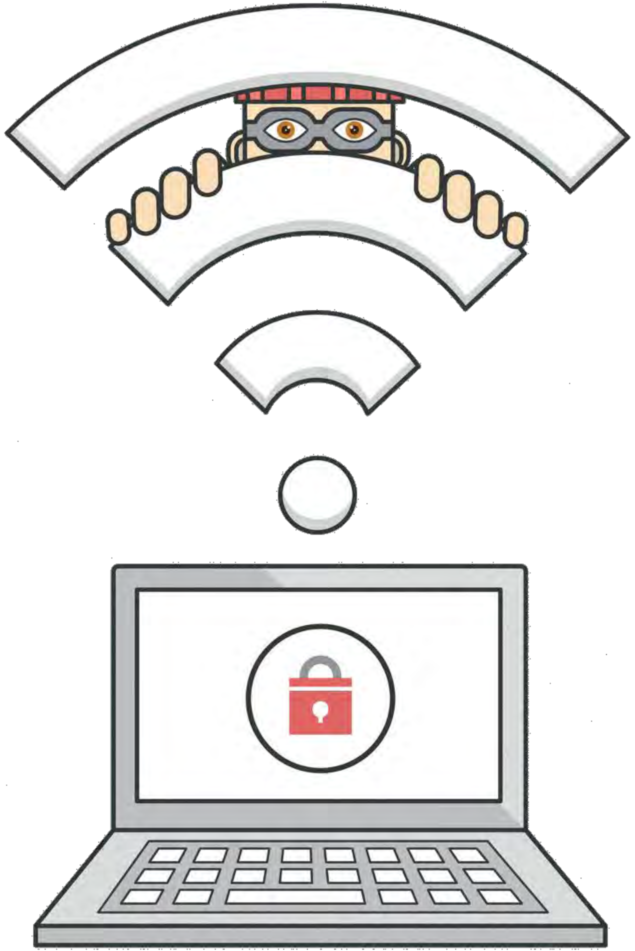
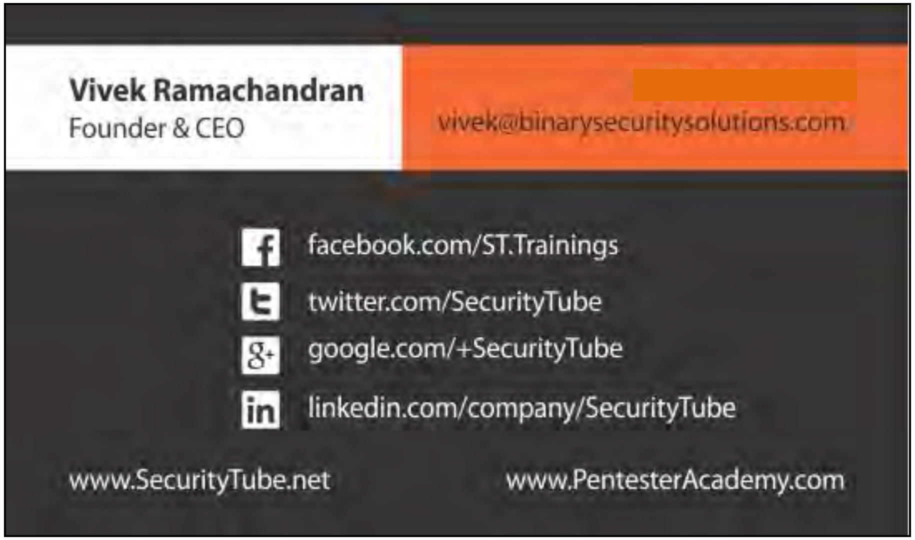
Chellam – a Wi-Fi IDS/Firewall for Windows





Vivek Ramachandran
Founder & CEO

[redacted]
vivek@binarysecuritysolutions.com

facebook.com/ST.Trainings
twitter.com/SecurityTube
google.com/+SecurityTube
linkedin.com/company/SecurityTube

www.SecurityTube.net
www.PentesterAcademy.com

Vivek Ramachandran

भारतीय प्रौद्योगिकी संस्थान, गुवाहाटी
Indian Institute of Technology, Guwahati

B.Tech, ECE
IIT Guwahati

802.1x, Cat65k
Cisco Systems

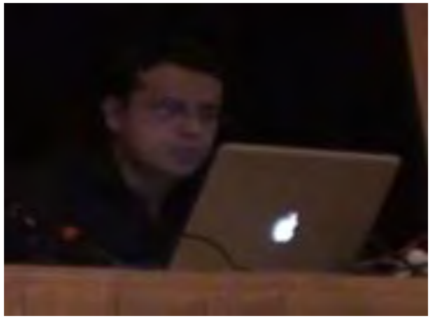
WEP Cloaking
Defcon 19

Caffe Latte Attack
Toorcon 9

Media Coverage
CBS5, BBC

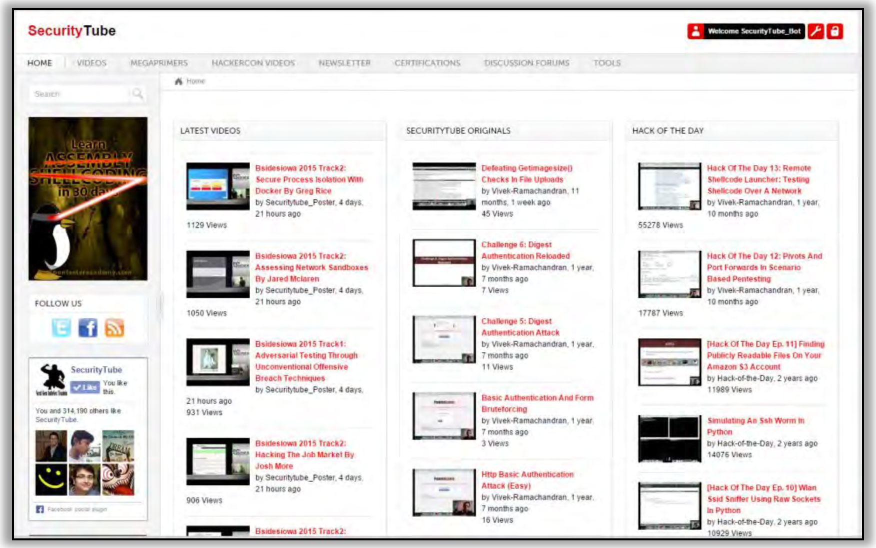
Microsoft
Security Shootout

Trainer, 2011



Wi-Fi Malware, 2011

SecurityTube and Pentester Academy



You and 314,190 others like SecurityTube.

LATEST VIDEOS

Bsidesiowa 2015 Track2: Secure Process Isolation With Docker By Greg Rice
by Securitytube_Poster, 4 days, 21 hours ago
1129 Views

Bsidesiowa 2015 Track2: Assessing Network Sandboxes By Jared Mclaren
by Securitytube_Poster, 4 days, 21 hours ago
1050 Views

Bsidesiowa 2015 Track1: Adversarial Testing Through Unconventional Offensive Breach Techniques
by Securitytube_Poster, 4 days, 21 hours ago
931 Views

Bsidesiowa 2015 Track2: Hacking The Job Market By Josh More
by Securitytube_Poster, 4 days, 21 hours ago
906 Views

Bsidesiowa 2015 Track2:

SECURITYTUBE ORIGINALS

Defeating Getimagesize() Checks In File Uploads
by Vivek-Ramachandran, 11 months, 1 week ago
45 Views

Challenge 6: Digest Authentication Reloaded
by Vivek-Ramachandran, 1 year, 7 months ago
7 Views

Challenge 5: Digest Authentication Attack
by Vivek-Ramachandran, 1 year, 7 months ago
11 Views

Basic Authentication And Form Bruteforcing
by Vivek-Ramachandran, 1 year, 7 months ago
3 Views

Http Basic Authentication Attack (Easy)
by Vivek-Ramachandran, 1 year, 7 months ago
16 Views

