the drones (while staying under the threshold for jamming and not disrupting anyone else).

"QUANTUM" CLASSIFICATION OF MALWARE

John Seymour
Ph.D. student, University of Maryland, Baltimore County

Sunday - 13:00 - Track Three

Quantum computation has recently become an important area for security research, with its applications to factoring large numbers and secure communication. In practice, only one company (D-Wave) has claimed to create a quantum computer which can solve relatively hard problems, and that claim has been met with much skepticism. Regardless of whether it is using quantum effects for computation or not, the D-Wave architecture cannot run the standard quantum algorithms, such as Grover's and Shor's. The D-Wave architecture is instead purported to be useful for machine learning and for heuristically solving NP-Complete problems.

We'll show why the D-Wave and the machine learning problem for malware classification seem especially suited for each other. We also explain how to translate the classification problem for malicious executables into an optimization problem which a D-Wave machine can solve. Specifically, using a 512-qubit D-Wave Two processor, we show that a minimalist malware classifier, with cross-validation accuracy comparable to standard machine learning algorithms, can be created. However, even such a minimalist classifier incurs a surprising level of overhead.

HIJACKING ARBITRARY .NET APPLICATION CONTROL FLOW

Topher Timzen
Security Researcher - Intel

Sunday - 12:00 - 101 Track

This speech will demonstrate attacking .NET applications at runtime. I will show how to modify running applications with advanced .NET and assembly level attacks that alter the control flow of any .NET application. New attack techniques and tools will be released to allow penetration testers and attackers to carry out advanced post exploitation attacks.

This presentation gives an overview of how to use these tools in a real attack sequence and gives a view into the .NET hacker space.

PIVOTING WITHOUT RIGHTS – INTRODUCING PIVOTER

Geoff Walton
Senior Security Consultant for Cleveland-based TrustedSec

Dave Kennedy (ReL1K/HackingDave)
Founder of TrustedSec and Binary Defense Systems

Sunday - 12:00 - Track Two

One of the most challenging steps of a penetration test is popping something and not having full administrative level rights over the system. Companies are cutting back on administrative level rights for endpoints or how about those times where you popped an external web application and were running as Apache or Network Service? Privilege escalation or pillaging systems can be difficult and require extensive time if successful at all. One of the most challenging aspects around pentesting was the need to have administrative level rights, install your tools, and from there leverage the compromised machine as a pivot point for lateral movement in the network. Well, the time has changed. Introducing Pivoter – a reverse connection transparent proxy that supports the ability to pivot with ease. Pivoter is a full transparent proxy that supports the ability to use limited rights on a system to pivot to other systems and attack transparently from your system at home. Port scans, exploits, brute forcing, anything you could do like you were on that network is now available through Pivoter. As part of this talk, we'll be releasing a new Metasploit module for shell DLL injection for AV evasion, a Linux version of Pivoter, a Windows version of Pivoter, and a PowerShell version of Pivoter. msf> run pivoter -> pentest as if you are on the internal network even if you don't have admin rights. Also during this talk, we'll be releasing a new major release of the Social-Engineer Toolkit (SET) which incorporates Pivoter into the payload delivery system.

STICK THAT IN YOUR (ROOT)PIPE & SMOKE IT

Patrick Wardle
Director of R&D, Synack

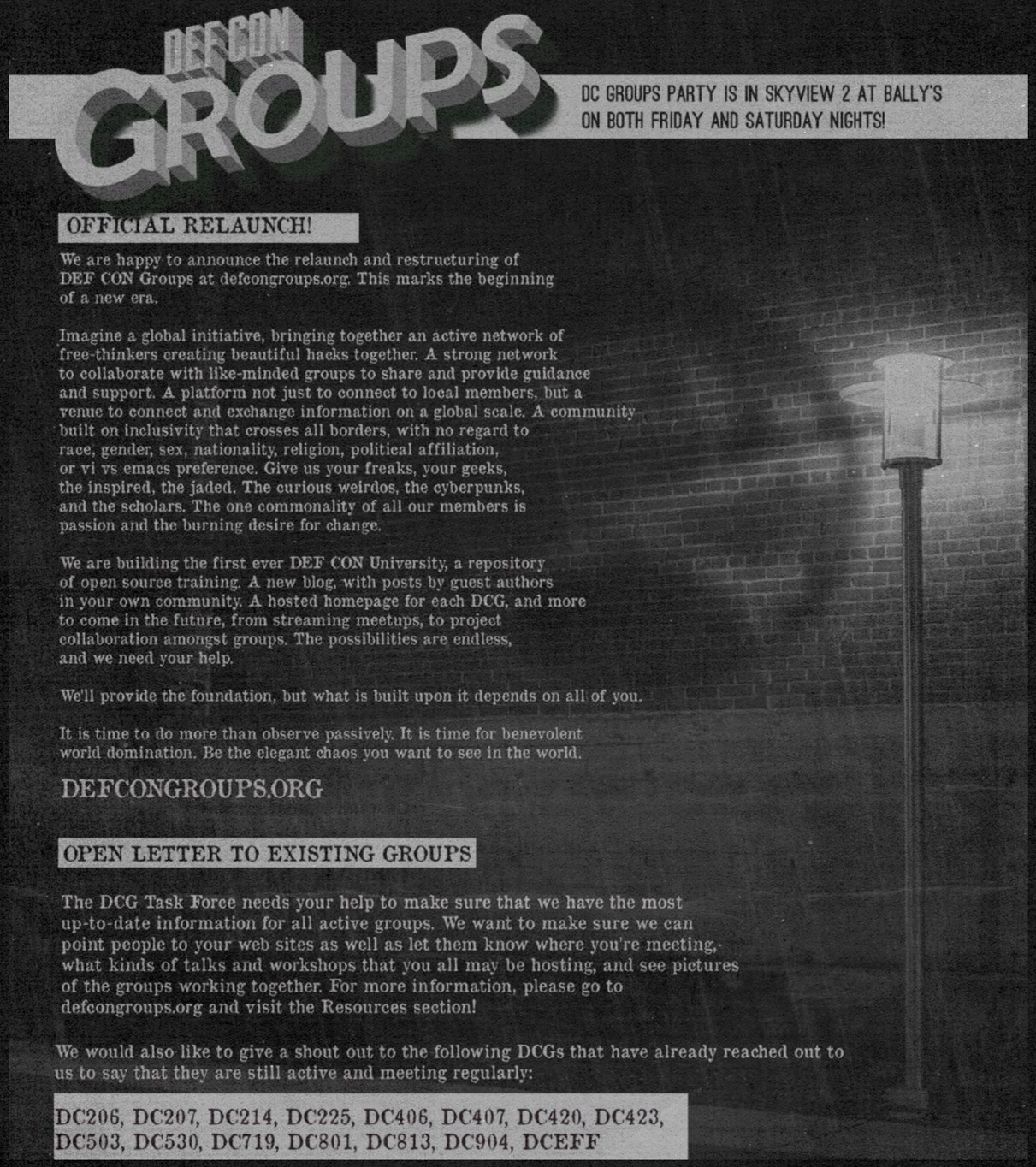
Sunday - 12:00 - Track Three

You may ask; "why would Apple add an XPC service that can create setuid files anywhere on the system - and then blindly allow any local user to leverage this service?" Honestly, I have no idea!

The undocumented 'writeconfig' XPC service was recently uncovered by Emil Kvarnhammar, who determined its lax controls could be abused to escalate one's privileges to root. Dubbed 'rootpipe,' this bug was patched in OS X 10.10.3. End of story, right? Nope, instead things then got quite interesting. First, Apple decided to leave older versions of OS X un-patched. Then, an astute researcher discovered that the OSX/XSLCmd malware which pre-dated the disclosure, exploited this same vulnerability as a 0day! Finally, yours truly, found a simple way to side-step Apple's patch to re-exploit the core vulnerability on a fully-patched system. So come attend (but maybe leave your MacBooks at home), as we dive into the technical details XPC and the rootpipe vulnerability, explore how malware exploited this flaw, and then fully detail the process of completely bypassing Apple's patch. The talk will conclude by examining Apple's response, a second patch, that appears to squash 'rootpipe'…for now.

DEF CON GROUPS

DC GROUPS PARTY IS IN SKYVIEW 2 AT BALLY'S ON BOTH FRIDAY AND SATURDAY NIGHTS!



OFFICIAL RELAUNCH!

We are happy to announce the relaunch and restructuring of DEF CON Groups at defcongroups.org. This marks the beginning of a new era.

Imagine a global initiative, bringing together an active network of free-thinkers creating beautiful hacks together. A strong network to collaborate with like-minded groups to share and provide guidance and support. A platform not just to connect to local members, but a venue to connect and exchange information on a global scale. A community built on inclusivity that crosses all borders, with no regard to race, gender, sex, nationality, religion, political affiliation, or vi vs emacs preference. Give us your freaks, your geeks, the inspired, the jaded. The curious weirdos, the cyberpunks, and the scholars. The one commonality of all our members is passion and the burning desire for change.

We are building the first ever DEF CON University, a repository of open source training. A new blog, with posts by guest authors in your own community. A hosted homepage for each DCG, and more to come in the future, from streaming meetups, to project collaboration amongst groups. The possibilities are endless, and we need your help.

We'll provide the foundation, but what is built upon it depends on all of you.

It is time to do more than observe passively. It is time for benevolent world domination. Be the elegant chaos you want to see in the world.

DEFCONGROUPS.ORG

OPEN LETTER TO EXISTING GROUPS

The DCG Task Force needs your help to make sure that we have the most up-to-date information for all active groups. We want to make sure we can point people to your web sites as well as let them know where you're meeting, what kinds of talks and workshops that you all may be hosting, and see pictures of the groups working together. For more information, please go to defcongroups.org and visit the Resources section!

We would also like to give a shout out to the following DCGs that have already reached out to us to say that they are still active and meeting regularly:

DC206, DC207, DC214, DC225, DC406, DC407, DC420, DC423, DC503, DC530, DC719, DC801, DC813, DC904, DCEFF

Demo Labs

ALL NEW FOR DEF CON 23!

DEF CON'S FIRST DEMO LABS IS A WIDE-OPEN AREA FILLED WITH DEF CON COMMUNITY MEMBERS SHARING THEIR PERSONAL, OPEN-SOURCE TECH PROJECTS. PRESENTERS WILL ROTATE IN AND OUT EVERY FEW HOURS. IT'S LIKE A POSTER-BOARD SESSION WITH MORE ELECTRONICS, OR LIKE A VERY FRIENDLY, LOW-STAKES 'SHARK TANK' DONE CAFETERIA STYLE.

WHERE: BALLY'S, IN THE GOLD ROOM.
WHEN: SATURDAY ONLY, FROM 10:00 TO 18:00
(TIMES VARY PER INDIVIDUAL LAB)
DEMO LAB DESCRIPTIONS & TIMES BELOW

PORTAPACK H1 PORTABLE SDR

Jared Boone
ShareBrained Technology

14:00 - 16:00

The PortaPack H1 turns a HackRF One software-defined radio into a portable, open-source radio research platform, consisting of an LCD screen, micro SD slot, audio interface, and controls. It's capable of signal monitoring, capture, and analysis, and fits in one hand.

Detailed Explanation of Tool:

The PortaPack H1 attaches to a HackRF One software-defined radio, and adds an LCD with touchscreen, audio interface, user controls, micro SD card, and a RTC battery. It utilizes the dual ARM Cortex-M processors on the HackRF One to provide a lightweight but capable radio research platform. Because of resource constraints, it was not possible to provide a complete operating system, so ChibiOS was utilized, with good results. Even with these constraints, this portable device can monitor, analyze, and record many types of narrowband radio signals. Since the design is open-source, developers can build on the existing software to support many other types of signals and applications.

MOZDEF: THE MOZILLA DEFENSE PLATFORM

Jeff Bryner
Security Researcher

10:00-12:00

MozDef is an open source SIEM overlay for Elastic Search that enables real-time alerting, investigations, incident response and automated defense in a modern, extensible fashion.

SPEEDPHISHING FRAMEWORK (SPF)

Adam Compton
Penetration Tester

10:00-12:00

SpeedPhishing Framework (SPF) is a new tool which can assist penetration testers in quickly/automatically deploying phishing exercises in minimal time. The tool, when provided minimal input (such as just a domain name), can automatically search for potential targets, deploy multiple phishing websites, craft and send phishing emails to the targets, record the results, generate a basic report, among performing other more advanced tasks.

EMANATE LIKE A BOSS: GENERALIZED COVERT DATA EXFILTRATION WITH FUNTENNA

Ang Cui
Chief Scientist, Red Balloon Security, Inc.

14:00 - 16:00

Funtenna is a software-only technique which causes intentional compromising emanation in a wide spectrum of modern computing hardware for the purpose of covert, reliable data exfiltration through secured and air-gapped networks. We present a generalized Funtenna technique that reliably encodes and emanates arbitrary data across wide portions of the electromagnetic spectrum, ranging from the subacoustic to RF and beyond.

The Funtenna technique is hardware agnostic, can operate within nearly all modern computer systems and embedded devices, and is specifically intended to operate within hardware not designed to act as RF transmitters.

We believe that Funtenna is an advancement of current state-of-the-art covert wireless exfiltration technologies. Specifically, Funtenna offers comparable exfiltration capabilities to RF-based retroreflectors, but can be realized without the need for physical implantation and illumination.

We first present a brief survey of the history of compromising emanation research, followed by a discussion of the theoretical mechanisms of Funtenna and intentionally induced compromising emanation in general. Lastly, we demonstrate implementations of Funtenna as small software implants within several ubiquitous embedded devices such as VoIP phones and printers, and in common computer peripherals such as hard disks, console ports, network interface cards and more.

CANTACT

Eric Evenchick
freelance embedded systems developer

10:00-12:00

CANtact is an open source CAN to USB tool that integrates with the SocketCAN utilities on Linux. It provides a low cost way to connect to in-vehicle networks on modern automobiles.

This talk will present the hardware tool, and software tools that assist with working on in-vehicle networks. Some of these are custom development around CANtact, and other are existing open source utilities (ie, Wireshark and Kayak).

BADGE JEOPARDY

Fuzzbizz
Badge Hacker

14:00 - 16:00

Hacker Jeopardy on Windows makes Richard Stallman cry. Fix that by running it on your Defcon badge!

Required: Parallax-based DC badge

Fuzzbizz started showing up to Defcon as a total noob five years ago. He just moved to California from Ireland and has somehow managed to get roped into cofounding an infosec company. Hopefully he doesn't fuck it up.

HAMSHIELD: A WIDEBAND VHF/UHF FM TRANSCEIVER FOR YOUR ARDUINO

Casey Halverson

16:00-18:00

The HamShield turns your Arduino into a VHF/UHF FM voice and data transceiver for the following frequencies:

136-170MHz, 200-260MHz, 400-520 MHz.

No need to worry about SDR and processing, as this is already taken care of on the chip level. The HamShield library provides easy voice and data capability and controls every aspect of the radio. New radio technologies and creations can be written in minutes using the Arduino IDE. The radio is plumbed into the Arduino, as well as a standard mobile headset jack. You can even plug it into your computer and control it with your Chrome browser. Multithreaded text messaging over APRS, anyone?

THE SHADYSHIELD: SOFTWARE-DEFINED TELEPHONY FOR ARDUINO

Karl Koscher
Researcher

16:00-18:00

The ShadyShield is an Arduino-compatible telephone interface for all of your old-school phone phreaking needs. The ShadyShield provides the raw analog audio, but what you do with that is up to you. We provide sample code implementing a 300 bps modem in software on the AVR, but the applications of the ShadyShield are only limited by your imagination. Want to build an auto-dialer? That's easy. Want to implement a BBS in a small, discreet form factor? The ShadyShield provides extra RAM via the SPI bus and a microSD connector for mass storage. Need a dumb dial-up terminal in a pinch? The ShadyShield has an RCA jack for NTSC/PAL output. We'll have some sample applications on display, plus a few surprises.

DIGITAL DISEASE TRACKING WEB APP

Efrain Ortiz
Dave Ewall

16:00-18:00

The tool is a an application that visualizes endpoint events into a timeline inspired by an epidemiological SIR graph. By plotting events over time by machine by event color type, its possible to spot patterns that the average endpoint security product misses. This free open source app is currently designed for one vendors endpoint security data, but is open to upgrading for other endpoint security products.

The Digital Disease Tracking Web App was developed as a after hours collaboration between Dave Ewall and Efrain Ortiz. Efrain Ortiz works at a large internet security company and Dave Ewall runs his own company.

