HTTPS://

Decrypting the Mystery

Slides: https://Cipafilter.com/brainstorm2019

Chris Cooper

Senior Network Engineer
Cipafilter

- Firewall &
  Content Filtering
  - Specialize in K-12

- Product Development
- Network Investigations
- Protocol Compatibility

HTTPS / SSL / TLS

Now, with 20% more acronyms!

HTTPS / SSL / TLS

What is HTTPS?
HTTPS is standard Hypertext Transport Protocol (HTTP), tunneled inside SSL/TLS.

What is SSL/TLS?
Security protocol designed to protect communication 3 ways:

1. Privacy
    - Stop passive snooping
2. Integrity
    - Stop tampering
3. Authentication
    - Stop interception
    - Requires 3rd party assistance

HTTPS / SSL / TLS

What's the difference between SSL and TLS? I hear people say both.

Secure Socket Layer (SSL)

- Created by Netscape in 1995
- SSL 2.0 / 3.0
- Deprecated in 2015

Transport Layer Security (TLS)

- IETF successor to SSL
- TLS 1.0 is standardized SSL 3.0
- TLS 1.0 / 1.1 / 1.2 / 1.3
- Still trying to shake the SSL nickname

While TLS is technically correct, the industry uses both interchangeably

HTTPS / SSL / TLS

Encryption gets complicated quickly

- Multiple types of encryption used
  - Certificate type (RSA, ECDSA)
  - Key exchange (RSA, DH, ECDHE)
  - Block cipher (AES, CHACHA20)
  - Message authentication (MD5, SHA256)
- 300+ valid cipher suites
  - Supported suites change with SSL/TLS version
- Client and server must negotiate which to use
  - Compatibility is a challenge
  - Can’t negotiate trust

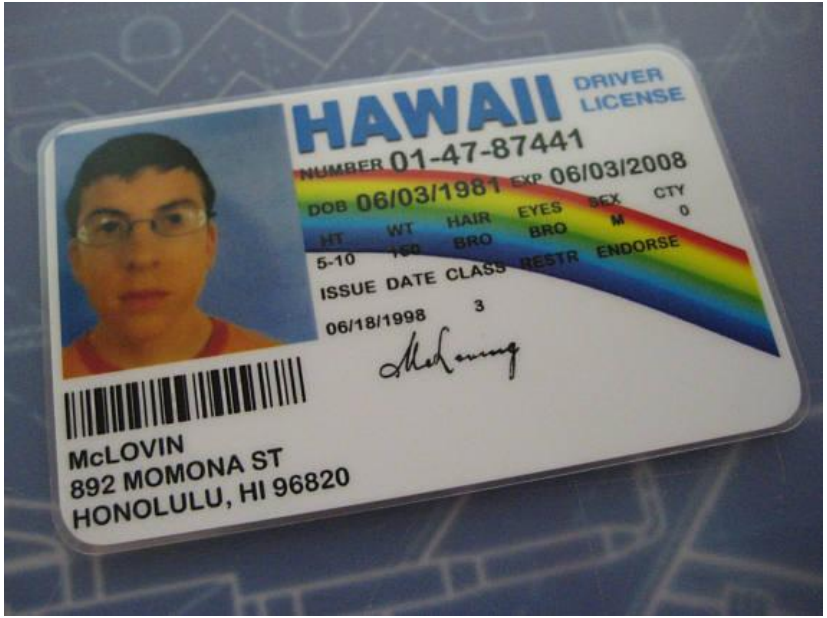
Chain of Trust

How do you trust someone you've never met?

Chain of Trust

How do you prove identity to a stranger?