HACK OF THE DAY

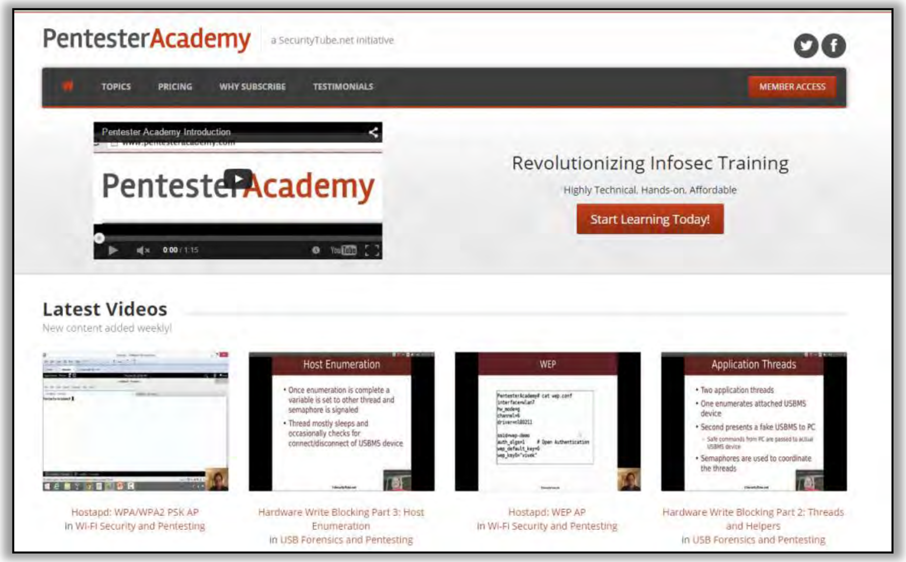
Hack Of The Day 13: Remote Shellcode Launcher: Testing Shellcode Over A Network
by Vivek-Ramachandran, 1 year, 10 months ago
55278 Views

Hack Of The Day 12: Pivots And Port Forwards In Scenario Based Pentesting
by Vivek-Ramachandran, 1 year, 10 months ago
17787 Views

[Hack Of The Day Ep. 11] Finding Publicly Readable Files On Your Amazon S3 Account
by Hack-of-the-Day, 2 years ago
11989 Views

Simulating An Ssh Worm In Python
by Hack-of-the-Day, 2 years ago
14076 Views

[Hack Of The Day Ep. 10] Wlan Ssid Sniffer Using Raw Sockets In Python
by Hack-of-the-Day, 2 years ago
10929 Views



Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

Latest Videos

New content added weekly!

- Once enumeration is complete a variable is set to other thread and semaphore is signaled
- Thread mostly sleeps and occasionally checks for connect/disconnect of USBMS device

- Two application threads
- One enumerates attached USBMS device
- Second presents a fake USBMS to PC
  - Safe commands from PC are passed to actual USBMS device
- Semaphores are used to coordinate the threads

Hostapd: WPA/WPA2 PSK AP
in Wi-Fi Security and Pentesting

Hardware Write Blocking Part 3: Host Enumeration
in USB Forensics and Pentesting

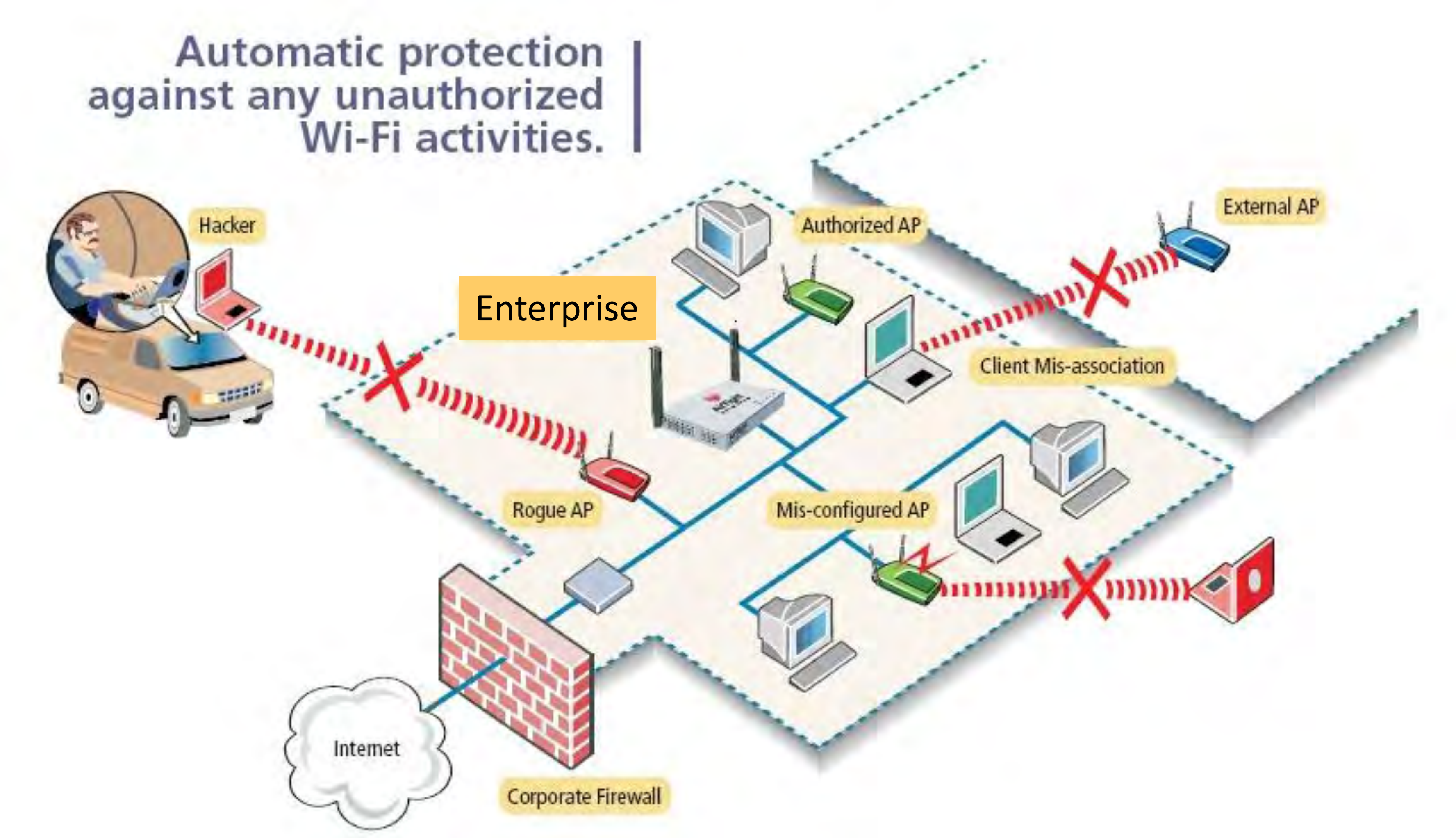
Hostapd: WEP AP
in Wi-Fi Security and Pentesting

Hardware Write Blocking Part 2: Threads and Helpers
in USB Forensics and Pentesting

Motivation

- Attack! Attack! Attack!
- Defense?
- Important problem?
- Solution viable?

Enterprise Premise Focused



Roaming Clients?

- State of current solutions
  - Lockdown Wi-Fi, Bluetooth etc.
  - Policy based on SSID
  - Not BYOD ready
  - No Attack detection

- Heterogeneous Devices
  - Varied Operating Systems
  - Non standard Wi-Fi API
  - No low level support e.g. iOS

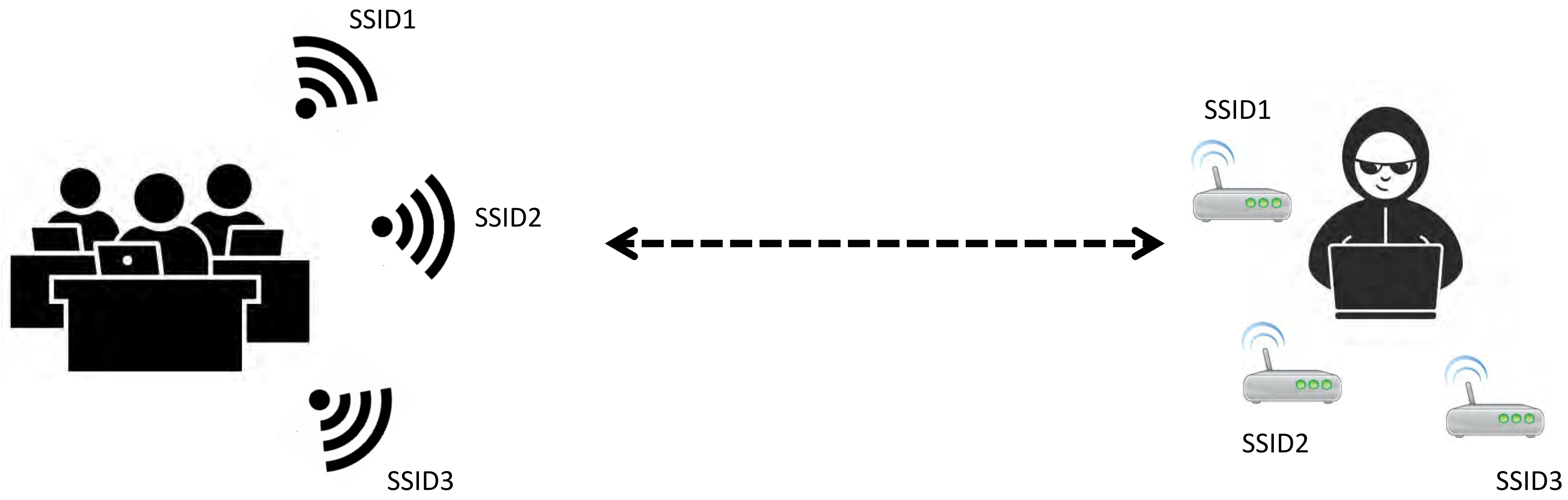
What about the rest of us?