THE DECK

Dr. Phil (Polstra)
Professor Bloomsburg University of Pennsylvania

12:00-14:00

The Deck is a version of Linux for the BeagleBone and similiar boards. The Deck is also the name of devices running The Deck used for pentesting. There are a number of addons to The Deck including: The 4Deck: Forensics USB Write blocking AirDeck: Flying hacking drone MeshDeck: Command and control multiple devices with 802.15.4 networks USBDeck: HID and Mass Storage attacks.

SWATTACK – SMARTWATCH ATTACK TOOL

Michael T. Raggo
Director, Security Research, Mobilelron, Inc

16:00-18:00

Security concerns about corporate data on smartwatches wasn't a topical concern until the release of the Apple Watch, yet wearables and smartwatches have been around for years. Our research and subsequent tool, SWATtack, brings to light the existing vulnerabilities of these devices when paired to a corporate-enabled mobile device. SWATtack incorporates our research of identified and reported vulnerabilities surrounding smartwatches and automates attack methods for accessing these devices, and pilfering data from them. From this we hope to raise security awareness surrounding these devices to ensure that when they are used in numerous practical methods, that they are used in a secure and effective manner.

CUCKOODROID

Idan Revivo
Mobile Malware Researcher, Check Point

Ofer Caspi, @shablolForce
Malware Researcher at Checkpoint Software Technologies.

CuckooDroid: an automated malware analysis framework based on the popular Cuckoo sandbox and several other open source projects. It features both static and dynamic APK inspection. Also, it provides techniques to prevent VM-detection, encryption key extraction, SSL inspection, API call trace, basic behavioral signatures and many other features. The framework is highly customizable and extensive - leveraging the power of the large, established Cuckoo community.

FIBER OPTIC TAPPING

Josh Ruppe

12:00-14:00

When you think of someone performing a standard man in the middle attack, what do you picture in your head? A network tap on copper cables? Someone using a WiFi Pineapple? Well what if the data being intercepted is leaving your home or coffee shop? Would you feel safer if your data was inside an optical fiber? You shouldn't. Fiber optics are just as susceptible to tapping as any other method of communication. In my demo lab, I will show you how fiber optic tapping works, how to conceal a tapping setup and how to defend against such an attack.

Tool Details: The tool I am using is known as a "Fiber Optic Clip-On Coupler". It is used by technicians to access talk fibers for testing purposes. However, it can also be used to "tap" the fiber without the need of a terminated end. The tool allows you to safely bend the fiber which in turn causes light to leak out through the fiber optic cladding. This enables complete and often undetected theft of data through a process not surprisingly known as "bending".

OMBUDS

Nick Skelsey
Systems Programmer

10:00-12:00

Ombuds resists censorship by storing public statement's in Bitcoin's block chain. It is meant to be used along side existing social media platforms to protect and distribute statements created by bloggers, activists and dissidents living under oppressive regimes. But if you are just worried that Twitter might delete your shitpost, you can use Ombuds to store it forever on the block chain.

SPHINX

Takehiro Takahashi
Security Researcher

14:00-16:00

Sphinx is a highly scalable open source security monitoring tool that offers real-time auditing and analysis of host activities. It works by having clients forward various types of event logs including process execution with cryptographic signature (MD5 hash), network activity, dll/driver loading, as well as miscellaneous system events to a Sphinx server where each event is recorded and analyzed.

With Sphinx, you can quickly find an answer to questions like:

can we get a list of every event that happened on machine X between date Y and date Z?

can we graphically trace what happened on my computer in the last 10 minutes because I feel there's something weird going on?

who has run a piece of malware whose existence cannot be detect by our existing Anti-Virus product on our network?

give me a list of program executions as well as dll loads whose reputation is questionable or bad.

are there Office application making outbound connection to China?

are there any dlls injected into explorer.exe whose digital signature does not belong to Microsoft?

You can build both simple and complex queries to search for threats. These queries can be run recurringly, and send alerts whenever there's a hit.

Tool details:

Sphinx works by having clients forward various types of event logs including process execution history with program's digital fingerprint (MD5 hash), network activity, dll/driver loading, as well as miscellaneous system events to a Sphinx server where each event is recorded and analyzed. These events are primarily generated through Sysmon, Microsoft's Sysinternal tool, and delivered to the server using nxlog, a robust open source log management tool.

On the server side, Sphinx receives the incoming data using Logstash, a popular log management tool with horizontal scalability. Logstash loads several plug-ins (including Sphinx's own Logstash plug-in) in order to normalize the data for analysis. The Sphinx plugin is primarily responsible for adding reputation information for events with MD5 hash. Sphinx uses the following sources to build its reputation table:

National Software Reference Library (NSRL), a project of the National Institute of Standards and Technology (NIST) which maintains a repository of known software, file profiles and file signatures for use by law enforcement and other organizations involved with computer forensic investigations. VirusTotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners.

VirusShare, a repository of malware samples to provide security researchers, incident responders, forensic analysts, and the morbidly curious access to samples of malicious code.

Finally, normalized data is stored in an Elasticsearch server. Elasticsearch is a highly scalable, open-source full-text search engine based on Apache Lucene. Users can use Sphinx's web UI to build/run queries, and detect threats. The web front end is also capable of graphically browsing program execution history or create an alert using saved queries. For example, you can have an alert set to trigger whenever Sphinx sees a program execution whose reputation is 'Harmful' OR 'Potentially Harmful' OR 'Unknown'.

HAKA - AN OPEN SOURCE SECURITY ORIENTED LANGUAGE

Mehdi Talbi
Security Researcher, Stormshield

16:00-18:00

Haka is an open source security oriented language that allows to specify and apply security policies on live captured traffic. The scope of this language is twofold. First of all, Haka is featured with a grammar allowing to specify network protocols and their underlying state machine. The specification covers text-based protocols (e.g. http) as well as binary-based protocols (e.g. dns). Secondly, Haka enables the specification of fined-grained security rules allowing end-users to filter unwanted packets and report malicious activities. Haka enables on the fly packet modification which allows to setup complex mitigation scenarios in case of attack detection. The main goal of Haka is to abstract low-level and complex tasks such as memory management and stream reassembly to non-developer experts. Haka aims to provide a simple and quick way to express security controls on existing, specific (e.g. scada) or new protocols (e.g. protocols over http).

QARK - ANDROID EXPLOITATION AND STATIC CODE ANALYSIS TOOL

Tony Trummer
Penetration Tester, LinkedIn

Tushar Dalvi
Senior Information Security Engineer, LinkedIn

14:00-16:00

QARK is an automated scanning and exploitation framework, for Android applications. It is designed to locate vulnerabilities and provide dynamically generated, Proof-of-Concept exploitation code, customized for the specific application being tested.

It can be used in a scriptable fashion, for integration into existing SDLC processes, or interactively, by security auditors, with the need to assess a fully built application, as it has the flexibility to work on either raw source code or previously built APKs. It even creates nice findings reports to keep your pointy-haired boss, client or compliance wonks happy.

QARK currently includes checks for improper TLS implementations, insecure Inter-Process Communications, insecure WebView configurations and several other common security vulnerabilities.

Additionally, QARK can serve as your Android security testing Swiss army knife. It includes a manual testing APK allowing you to configure various testing scenarios without having to write all the nasty Java yourself.

Most importantly, QARK has been designed to encourage a community-based approach to application security, by eliciting contributions from the open-source community, allowing for all Android app developers and testers to share in a common body of knowledge for securing their applications.

So, stop by for a demonstration or further details, find a 0-day in your Android app and learn how you can contribute to, and benefit from, QARK. Hurry before we get too drunk!

RUDRA

Ankur Tyagi (7h3rAm)
Malware Research Engineer, Qualys Inc

12:00-14:00

Rudra aims to provide a developer-friendly framework for exhaustive analysis of pcap files (later versions will support more filetypes). It provides features to scan pcaps and generates reports that include pcap's structural properties, entropy visualization, compression ratio, theoretical minsize, etc. These help to know type of data embedded in network flows and when combined with flow stats like protocol, Yara and shellcode matches eventually help an analyst to quickly decide if a test file deserves further investigation.

SHEVIRAH

Georgia Weidman
Founder, Bulb Security LLC

12:00-14:00

Shevirah (formerly the Smartphone Pentest Framework) is a provider of testing tools for assessing and managing the risk of mobile devices in the enterprise and testing the effectiveness of enterprise mobility management solutions. Shevirah allows security teams and consultants to integrate mobility into their risk management and penetration testing programs.

SECBEE - AN AUTOMATED ZIGBEE SECURITY SCANNER

Tobias Zillner
Senior IS Auditor, Cognosec

12:00-14:00

The tool demonstrated will be a ZigBee security testing tool. It is basically a kind of ZigBee vulnerability scanner. So developers and security testers can check the actual product implementation for ZigBee specific vulnerabilities.

Currently it supports command injection, scan for enabled join, sniff network keys in plaintext and encrypted with the ZigBee default key and a return to factory device reset.

A complete device takeover feature is under development. The final goal is to test for the correct application and implementation of every ZigBee security service.

FIND IT IN SKYVIEW 5-6, BALLY'S NORTH TOWER ON THE 26TH FLOOR, ACTION STARTS AT 22:00

Workshops

INTRODUCING DEF CON WORKSHOPS

With new hotel space comes new opportunities, and I've wanted to try workshops and trainings for years but we've never had the room once we filled up the Rio. DEF CON is pleased to bring you free workshops, thanks to the trainers and speakers willing to help spread their knowledge.

The workshops are either 4 hours or 8 hours long with an hour break for lunch. Below is the current schedule of what's happening.

Interested? Hopefully you pre-registerd for your seat before the con. If you are just finding out now that's unfortunate BUT_people do change their plans. Keep an eye on our @_defcon_ twitter for news and announcement with the hashtag #DEFCONWORKSHOPS, we will put out a blast on social media if more spots open up while at the con. They will be first come first serve.

WHEN: Friday, Saturday. 09:00 - 13:00 (Break) 14:00 to 18:00
WHERE: The 3rd floor of Ballys South tower, The Jubilee Tower. Las Vegas Ballrooms 1-7.
WHAT: Schedule and Descriptions below.

- The Dark Tangent -

EMBEDDED SYSTEM DESIGN: FROM ELECTRONICS TO MICROKERNEL DEVELOPMENT

Rodrigo Maximiano Antunes de Almeida
Professor, Federal University of Itajubá

Las Vegas Ballroom 7
Saturday, 09:00 - 13:00 (Break) 14:00 to 18:00
Max class size: 40

The workshop consists of a introduction on the embedded systems design. At first part of the workshop we'll build a simple electronic embedded system design (microcontroller+LCD). This system will be used as target platform. Using this platform the low level side of C language as bit-wise operations, pointers to fixed memory addresses and microcontroller peripherals-access will be presented. In the second part of the workshop a full embedded microkernel will be developed. Some programming structures and libraries will be coded by the presents to suit the low memory requirements of the embedded system. They will have a better understanding on the electronics-programming relationship and how these questions can impact on the kernel development. The attendants will get a deep knowledge in the kernel basic functions (processes scheduling, i/o drivers controller, etc) and its relation to electronics circuitry. Its recommended to bring your laptop to the practical activities.

VIOLENT PYTHON

Sam Bowne
Security Researcher

Las Vegas Ballroom 5
Friday, 09:00 - 13:00
Max class size: 50

Even if you have never programmed before, you can quickly and easily learn how to make custom hacking tools in Python. In hands-on projects, participants will create tools and hack into test systems, including:

- Port scanning
- Login brute-forcing
- Port knocking
- Cracking password hashes
- Sneaking malware past antivirus engines

With just a few lines of Python, it's easy to create a keylogger that defeats every commercial antivirus product, from Kaspersky to FireEye.

Technical Requirements:

Participants need a computer (Windows, Mac, or Linux) with VMware Player or VMware Fusion. USB thumbdrives will be available with Kali Linux to use. All the class materials are freely available on my Web page (samsclass.info) for anyone to use.

Prerequisite Knowledge:

Participants should be familiar with basic networking and security concepts like TCP/IP and brute force attacks. Previous programming experience is helpful but not necessary.

SECURITY AUDITING MOBILE APP

Sam Bowne
Security Researcher

Las Vegas Ballroom 5
Saturday, 09:00 - 13:00
Max class size: 50

Android apps are very insecure—70% of the ones I've tested have vulnerabilities in the OWASP Mobile Top Ten. iOS apps have similar problems, but they are ten times less common, in my tests. It's simple to test for common vulnerabilities with a few free tools: Android Studio, Genymotion, Burp, and apktool.

We will test for insecure network transmission, insecure local storage, and insecure logging. But the most common problem is failure to verify app signatures, so that apps can be modified and Trojan code can be added. Students will do that to a real financial app, creating a proof-of-concept that leaks out private data such as username and password.

Participants must bring laptops. Macs work best, but PCs can also be used. Linux works better than Windows. Students will set up their laptops, find vulnerabilities in real apps, and exploit them. Also bring any mobile devices you'd like to test, such as iPhones.

RUNNING KALI ON A RASPBERRY PI AND OTHER FUN TRICKS

Dallas
Security Researcher

Las Vegas Ballroom 4
Saturday, 09:00 - 13:00 (Break) 14:00 to 18:00
Max class size: 25
Saturday, 09:00 - 13:00 (Break) 14:00 to 18:00
Max class size: 25

Like Hacking? Like Hardware? Lets have some fun with both. We will have a couple of kits onsite, most were pre-sold so we knew what to order (there is always next year). But check in, if we have a kit you can get it!

We will discuss Raspberry Pi as a hardware platform, build a stock OS and then build a Kali installation with all kinds of tips and tricks around security, programming, using the Raspberry PI, wireless hacking and more as we go through it! You will leave with a complete setup ready to go when you are done. This will include a Raspberry Pi, Wireless Card, Memory, Case, Keyboard, LCD Display and more surprises (if you get the kit). You will need to bring your laptop to have the best experience, but can be done without (but not recommended). A manual link will be included as well. You will leave with a great platform for expanding into programming, security or home automation.

You don't have to be an expert, just have a fair understanding of networking and a desire to learn and share. We are going to talk about and walk through a lot of topics involving the hardware, sensors, cameras, software, OS and capabilities. You will need your laptop.

Pre-Order kit will be approx $135.00 and be ready for you when you get to the class, you will assemble in class. Kit essentially includes..:

- Raspberry Pi 2 w/ Case
- 2 – 8 Gig SD Cards loaded with Kali and Raspbian image
- Wireless USB 'Card'
- Micro Combo Keyboard / Mouse (Wireless)
- Micro Composite Display w/ cable (for Raspberry Pi 2)
- MicroUSB AC Adapter
- Network Cable from your PC to Pi
- Other Goodies in the Kit.

You will need your laptop to connect to the Pi once we get the OS installed and operational, unless you enjoy looking at a very small screen.

Internet is generally unreliable, so we will base the class assuming it may not work well, but if it does you will have additional options.

We will post notes from the class on the DEF CON website after the con.

CRYPTO FOR HACKERS: THE WORKSHOP

Eijah
Founder, demonsaw

Las Vegas Ballroom 5
Friday and Saturday, 14:00 to 18:00
Max class size: 50

Love Crypto? Hate DRM? Then let's hack the shit out of AACS together.

Crypto for Hackers: The Workshop is the continuation of the Crypto for Hackers talk. We'll spend 4 hours working our way through a variety of C++ crypto exercises designed specifically for DEF CON attendees. We'll implement and use all five types of crypto algorithms discussed in the talk, including ciphers (e.g. AES), hash functions (e.g. SHA-512), hash-based message authentication codes (e.g. HMAC-SHA-512), key agreement schemes (e.g. Diffie-Hellman), and password-based key derivation functions (e.g. PBKDF2).

Next we'll put our new crypto knowledge to the test and attempt to reproduce the AACS memory hack I did when I released the first Blu-Ray device key to the world: AA856A1BA814AB99FFDEBA6AEFBE1C04. You'll have actual PowerDVD memory dumps that you'll need to parse, analyze, and then figure out how to reverse engineer. I'll provide guidance and oversight, but you'll be the one writing the code, exploiting the vulnerabilities, and finding the AACS encryption keys.

Please note that this is an intermediate-level, technical workshop and requires that all attendees have a strong working knowledge of C++. While attending the Crypto for Hackers talk is extremely helpful, it is not required. As part of the workshop I'm providing a free and open-source crypto library that I wrote called demoncrypt. This is the same library used by demonsaw, the secure and anonymous content sharing application that I launched last year at DEF CON. Bring your laptop, your favorite C++ 11 compiler (>= gcc 4.7 or msvc 2013), and a strong attitude of civil disobedience.