- Trusted 3rd party verifies identity
  - Certificate authority
- Provides tamper-resistant proof
  - Digital signature on certificate
- Intermediates create chains of trust
  - Server provides whole chain



Chain of Trust

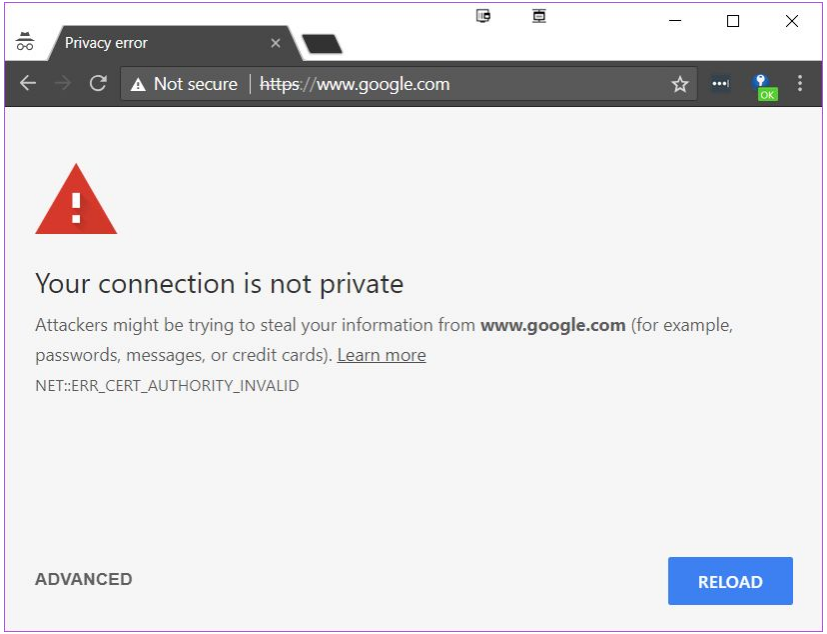
What about fake certificates?

- 200+ Root certificate authorities
  - 1000+ intermediates
- Any CA signature is valid
  - Only takes 1 bad apple
  - Startcom, TurkTrust, Symantec
- Solution: Certificate Pinning
  - Limits cert to CA / intermediate

Chain of Trust

Certificate Pinning

- Application hard-codes certs
  - Pinning is per application
- All operating systems
  - Chrome / Firefox for select sites
  - Desktop apps: Dropbox
  - Android / iOS: Twitter
- Users can not click through warnings



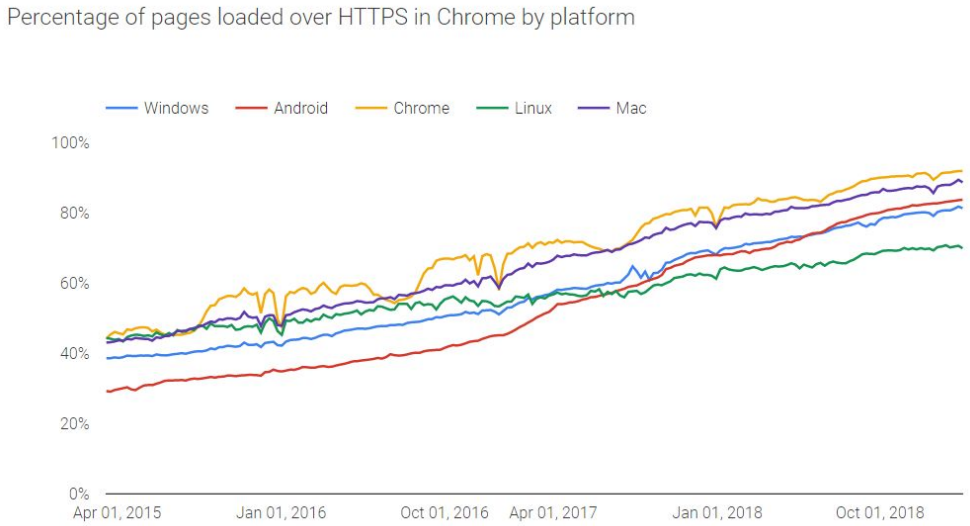
Why Is SSL Decryption Important?

Why Is SSL Decryption Important?

85% of traffic is now encrypted
Up from 66% in 2017, 53% in 2016

95% of Google traffic is encrypted
100% for Search, Mail, and Drive

Encryption is increasing
Let's Encrypt made it free & easy
Google Search prefers encrypted sites



Chrome 70 is increasing "Not secure" flag for HTTP sites

Source: https://transparencyreport.google.com/https/overview

Why Is SSL Decryption Important?