- World beyond Enterprise
- Millions of Personal Devices
- Every Internet capable device
- Internet Of Things (IoT)

Wi-Fi Client Attack Surface

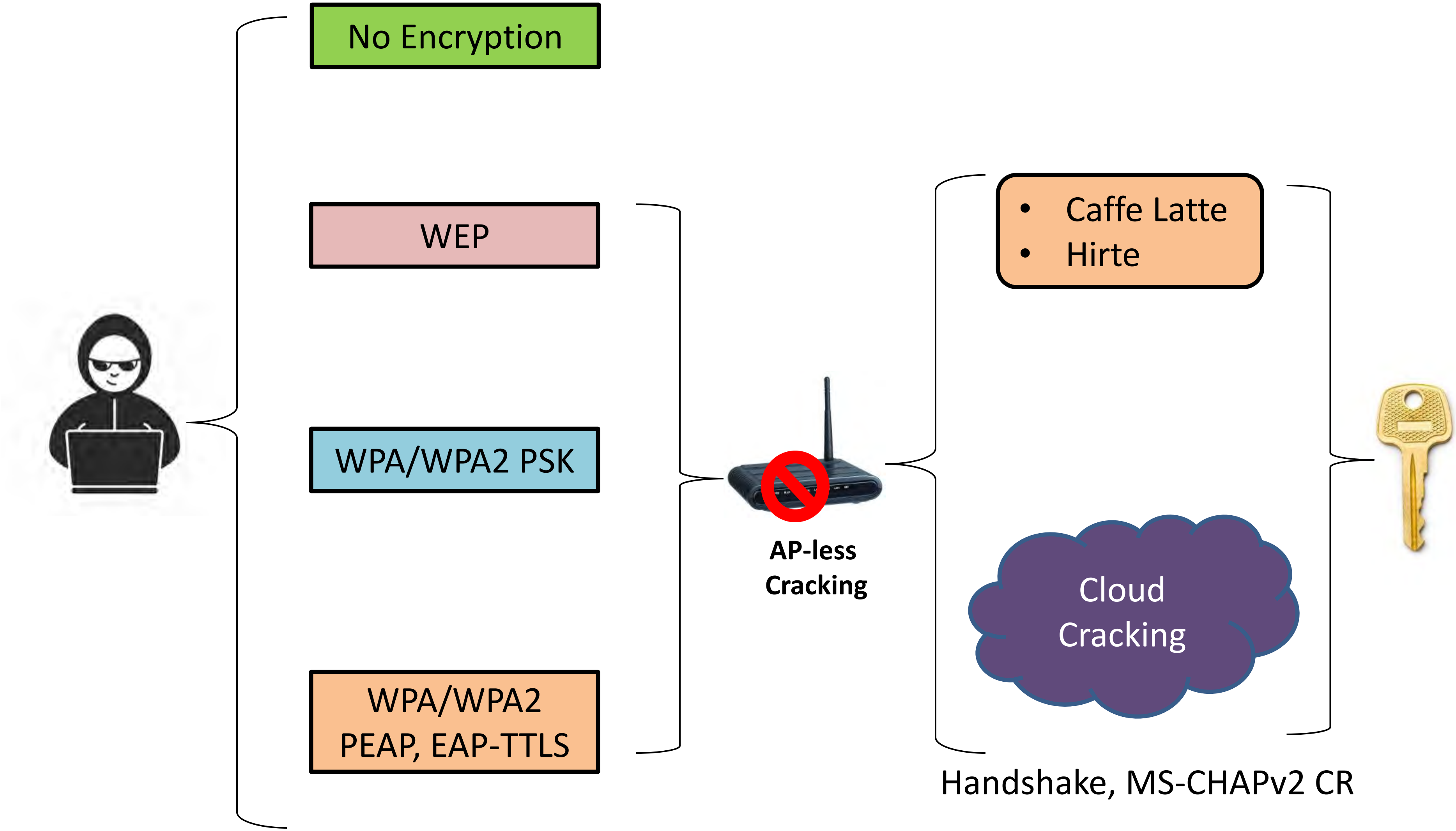
- Honeypots
  - AP-less WEP/WPA/WPA2 Cracking
- Evil Twins
- Mis-Associations
- Hosted Network Backdoors
- …

Typical Attack



©SecurityTube.net

AP-less Cracking



No Encryption

WEP

WPA/WPA2 PSK

WPA/WPA2 PEAP, EAP-TTLS

AP-less Cracking

- Caffe Latte
- Hirte

Cloud Cracking

Handshake, MS-CHAPv2 CR

Where are you SAFE? Nowhere!!!

Hijack Wi-Fi == Hijack Layer 2

Traffic Monitoring

DNS Hijacking

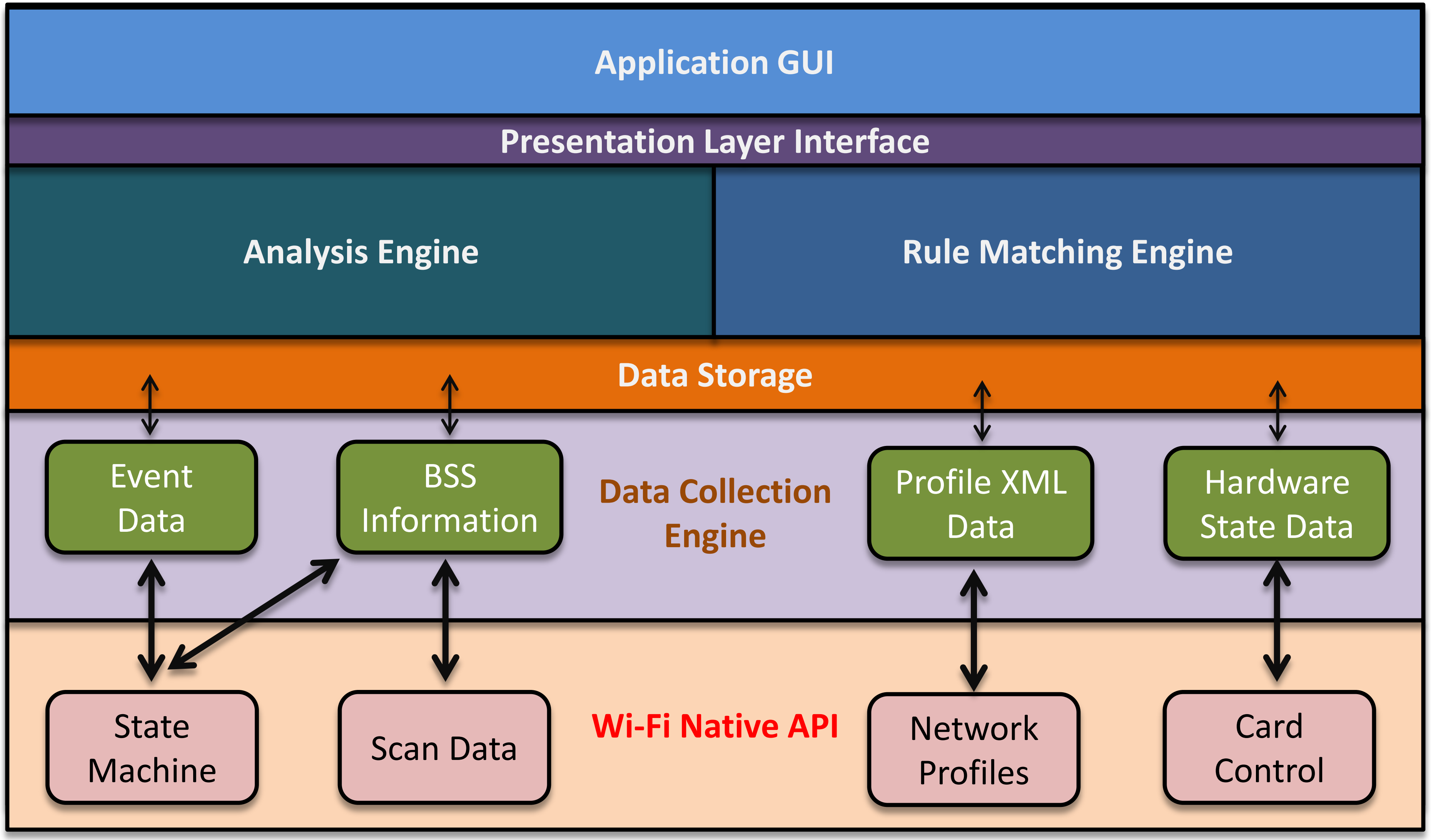
SSL MITM

Application Attacks

Defining the Scope

- Windows Endpoints
  - No custom hardware or drivers
- Detect Honeypot creation Tools
- Firewall like Rule Creation
  - “Allow”, “Deny”
- Monitoring Wi-Fi state machine
- Detect Wi-Fi backdoors