THE ART OF VOIP HACKING

Fatih Ozavci
Security Researcher

Christos Archimandritis
Security Researcher

Las Vegas Ballroom 6
Saturday, 09:00 - 13:00 (Break) 14:00 to 18:00
Max class size: 50

VoIP attacks have evolved, and they are targeting Unified Communications (UC), commercial services, hosted environment and call centres using major vendor and protocol vulnerabilities. This workshop is designed to demonstrate these cutting edge VoIP attacks, and improve the VoIP skills of the incident response teams, penetration testers and network engineers. Signalling protocols are the centre of UC environments, but also susceptible to IP spoofing, trust issues, call spoofing, authentication bypass and invalid signalling flows. They can be hacked with legacy techniques, but a set of new attacks will be demonstrated in this workshop. This workshop includes basic attack types for UC infrastructure, advanced attacks to the SIP and Skinny protocol weaknesses, network infrastructure attacks, value added services analysis, Cdr/Log/Billing analysis and Viproy use to analyse signalling services using novel techniques. Also the well-known attacks to the network infrastructure will be combined with the current VoIP vulnerabilities to test the target workshop network. Attacking VoIP services requires limited knowledge today with the Viproy Penetration Testing Kit (written by Fatih). It has a dozen modules to test trust hacking issues, information collected from SIP and Skinny services, gaining unauthorised access, call redirection, call spoofing, brute-forcing VoIP accounts, Cisco CUCDM exploitation and debugging services using as MITM. Furthermore, Viproy provides these attack modules in the Metasploit Framework environment with full integration. The workshop contains live demonstration of practical VoIP attacks and usage of the Viproy modules.

In this hands-on workshop, attendees will learn about basic attack types for UC infrastructure, advanced attacks to the SIP protocol weaknesses, Cisco Skinny protocol hacking, hacking Cisco CUCDM and CUCM servers, network infrastructure attacks, value added services analysis, Cdr/Log/Billing analysis and Viproy VoIP pen-test kit to analyse VoIP services using novel techniques. New CDP, CUCDM and Cisco Skinny modules and techniques of Viproy will be demonstrated in the workshop as well.

Who should attend

Penetration testers, VoIP engineers, security engineers, internal auditors and all hackers who have a wireless card and a VM player.

Workshop Requirements

Participants should have an up to date Kali Linux virtual machine with Metasploit Framework. (The disk image will be provided by the tutors)

IOS APPLICATION EXPLOITATION

Prateek Gianchandani
Security Researcher

Las Vegas Ballroom 4
Friday, 09:00 - 13:00 (Break) 14:00 to 18:00
Max class size: 50

This will be an introductory course on exploiting iOS applications. The training will be based on exploiting Damn Vulnerable iOS app and other vulnerable apps which are written by the trainer in order to make people understand the different kinds of vulnerabilities in an iOS application. This course will also discuss how a developer can secure their applications using secure coding and obfuscation techniques. After the workshop, the students will be able to successfully pentest and secure iOS applications.

The following vulnerabilities in iOS applications will be discussed…

- Insecure Data Storage
- Extension Vulnerabilities
- Attacks on third party libraries
- Jailbreak Detection
- Runtime Manipulation
- Piracy Detection
- Sensitive information in memory
- Transport Layer Security (http, https, cert pinning)
- Client Side Injection
- Information Disclosure
- Broken Cryptography
- Security Decisions via Untrusted input
- Side channel data leakage
- Application Patching

ADVANCED CYBER EXERCISES

Andrea Guerber
Delta Risk LLC, A Chertoff Company

Las Vegas Ballroom 7
Friday, 09:00 - 13:00
Max class size: 50

This workshop discusses the rationale, types, structure, organization, execution, and value of cyber exercises. The course discusses the four phases of exercises: objective setting, planning, execution, and evaluation, compares methodologies with the national HSEEP (Homeland Security Exercise and Evaluation Program) and highlights execution considerations and risk management of "live-fire" cyber exercises on operational networks. Students are presented an overview of advanced cyber exercises, moving beyond traditional table-top exercises, and the considerations for running cyber exercises on both operational and closed-range networks.

EXPLOITED HOST ANALYSIS

Robin Jackson
WT Forensics

Ed Williams
WT Forensics

Las Vegas Ballroom 1
Friday & Saturday, 09:00 - 13:00 (Break) 14:00 to 18:00
Max class size: 50

Exploited Host Analysis is an 8 hour overview into the various techniques used to examine a host machine and it's corresponding network traffic to determine what happened, who did it and when. The course will briefly cover the fundamentals of Digital Forensic analysis including Locard's Exchange Principle, the order of volatility, methods and tools for acquisition and proper evidence documentation and handling. After the overview students will be led through various scenarios including:

- Packet capture analysis
- Memory Analysis using Volatility
- Log file analysis
- Deobfuscation and analysis of a web shell
- Disk analysis including timeline creation
- Registry analysis and deobfuscation of registry only malware

There will be a ton of examples and the emphasis will be upon the use of free and open source tools to achieve results. Of course we'll only really scratch the surface of each topic but we'll give you plenty of online resources to continue your exploration of Digital Forensics.

ARM FOR PENTESTERS

Aseem Jakhar
Security Researcher

Las Vegas Ballroom 6
Friday, 09:00 - 13:00 (Break) 14:00 to 18:00
Max class size: 20

The workshop is aimed at Pentesters and security professionals who want to get into pentesting ARM based systems such as smart phones, IoT devices, TVs etc. We will use Android as the ARM based platform for the workshop and take a deep dive into ARM assembly, Android Native development components, buffer overflows and shellcoding. The workshop introduces the attendees to the ARM Android platform including the intrinsic technical details and security issues using a balanced proportion of theory and extensive hands-on and exercises. It provides a base for the attendees to start researching on ARM based systems.

- Modules
- Android Native Dev Primer
- ARM Architecture
- Assembly
- Call conventions
- Shellcoding
- Runtime Code injection using Indroid
- Buffer overflows

ANALYZING INTERNET ATTACKS WITH HONEYPOTS

Ioannis Koniaris
Security Engineer, Yelp

Las Vegas Ballroom 3
Friday, 09:00 - 13:00
Max class size: 50

In the field of computer security, honeypots are systems aimed at deceiving malicious users or software that launch attacks against the servers and network infrastructure of various organizations. They can be deployed as protection 'mechanisms for an organization's real systems, or as research units to study and analyze the methods employed by human hackers or malware. In this workshop we will outline the operation of two research honeypots, by manual deployment and testing in real time. A honeypot system will undertake the role of a web trap for attackers who target the SSH service in order to gain illegal server access. Another one will undertake the role of a malware collector, usually deployed by malware analysts and anti-virus companies to gather and securely store malicious binary samples. We will also talk about post-capturing activities and further analysis techniques. As an example, we will see how to index all the captured information in a search engine like Elasticsearch and then utilize ElastAlert, an easy to use framework to setup meaningful alerting. Lastly, visualization tools will be presented for the aforementioned systems, plus a honeypot bundle Linux distribution that contains pre-configured versions of the above tools and much more related utilities, which can make the deployment of honeypots in small or large networks an easy task.

POFFENSIVE AND DEFENSIVE: ANDROID REVERSE ENGINEERING

Tim "Diff" Strazzere
Red Naga

Jon "jcase" Sawyer
Red Naga

Caleb Fenton
Red Naga

Las Vegas Ballroom 2
Friday, 09:00 - 13:00 (Break) 14:00 to 18:00
Max class size: 40

Thinking like an attacker, you will learn to identify juicy Android targets, reverse engineer them and find vulnerability and write exploits. We will deep dive into reverse engineeriing Android frameworks, applications, services and boot loaders with the end goal of rooting devices.

Approaching from a defensive perspective, we will learn quickly triage applications to determine maliciousness, exploits and weaknesses. After learning triage skills we will deep dive into malicious code along while dealing with packers, obfuscators and anti-reversing techniques.

Between the two aspects of this class, you should walk away with a basic overall of your reversing engineering knowledge and a strong understanding of how to further develop your skills specifically for mobile platforms.

Prerequisites:

We would expect students to know minimal reverse engineering concepts, would also be good though not required to have some of the following non-free tools;

- IDA Pro
- Hopper
- JEB

FROM SPAM TO THREAT INTEL

Robert Simmons
Senior Threat Intelligence Researcher, ThreatConnect, Inc

Las Vegas Ballroom 7
Friday, 14:00 to 18:00
Max class size: 30

You get massive amounts of spam. I get massive amounts of spam. I love to get massive amounts of spam, and I try to find ways to get more spam every day. Why? Because it is a rich source of threat data!

The author of a new variant of Zeus has just finished a build and is going to spray the internet with copies of it. Why should you wait until someone submits it to an online virus scanner when you can have the bad guy email it directly to you!

This workshop will walk you through three basic tools that will allow you to turn your deluge of spam first into usable data, then convert it into usable threat intel. The first tool is ElasticSearch. You will learn how to convert all your spam's component parts into a JSON document and ingest it using ElasticSearch. It can then be visualized to make pretty graphs. From there, you have two basic vectors of maliciousness: URLs and Attachments. You will then learn how to use the tool Thug, a low interaction honey client, to analyze the URLs. In the other department, attachments, you will learn how to use Cuckoo Sandbox to analyze the email attachments along with any payload binaries captured by Thug. Fortunately both of these tools produces JSON output, and you will learn how to feed that back into ElasticSearch for final analysis and visualization. You will learn a small bit of Python code (nothing to be afraid of) that will do some basic data transformation and data movement from tool to tool.

This is not a workshop about how to build or muck around with putting the system together. All the components that we will use come pre-configured so we can dive right into understanding the tools' output and comprehending how to extract actionable intelligence from these tools.

EXCUSE ME, YOUR RFID IS SHOWING

Valerie Thomas
Securicon

Terry Gold
iDanalyst LLC

Las Vegas Ballroom 3
Friday, 14:00 to 18:00
Max class size: 30

In the hacking world, physical access is king. Many organizations rely on RFID technology to control physical access to a variety of assets, critical infrastructure and core operations but few understand its proprietary architecture and real-world implementation. This workshop covers how physical access control systems work from the ground up including architecture, common policy, and components. We'll deep dive into the world of RFID starting with raw data analysis via oscilloscope and move on to access card technology data structures and formats. Then we'll put it all together to form attacks on various card technologies that can be utilized in red team operations in a variety of environments.

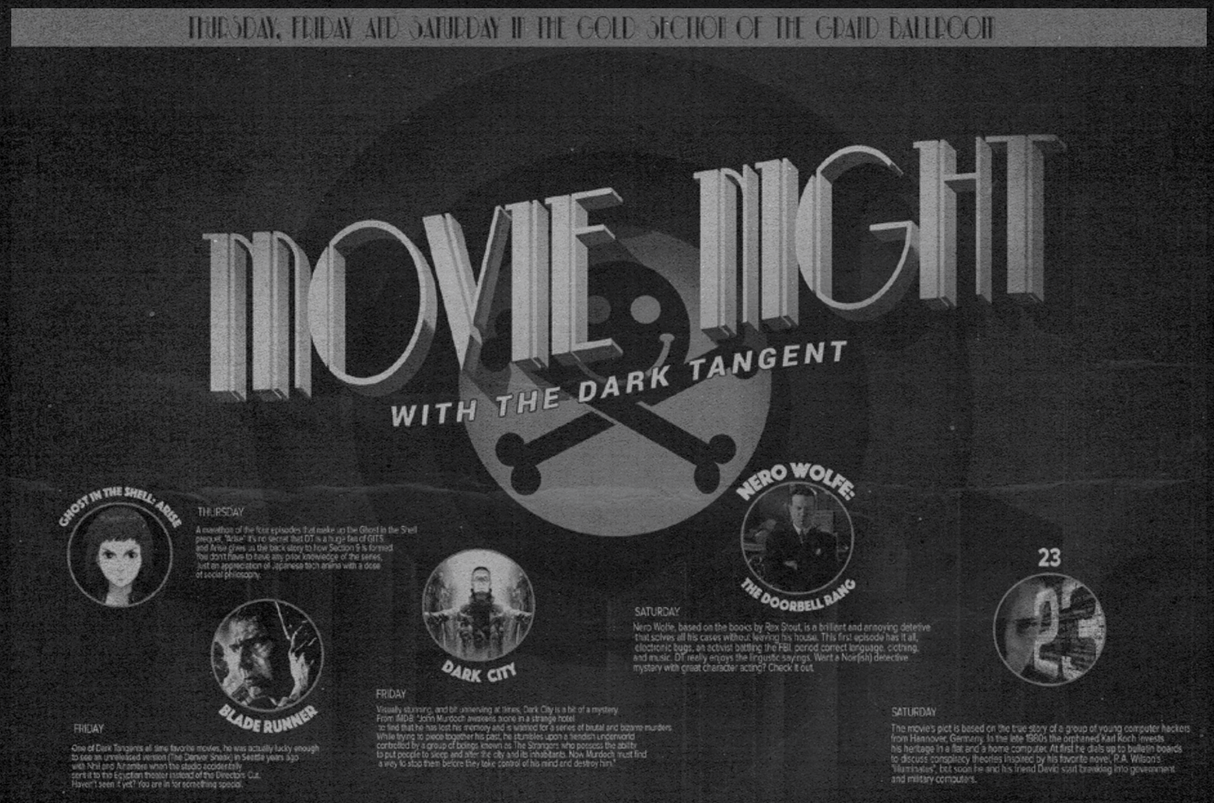
For students who wish to participate in the hands-on portion of the workshop, a laptop with Windows 7 or 8 (native or virtual machine) is required. Tweet questions to @hacktress09 and @TerryGold2048 with #YourRFIDIsShowing.

FROM 0 TO PWND - THE ULTIMATE SOCIAL ENGINEERING PRIMER

Valerie Thomas
Securicon

Las Vegas Ballroom 3
Saturday, 09:00 - 13:00 (Break) 14:00 to 18:00
Max class size: 50

Are you a pen tester in need of social engineering training? Perhaps you just want an understanding of what social engineering is all about. This workshop has something for everyone. First we'll begin with the basics of social engineering and why it works, then dive into non-traditional topics such as spycraft, acting, pressure sales, and the psychology behind them. Next we'll build upon that knowledge to create social engineering attacks. We'll cover the steps of the social engineering process from planning to post-attack including real-world examples. We'll end the day with the basics of appearance hacking and utilizing social engineering in physical penetration testing.



Villages

IT TAKES A VILLAGE TO RAISE A HACKER.

BIOHACKING VILLAGE

It's time for hackers and non-silicon squishy organic matter to make amends. DEF CON is excited to announce this year's soft launch of the Biohacking Village (BHV) an area of the con for years to come that will facilitate the tinkering of biology, whether it's augmenting ourselves or synthesizing new forms of life. Come drop by the BHV tables in the contests area to learn more (and get involved!) and head to the village talks area to catch some BHV talks! More info can be found at http://dcbhv.org

CAR HACKING VILLAGE

New to DEF CON 23, the Car Hacking Village sets out to explore the hardware and techniques of modern vehicle hacking. Sup by to learn how to hack vehicle electronic systems. At the Car Hacking Village you will be introduced to car interface hardware, car disassembly hardware, hacking methods in a large open environment. So whether you've hacked for years or are just interested in the study if car hacking, stop by and hack with us.

CRYPTO & PRIVACY VILLAGE

The Crypto & Privacy Village explores the relationship between cryptography, the mathematical study of secret-keeping, with privacy, the human need to keep certain types of information secret.

We provide a space to learn how to secure your own systems, while also picking up some tips and tricks on how to break classical and modern encryption.

Come listen to talks, learn about encryption, privacy enhancing tools, solve puzzles, read a book, or just hang out. To find out more about our scheduled events at DEF CON 23, check out https://cryptovillage.org/ !

Hardware Hacking Village

The HHV has been around since DC16 when Lost and Russ conceived of the idea of bringing hardware to the masses and the HHV has continued to evolve. Besides hosting community soldering stations for badge and kit work we offer talks relating to hardware, mini breakout sessions on a variety of topics and are always there to guide you in finding people that have like interests. Remember you will get the most out of the HHV by talking to people working on projects and sharing ideas.

Friday, Saturday 1000 - 2000 Sunday 1000 - 1300

ICS VILLAGE

RING RING RING

You spill your mug as the phone jolts you awake. "Its going to be one of those days…" Glancing at your drink soaking into the carpet, you decide you're not in the mood to deal with it now.

RING RING RING

"What is it, Penelope? I thought I left instructions not to be disturbed."

"Sorry to interrupt, Detective VanNorman, but there's a real creepy guy on the line for ya. He wants you to do somethin' for him. And no, I didn't ask what. Just take the call, boss - you know how much I hate these creeps."

