TLS Canary

Keeping your dick pics safe(r)

US

- Evilrob
  - Rob Bathurst
  - Director for Healthcare/Biomedical Security
  - Cylance
- xaphan
  - Jeff Thomas
  - Plays with other people's computers
  - Is barely awake right now

"The good news is that there's no program named the 'dick pic' program. The bad news... they are still collecting everybody's information, including your dick pics."

-- Edward Snowden

Wouldn't we all?

(Please don't sue us, John.)

How the Tubes Work

- HTTP
  - Your data is not protected
    - Duh
      - I mean really
  - How your data is protected
    - HTTPS
    - Encryption suites

Tubes Part Two

- HTTPS
  - SSL
    - Where did it come from?
    - How does it work?
    - Why it's old and busted
  - TLS
    - New and Improved!
  - VPN
    - VPN everything?
    - End-to-End vs VPN
    - Difficulty

More Tubes!

- SSH
  - Does it blend?
- SFTP
  - Does it blend?
- DNSSEC
  - Does it blend?

Certificates

- WTF?
- How do they work?
- What do we do with them?
- What are Cert Chains?
- What is Cert Pinning?

WTF is this cert for?

- History
  - Secure Networking Program
  - Netscape
    - Dr. Taher Elgamal
    - SSL
  - RFC 6101
    - SSL 1.0
  - RFC 6176
    - TLS 1.2
  - TLS 1.3 (draft)

How does a cert work (basically)?

- It's all built on trust
  - It doesn't always work
  - And is broken
- Legit certs are signed by a trusted CA
- Our browsers trust anything signed by that root CA
  - You can't change that
- Sessions get negotiated by magic
- You send your dick pics through

What do we do with them?

- Literally anything related to identity
  - Device certs
  - User certs
  - Application certs
  - Oprah Style distribution
    - Certs for your mom!
    - Certs for your cat!
    - Certs for everyone!

Why This?

- Do we hate TLS?
  - Are you sure?
- VPNs suck
- Things we actually like
  - Ourselves
  - Some of you
  - Systems that are not built on blind trust

Chain of Fools

- I am trusted by the world
  - You trust me
  - You pay me money
  - I sign your cert
- Your cert is now trusted by anyone who trusts me
  - Which is everyone, because I'm in your root store doing root stuff
- You can now say you're whoever you asked to be
  - mail.google.com vs *.google.com

Pinning

- Conceptually how we should be doing all applications and sites
  - Trust this and this only
- Hard to configure
- Implementation varies
  - Google HSTS
- Hong Kong Post Office cannot issue a cert for your SendDickPicsToEveryone application
  - App only trusts that app cert signed by you

Interception

- Cue scary music!
- iOS trusts about 226
  - Does not ask you if it's ok
- HTTPS breakdown
  - MiTM

Interception

- Abnormal “Secure” Communication
  - Legal stuff
    - Work machines
    - Load balancers
    - .gov request
  - Not so good (but maybe secretly legal)
    - .gov demand
    - Criminals (see previous)
    - Advertisers

MiTM Demo

TLSCanary

- Our goals
  - Protecting your dick pics from bored analysts
  - User awareness
  - Stopping shady shit
- What the tool does
  - Cert Diff
  - In-plugin cert pinning
  - Root certificate audit
  - Let you know some bad shit may be happening

TLSCanary

- What it doesn't do
  - Protect you from a compromised site
  - Protect you from hijacked
  - Protect your dick pics at rest

TLSCanary Network

- Dead Birds everywhere
  - Global network
- Scalable
- How it works
  - A site presents a TLS cert to you
  - You send the cert chain to TLSCanary
  - TLSCanary grabs the site's cert chain
  - TLSCanary reports the diff result to you

TLSCanary Demo

Why Use TLSCanary

- It’s designed to help you have greater awareness
- We do not cache request data
- It’s lightweight
- We value the safety of your dick pics
- Why not?
  - Really, bro.
    - Use it.

Why Not to Use it?

- No reason I can think of.
- Unless you don’t trust us?
- You shouldn’t trust us.

Where to Find TLSCanary?

- https://tlscanary.com

How to Contribute

- https://github.com/tls-canary

~~Beer~~ Scotch and Questions