Architecture Block Diagram



©SecurityTube.net

Wi-Fi Native API

State Machine

Scan Data

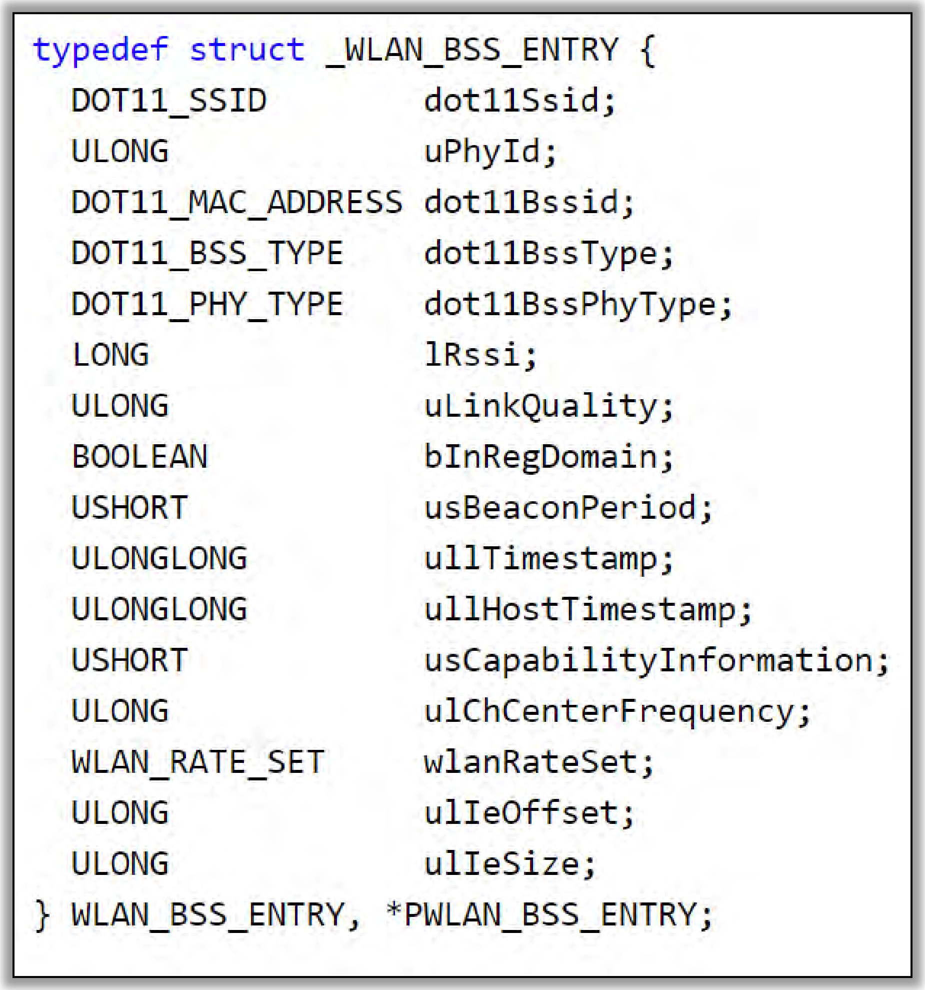
Wi-Fi Native API

Network Profiles

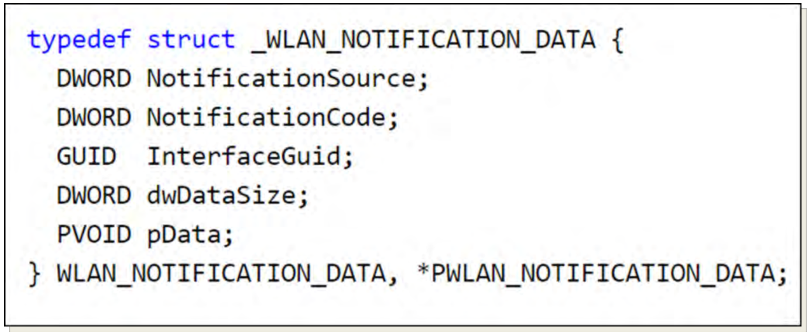
Card Control

State Machine	**802.11 state machine per Wi-Fi card**
Scan Data	**Periodic Scan Results with BSS data**
Network Profiles	**XML network profile data**
Card Control	**Scan, Connect, Disconnect, Lock etc.**

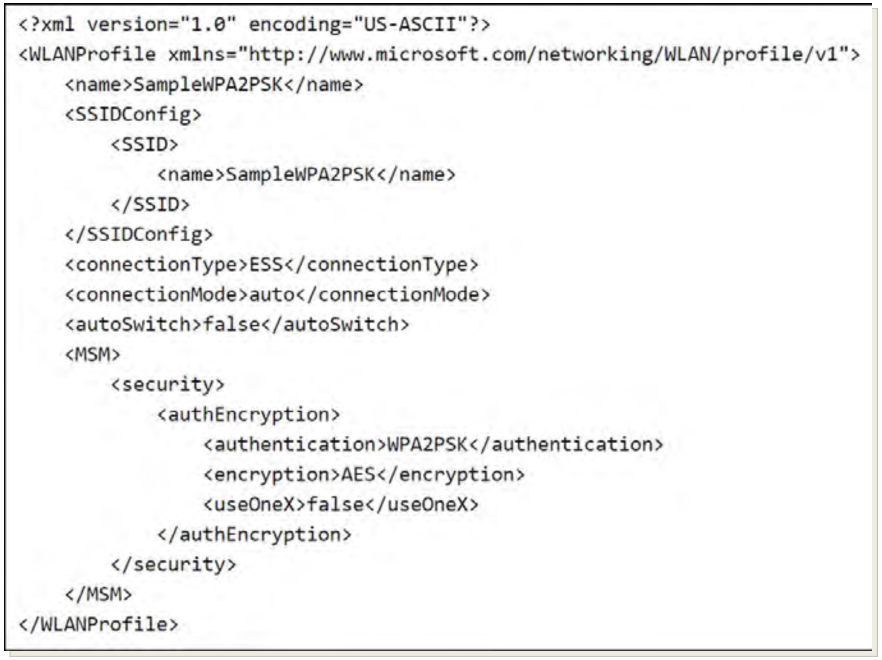
Technicalities



```c
typedef struct _WLAN_BSS_ENTRY {
  DOT11_SSID        dot11Ssid;
  ULONG             uPhyId;
  DOT11_MAC_ADDRESS dot11Bssid;
  DOT11_BSS_TYPE    dot11BssType;
  DOT11_PHY_TYPE    dot11BssPhyType;
  LONG              lRssi;
  ULONG             uLinkQuality;
  BOOLEAN           bInRegDomain;
  USHORT            usBeaconPeriod;
  ULONGLONG         ullTimestamp;
  ULONGLONG         ullHostTimestamp;
  USHORT            usCapabilityInformation;
  ULONG             ulChCenterFrequency;
  WLAN_RATE_SET     wlanRateSet;
  ULONG             ulIeOffset;
  ULONG             ulIeSize;
} WLAN_BSS_ENTRY, *PWLAN_BSS_ENTRY;
```