Before you can object, you hear the click. She's already switched the call. "They're called customers, Penelope," you mumble, wiping your drink off your pants.

"Oh, I'm no customer, Detective VanNorman." The voice sounds like a thousand people, all talking at once in a large hall. "My apologies, I didn't mean to wake you, but I have some very pressing business to attend to and I need your help."

"Who is this? What business?"

"My name is not important, but you can call me Phaktor" intones the many-voiced man. "I need you to come down to the Nucle-sol-hydro-gas plant tonight."

"Oh? And why should I do that?"

"Because I've taken advantage of a few vulnerabilities that might interest you. Perhaps a hard-coded credential for a PLC allowed me to change a setting so that valves won't close when they should. Maybe I've been feeding a historian false data for weeks, so the cooling system isn't kicking in when it needs to. A buffer overflow here, a denial of service there, and before you know it…your plant is going to explode! Ha ha ha ha ha!"

"What? You can't do that! Nobody knows how to use those things, they're unhackable!"

"Oh, but some people do. And you had better learn fast if you're going to stop me. Find my ICS exploits by midnight tonight and your city is safe. Otherwise, its going to be a cold, dark winter for Citiesville…"

The line goes dead. "Hello?? Wait! Where am I supposed to learn how to hack and protect an ICS system?" You slam the phone on your desk in frustration, wiping half the paperwork of your desk. Something on the floor catches your eye. Its your DEF CON badge from last year. You vaguely remember there being an ICS Village last year, though it was hard to find because there wasn't a sign. You remember there were robots and switches attached to PLCs ripe for the hacking, and a whole wall of equipment that you didn't understand that blinked and lit up the room like Christmas. Presentations went all day, and people who actually knew what an HMI was helped others to fulfill their fantasies of scanning and hacking a control system without getting thrown in the clink. You heard the ICS Village was back again this year, and better than ever.

You don't have any time to lose. You grab your black "There's no place like 127.0.0.1" t-shirt, the fedora perched on top of the coat rack, throw on your trench coat, and run out the door.

…Hours later, you find yourself entering the dark hall of the Citiesville Nucle-sol-hydro-gas plant. A fluorescent light dances on your fedora as it flickers. You hear Phaktor's last words echoing in your ears, "Find my ICS exploits by midnight tonight and your city is safe. Otherwise, its going to be a cold, dark winter for Citiesville…"

"Bring it on, Phaktor. Bring it on."

IOT VILLAGE

Organized by security consulting and research firm Independent Security Evaluators (ISE), the IoT Village delivers thought leadership advocating for security advancements in Internet of Things (IoT) devices. The village will consist of the following events: a 0-day vulnerability identification contest; an in person objective-based contest, similar to a CTF; a surprise contest that will take place at a random time throughout the conference; a bring your own device demonstration; workshops, tutorials, demos, q&a, panels, games, or anything else that is awesome and related to the Internet of Things.

LOCKPICK VILLAGE

Want to tinker with locks and tools the likes of which you've only seen in movies featuring police, spies, and secret agents? Then come on by the Lockpick Village, run by The Open Organization Of Lockpickers, where you will have the opportunity to learn hands-on how the fundamental hardware of physical security operates and how it can be compromised.

The Lockpick Village is a physical security demonstration and participation area. Visitors can learn about the vulnerabilities of various locking devices, techniques used to exploit these vulnerabilities, and practice on locks of various levels of difficultly to try it themselves.

Experts will be on hand to demonstrate and plenty of trial locks, pick tools, and other devices will be available for you to handle. By exploring the faults and flaws in many popular lock designs, you can not only learn about the fun hobby of sport-picking, but also gain a much stronger knowledge about the best methods and practices for protecting your own property.

Friday, Saturday 1000 - 2000 Sunday 1000 - 1300

SOCIAL ENGINEERING VILLAGE

The Social Engineer Village (or SEVillage) is the place to come and discuss, learn and debate all things social engineering. This year the SEVillage will contain the SECTF, the SECTF4Kids and the new DEF CON Social Engineering Track. Don't forget to join us for the live SEPodcast Sunday AM for a fun and lively discussion on social engineering.

For more details on the schedule visit: http://www.social-engineer.org/social-engineer-village/

Time: Friday 0900 to Sunday 1300

TAMPER EVIDENT VILLAGE

"Tamper-evident" refers to a physical security technology that provides evidence of tampering (access, damage, repair, or replacement) to determine authenticity or integrity of a container or object(s). In practical terms, this can be a piece of tape that closes an envelope, a plastic detainer that secures a hasp, or an ink used to identify a legitimate document. Tamper-evident technologies are often confused with "tamper resistant" or "tamper proof" technologies which attempt to prevent tampering in the first place. Referred to individually as "seals," many tamper technologies are easy to destroy, but a destroyed (or missing) seal would provide evidence of tampering! The goal of the Tamper-Evident Village is to teach attendees how these technologies work and how many can be tampered with without leaving evidence.

Friday, Saturday 1000 - 2000 Sunday 1000 - 1200

WIRELESS VILLAGE

The Wireless Village is the place to go to learn about all things related to radio frequency - Wifi, RFID, SDR, Bluetooth, etc. There will be presentations from well know experts in many fields as well as tutorials and question and answer sessions. Come meet the authors of your favorite wireless related tools! If you want to learn the latest in real world penetration testing using wireless from the best and the brightest, this is the place. If you want to be on the cutting edge of wireless technology by learning how to use your new hackrf or bladerf, The Wireless Village cannot be missed. We even have training classes so you can get your amateur radio license.

Friday, Saturday 1000 - 2100 Sunday 1000 - 1300

ANNOUNCING THE DATA VILLAGE AT DEF CON 23

The Data Village is an evolution of the Data Duplication Village from last year, and it hhas grown and split into two different parts: One part is hard drive data duplication, and one part is peer to peer data sharing over high speed WiFi (802.11AC), gig wired, and P2P file sharing and leeching.

Here is how it will work:

Drive Duplication: DEF CON will provide a core set of drive duplicators as well as content. Label your drive(s) with your name, which collection number you want on it, how to contact you, and then check it in. It will be put in the queue for duplication on a first come - first served basis. 14 hours later it is done. CHECK IN STARTS ON THURSDAY in the contest area.

What to bring:

_ 6TB SATA3 new drive(s) - If you want a full copy of everything you will need three.

Here is what is available:

- 6TB drive 1-3: All past hacking convention videos that DT could find, built on last years collection
- 6TB drive 2-3: freerainbowtables.com hash tables (1-2)
- 6TB drive 3-3: GSM A5/1 hash tables plus remaining freerainbowtables.com data (2-2)

Data Sharing:

This year we are trying an alpha test of file sharing in the Data Village. The network will allow peer / host discovery so p2p programs like bittorrent and eMule will work. The down side is that without isolation your system can be scanned so take the appropriate precautions!

There will be two ways to UPLOAD (share) files:

1 - P2P Bittorrent sharing:

Build your torrent

For the files you want to share and use udp://10.0.0.2:1337 as the tracker address. Name your torrent something descriptive so people know what they are going to download.

Share your torrent

1. ftp upload your torrent(s) to 10.0.0.2 in the directory called "upload-torrents-here" This is the watch folder for the bittorrent server, and this will trigger an automatic download of your files. This way once you share your torrent with the p2p server 100% it will continue to be seeded even once you leave the network.

2 - Old school FTP uploads. ftp to 10.0.0.2 and drop your files in the "uploads" directory.

And there are two ways to DOWNLOAD files:

1 - BITTORRENT: Configure your bittorrent client to allow peer discovery to make things easier. Now find files you want to download!

1. ftp://10.0.0.2/ and browse the "upload-torrents-here" folder. this is where all the shared torrents live. Now download the torrents you want and help seed them.

2 - Old school FTP downloads. ftp to 10.0.0.2 and go crazy.

You can run your own servers and services, and don't forget to post on the white board any ip addresses to any servers you want to advertise.

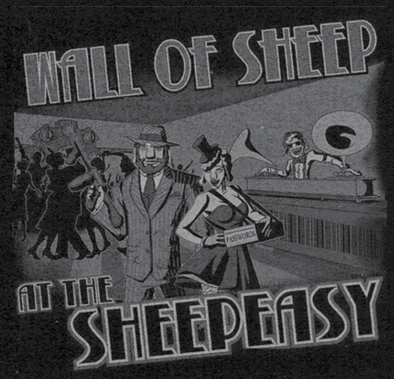
NOTES

Duplicating a 6TB (About 5.46 usable) drive at ~110 Megabytes a second comes out to about 13.8 hours. I'll know more once I to a test duplication. This means the first dupe will start early in the morning, and the second dupe late at night. We will create a schedule so you know when the deadlines to check in drive is.

Last year we had four 1:11 duplication towers going all con long. This year we are switching to a cheaper solution with only two 1:11 towers and eight 1:5 duplicators. Last year we had 44 drives maximum duplicating at a time. This year we will have 62.

Packet Hacking Village

The Packet Hacking Village welcomes all DEF CON attendees, for those that are new to DEF CON to the seasoned professionals roaming the halls; there is something for every level of security enthusiast. This village has been created to help enlighten the community through education and awareness. This is where you can find:



The Legendary "Wall of Sheep" which gives attendees a friendly reminder to practice safe computing by using strong end to end encryption. Packet Detective, an education system dedicated to helping attendees start their quest towards a black belt in Packet-Fu. Wi-Fi Sheep Hunt, an exciting wireless competition where anything wireless go's and catching sheep is the goal. Emerging Technology Showcase, an area dedicated to showing off new research, tools and techniques that are used to educate the masses on proper and safe security practices as well as discuss issues/concerns that need to be addressed by vendors. WoSDJCO, listen to some of the hottest DJ's at con spinning for your enjoyment. And... Capture The Packet, the ultimate network forensic been honored by DEF CON as a black badge event four years in a row.

PACKET DETECTIVE

Are you interested in learning the art of Network Forensics?

Do you want to understand the techniques people use to tap into a network, steal passwords and listen to conversations?

If you answered yes to any of those questions, then Packet Detective is for you!

For well over a decade the Wall of Sheep has shown people how important it is to use end to end encryption to keep sensitive information private (i.e. your password). Using a license of the world famous Capture The Packet engine from Aries Security we have created a unique way to teach hands-on skills in a controlled real-time environment. Join us in the Packet Hacking Village to start your quest in getting a black belt in Packet-Fu.

EMERGING THREAT SHOWCASE

The invariable problem with new technologies is the potential for new attack vectors. Some of these present themselves as improper validation checking, poorly designed or implemented protocols or defective products all together. This area of the village is dedicated to showing off new research, tools and techniques that are used to educate the masses on proper and safe security practices as well as discuss issues/concerns that need to be addressed by vendors. This year's focus will be on mobile threats and security.

WIFI SHEEP HUNT

Calling all you wireless and RF sniffing packet junkies, you spectrum analyzer gurus, hackers, and those that aren't so-much. The Wifi Sheep hunt is in its third year at DEF CON. This Challenge is DEF CON wide competition so break out your RF gear and start looking for transmitting signals, because if it can transmit RF, it might just be on your quest. Start by obtaining a "Wifi Sheep Hunt License" from the Game Warden at the Wifi Sheep Hunt Table. Solve the encoded riddle, using the license as a map, begin your quest. This challenge requires more than just RF interception, decoding and detection skills, you must be able to exercise your hacking and analytical skills to really put the sheep back in the barn.

CAPTURE THE PACKET "CTP"

A game where teams of two compete by monitoring the "live" CTP network traffic in the ultimate network forensics and analysis competition. If you are a Network Samurai who focuses on the defensive arts, this game is for you; there is no attacking. Compete against the best analysts, network engineers and forensic experts in the world by using your Packet FU and analytic skills to beat your opponent and prove you can "Capture The Packet". Contestants will monitor an extremely hostile enterprise class network to look for clues, solve challenges and if they score high enough they may move to the next round. Finals will be held Saturday evening where they have a chance to compete for amazing prizes. If this sounds right up your alley, you can register your team of two on-line at captureThePacket.com or at the CTP table in the Packet Hacking Village. Once you register stay tuned by following our Twitter feed, Facebook page and Web pages for dates and times your team will compete, as well as prizes that will be awarded.

WALL OF SHEEP SPEAKER WORKSHOPS

This year, we have accepted content that focuses primarily on practice and process. The intent is to provide skills that can be immediately applied during and after the conference. Our audience ranges from those who are new to security to the most seasoned practitioners in the security industry. Expect a wide variety of talks for all skill levels!

Topics may include:

- Tools on network sniffing, intrusion detection and monitoring, forensics
- Tools for data collection (e.g., Yara, Cuckoo Sandbox)
- Python & Ruby programming for security practitioners
- Hardening the enterprise using open source tools
- Getting multi-vendor tools working together
- Tool/task-automation and optimization
- Incident response process and procedures

Thursday - Saturday 0900 - 1900 Sunday 1000 - 1300

The Knights Templar had 23 Grand Masters.

Packet Hacking Village Talks

Friday, August 7

10:00

TOOLS AND TECHNIQUES USED AT THE WALL OF SHEEP

Ming Chow

Ming will demonstrate how to capture and analyze packets using the tools that are used by the shepherds at the Wall of Sheep. The tools include Wireshark, tcpdump, dsniff, and ettercap. Attendees do not need to have any networking or security experience but are expected to bring their own laptop. For the purpose of this session, a *nix environment will be used (e.g., Linux, Mac OS X).

11:00

MOBILE DATA LOSS - THREATS & COUNTERMEASURES

Michael Raggo, Director, Security Research, MobileIron

Current attack vectors indicate that malware, spyware, and other nefarious attacks are targeting mobile devices for financial gain, cyber espionage, or to simply damage company reputation. Additionally, the threat from the inside has also increased, leading to intentional and unintentional data leakage for many companies. This presentation will review best practices and strategies for controlling the dissemination of data on mobile devices by analyzing current mobile attack vectors and countermeasures.

12:00

SNIFFING SCADA

Karl Koscher

Over the past few years, interest in ICS/SCADA systems security has grown immensely. However, most of this interest has been focused on IP-connected SCADA networks, largely ignoring numerous deployments relying on other technologies such as wireless serial links. In this talk, I'll introduce a new GNU Radio module which lets you sniff (and potentially speak with) SCADA networks that use a popular RF modem for their communications. I'll also describe the process of reverse-engineering the proprietary RF protocol used. Finally, I'll talk about the higher-layer protocols used in SCADA networks, including ModBus and DNP3, demonstrate how we are able to monitor the (unencrypted and unauthenticated) sensing and control systems used by a large electricity distribution network, and discuss some of its implications.

13:00

DNSTAP - A STANDARD INTERFACE TO REAL TIME DNS TRANSACTION FLOWS

Paul Vixie

DNS is a high volume low latency datagram protocol at the heart of the Internet — it enables almost all other traffic flows. Any analysis of network traffic for security purposes will necessarily include contemporaneous DNS traffic which might have resulted from or directed that traffic. Netflow by itself can answer the question, "what happened?" but it cannot by itself answer the equally important question, "why?"

Collecting DNS query and response data has always been challenging due to the impedance mismatch between DNS as an asynchronous datagram service and available synchronous persistent storage systems. Success in DNS telemetry has historically come from the PCAP/BPF approach, where the collection agent reassembles packets seen 'on the wire' into DNS transaction records, with complete asynchrony from the DNS server itself. It is literally and always preferable to drop transactions from the telemetry path than to impact the operation a production DNS server in any way.

BPF/PCAP is not a panacea, though, since the complexity of state-keeping means that most passive DNS collectors are blind to TCP transactions, and all are blind to data elements which don't appear on the wire, such as cache purge or cache expiration events, or to "view" identifiers or current delegation point. The Farsight Security team has therefore designed a new open source and open protocol system called 'dnstap' with a transmission/reception paradigm that preserves the necessary lossiness of DNS transaction collection while avoiding the state-keeping of BPF/PCAP based systems.

This talk will cover passive DNS including collection, sharing, post-processing, database construction, and access, using the Farsight Security system as a model. 'dnstap' will be introduced in that context, including a status report and road-map.

14:00

HACKER'S PRACTICE GROUND

Lokesh Pidawekar

Learning Hacking legally and economically is not a myth anymore. You will witness how to create a practice ground to hone the skills of hacking. The talk will take you through infrastructure, tools and techniques of practicing hacking. It will also cover information about online hacking challenges and breaking into bug bounty programs. Expect lot of demos.