Encrypted

- Full URL
  - https://sites.google.com/site/newgames/
- Content
  - Keywords & Search terms
- Malware
  - Phishing sites
  - Viruses

Not Encrypted

- Destination IP address
  - Many sites can use same IP
- Names on Certificate
  - Hundreds of Alt-names
- Hostname
  - Server Name Indication
  - Proxy protocol
  - https://sites.google.com/

SSL/TLS Decryption

How to break the unbreakable

SSL/TLS Decryption

Decrypting SSL/TLS violates the core design principles of SSL/TLS

- **There is no “it just works”**
- **Good intentioned tools can be abused**
  - **Web filters**
  - **Snooping ISP**
  - **Malicious hackers**
  - **Foreign governments**

Compliance from the client is required

- **Capture data outside of encryption**
- **Intercept and break encryption (Man-in-the-Middle)**

SSL/TLS Decryption

Capturing data outside decryption

- Must be done on per-application basis
- Each application needs to support it
    - Chrome Extensions
- Non-supported apps are undetected
    - Opt-in detection
    - Filtering is controlled by the client

Use Cases:

- Good for Chromebooks without Google Play Store
- Poor for Windows, Mac, Android, iPad

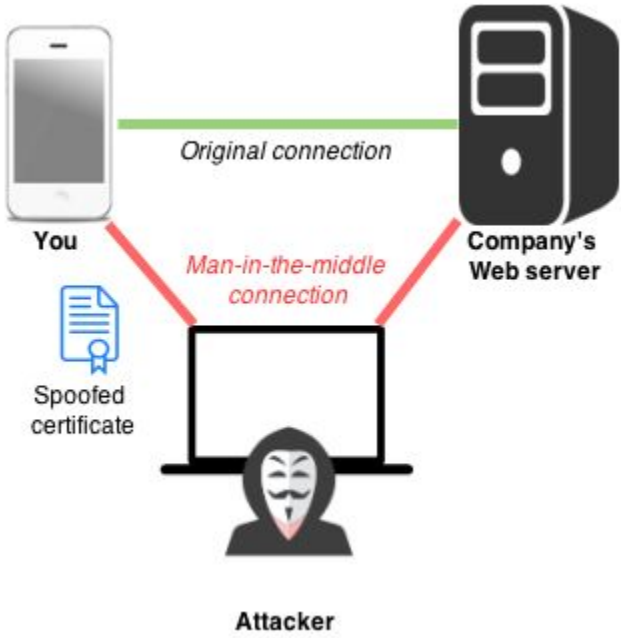
SSL/TLS Decryption

Breaking encryption

- Must be in the middle of the connection
  - In-line
  - DNS
  - Proxy / PAC
- Clients must trust certificates
  - Trust certificate authority
- Unsupported clients get warnings

Use cases:

- Works equally with anything that can install a new root certificate authority
  - Deploy tools built in



Common Issues

There’s always a catch...

Common Issues

Certificate Pinning

- Per app issue
- Some disable for User CA
  - Chrome

Suggestions

- Use website version
- Exempt sites
- Contact app manufacturer

Can’t Install Certificate

- Embedded devices
  - Printers
  - Payment Systems

Suggestions

- Contact Manufacturer
- Exempt sites
- Exempt Device

Common Issues

Independent Certificate Store

- Browser ignores system store
  - Firefox
  - iOS Chrome < M48

Suggestions

- Independently install cert
- Contact manufacturer

User Certificate Store

- Each user needs to trust CA
- System processes don’t trust CA
  - Windows Updates
  - Chromebook Logins

Suggestions

- Install as System when possible
- Exempt sites from decryption

Common Issues

BYOD

- Each user needs to trust CA
- Android requires PIN / Lock
- User support

Suggestions

- Policy
- Different filtering rules
  - Segment network

Protocol Compatibility

- Hard to troubleshoot
- Very new protocols
- Very old devices

Suggestions

- Update firmware
- Contact manufacturer(s)
- Exempt sites
- Exempt device

Tips for Success

Tips for Success

- Deploy root CA early
  - Decrypt single test site
- Learn your tools
  - Know how to exempt single sites / devices
  - Check for compatibility lists
- Prepare your policy
  - Workflow when problems occur
  - What exceptions will be made?
- Go slow
  - Decrypt few non-critical sites
  - One group at a time
- Work with your vendor
  - They have experience

Questions?

Slides: https://Cipafilter.com/brainstorm2019