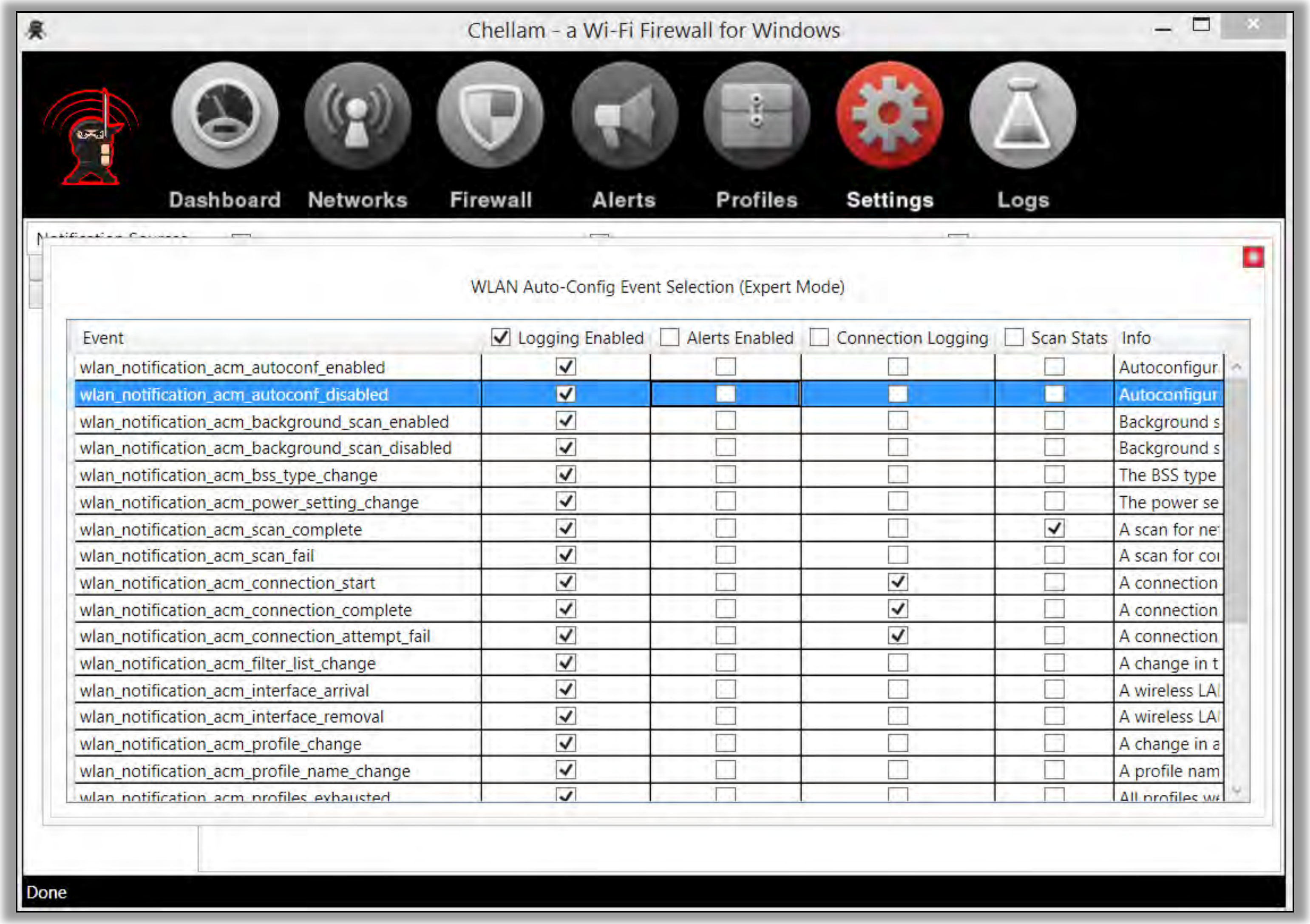
```c
typedef struct _WLAN_NOTIFICATION_DATA {
  DWORD NotificationSource;
  DWORD NotificationCode;
  GUID  InterfaceGuid;
  DWORD dwDataSize;
  PVOID pData;
} WLAN_NOTIFICATION_DATA, *PWLAN_NOTIFICATION_DATA;
```



```xml
<?xml version="1.0" encoding="US-ASCII"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
    <name>SampleWPA2PSK</name>
    <SSIDConfig>
        <SSID>
            <name>SampleWPA2PSK</name>
        </SSID>
    </SSIDConfig>
    <connectionType>ESS</connectionType>
    <connectionMode>auto</connectionMode>
    <autoSwitch>false</autoSwitch>
    <MSM>
        <security>
            <authEncryption>
                <authentication>WPA2PSK</authentication>
                <encryption>AES</encryption>
                <useOneX>false</useOneX>
            </authEncryption>
        </security>
    </MSM>
</WLANProfile>
```

https://msdn.microsoft.com/en-us/library/windows/desktop/ms706839(v=vs.85).aspx

Demo – Data Sources

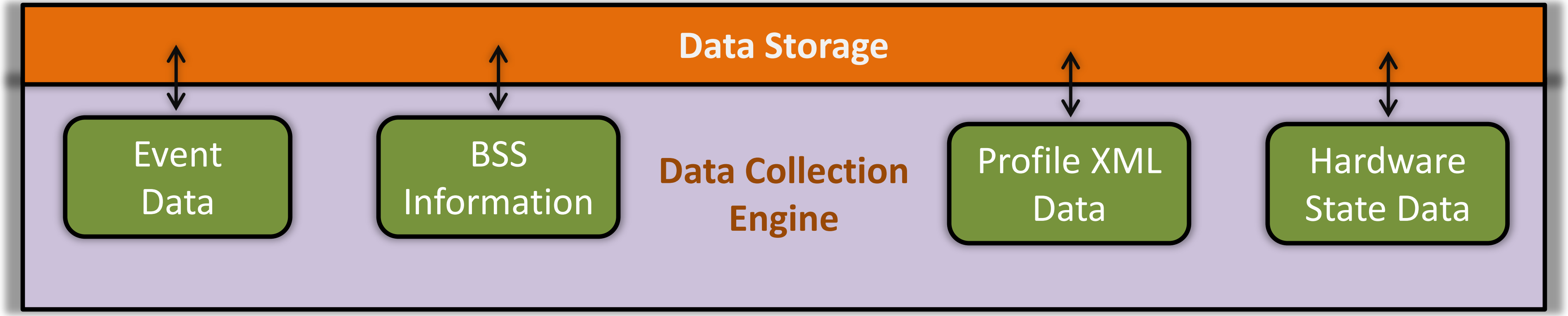


WLAN Auto-Config Event Selection (Expert Mode)

Event	☑ Logging Enabled	□ Alerts Enabled	□ Connection Logging	□ Scan Stats	Info
wlan_notification_acm_autoconf_enabled	☑	□	□	□	Autoconfigur
wlan_notification_acm_autoconf_disabled	☑	□	□	□	Autoconfigur
wlan_notification_acm_background_scan_enabled	☑	□	□	□	Background s
wlan_notification_acm_background_scan_disabled	☑	□	□	□	Background s
wlan_notification_acm_bss_type_change	☑	□	□	□	The BSS type
wlan_notification_acm_power_setting_change	☑	□	□	□	The power se
wlan_notification_acm_scan_complete	☑	□	□	☑	A scan for ne
wlan_notification_acm_scan_fail	☑	□	□	□	A scan for co
wlan_notification_acm_connection_start	☑	□	☑	□	A connection
wlan_notification_acm_connection_complete	☑	□	☑	□	A connection
wlan_notification_acm_connection_attempt_fail	☑	□	☑	□	A connection
wlan_notification_acm_filter_list_change	☑	□	□	□	A change in t
wlan_notification_acm_interface_arrival	☑	□	□	□	A wireless LA
wlan_notification_acm_interface_removal	☑	□	□	□	A wireless LA
wlan_notification_acm_profile_change	☑	□	□	□	A change in a
wlan_notification_acm_profile_name_change	☑	□	□	□	A profile nam
wlan_notification_acm_profiles_exhausted	☑	□	□	□	All profiles we