15:00

GLOBAL HONEYPOT TRENDS

Elliot Brink

Many of my computer systems are constantly compromised, attacked, hacked, 24/7. How do I know this? I've been allowing it. This presentation will cover over one year of research running several vulnerable systems (or honeypots) in multiple countries including the USA, mainland China, Russia and others. We'll be taking a look at: a brief introduction to honeypots, common attacker trends (both sophisticated and script kiddie), brief malware analysis and the statistical analysis of attackers based on GeoIP. Are there differences in attacks based on where a computer system is located? Let's investigate this together! Beginners to the topic of honeypots fear not, the basics will be covered.

16:00

REMAINING COVERT IN AN OVERT WORLD

Mike Raggo, Chet Hosmer

With the explosion of social media, sharing apps, and an overall world of overtness, some of us are seeking ways to communicate covertly and protect our privacy. This has prompted the emergence of new and enhanced covert communications. This includes methods for hiding data within apps, communication protocols, and even enhanced techniques for hiding data within data. In this talk we'll explore the most recent techniques for secret communications and hiding data, while also exploring new ideas for covert storage in wearables, mobile devices, and more with walkthroughs and demos.

17:00

Violating Web Services

Ron Taylor

The majority of today's mobile applications utilize some type of web services interface (primarily SOAP and REST) for connecting to back end servers and databases. Properly securing these services is often overlooked and makes them vulnerable to attacks that might not be possible via the traditional web application interface. This talk will focus on methods of testing the security of these services while utilizing commercial and open source tools. We will also highlight some web services of well-known sites that have been recently violated.

PACKET VILLAGE TALKS (CONT.)

Saturday, August 8

10:00

HOW MACHINE LEARNING FINDS MALWARE NEEDLES IN AN APPSTORE HAYSTACK

Theodora Titonis

Machine learning techniques are becoming more sophisticated. Can these techniques be more affective at assessing mobile apps for malicious or risky behaviors than traditional means? This session will include a live demo showing data analysis techniques and the results machine learning delivers in terms of classifying mobile applications with malicious or risky behavior. The presentation will also explain the difference between supervised and unsupervised algorithms used for machine learning as well as explain how you can use unsupervised machine learning to detect malicious or risky apps.

What you will learn:

Understand the difference between advanced machine learning techniques vs. traditional means.

Recognize different types of algorithms used to improve mobile security.

Understand how you can use unsupervised machine learning to detect malicious or risky apps.

11:00

MITM 101: EASY TRAFFIC INTERCEPTION TECHNIQUES USING SCAPY

Bob Simpson

Performing man-in-the-middle attacks takes a little planning and practice, but you will soon find that it is one of the most powerful and useful skills you can develop. Once you get the hang of it, Scapy makes it easy to target a specific box or a whole network, and whether you have physical access or remote penetration, you can use MITM to open up new possibilities.

12:00

I SEE YOU

Brian Wohlwinder, Andrew Beard

In this talk, we will dive into the data captured during last years Wall of Sheep applications and protocols that are giving your away credentials. This is something that anyone, with the right level of knowledge and inclination, could certainly do with a few basic ingredients. We will enumerate them. The dataset we will focus on was gathered as part of the Wall of Sheep contest during DEF CON 22. While this data was gathered using an off the shelf technology, that platform will not be the topic we discuss. Rather, we will focus on the types and scope of data sent totally in the clear for all to see. Additionally, we will discuss the ramifications this might have in a less "friendly" environment — where loss of one's anonymity, might really, really suck. Finally, we will discuss and recommend ways you can hamper this type of collection.

13:00

POWERSHELL FOR PENETRATON TESTERS

Nikhil Mittal

PowerShell has changed the way Windows networks are attacked. It is Microsoft's shell and scripting language available by default in all modern Windows computers. It can interact with .NET, WMI, COM, Windows API, Registry and other computers on a Windows network. This makes it imperative for Penetration Testers and Red Teamers to learn PowerShell. This talk looks at various attacks and tasks performed by penetration testers and red teamers during different phases of an assessment and utilize PowerShell to make them easy and much more powerful. Various techniques like in-memory shellcode execution from a Word macro, dumping system secrets in plain, using innovative communication channels, lateral movement, network relays, using Metasploit payloads without detection etc. would be discussed.

14:00

THE PACKETS MADE ME DO IT: GETTING STARTED WITH DISTRIBUTED FULL PACKET CAPTURE USING OPENFPC

Leon Ward

Network security analysts love to see packets, however most commercial security products don't record them, instead they provide packet-less event messages that can leave you asking yourself "Did that event really happen?" This talk investigates this situation and covers the history that lead the speaker to start an Open Source project that has helped him to enrich security detection events with packets as required.

OpenFPC is a packet capture framework that is designed to help retro-fit full packet data into external existing packet-less event generating tools (think Intrusion detection, firewalls, SIEMs, or log managers). Learn how to rapidly deploy a distributed full packet capture system using only a few commands, and then enrich other tools with it to augment your current event analysis process.

15:00

IS YOUR ANDROID APP SECURE?

Sam Bowne

It's easy to audit Android app security, and very important, because most of them have one or more of the OWASP Mobile Top Ten Risks. I tested the top ten US bank apps, stock trading apps, and insurance apps, and 70% of them were insecure. I'll demonstrate how to find SSL validation failures and how to add Trojans to vulnerable apps to create a Proof-of-Concept. Complete instructions for all these tests are available free at samsclass.info.

16:00

SUP3R S3CR3T!

??

17:00

CREATING REAL THREAT INTELLIGENCE WITH EVERNOTE

grecs

In the presentation that threat intel vendors do not want you to see, threat data from open source and home grown resources meets Evernote as the ultimate braindump repository with the outcome of producing real actionable threat intelligence that your organization can leverage to stop the bad guys. This presentation discusses an experiment of using Evernote as a informal threat intelligence management platform, the specific concepts and strategies used, and its overall effectiveness. Specific topics covered include the advantages of using an open and flexible platform that can be molded into an open/closed source threat data repository, an information sharing platform, and an incident management system. Although using Evernote in this way in large enterprises is probably not possible, organizations can apply the same reference implementation to build similarly effective systems using open source or commercial solutions.

18:00

HACKING THE NEXT GENERATION

David Schwartzberg

Kids are wired to learn. They are learning while they are playing, so why not give them an environment where they can play while they are learning. A combination of a speaking track, workshops, and an open area of stations complementing each other enables the attendees to expand and enlighten their technical interests. For innovation to perpetuate, it's imperative that today's young users are exposed to the bigger picture of how we got here and to help realize their potential. You can come learn more about how Hak4Kidz is making a difference and how you can potentially organize a Hak4Kidz in your local city.

Sunday, August 9

11:00

802.11 MONITORING WITH PCAP2XML/SQLITE

Vivek Ramachandran

802.11 monitoring, attack detection and forensics has always been hard. It's almost immpossible to get any meaningful inference if one relies only on Wireshark filters. This is why we created Pcap2XML/SQLite, a tool to convert 802.11 trace files into equivalent XML and SQLite formats. Every single packet header field is mapped to a corresponding SQLite column. This allows us to create arbitrary queries on the packet trace file and we will show how this can be used for attack detection and forensics with live examples.

12:00

THE DIGITAL COCKROACH BAIT STATION: HOW TO BUILD SPAM HONEYPOTS

Robert Simmons

Spam honeypots are an excellent way to gather malware binaries as well as malicious URLs that attackers use to infect their targets. Many malware campaigns are shotgun blasts of emails sent to very large numbers of email addresses. If you can get your bait address on their list, they essentially send you a copy of the malware or the URL that leads to it. This talk will cover how to setup a spam honeypot for gathering these types of threats. It will also cover how to efficiently sort through the data coming in, what data points are valuable to include in your analysis, and finally how and where to share the threat data that you are gathering. The goal is to give one the tools they need to protect themselves from emerging threats as they appear in the wild.

13:00

FISHING TO PHISHING: IT'S ALL ABOUT SLIMY CREATURES

Wayne Crowder

Fishing at a professional level shares a lot of traits with security professionals. Deep analysis of the environment, weather, and water conditions. A passion and certain stubbornness are what successful professional fisherman have. A security analyst requires similar skills and motivations to achieve their objectives. Not surprisingly, if you can market yourself well, you don't have to be the best at either industry to make money. This talk will poke fun at both of the industries work in and love. The technology available now for those how like to chase slimy creatures is nothing short of amazing. The sonar and mapping market has made the learning curve on most lakes very short for those who can afford the devices. The growth of this industry has left these units open for an interesting security review.

We will take a fun journey researching a powerful, yet poorly implemented network device found on a lot of fishing boats. Abuse of the lack of controls can lead to a bad day on the water. Imagine a fishing pole that could also double as an omnidirectional Wi-Fi antennae showing the poached signals and "hot spots" of other anglers. The talk will be fun, a little tongue-in-cheek, but more importantly should show the risks of enabling Wi-Fi for just about every device with a display. The underlying hardware and software of the units will be discussed. If the fish aren't biting, the "custom" build loaded on a device can pass the time as if you were home. The talk will conclude with thoughts about a few other examples where screen sharing over Wi-Fi could lead to problems. I will challenge attendees to think differently about the Internet of Things and how hacking and security research is crucial to make things safer, smarter and better. Or, just come to watch fishing porn.

14:00

FROM XSS TO ROOT ON YOUR NAS

Tony Martin

Home Network Attached Storage devices (NAS) are gaining in popularity because of the simplicity they offer to manage ever-growing amounts of personal data. The device's functionality is extending beyond a data store, adding functionality to become the central content management system, multimedia center, network management point and even automation hub for the home and small business. The devices offer accessibility to local and remote users as well as to untrusted users via data shares. These capabilities expose all stored data and the device itself to outside/remote attackers. This talk will demonstrate NEON TOOL; by leveraging multiple vulnerabilities, it allows a remote attacker to gain root access on a popular home NAS device. The talk will cover the problems that XSS, in conjunction with other weaknesses, can create. It will address how these vulnerabilities were uncovered, possible mitigations, how to work responsibly with the vendor to ensure a timely resolution and an investigation into the fixes employed.

Kurt Cobain was born in 1967 and died in 1994.

1 + 9 + 6 + 7 = 23.

1 + 9 + 9 + 4 = 23.

Nobel prize winner John Forbes Nash, subject of the film "A Beautiful Mind", was obsessed with the number 23. Nash published 23 scientific articles, and claimed to be Pope John XXIII.

SOCIAL ENGINEERING VILLAGE TALKS

Friday, August 7

16:00

YELLOW MEANS PROCEED WITH CAUTION - APPLIED DE-ESCALATION FOR SOCIAL ENGINEERING

Noah Beddome

Directing the nature and dynamic of social interactions is at the heart of social engineering. One of the most impactful forms of this is being able to make a functional interaction out of a hostile or uncomfortable one. During this talk we will look at the different levels of intensity within interactions and ways to manage them.

BIO: Noah Beddome is Former Marine and a present security consultant. His professional focus is on attack simulation with special emphasis on physical and interpersonal social engineering.

17:00

"I DIDN'T THINK IT WAS LOADED" AND OTHER MENTAL DERPS

Michele Fincher

How many of you have ever yelled "Hey, watch this!" and lived to tell the tale? This year's exciting glimpse into psychology and its application to security is around the fun topic of decision-making. Psychologists estimate that we make thousands of decisions a day. THOUSANDS. Now, many of these are trivial, but at least some of them have the potential to impact the security of your organization. We all think we're great decision makers, and we're all wrong at some point in our lives. Join me to get a better understanding of how and why we make our choices, and what you can do to improve your skills and guide your users to a happier (and safer) place!

18:00

UNDERSTANDING SOCIAL ENGINEERING ATTACKS WITH NATURAL LANGUAGE PROCESSING

Ian Harris

Social engineering attacks are a growing problem and there is very little defense against them since they target the human directly, circumventing many computer-based defenses. There are approaches to scan emails and websites for phishing attacks, but sophisticated attacks involve conversation dialogs which may be carried out in-person or over the phone lines. Dialog-based social engineering attacks can employ subtle psychological techniques which cannot be detected without an understanding of the meaning of each sentence.

We present a tool which uses Natural Language Processing (NLP) techniques to gain an understanding of the intent of the text spoken by the attacker. Each sentence is parsed according to the rules of English grammar, and the resulting parse tree is examined for patterns which indicate malicious intent. Our tool uses an open-source parser, the Stanford Parser, to perform parsing and identify patterns in the resulting parse tree. We have evaluated our approach on three actual social engineering attack dialogs and we will present those results. We are also releasing the tool so you can download it and try it for yourself.

19:00

I AM NOT WHAT I AM: SHAKESPEARE AND SOCIAL ENGINEERING

John Ridpath

Teeming with experts in manipulation – from Machiavellian villains like Iago and Richard III, to more playful tricksters like Puck and Viola – William Shakespeare's plays offer a surprising and fresh perspective on the art of social engineering. Via a deep analysis of the language and actions of these characters, we will explore Shakespeare's skill in pretexting, spearphishing and baiting. With his mastery of the English language and appreciation of human psychology, there's still a lot to learn from Shakespeare.

20:00

CLASSIFY TARGETS TO MAKE SOCIAL ENGINEERING EASIER TO ACHIEVE

Heng Guan

There are so many factors (culture, age, gender, level of vigilance, when to choose…) will affect the realization of each Social Engineering action. Since information gathering is needed, why not classify the targets first to increase the success rate? When people get trained, how to accomplish social engineering once more? This is a discussion about how to bypass the human WAF according to different characteristics, as a complement to existing research.

Saturday, August 8

16:00

BREAKING IN BAD! (I'M THE ONE WHO DOESN'T KNOCK)

Jayson Street

I start off the talk describing each one of the below listed attack vectors I use. I tell a story from each of them I show video of me breaking into a bank in Beirut Lebanon. I show video of gaining access to USA State Treasury office. The most important part of my talk is not that at all. I spend the entire last half of the talk creating a security awareness talk! Where I go into ways to spot me (or any attacker) I show the different tools and devices users should be aware of. I show how users should approach a situation if someone like me is in the building or interacting with them online. I basically use this talk to entertain the security people in the audience enough that they will take this back to their work and share my PowerPoint and video of my talk with their executives and co-workers.

17:00

TWITTER, ISIL, AND TECH

Tim Newberry

There is a concerted effort by researchers to understand how the Islamic State of Iraq and Levant (ISIL) is capable of influencing and radicalizing socially vulnerable audiences around the world via digital means. These efforts are demonstrated in a limited body of research that are often times rooted in conventional processes, therefore, having limited direct application to today's dynamic, open-source digital environment. This environment affords a challenging, yet unique, opportunity to employ open source machine learning techniques guided by social learning and routine activities theory from the criminological field of study. This presentation will discuss a human driven, but machine assisted framework for identifying ISIL methods and victims in order to facilitate an effective counter-narrative for engaging the victims prior to influence happening. The framework utilizes historically based research designs to develop the frameworks, but machine learning to train classification algorithms utilizing data pulled from the Twitter API for modern application. The Scikit-Learn set of tools for Python were used to rapidly prototype tools for data mining and data analysis.

18:00

A PEEK BEHIND THE BLUE MASK: THE EVOLUTION OF THE SECTF

Chris Hadnagy

Join HumanHacker in an in-depth exploration of the mysterious world of the SECTF. From a small competition demonstrating a live compromise of fortune 500 companies to a full-scale village, how has the Social Engineering CTF evolved? What are the greatest takeaways from hosting 6 years of CTF competitions? It's not often you get to hear what goes on behind the scenes. This informative talk will help social engineers, pentesters and future SECTF contestants alike understand how the Social Engineering CTF works. How are results calculated? What attack vectors have the highest success rate? What's in a theme? What implications does the contest have for the world of SE and the state of corporate security? He'll discuss expectations from the highest caliber social engineers and how he's seen social engineering attacks evolve throughout the years. Part education, part documentary, this presentation is an ode to all things SE from the man who started it all.

19:00

UNDERSTANDING END-USER ATTACKS – REAL WORLD EXAMPLES

Dave Kennedy

From our own analysis, phishing attacks for the first time are the number one attack vector superseding direct compromises of perimeter devices. Endpoints are now subjective to a number of different types of attacks and it's all around targeting the user. This talk will walk through a number of targeted attacks that elicit social engineering aspects in order to gain a higher percentage of success against the victims. Additionally, we'll be covering newer techniques used by attackers to further their efforts to move laterally in environments. Social engineering is here to stay and the largest risk we face as an industry – this talk will focus on how we can get better.

20:00

PHISHING: RECON TO CREDS WITH THE SPEEDPHISHING FRAMEWORK

Adam Compton & Eric Gershman

This presentation will quickly explore some of the common phishing attack tools and techniques. Additionally, there will be a demo of a new tool, which can assist penetration testers in quickly deploying phishing exercises in minimal time. The tool can automatically search for potential targets, deploy multiple phishing websites, craft/send phishing emails, record the results, generate a basic report, among other bells and whistles.

2015 Capture the Flag

DEF CON CAPTURE THE FLAG

Legitimate Business Syndicate returns for their 3rd year to host Capture The Flag at DEF CON 23. Their first year they changed things up with a game running all on ARM processors. Last year had a surprise twist with one of the challenges running on a custom designed electronic badge with processor core embedded in an FPGA! This year who knows? Come check out the CTF room in the Bally's Event Center to find out.

WHAT IS CAPTURE THE FLAG?

DEF CON Capture The Flag is a competitive, attack-defense hacking competition.

Each team starts with an identical set of network services. Teams use their understanding of these services to attack opponents, while simultaneously defending their own network from other teams. Services may range from a simple mail server to complex virtual machines running invented bytecode.

The scoring system deposits flags in these services and checks for presence of flags on a regular basis. Stealing flags constitutes the offensive aspect of the game. Protecting flags from exfiltration while keeping them available for uptime checks is the defensive aspect.

COMPETITORS

Teams must be invited to compete in this CTF competition. Invitations are extended to the winning team of the previous years DEF CON CTF and the winners of several highly respected CTF competitions throughout the year. The remaining slots were filled with the highest scoring teams from our own qualification event held in May.

This years participating teams are:

Plaid Parliament of Pwning (defending champions), Bushwhackers, Samurai, HITCON, DEFKOR, 9447, Gallopsled, blue-lotus, !SpamAndHex, CORNDUMP, 0ops, 0daysober, Dragon Sector, Shellphish, and LC□BC.

THE CTF ROOM

The CTF room will be open for everyone to drop by, watch videos, gawk at teams, and enjoy a DJ set or two throughout the contest. Enjoy yourself, but please be respectful and do not interrupt hackers at work. Above all, don't be a jerk. If you have questions about the contest, talk to a member of Legitimate Business Syndicate. Competitors may also be willing to talk when they are not engrossed in the game.

THANK YOU

We would like to thank CTF competitors around the world for this wonderful opportunity. We would not be able to run this competition without your skills and persistence to inspire us and make it all worthwhile.

Game announcements will be posted to https://twitter.com/legitbs_ctf. We also keep a scoreboard on the wall in the competition room. Final results will be announced during DEF CON closing ceremonies.

Thanks,

Legitimate Business Syndicate

https://legitbs.net

Classifieds

CONTESTS PIT HACKER AGAINST HACKER.

BEARD AND MOUSTACHE COMPETITION

Held every year since DEF CON 19 in 2011, the DEF CON Beard and Moustache Contest highlights the intersection of facial hair and hacker culture.

There are four categories for the competition:

Full beard: Self-explanatory, for the truly bearded.

Partial Beard: For those sporting Van Dykes, Goatees, Mutton Chops, and other partial beard styles

Moustache only: Judging on the moustache only, even if bearded. Bring your Handlebars, Fu Manchus, or whatever adorns your upper lip.

Freestyle: Anything goes, including fake and creatively adorned beards. Creative women often do well in the Freestyle category.

Twitter: @ DCBeardContest
https://twitter.com/DCBeardContest

Web page: http://www.dcbeard.com/

BEVERAGE COOLING CONTRAPTION CONTEST

Do you like warm beer? Is the weather horrible and the conference called BIKINI? Of course not, this is DEF CON! We like our beer test fluid to be ICE COLD. Unfortunately the British appear to have invaded the cooler and the test fluid is ungodly warm. We need you to help us cool it. Exercise your right to bear mad science with fun prizes and fame to the one who can chill our test fluid to the target temperature in the shortest time. You can bring a device or hack one together during the contest. As an added bonus you can help us dispose of the free test fluid. So join us for what is sure to be a blast!

BLACK BAG

In DEF CONs of yesteryear, attendees witnessed Gringo Warrior...a scenario-based escape game. From the same people who brought you that lockpicking and physical security contest, we now have Black Bag! Instead of merely focusing on your ability to pick locks as you seek an exit, this contest is framed around getting IN and getting back OUT again.

Throughout day one of DEF CON (Friday) you will follow clues and gather intelligence in order to learn details of your target: a rogue covert operative who is staying on-site. The first seven teams of three players each (more than 7 teams might also be possible) to tell us where this target individual can be found will get to participate in the main round the next day.

On Saturday, teams will be tasked with covertly entering the target's room, picking locked cases and cabinets in order to gather intelligence, and then egressing with as much information as possible in under 10 minutes. Expect a variety of real-world physical pen testing tools to make an appearance, and each team will be equipped with a CORE Group / Lares Consulting Red Teamer bag. Follow us on Twitter (@COREblackbag) to stay abreast of all that is planned!

@COREblackbag

Friday 1200 - 1400, Saturday 1300 - 1700

COINDROIDS

COINDROIDS

The year is 20X5 and humanity has fallen: now there are only Coindroids. The machines we designed to manage our finances have supplanted and destroyedthe human race by turning our own economy against us. Now they battle each other in the ruins of our fallen cities, driven by a single directive: money is power.

Battle your way to the top of the leaderboard by attacking rival droids, upgrading your shiny metal ass and finding bosses hidden throughout the conference. Be sure to keep an eye out for one very rare relic!

New to cryptocurrencies? No DEFCOIN to play with? Not a problem! Just come visit our booth in the contest area and we can help get you started.

CRACK ME IF YOU CAN

For the 6th year in a row, Crack Me If You Can returns with the largest password cracking competition in the solar system. Teams across the planet will go head to head once more in the 48 hour fight against sleep and hashes to be crowned the 2015 winners and gain smack talking rights. Bigger challenges, harder algos, awesome prizes... Fire up the compute clusters, stock up on energy drinks, put the nearest pizza place on speed dial, and stand the hell by for Crack Me If You Can 2015. At contest start, we will release tens of thousands of passwords hashed with a variety of algorithms, both common and uncommon. Crack as many as you can, more points for harder hashes.

"Pro" and "Street" team compete for a different set of prizes this year. So experts and beginners will have lots of fun.

CRASH & COMPILE

Do you think you can code? Do think you can code while drinking? We're not talking about coding in the warm safe confines of your cubicle. No, this is programming for sport. It's live competition, against the clock, and the other teams. We're looking for nine teams who believe they have the smarts to solve our programming challenges. Crash and Compile isn't for the weak. It's not just about laying down some sweet sweet code, it's about the style in which you do so. Sound fun? We think it is.

Crash And Compile is a ACM-style programming contest crossed with a drinking game, where teams of two people try to solve as many programming problems as they can. As teams compile and run their programs, each time their code fails to compile, produces the incorrect output or segfaults, the team must drink. Meanwhile, our lovely Team Distraction will be doing what they can to make the job of programming while intoxicated all the more difficult and/or enjoyable. Interested? Teams can sign up in the Contest Area on Friday.

DEF CON BOTS

DEFCON BOTS
BUILD/CODE/SHOOT

Contestants will build autonomous robots capable of shooting lasers at moving targets. The targets will move on a track in waves that are increasingly difficult. To win your robot must survive the most number of waves.

DEF CON DARKNET PROJECT

DEFCON DARKNET

The DarkNet Project: a mission to secure a safe, independent, and self-sustaining community, free from intrusion and infiltration by those who would enslave us to their own ends. Our opponents are many and they grow ever more capable — spying on us through our information streams and trying to control us through messages displayed to us wherever we go.

We will resist.

Join us and you will be sent on quests to improve your current technical knowledge. You will meet others like you; you will learn from each other and grow stronger together. You will discover hidden messages and uncover those attempting to deceive us. You will rise through the ranks as you go, and you will get your chance to take on the man running the show by using all of the knowledge that you have acquired.

You know that you have what it takes to join us.

What are you waiting for?

HACKER JEOPARDY

DEF CON's oldest and most popular contest is back for its very adult 21st birthday. Hop aboard the fastest train to Blitzville, filled with beer, babes, hunks, drunks, hilarity, humiliation, tough answers to questions, and more beer.

We're making history, people. You gotta be there!

HACKER JEOPARDY TRIALS

Do you have what it takes to be a Hacker Jeopardy contestant? Grab two of your buddies and haul ass down to the contest stage to experience a lightening round trial (no daily doubles, or beer) to validate your skills as a potential team BEFORE we let you on the big stage.

HACKFORTRESS

Hackfortress by the numbers: It's 30 minutes of non-stop, no holds barred, hacking and Team Fortress 2 action. In those 30 minutes, 6 TF2players and 4 Hackers will square off against another team of TF2 players and hackers. Your goal: to score as many points as possible. How do you score points? By solving hack puzzles of all shapes and sizes. Those range from the ridiculous to the obscenely technical. You can also score points in TF2 by doing what you normally do in that game: Dominate, kill, capture, take revenge. That's not where the fun ends though. Want to block your opponents from submitting a challenge? Want to set them on fire? Of course you do. Who wouldn't? As you accomplish tasks you'll earn coins that can be spent in our "hackconomy". Once the thirty minutes is up, the team with the most points wins.

Friday, Saturday 1000 - 1700 Sunday 1000 - 1300

NETWORK FORENSICS PUZZLE CONTEST

Introduction: DEF CON 23 has finally arrived! As the largest hacking conference takes over Las Vegas, even more attendees have flocked in to experience all that DEF CON has to offer. Amongst this years diversely skilled, and potentially crazed attendees, one individual in particular is attracting attention and sparking rumors that we cannot seem to ignore. A deranged man has been spotted wandering throughout DEF CON preaching about aliens and attempting to recruit guests to assist him with some sort of extra terrestrial mission. Unfortunately no one has been able to identify the man, however it has been confirmed that he is convinced he has established communication with an alien race. If such claims turn out to be true, this would completely alter the world, as we know it. Though the source of this information has yet to be confirmed, many individuals are convinced there is some truth behind his claims and seek assistance in further investigating these allegations. As a skilled attendee of this convention we require your assistance in uncovering the facts behind these rumors and ultimately advancing the worlds knowledge of the alien race. Can you perform this ET investigation?

OPENCTF

A little over thirty years ago, an important decision was made by the Supreme Court of the United States. Sony's Betamax Video Tape Recorder, and the time-shifting it enabled, were ruled legal, creating the precedent necessary for countless technological innovations we now use every day. But what if, as it very nearly did, that decision had gone the other way? V& invites you to find out at OpenCTF: DRMageddon.

In OpenCTF, teams compete to solve hacking challenges in a wide variety of categories, including web, forensics, programming, cryptography and reverse engineering. There will be challenges for all skill levels. If you've never played in a capture the flag contest before, please feel free to stop by anyway - we'll explain how it works and do what we can to set you up with a team.

ROBOCALLS: HUMANITY STRIKES BACK

"Rachel from cardholder services" - the annoying robo-mosquito sucking consumers' blood and mobile minutes – is back! The FTC receives more complaints about voice spam and robocalls than anything else, and complaints about telephony denial of service attacks are growing. Help protect consumers from Rachel and her minions by creating a crowd-source honeypot that will help experts and authorities shut down illegal phone spammers' operations. Winners get cash prizes plus lots of press/kudos/bragging rights. Full contest rules, judging criteria, etc. are available on the contest website.

SCAVENGER HUNT

The strangest, loudest, most chaotic and quite possibly the most infamous game at DEF CON...the Scavenger Hunt! Back once again with a list full of crazy tasks and hard to find items. It's a test of creativity, determination, brains, and above all, the hacker mentality.

SCHEMAVERSE

SCHEMAVERSE

The Schemaverse [skee-muh vurs] is a space battleground that lives inside a PostgreSQL database. Mine the hell out of resources and build up your fleet of ships, all while trying to protect your home planet. Once you're ready, head out and conquer the map from other DEF CON rivals.

This unique game gives you direct access to the database that governs the rules. Write SQL queries directly by connecting with any supported PostgreSQL client or use your favourite language to write AI that plays on your behalf. This is DEF CON of course so start working on your SQL Injections - anything goes!

Winners could take home the custom made 2015 Sequel Cup, Bitcoin and other swag.

Looking to sign up or need a hand? Come visit us at our booth in the Contest Area.

SECTF

The SECTF is back for its 6th year to again see if social engineering is a threat to corporate America. This year we have a blend of men and women from the skilled to the n00bies all trying their hand in the booth. Which industry will we try this year? How many contestants do we have? What are the twists and turns we have planned out? You will have to come to find out. Join us starting Friday at 1000 to find out.

Friday 1000 to 1600 Saturday 1000 to 1600

SECTF4KIDS

Teaching kids critical thinking skills and how to solve problems with the greatest computer they own - their brains - is the goal of this exciting and fun day long challenge for any kid ages 5-12. Puzzles, ciphers, locks, elicitation, and of course the occasional nerf gun are all part of the SECTF4Kids. This year the theme is "The Amazing Race".

Saturday 0900 to 1700

SHORT STORY CONTEST

Run entirely online on the forums.defcon.org and completing-months BEFORE con begins, to participate you must have an account on the forums and follow the contest Twitter account @dcshortstory. Submission guidelines are outlined in "Da Rules" on the forums.

First place receives (2) Human badges, Second place receives (1) Human badge, and by People's Choice poll, one author receives (1)Human badge as well! All stories, regardless of placement, are included as a file on the official DEF CON swag DVD and the winners listed in the official DEF CON schedule pamphlet. Rules, stories and polls are posted on the forums. defcon.org each year!

This contest is no joke, so if you choose to try your luck at pen to paper, take it seriously, and write the best that you can write. This contest was begun by Nikita, bequeathed to Eris and we receive high quality writing, more stories every year and the competition is fierce! So pick up your quill, your stylus, your typewriter or tablet and dazzle our mind's eye!!

FIRST PLACE 2015: "The Big Denial of Service" by Tess Schrodinger

SECOND PLACE 2015: "Even Death May Die" by John McNabb

PEOPLE'S CHOICE 2015: "Weird Net Blues" by Rob Pait

TAMPER EVIDENT CONTEST

This contest evaluates defeats (which gamut from the exceptional to the mundane) primarily against a range of commonly available low to high-level security products. We'll list the exact products in mid June after we've secured everything. The judging system will remain the same with three impartial judges will evaluate each box and score it based off a -1 (No attempt made) to +3 (holy shit without the video and pics we'd never known!) with the possibility of more with a truly Uber defeat!

This contest started because Everyday, every one of us comes into contact with many tamper evident technologies. From your groceries and medications, to your postage and home electronics. All too often in the past people have assumed they were safe; that these technologies we're too difficult to defeat or required too much time before someone noticed.

For five years, the DEF CON Tamper Evident contest has been proving that assumption work. Dead wrong.

This team-focused contest includes tapes, seals, locks, tags, even evidence bags amongst other methods where we actively seek out new and exciting methods of defeat.

Friday, Saturday 0900 - 1730 Sunday 1100 - 1300 in LPV/TE Village

TCP/IP DRINKING GAME

Back by explicit demand of the maker, TCP/IP drinking game challenges your detailed knowledge of the most prevalent suite of protocols on the Internet! Contestants will be expected to sit on stage, in public forum, and take the most absurd questions about TCP/IP Suite from both the host and visiting questions from the audience. Fail to know a Flag setting? Didn't convert your hex fast enough? Prepare to drink!

Friday 1700 on Contest Stage

WARLOCK GAM3Z

warl0ck gam3z

warl0ck gam3z is a hands-on 24/7; throw-down, no-holds-barred hacker competition focusing on areas of physical security, digital forensics, hacker challenges and whatever craziness our exploit team develops.

This is an online framework so participants can access it regardless of where they are or what network they are connected to via laptop, netbook, tablet or phone.

Most challenges require participants to download something that pertains to the problem at hand and solve the challenge using whatever tools, techniques or methods they have available.

One participant will become the leader of the board and they control which challenges are available. Being the leader of the board is a double edge sword. Regular participants may choose to back out of a challenge if they cannot solve it but once the leader of the board selects a challenge; they must answer/solve it or be passed by a new leader as they are not afforded the same luxury of just backing out. And just to keep it interesting, occasionally ""The Judge"" challenge comes out and is made available to everyone except the current leader of the board.

There are a multitude of point gainers outside the confines of the board challenges. Extra point gainers will randomly appear on the game board in the form of The Judge, Bonus Questions, Free Tokens, One Time Tokens, Movie Trivia Quotes, Scavenger Hunts (online and onsite), Lock Picking (onsite) and Flash Challenges. Be careful of the 50/50 Token which may add or subtract points to your score.