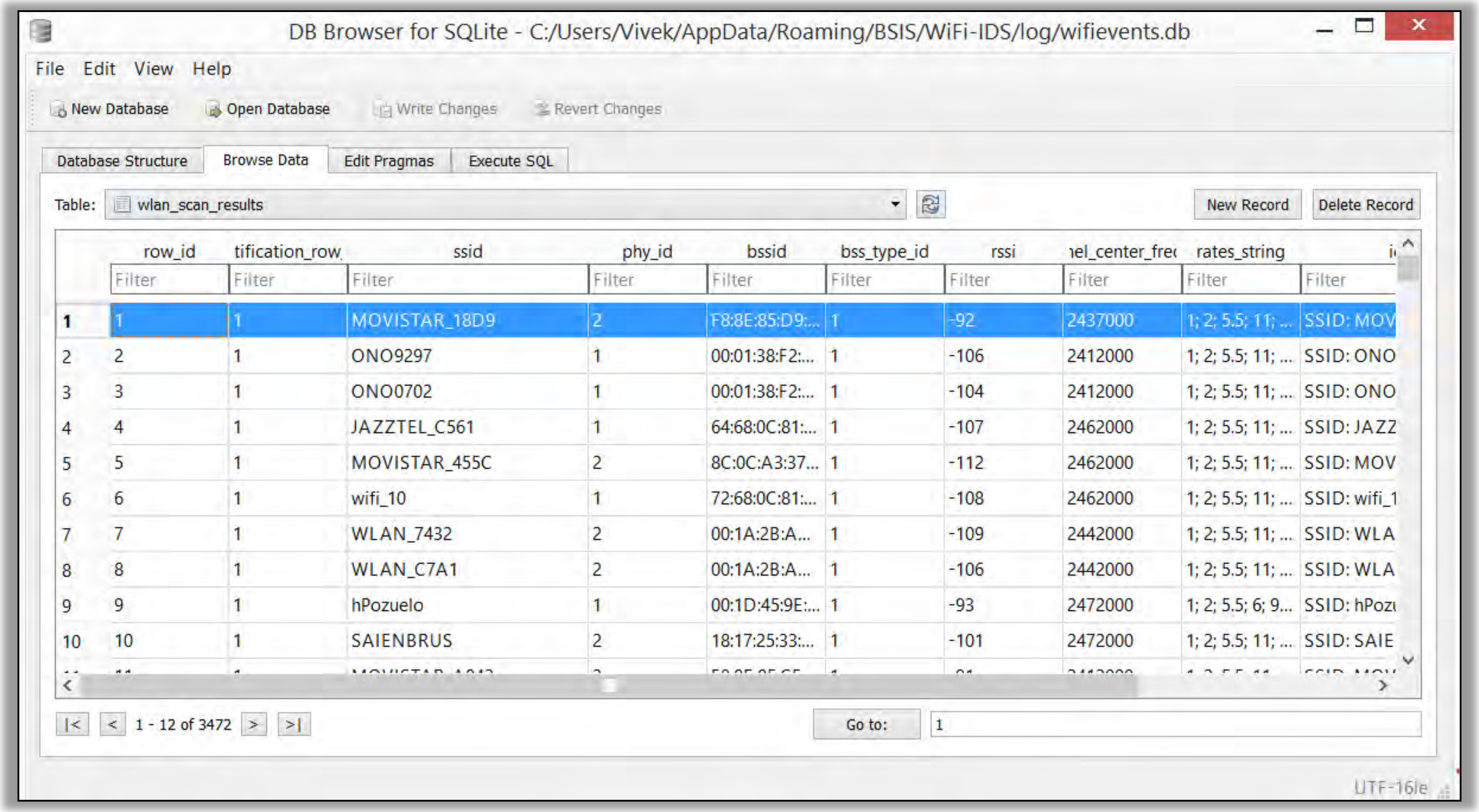
Done

Data Collection and Storage



- Stored in SQLITE databases
- Makes it easy to write plugins
- 3rd party tools can use the database

Demo – SQLITE DB Data



DB Browser for SQLite - C:/Users/Vivek/AppData/Roaming/BSIS/WiFi-IDS/log/wifievents.db

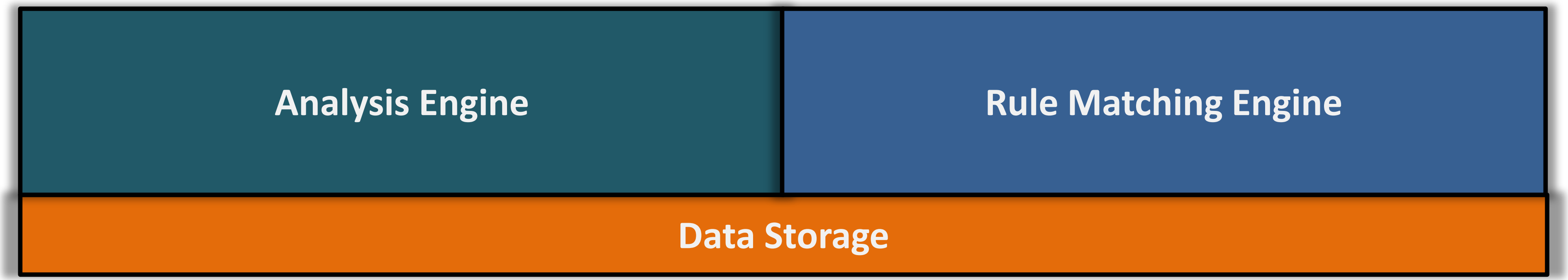
Table: wlan_scan_results

	row_id	tification_row	ssid	phy_id	bssid	bss_type_id	rssi	ıel_center_fre	rates_string	i
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	1	MOVISTAR_18D9	2	F8:8E:85:D9:...	1	-92	2437000	1; 2; 5.5; 11; ...	SSID: MOV
2	2	1	ONO9297	1	00:01:38:F2:...	1	-106	2412000	1; 2; 5.5; 11; ...	SSID: ONO
3	3	1	ONO0702	1	00:01:38:F2:...	1	-104	2412000	1; 2; 5.5; 11; ...	SSID: ONO
4	4	1	JAZZTEL_C561	1	64:68:0C:81:...	1	-107	2462000	1; 2; 5.5; 11; ...	SSID: JAZZ
5	5	1	MOVISTAR_455C	2	8C:0C:A3:37...	1	-112	2462000	1; 2; 5.5; 11; ...	SSID: MOV
6	6	1	wifi_10	1	72:68:0C:81:...	1	-108	2462000	1; 2; 5.5; 11; ...	SSID: wifi_1
7	7	1	WLAN_7432	2	00:1A:2B:A...	1	-109	2442000	1; 2; 5.5; 11; ...	SSID: WLA
8	8	1	WLAN_C7A1	2	00:1A:2B:A...	1	-106	2442000	1; 2; 5.5; 11; ...	SSID: WLA
9	9	1	hPozuelo	1	00:1D:45:9E:...	1	-93	2472000	1; 2; 5.5; 6; 9...	SSID: hPozu
10	10	1	SAIENBRUS	2	18:17:25:33:...	1	-101	2472000	1; 2; 5.5; 11; ...	SSID: SAIE