The game board contains a scoring area so participants can view current standings, as well as an embedded chat function for those that may want to taunt their competitors, or work with other participants as part of a team. There is always on onsite moderator to assist participants that may be experiencing issues as well.

All events that occur on the game board are sent off to Twitter as they happen. These include items such as participants signing up, leader of the board changes, scoring updates and challenge updates. Additionally, our Facebook site will be populated with information regarding the challenge and the current state of events.

@Gam3z_Inc
https://warl0ck.gam3z.com/defcon
https://www.facebook.com/Gam3zInc
http://www.youtube.com/user/Gam3zInc

Friday, Saturday 0900 - 2100 Sunday 1000 - 1300

WIRELESS CTF

The DEF CON 23 Wireless Capture the Flag (WCTF) is a trip through the useable RF spectrum. Challenges will involve all of the physics and RF theory that we have all come to love so much. You will be using tools like the RTL-SDR, HackRF, BladeRF, your cell phone, and various 802.11 radios. Although not all are necessary to compete, they will help. The WCTF can be completed with experience ranging from a little knowledge to a pen-tester's capability, and $40 to $4000 worth of equipment.

Regardless of what you bring, the key is to read the clues and determine the goal of each step. We teach along the way, so if you are a N00b, we will help you learn strategies to get you to competition level. This year we maintain certain aspects of past WCTFs but are also introducing new challenges. For example, as in past WCTFs, you will need to sit for a while and hack at crypto and break into networks. But, unlike past WCTFs, you need to break out your war-walking shoes because you will be tracking and finding hidden nodes and possibly even remote sites — and not all of them will be WiFi.

We will also be holding the very popular, RF Signal Drinking Game. There will be clues everywhere, and we will provide periodic updates so make sure you pay attention to what's happening at the WCTF Control Center, on Twitter, the interwebz, etc. If you have a question - ASK, and we will determine if we will answer.

FLAGS:
Flags will range from transmissions in the spectrum to pass-phrases used to gain access to wireless access points. Once you capture the flag, submit it right away because some flags are worth more points the sooner they are submitted (e.g., timed challenges) and others will be awarded negative points (e.g., false flags). Offense and defense are fully in play by the participants, the WCTF organizers, and the Con itself.

DRUNK HACKER HISTORY

New this year for DEF CON 23, we bring you a contest unlike anything you've ever seen before (and may never see again). The DEF CON community has a rich history. It is a history is filled with colorful adventures, half-truths and angry hotel managers. This contest will brush the dust off some of the most celebrated, obscure and redacted moments in Hacker History through the interpretation of a group of pre-selected contestants with the help of C2H6O. Each contestant will be "prepared" for their participation by our contest staff before being brought in front of a panel of judges. A topic will be randomly selected pointing to a moment of hacker history and the contestant will have 5-7 minutes to provide their account. Points will be given for accuracy, level of "focus", and other areas just made up on the fly by the judges, and in the end the contestant with the most points will be crowned the "Drunk Hacker History" champion for 2015. Note: This is not a Black Badge contest (yet).

INTELCTF

IntelCTF is designed to immerse you into the world of threat intelligence by creating "real-world feeling" counter-intelligence scenarios. Participants are briefed on their "contract" obligations and the objectives of their mission. Intelligence points (flags) will be submitted to the scoring engine which will track team progress and provide feedback on your mission status. Your team wins by completing the mission objectives (submitting all the flags) and identifying your primary target. Do this before the other contractors (teams) and you will be recognized for your accomplishments.

Classifieds

VENDORS PEDDLE THEIR NEFARIOUS WARES

BREAKPOINT BOOKS

http://breakpointbooks.com

BreakPoint Books is your official conference bookstore on site at DEF CON. We'll have all your favorite books for sale and we're conveniently located in the Vendor Area. Make sure to stop by and view the titles in stock and purchase a few written by some of your favorite authors!

BUMP MY LOCK

http://bumpmylock.com/

Bump keys, lock picks and training tools. Bump My Lock has served

thousands of customers worldwide since 2007. If we don't have it at the booth, go to our site http://www.bumpmylock.com. Free demonstrations and training at our booth.

Bump My Lock is celebrating our 6th year at DEF CON by showcasing our own line of lock picks!! This year, we will feature our Black Diamond sets and our Ruby sets. So come see us for all your Lock Pick Sets, Bump Keys, Clear Practice Locks, Jackknife Pick Sets, Hackware, and more.

Need more help? We have a vast number of articles and videos on lock picking on our blog or your tube channel. If you are a beginner or a master locksmith we have the tools for you.

As always, a percentage of our proceeds will go to the Miracle Match Foundation.

Long live Barcode!

CAPITOL TECHNOLOGY UNIVERSITY

https://captechu.edu

Capitol Technology University, located in Laurel Maryland, offers degrees in engineering, computer science, cybersecurity, and business. Offering online certificates, bachelor's and master's degrees, which includes a master's in astronautical engineering. As well as doctoral programs in cybersecurity and management and decision sciences. Capitol is regionally accredited by Middle States Association of Colleges.

CARNEGIE MELLON UNIVERSITY

https://ini.cmu.edu

The Information Networking Institute (INI) offers full-time master's degrees in information security at Carnegie Mellon University, the home and hotbed of smart students who desire to make an impact, whether it be starting the campus grappling club or dominating in Capture the Flag. The INI offers interdisciplinary programs with curricula that span several top-ranking colleges. As a result, the graduates of the INI move on to apply their know-how at some of the most competitive places, like Silicon Valley, Wall Street, and the DoD, as well as their own startups. Full scholarships are available for U.S. citizens. Talk with Kari for details.

CHECKMARX

http://www.checkmarx.com

Checkmarx is a leading developer of software solutions used to identify, fix and block security vulnerabilities in web and mobile applications.

Concentrated on Code security and application security education, the company's customers include 4 of the world's top 10 software vendors and many Fortune 500 and government organizations, including Samsung, Salesforce.com, Coca Cola and the US Army.

Checkmarx's (CxSAST) brings Static Analysis to an unmatched level in terms of accuracy, ease of use and most importantly innovation. Adapting to the constant change of the development environment and the attack landscape Checkmarx is leading the Application Security field with the ability to Educate developers, detect vulnerabilities and mitigate application attacks in real time while supporting and integrating within Continuous Delivery environments using Agile adaptation engines specifically designed for the task. **Checkmarx offers a suite of application security solutions from code development to live production:**

CxSAST -Static Application Security Testing (SAST) Identify and fix security vulnerabilities in the source code, at the early stages of the application development. The solution enables full automation by integration into the Software Development Lifecycle (SDLC).

CxRASP - Runtime Application Self Protection (RASP) - Block attacks in real time while correlating data with CxSAST to ensure a complete cycle of detection, prevention and mitigation.

Game of Hacks - Secure Coding Education - Hands on secure coding training based on gamification, using your own code base and real life security vulnerabilities.

COBALT STRIKE

http://advancedpentest.com

Cobalt Strike is a red team toolset made to evaluate security operations and train incident response staff. Cobalt Strike focuses on flexible covert communication, post-exploitation, and long-term operations to help you credibly emulate an advanced actor in your network.

DUAL CORE

http://dualcoremusic.com

Dual Core - drink all the booze, hack all the things. The group has toured all over the US and UK, and has played shows even further from home including Europe and South America. Their latest album, 'All The Things', debuted at #1 on Bandcamp. You can stream them on Spotify, Rdio, and Pandora. Albums can be purchased from iTunes and Amazon, or pirated with bittorrent.

DUO SECURITY

http://www.duosecurity.com

Duo Security is a cloud-based access security provider protecting the world's fastest-growing companies, including Twitter, Etsy, NASA, Yelp, and Facebook. Duo's easy-to-use two-factor authentication technology can be quickly deployed to protect users, data, and applications from breaches and account takeover. Try it for free at www.duosecurity.com.

EFF

https://www.eff.org

The Electronic Frontier Foundation (EFF) is the leading nonprofit **organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy and free expression online through a strategic combination of impact litigation, policy analysis, education, and grassroots activism. We empower tinkerers, creators, coders, and consumers to reclaim freedom as our use of technology grows.**

FREEDOM OF THE PRESS FOUNDATION

https://freedom.press

Freedom of the Press Foundation (FPF) is a non-profit organization that supports and defends journalism dedicated to transparency and accountability. FPF maintains the SecureDrop project, an open-source whistleblower submission system originally created by Aaron Swartz and teaches journalists how to use secure communications tools.

GHETTO GEEKS

http://ghettogeeks.com

Well we're back at it again, and have been working hard all year to bring you the freshest awesome that we can. If you have been to DEF CON, layerone, toorcon, phreaknic, or other conferences we have been at, you definitely know what so of shenanigans we are up to. If you have never seen us, feel free to come by and take a look at what we have to offer.

Always fun, always contemporary, GhettoGeeks has some for the tech enthusiast (or if you prefer, hacker)

GUNNAR

http://www.gunnars.com

GUNNAR is the only patented computer eyewear recommended by doctors to protect and enhance your vision. In short, we help with all issues associated with digital eye strain, including: dry, irritated eyes, blurred vision, headaches, glare, effects of artificial blue light and tired eyes. The result - improved clarity, focus and performance. Prescription eyeglasses are also available.

HACKERS FOR CHARITY

http://www.hackersforcharity.org

Hackers for Charity is a non-profit organization that leverages the skills of technologists. We solve technology challenges for various non-profits and provide food, equipment, job training and computer education to the world's poorest citizens.

HACKER STICKERS

http://hackerstickers.com

HackerStickers.com offers unique t-shirts, stickers, hardware, hacks and lock picks for hackers, whitehats and nerds alike. Follow us on Facebook and Twitter (@HackerStickers) for sneak peaks on new designs and special offers.

HACKER WAREHOUSE

http://hackerwarehouse.com

HACKER WAREHOUSE is your one stop shop for hacking equipment. We **understand the importance of tools and gear which is why we strive to** carry only the highest quality gear from the best brands in the

industry. From WiFi Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Check us out at HackerWarehouse.com

HAK5

http://hak5.org

Complete your Hacking Arsenal with tools from Hak5 - makers of the infamous WiFi Pineapple, USB Rubber Ducky, and newly released LAN Turtle. The Hak5 crew, including hosts Darren Kitchen, Shannon Morse and Patrick Norton, are VENDING ALL THE THINGS and celebrating 10 year of Hak5! Come say EHLO and check out our sweet new tactical hacking gear! Everything from WiFi Hot-Spot Honey-Pots to Keystroke Injection tools, Software Defined Radios and Covert LAN Hijackers are available at the Hak5 booth.

ITUS NETWORKS

https://itusnetworks.com

ITUS Networks is a security company based in Silicon Valley that makes a small form factor network appliance to protect homes and small businesses from cyber attacks. Our powerful yet affordable network security appliances protect a wide variety of internet enabled devices from exploits, malware, and other nasty things online.

DJ MISS JACKALOPE

http://dj-jackalope.com

Miss Jackalope is the DEF CON resident DJ. Since DC7, she's been a regular whom you most likely have seen spinning at the EFF Summit, huge DEF CON parties everywhere, or maybe you have even been to BruCON in Belgium and taken a DJ workshop she has co-presented. She plays drum and bass, breaks, and techhouse. Countless networks have been conquered by Red Teams while listening to her mixes. Come by her booth and see what fun Miss Jackalope swag and mixes are up for grabs this year twitter:@djjackalope

KEYPORT

http://mykeyport.com

Keyport® is an everyday multi-tool that holds up to six keys and/or EDC tools (USB flash drive, mini-light, pen, bottle opener, and more) into a streamlined device that replaces your keychain. We have a brand new limited edition DEF CON 23 Keyport design & all products are 10% off + free key duplication onsite w/your purchase. Don't forget to bring your keys to the show!

NO STARCH PRESS

http://www.nostarch.com

Thanks to you, we've been publishing great books for hackers since 1994; each one still handcrafted like a good bottle of bourbon. We read and edit everything we publish — titles like The Smart Girl's Guide to Privacy, Black Hat Python, Teach Your Kids to Code, Automate the Boring Stuff with Python, Statistics Done Wrong, LEGO books, the Manga Guides to math and science, and more. Everything in our booth is 30% off (maybe a little more) and all print purchases include DRM-free ebooks. We've got new swag and samples of some forthcoming titles, too.

NUAND

http://nuand.com/

Nuand provides low-cost, USB 3.0 SDRs (Software Defined Radio) for enthusiasts, and experts a like. After a successful Kickstarter, bladeRF is now available and ready for use in your projects! Stop by our table to see our demos and find out more about bladeRF, GNURadio, OpenBTS and Software Defined Radios!

PAYATU TECHNOLOGIES

http://www.payatu.com

Payatu Technologies is a boutique security testing company specialized in Mobile, cloud, IoT, application and product security testing. We are also the organizers of nullcon International Security Conference and newly launched hardware security conference - hardwear.io to answer the growing need for hardware security research.

hardwear.io was conceptualised to provide the IT and security community with a platform to discuss and solve issues pertaining to hardware security. The objective of the conference revolves around four key concerns in hardware, firmware and related protocols i.e. backdoors, exploits, trust and attacks (BETA). It is Scheduled on 1-2 Oct 2015, in The Hague, Netherlands.

PENTESTER ACADEMY

http://pentesteracademy.com/

Pentester Academy is trusted by hackers and pentesters from over 90+ countries for their online infosec training needs. Our course authors are top researchers, book authors, conference speakers and most importantly real world practitioners which keeps our courses current and highly technical.

Our online database of courses spans over 120+ hours of rich video content, live demos and labs in topics like Web, Network, Wi-Fi and Mobile Pentesting, Assembly Language and Shellcoding (x86/x86_64), Python, Powershell and JavaScript scripting to create your own tools, USB Forensics, Linux Forensics, Hacker Gadget etc. and a host of other topics.

Our courses are comprehensive, hands-on, highly technical yet the most affordable in the entire industry. We have a ton of free videos on our website for potential customers to evaluate and decide for themselves.

PWNIE EXPRESS

https://www.pwnieexpress.com

Pwnie Express solutions mitigate the growing attack surface created by the emerging threat vector from the Internet of Everything. This includes high-risk BYOx, vulnerable IoT devices, and purpose-built malicious hardware.

Founded in Vermont in 2010 to leverage and build upon the power of open source tools, Pwnie Express sensors are providing previously unattainable intelligence to more than 1,500 companies globally. The list ranges from Fortune 500 companies to government agencies and security service providers, helping them bolster their security while meeting compliance requirements.

Pwnie has come a long way from building single sensors in Dave's basement, but the company is still dedicated to creating game-changing products and services for our customers and the global InfoSec community to improve the security of our Internet-connected world.

QIHOO360 UNICORN TEAM

http://www.360safe.com

Qihoo360's UnicornTeam consists of a group of brilliant security researchers. We focus on the security of anything that uses radio technologies, from small things like RFID, NFC and WSN to big things like GPS, UAV, Smart Cars, Telecom and SATCOM. Our primary mission is to guarantee that Qihoo360 is not vulnerable to any wireless attack. In other words, Qihoo360 protects its users and we protect Qihoo360.

During our research, we create and produce various devices and systems, for both attack and defence purposes. For example:

SkyScan: An enterprise scale wireless intrusion prevention system originally designed to protect Qihoo360's internal WiFi network but has now been made available as a commercial wireless security solution.

HackID: A RFID entry badge spoofer.

SecUSB: A USB cable bridge that is used to protect mobile devices when users connect them to malicious charger.

To facilitate the work of you fellow security researchers or hackers if you prefer, we bring our whole 'arsenal' to DEF CON 23.

RAPID7

http://www.rapid7.com

Rapid7 cybersecurity analytics software and services reduce threat exposure and detect compromise for 3,500 organizations, including 30% of the Fortune 1000. From the endpoint to cloud, we provide comprehensive real-time data collection, advanced correlation, and unique insight into attacker techniques to fix critical vulnerabilities, stop attacks, and advance security programs.

SECURE IDEAS

https://www.secureideas.com

Professionally Evil is the tag line or motto of Secure Ideas. We are often asked what it means and why we use it.

Professionally Evil is the idea that to understand vulnerabilities and risk, we have to understand how an attacker will use the vulnerabilities in a network or application to attack the organization. This goes beyond simply finding flaws or even exploiting them. It involves understanding the issues and how they can affect the organization.

SECURE NINJA

https://secureninjo.com

SecureNinja provides specialized cybersecurity training and consulting services. In addition, SecureNinjaTV produces cybersecurity video tutorials and coverage of hacker events from around the world- found at YouTube.com/SecureNinja. For our annual participation as a DEF CON vendor, SecureNinja creates an exclusive batch of NinjaGear for ninjas of all ages.