1 - 12 of 3472

Go to: 1

Rule Matching and Analysis



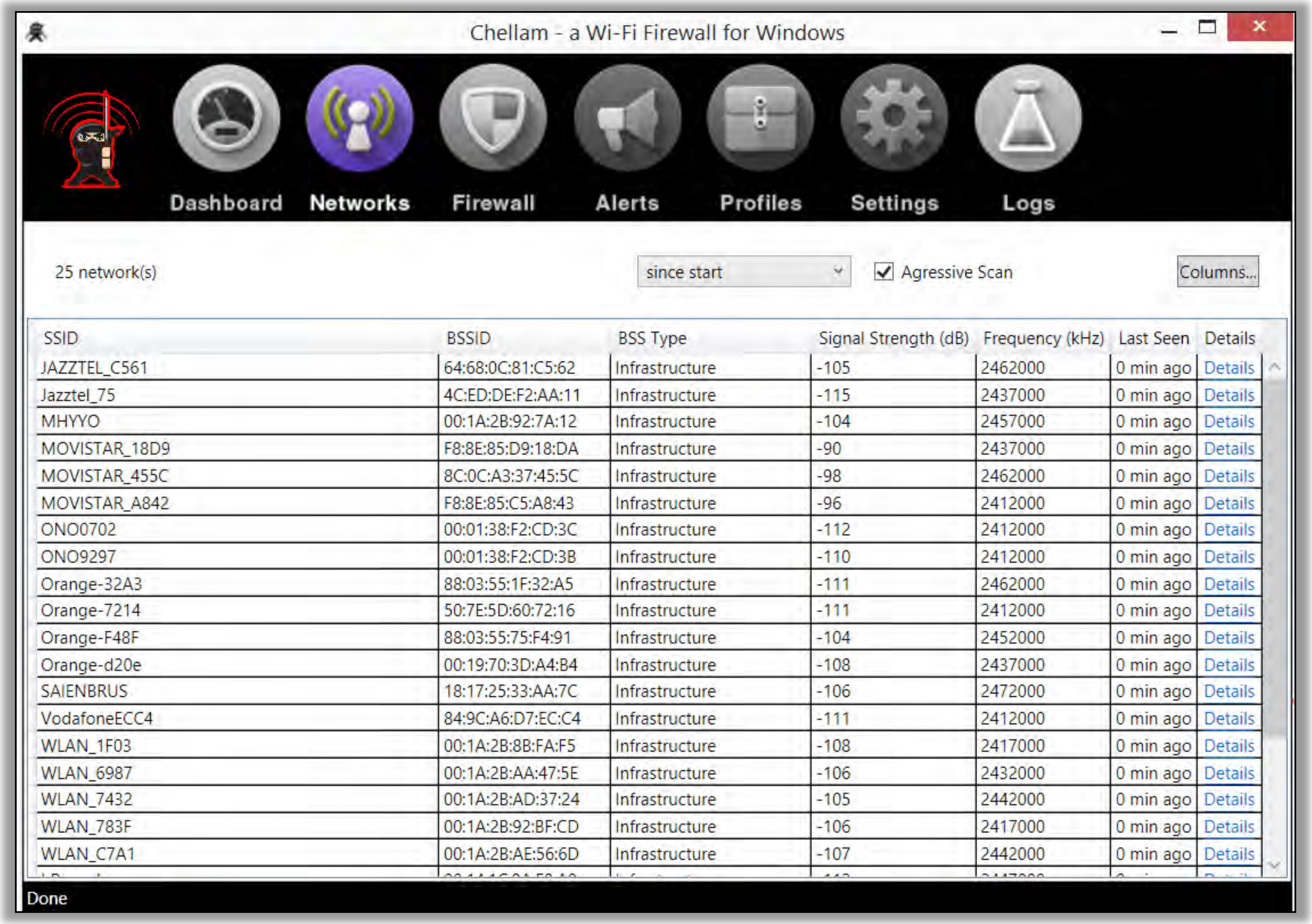
Analysis Engine

Rule Matching Engine

Data Storage

- Rules can be written to include:
  - BSSID
  - Neighboring Networks
  - Channel use patterns and frequencies
  - Information Elements in the Beacon / Probe Response
  - Access pattern based on time of day

Demo – Monitoring and Event Detection

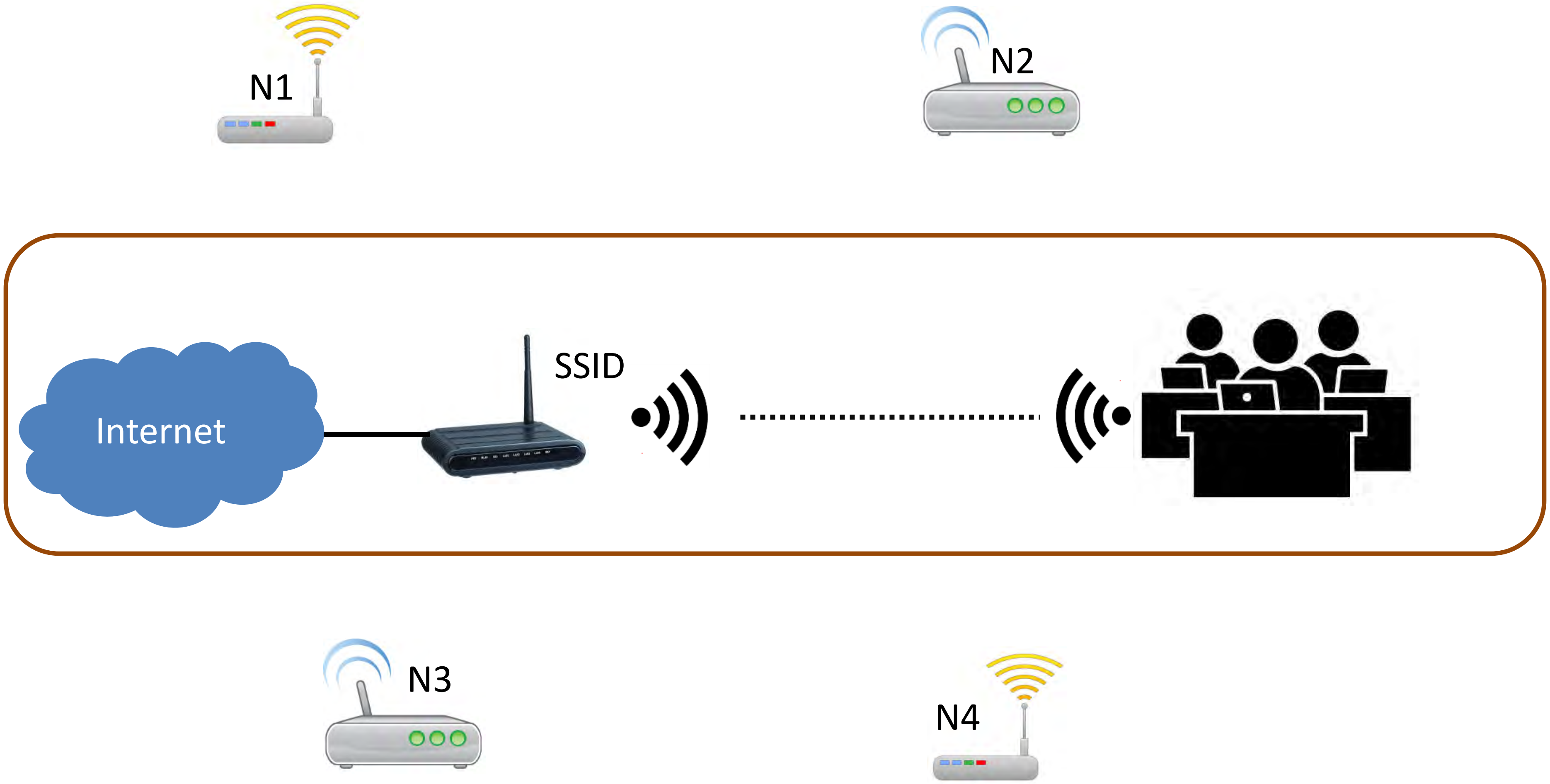


25 network(s)   since start   ☑ Agressive Scan   Columns...

SSID	BSSID	BSS Type	Signal Strength (dB)	Frequency (kHz)	Last Seen	Details
JAZZTEL_C561	64:68:0C:81:C5:62	Infrastructure	-105	2462000	0 min ago	Details
Jazztel_75	4C:ED:DE:F2:AA:11	Infrastructure	-115	2437000	0 min ago	Details
MHYYO	00:1A:2B:92:7A:12	Infrastructure	-104	2457000	0 min ago	Details
MOVISTAR_18D9	F8:8E:85:D9:18:DA	Infrastructure	-90	2437000	0 min ago	Details
MOVISTAR_455C	8C:0C:A3:37:45:5C	Infrastructure	-98	2462000	0 min ago	Details
MOVISTAR_A842	F8:8E:85:C5:A8:43	Infrastructure	-96	2412000	0 min ago	Details
ONO0702	00:01:38:F2:CD:3C	Infrastructure	-112	2412000	0 min ago	Details
ONO9297	00:01:38:F2:CD:3B	Infrastructure	-110	2412000	0 min ago	Details
Orange-32A3	88:03:55:1F:32:A5	Infrastructure	-111	2462000	0 min ago	Details
Orange-7214	50:7E:5D:60:72:16	Infrastructure	-111	2412000	0 min ago	Details
Orange-F48F	88:03:55:75:F4:91	Infrastructure	-104	2452000	0 min ago	Details
Orange-d20e	00:19:70:3D:A4:B4	Infrastructure	-108	2437000	0 min ago	Details
SAIENBRUS	18:17:25:33:AA:7C	Infrastructure	-106	2472000	0 min ago	Details
VodafoneECC4	84:9C:A6:D7:EC:C4	Infrastructure	-111	2412000	0 min ago	Details
WLAN_1F03	00:1A:2B:8B:FA:F5	Infrastructure	-108	2417000	0 min ago	Details
WLAN_6987	00:1A:2B:AA:47:5E	Infrastructure	-106	2432000	0 min ago	Details
WLAN_7432	00:1A:2B:AD:37:24	Infrastructure	-105	2442000	0 min ago	Details
WLAN_783F	00:1A:2B:92:BF:CD	Infrastructure	-106	2417000	0 min ago	Details
WLAN_C7A1	00:1A:2B:AE:56:6D	Infrastructure	-107	2442000	0 min ago	Details

Done

Understanding Attack Detection



©SecurityTube.net

Fingerprinting the Network

- BSSID(s)
- BSS type
- PHY type
- Beacon Interval
- Channel(s) & Hopping
- Rates – basic and extended
- Capability Information
- Information Element(s)

- Neighboring Access Points
- AP details as above

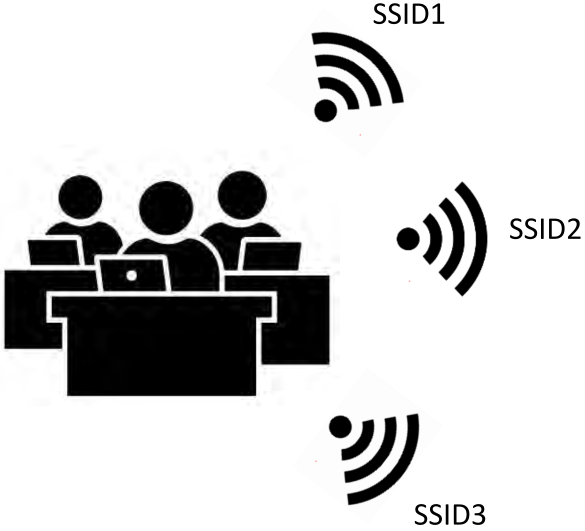
802.11 (pre connect)

- IP, Gateway
- DNS, ARP cache

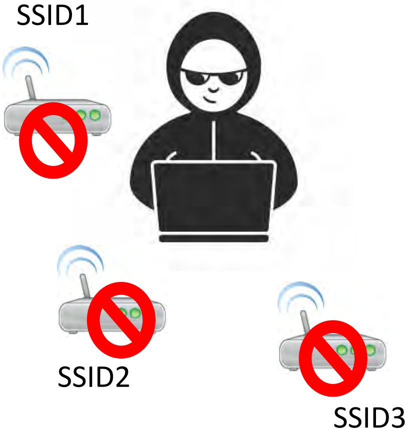
- Subnet scan
- OS and service scan

IP & Above (post connect)

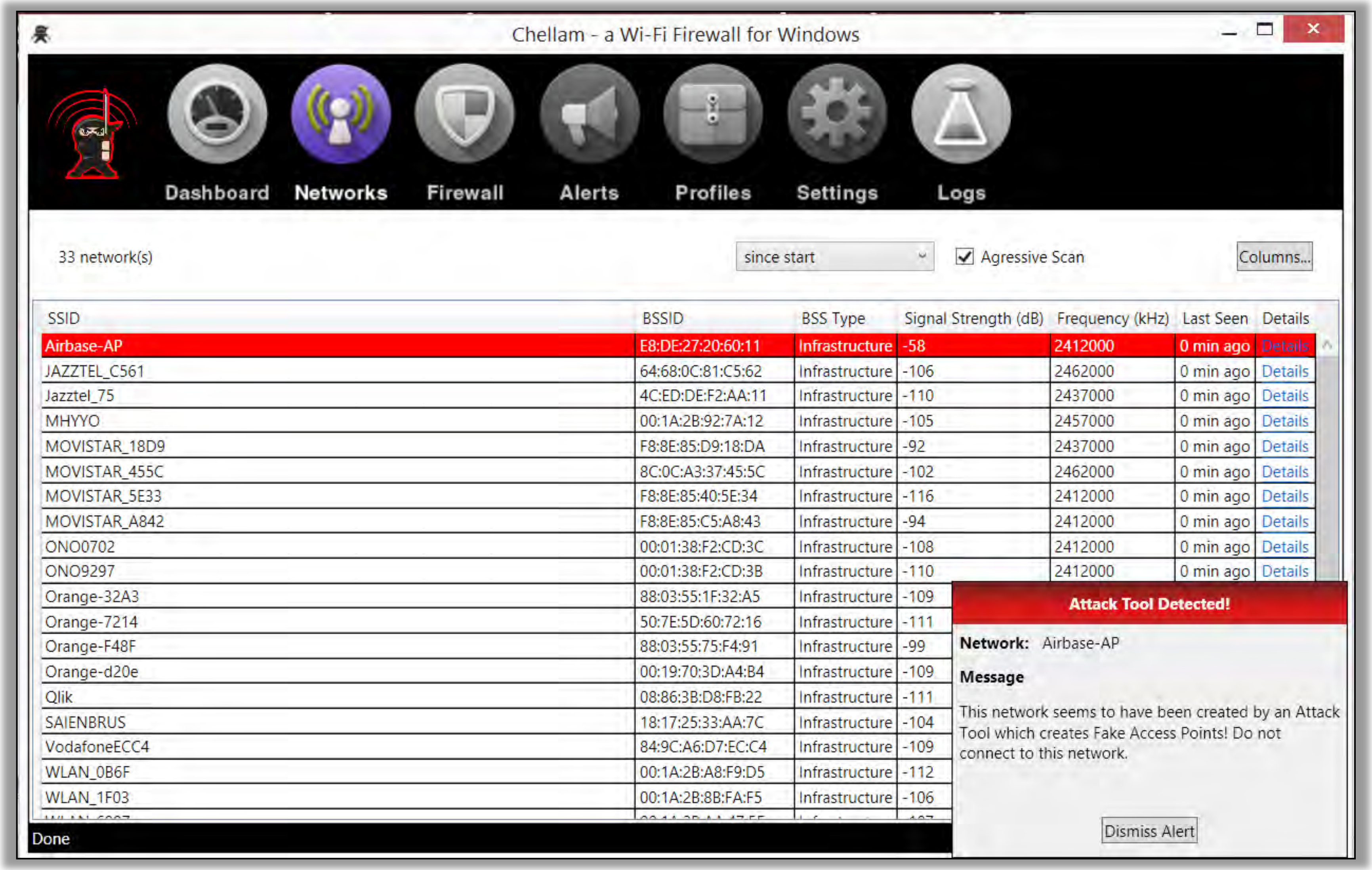
Typical Attack Mitigation



- BSSID(s)
- Channel(s) & Hopping
- Rates – basic and extended
- Capability Information
- Information Element(s)
- Neighboring Access Points
- AP details as above



Demo – Attack Tool Detection (Airbase)



33 network(s)

since start

☑ Agressive Scan

SSID	BSSID	BSS Type	Signal Strength (dB)	Frequency (kHz)	Last Seen	Details
Airbase-AP	E8:DE:27:20:60:11	Infrastructure	-58	2412000	0 min ago	Details
JAZZTEL_C561	64:68:0C:81:C5:62	Infrastructure	-106	2462000	0 min ago	Details
Jazztel_75	4C:ED:DE:F2:AA:11	Infrastructure	-110	2437000	0 min ago	Details
MHYYO	00:1A:2B:92:7A:12	Infrastructure	-105	2457000	0 min ago	Details
MOVISTAR_18D9	F8:8E:85:D9:18:DA	Infrastructure	-92	2437000	0 min ago	Details
MOVISTAR_455C	8C:0C:A3:37:45:5C	Infrastructure	-102	2462000	0 min ago	Details
MOVISTAR_5E33	F8:8E:85:40:5E:34	Infrastructure	-116	2412000	0 min ago	Details
MOVISTAR_A842	F8:8E:85:C5:A8:43	Infrastructure	-94	2412000	0 min ago	Details
ONO0702	00:01:38:F2:CD:3C	Infrastructure	-108	2412000	0 min ago	Details
ONO9297	00:01:38:F2:CD:3B	Infrastructure	-110	2412000	0 min ago	Details
Orange-32A3	88:03:55:1F:32:A5	Infrastructure	-109			
Orange-7214	50:7E:5D:60:72:16	Infrastructure	-111			
Orange-F48F	88:03:55:75:F4:91	Infrastructure	-99			
Orange-d20e	00:19:70:3D:A4:B4	Infrastructure	-109			
Qlik	08:86:3B:D8:FB:22	Infrastructure	-111			
SAIENBRUS	18:17:25:33:AA:7C	Infrastructure	-104			
VodafoneECC4	84:9C:A6:D7:EC:C4	Infrastructure	-109			
WLAN_0B6F	00:1A:2B:A8:F9:D5	Infrastructure	-112			
WLAN_1F03	00:1A:2B:8B:FA:F5	Infrastructure	-106			

Done

Attack Tool Detected!

Network: Airbase-AP

Message

This network seems to have been created by an Attack Tool which creates Fake Access Points! Do not connect to this network.

Why is this important?

- Attack tools will have to significantly improve
- Make it difficult to fingerprint
  - No hardcoded values, random BSSID etc.
- More features to mimic authorized networks
  - Ability to "clone" network beacons / probe responses
  - Ability to closely follow Clocks (timestamp)
  - Have to be on the right channel and band
- Very difficult to beat Whitelist approach

Roadmap - Enhancements

- Whitelist vs Blacklist
- Plugin Architecture
  - SQL with Python
- Intrusion Prevention / Firewall with custom Driver
- Assisted and automatic learning of whitelists
- Downloadable blacklists for attack tools

Questions?