For the first time this year, we will offer a membership package to our new Online SenseiSeries training portal- complete with gear to transform participants into true cybersecurity ninjas!

SECURITY SNOBS

https://SecuritySnobs.com

Security Snobs offers High Security Mechanical Locks and Physical Security Products including door locks, padlocks, cutaways, security devices, and more. We feature the latest in security items including top brands like Abloy, BiLock, Anchor Las, EVVA, TiGr, and Sargent and Greenleaf. Visit https://SecuritySnobs.com for our complete range of products. Stop by our booth and get free shipping on items for the month following the conference. We will have new security products, and new lines from some of our top vendors. This year we are bringing a range of large lot high security locks for purchase at low cost too!

SECURITY WEEKLY

http://securityweekly.com

The Security Weekly mission is to provide free content within the subject matter of IT security news, vulnerabilities, hacking, and research. We strive to use new technologies to reach a wider audience across the globe to teach people how to grow, learn, and be security ninjas. The mixture of technical content and entertainment will continue to set a new standard for podcasting and Internet TV.

SEREPICK

http://www.serepick.com

Manufacturer of Lock Picks & COVERT ENTRY TOOLS

With the largest selection of lock picks, covert entry and SERE tools available at DEF CON it's guaranteed we will have gear you have not seen before. New tools and classics will be on display and available for sale in a hands on environment. Our Product range covers Custom Titanium toolsets, Entry Tools, Practice locks, Bypass tools, Urban Escape & Evasion hardware and items that until recently were sales restricted. SPARROWS LOCK PICKS and TOOLS will be displaying a full range of gear including their newly released COMB 45., Mantis and MAGNETO. The PLISSKEN set will also be available to the public for the first time in limited quantities. All products will be demonstrated at various times and can be personally tested for use and Efficacy.

SHADOWVEX

http://store.shadowvexindustries.com

Shadowvex Industries is celebrating 20 years of involvement with DEF CON! We specialize in hacker relevant-limited edition-artistically driven Clothing, DJ Mixes, Stickers, Art Prints, Buttons and more. Follow the music in the vending area and stop by our booth to see and hear what inspires our community!

SILENT CIRCLE

http://www.silentcircle.com

Silent Circle is a leader in enterprise privacy, delivered through a revolutionary platform of devices, software and services, starting with ZRTP to build a fundamentally different mobile architecture.

Now led by Bill Conner, the former Entrust President and CEO and Nortel President, Silent Circle was co-founded by Mike Janke, former Navy SEAL and security expert; Phil Zimmermann, co-founder of PGP, developer of the ZRTP protocol and 2015 inductee into the Internet Hall of Fame; and Jon Callas, creator of Apple's whole disk encryption software and co-founder of PGP Corporation.

Silent Circle is headquartered in Switzerland, home to the world's best privacy laws. For more information on Silent Circle, go to: https://

SIMPLE WIFI

http://simplewifi.com

For PenTesting and unwired Internet Security Specialists: Wireless, WiFi antennas, cables, connectors, USB and Ethernet wireless high power cards and devices, other interesting goodies to be seen only at the table! And new design T-shirts.

THE SOURCE OF KNOWLEDGE

https://www.sourceofknowledge.com

Source of Knowledge (SOK) is the leading educational content capture and distribution company for the IT industry, focusing on software, hardware and firmware user groups and computer security groups.

THREATFORGE

https://app.threatforge.com

ThreatForge is the world's first fully integrated security training and assessment platform. Our platform allows individuals to access training content and gain hands-on technical experience through lab environments and threat simulation activities. Train, assess and provide users with a place to practice newly learned skills is a safe, virtualized workspace. Challenges allow members to put their capabilities to the test. Live systems mimicking real attacks require participants to call upon new skills for successful completion. Numerous organizations of all sizes leverage our immersive threat simulation environment to give users on-the job experience before a breach actually occurs.

TOOOL

http://toool.us/

The Open Organisation Of Lockpickers is back as always, offering a wide selection of tasty lock goodies for both the novice and master lockpicker! A variety of commercial picks, handmade picks, custom designs, practice locks, handcuffs, cutaways, and other neat tools will be available for your perusing and enjoyment! Stop by our table for interactive demos of this fine lockpicking gear or just to pick up a T-shirt and show your support for locksport.

All sales exclusively benefit TOOOL, a non-profit organization. You can purchase picks from many fine vendors, but ours is the only table where you know that 100% of your money goes directly back to the locksport and hacker community.

UNIVERSITY OF ADVANCING TECHNOLOGY

http://uat.edu

The University of Advancing Technology (UAT) is a private university located in Tempe, Arizona, offering academic degrees focused on new and emerging technology disciplines. UAT offers a robust suite of regionally accredited graduate and undergraduate courses ranging from Computer Science and Information Security to Gaming and New Media. UAT has been designated as a Center for Academic Excellence in Information Systems Security Education by the US National Security Agency. Programs are available online and on-campus.

UNIX SURPLUS

http://UnixSurplus.com

"Home of the $99 1U Server"

1260 La Avenida St Mountain View, CA 94043

Toll Free: 877-UNIX-123 (877-864-9123)

Classifieds

HACKER EVENTS DRAW "BAD ELEMENT"

5TH DEF CON BIKE RIDE

For the 5th straight year, Friday morning at 6am, a bunch of hackers go to McGhies Bike shop, rent bikes and ride a 20 mile loop out to Red Rocks and back. At 6am. In the desert. It's a fun time. We have a follow car in case you blue screen, and the beasts do an extra 2 miles and climb up 1000 ft to the top of a vista. See www.cycleoverride.org or @cycle_override.org for more info.

BE THE MATCH REGISTRY DRIVE

Interested in participating in a cool lifehack? When you join the Be The Match Registry® at DEF CON, you become part of every patient's search for a bone marrow donor. Thousands of patients with blood cancers like leukemia and lymphoma, sickle cell and other life-threatening diseases need a bone marrow transplant. You could be the one to save a life.

www.bethematch.org

DEAF CON

DEAF CON's mission is to encourage many Deaf and Hard of Hearing (HH) hackers to attend DEF CON, help provide these hackers with partial or full services, and provide a place for Deaf/HH hackers to meet up and hangout. The meet-up is an unofficial DEF CON event and open to everyone who would like to attend. We also provide American Sign Language interpreters funded by independent donations. If you would like to use our interpreting services, please follow us on twitter @_DEAFCON_ for information about where our interpreters will be during the con!

*DEAF CON is not affiliated with the CART services provided in the Speaker tracks during previous cons.

DEF CON SHOOT

The DEF CON Shoot is an opportunity to see and possibly fire some of the guns belonging to your friends while taking pride in showing and firing your own steel, as well, in a relaxed and welcoming atmosphere.

We gather together out in the desert in the days before the start of DEF CON every year and it's always a terrific time for everyone.

Taking place both on the late afternoon of Wednesday and the morning hours of Thursday (with a campout in between for anyone who is so inclined) this is a great way to get yourself some peace and quiet (punctuated by big booms) before the chaos of DEF CON gets fully underway.
If you like guns and want to put tiny holes into lots of things out in the desert, come join us!

Wednesday 1600 CONTINUOUSLY THROUGH Thursday 1300

HACKER KARAOKE

Do you like music? Do you like performances? Want to BE the performer? Well trot your happy ass down to the fourth annual Hacker Karaoke, DEF CON's on-site karaoke experience where you can be a star, even if you don't know it. Don't want to be a star? At Hacker Karaoke you can also take pride in making an utter fool of yourself.

Friday & Saturday Night at 9PM in Skyview 1

MOHAWKCON

Get your head buzzed at DEF CON to support the Electronic Frontier Foundation, Hackers For Charity, and your favorite Hackerspaces!

WTF is this all about? We could say we're making a statement about how punk values reflect the fight for digital freedoms, but we'd be full of shit.

We do it because it's fun, and you're all awesome.

@MohawkCon
https://www.facebook.com/MohawkCon

Friday, Saturday 1000 - 1700 @ Contest Area

QUEERCON

Mixer: Thursday - Sunday, 4p @ courtesy suite*
QC12 Pool Party - Friday 8p to 3a @ Bally's Pool
They call it 'Le Gay Paree' for a reason! In our 12th-annual event lineup and first time at Paris/Bally's Las Vegas, Queercon invites all LGBT Defcon attendees and friends to meet & mingle in our open and casual environment. At 4pm every day of the conference, join us and 100+ others at the QC courtesy suite (room #TBD*) in the Bally's Jubilee tower to hang out, trade stories, and enjoy our staffed cocktail bar. Open to everyone, no Defcon badge required.
QC12 POOL PARTY: Doors at 8pm at the Bally's Hotel pool area, where we have some of the best international DJs spinning all night long! The bars will be pouring, no Defcon badge required, and yes the pool will be OPEN. This is the Friday night party not to be missed, so be cool and be there.
(*Suite number is on queercon.org, our mobile app, Facebook, Twitter... etc. You'll find it!)

LAWYER MEETUP

If you're a lawyer (recently unfrozen or otherwise), a judge or a law student please make a note to join your host Jeff McNamara at 6pm on Friday, August 7th for a friendly get-together, followed by dinner/drinks and conversation.

Saturday 1800 - Club 22 (22nd floor Bally's North Tower)

FRIENDS OF BILL W. MEETINGS

Sin City is a lot to take in. Friends of Bill W. joining us for DEF CON 23 are invited to take a break from the Vegas of it all with meetings at noon and five p.m., Thursday, August 6 through Sunday, August 9. Your hosts will be Jeff Mc and Edward B.

Thursday-Sunday at 1200 and 1700 - Ballys North Tower Office (Past Skyview 4)

SHOUT OUTS!

Dark Tangent would like to draw attention to the amazing community that makes DEF CON possible. You can see below how many people are involved to pull off the con, many of them doing different things over the years, but always working to make things better. Without stealing the thunder from all the department leaders below I'd like to thank all the organizers of all the contests that bring the content, contests, villages and events. I'd like to thank the speakers, artists, musicians, and Goons. Thanks to Jayson Street and his team for stepping up to relaunch and manage the DEF CON Groups. I'd like to thank the year round crew, Nikita, Neil, Will, Cheryl, Jeff, and Darington. Finally I'd like to thank the management at Paris and Ballys for being professional and great to work with. Thank you everyone for an amazing year!

Agent X would like to thank the Speaker Operations staff for another year of great service to DEF CON and it's speakers. These goons are #2, Code24, bitmonk, jur1st, Shadow, Vaedron, goekesmi, Scout, CLI, gattaca, Crash, Round River, idontdrivecars, Notkevin, Froggy, Jinx, Pasties, Bushy, Kale, pwcrack, Mnky and AMFYOYO!

Cjunky would like to thank Alex C, Amber, Angie, b0n3z, BeaMeR, blak, Br1ck, Captain, Carric, Chosen1, CHRIS, cRusad3r, cyber, cymike, Dallas, Darkwolf, dc0de, DeeLo, digunix, dr.kaos, dr3t, DrFed, echosixx, Emergency Mexican, Faz, flea, FoxCaptain, Freshman, GM1, Gonzo, HattoriHanzo, iole, JAFO, Jake, johnd, JustaBill, Knox, krassi, KRS, kruger, Lordy, M0rphix, mattrix, mauvehed, MAXIMUS, Montell, mrb0t, nynex, P33v3, pfriedma, phreck, Plasma, precore, quiet, Red, rik, Salem, Siviak, SkyDog, SomeNinjaMaster, Sonicos, sp00ns, stan, Synn, tacitus, TBD, timball, Trinity, Vidiot, Viss, wald0, WarFlower, WHAM, WhiteB0rd for their help this year. Thank you also to all the retiring goons. We will miss you. Pax Per Imperium.

ChrisAM would like to thank everyone responsible for this year's entertainment & decor: Great Scott, Krisz Klink, Zziks, Mindy, Kermit, djdead, Zebbler Studios, Mobius, and SomaFM.

effffn, the DEF CON organization and the hacker community would like to once again thank the NOC team: mac, videoman, #sparky, rukbat, booger, naifx, arh@wk, char, _CRV, c0mmiebstrd and serif. This crew also known as "effffn's 12" devote their DEF CON experience to hard work during the entire week and it doesn't make it any easier when we switch to a new venue. They are also involved in planning this throughout the year so everyone can comfortably internetz in most of the places of the convention centers and watch the talks in their hotel rooms during the con.

Grifter would like to thank the entire Contest, Events, Villages, and Parties team. Huge, HUGE, thanks to Pandero and c0l3slaw for the countless hours spent keeping things rolling without a hitch. Many thanks to 0x58, afterburn, Bo Knows, bombnav, cyungle, haxagoras, Knight Owl, phartacus, phorkus, rugger, shaggy, Stumper, and tener for all the early mornings and late, late nights. Much love to the DEF CON HQ team of RussR, Nikita, Neil, Darington, Charel, Will, and of course, The Dark Tangent, without whom we would be utterly lost. We're also pouring out a 40 for Hackajar who, even though he's taking a year off, will always be a C&E Goon. And last, but certainly not least, we can't thank enough the many, many, organizers of all the C\E\V\P content, for helping us make countless DEF CON attendees say "Talks? ...What talks?"

InfoBooth would like to thank Krav, PEZhead, ScurryFool, sl3ppy, Jerel, TC, LittleBruzer, Fran, Turb1n3, Jimmy, jimi2x, Lita, Melloman, Algorythm, jixion, Cheshire, jaffo, madstringer, Sanchez, John Titor. Also a big shout out to Whitney and Sean for the work on the mobile apps.

1o57 would like to thank: ln, 2168, DT, Russmania, Neil of Fortune and Kita, Zant, Clutch, APG, Will, Charel, all the mC vets, and all those who help keep mystery in the world.

Nikita would like to thank the DEF CON CFP Review Board for their hard work, dedication, and long hours. Thanks to: CJ, Dead Addict, DT, Grifter, HighWizard, Jennifer Granick, Jericho, LosT, Mouse, Roamer, Suggy, TW, Vertigo, Vyrus, Weasel, Wiseacre, Zoz. Special Thanks to Charel, Crypt, Grifter, Leah, Neil, Pyr0, Russ, and the Workshops Goons. Sincere appreciation to all the DEF CON Speakers who bring us their hacks every year without fail, we heart you. Thank you for helping countless DEF CON attendees wake up with fresh brewed pwns at 10am on Sunday.

Production would like to thank Betsy for showing us how it's done, Russ for getting the ball rolling early and smoothly, DT's foresight and willingness to adapt, Charel for her Hotel Wrangler Merit Badge, and all Goons, no matter what color their shirt is or was.

A huge thanks to all the Press Goons: Mel, Lin, Linda, Grace, Alex, David, Jhayne, Jim, Jen, Jeff and Nicole who work hard to ensure coverage of the research and other awesomeness of DEF CON so it can be shared with the rest of the global community.

Registration would like to thank: Production and QM, for logistical assistance; the goons engineering the lines, for keeping everyone safe; the Info Booth team, for backing us up; and the attendees, for their patience.

Russ would like to thank all the goons, who have dedicated so much time to this conference, throughout the year. Specifically, a huge thanks to Nikita, Neil, Charel, Will, Lockheed, Heather, the Dark Tangent, and hazmat; for helping me make the full transition into trying to manage this circus we like to call a conference. Thank you to all the Department leads and their 2nd, who have each repeatedly stepped up to provide input, advice, and guidance over the last year. I'd like to point out Grifter and Panadero, specifically, for agreeing to lead the Contest and Events, even with only a few months left before the conference. Thanks to all our contests, events, villages, and artists for creating awesome content, and keeping the conference unique and interesting. A huge shout out to the Security Tribe and the 303, and an embarrassing shout out to our kids, attending DEF CON for the first time: BreRog, ceris, kyndabug, and MoRo.

TheCotMan offers thanks to Nulltone and Simon for starting the DEF CON forums in 2001 and all past mods that have since retired. Thanks to present Admins: Dark Tangent, Chris, Neil, and Mods: ASTCell, Thorn, AlxRogan, BlackBeetle, Blakdayz, Noid, and Russ. You all help keep the forum clear of spam and abuse. Thanks! A double-thanks to Dark Tangent, giving forums life with a server, network access and support.

The Vendor Goons would like to than the vendors, without whom the vendor area would not exist. Also, the attendees who come to the vendor area to support the vendors. We would like to thank everyone from DEF CON production for supporting us and helping to make this conference as awesome as it is. Finally, the Head Vendor Goon would like to thank all the other Vendor Goons for doing a great job year after year. Thanks to you all!