

Chrome Security Special Sauce

A few of the key ingredients in the Chrome browser that help keep you safe on the web.

Disclaimers

- I'm not a developer.
- This talk will not make you a better developer.
- This is the first time I'm giving this...



Chrome's Core Principles



Speed, Simplicity, Security



Chrome's Core Principles



Everyone is
responsible for
this stuff...

Speed, Simplicity, Security

Chrome Security Team

- 20+ full-time engineers
- Design and implement security features
- Find (and fix) security bugs
- Vulnerability response
- Whatever else!

but some people get
to obsess about it.



Browser Security?

- Internet crime... it ain't just a fad.
- Everyone uses a browser (all day, every day)!
- Attacker has easy, remote access.
- Browser software is hard to secure.
 - Millions of lines of security-critical code
 - Constantly changing
 - Huge exposure to untrusted content



Top Threats on the Web

- **Browser Exploits**
- **Phishing & Malware Sites**
- **Attacks to SSL**

Browser Exploits

Malicious code that aims to achieve remote code execution on victim's computer by exploiting a security bug in the browser.

Common Targets

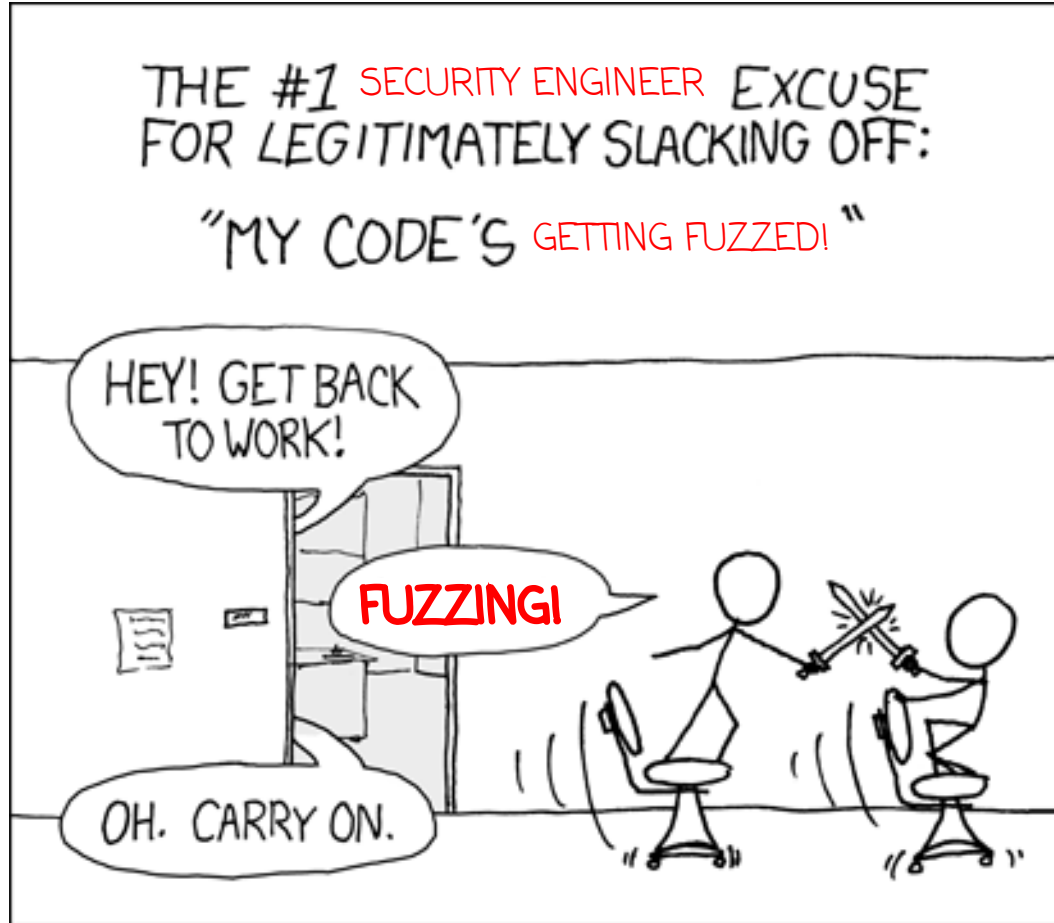
- Browser code
- Plugins! (E.g. Flash, PDF, Quicktime, Java)

Counterthreat

Step 1: Find and fix security bugs. Update users.

Step 2: Acknowledge the reality of bugs. Build defense in depth.

1. Find Bugs via Fuzzing



Fuzzing

Basic Idea

```
while true; do  
    dd if=/dev/urandom bs=1024 count=1 | /path/to/Chrome  
done;
```

Optimizations

- **Code coverage** : more LOCs, more bugs!
- **Performance**: fastest fuzzer wins! (2000+ cores)
- **Reproducibility**: gotta reproduce those crashes.
- **Test case creation**: mutation vs. generation.

Fuzzing

Targets

- Chromium code
- third_party code (Foxit PDF reader, ffmpeg, Little CMS, libexif, and many more...)
- third party binaries too! (Flash, Adobe Reader)

2. Pay for Bugs

Jan 2010: Launched Chrome Vulnerability Reward Program; Pay out \$500 - \$1337 for bugs.

July 2010: Top reward increased to \$3133.7!

Nov. 2010: Launched Web VRP

Feb 2012: Scope expanded to Chrome OS (Linux kernel, Flash, ...) plus bonuses for fixes.

Aug 2012: More bonuses, top reward of \$10,000+, more flexibility to focus on exploitability

Aug 2013: \$5,000 for common class of reports.

3. Pay for Exploits

Feb 2011: Google sponsors \$20,000 top-up reward for Chrome at Pwn2Own 2011

March 2012: Pwnium 1

Oct 2012: Pwnium 2

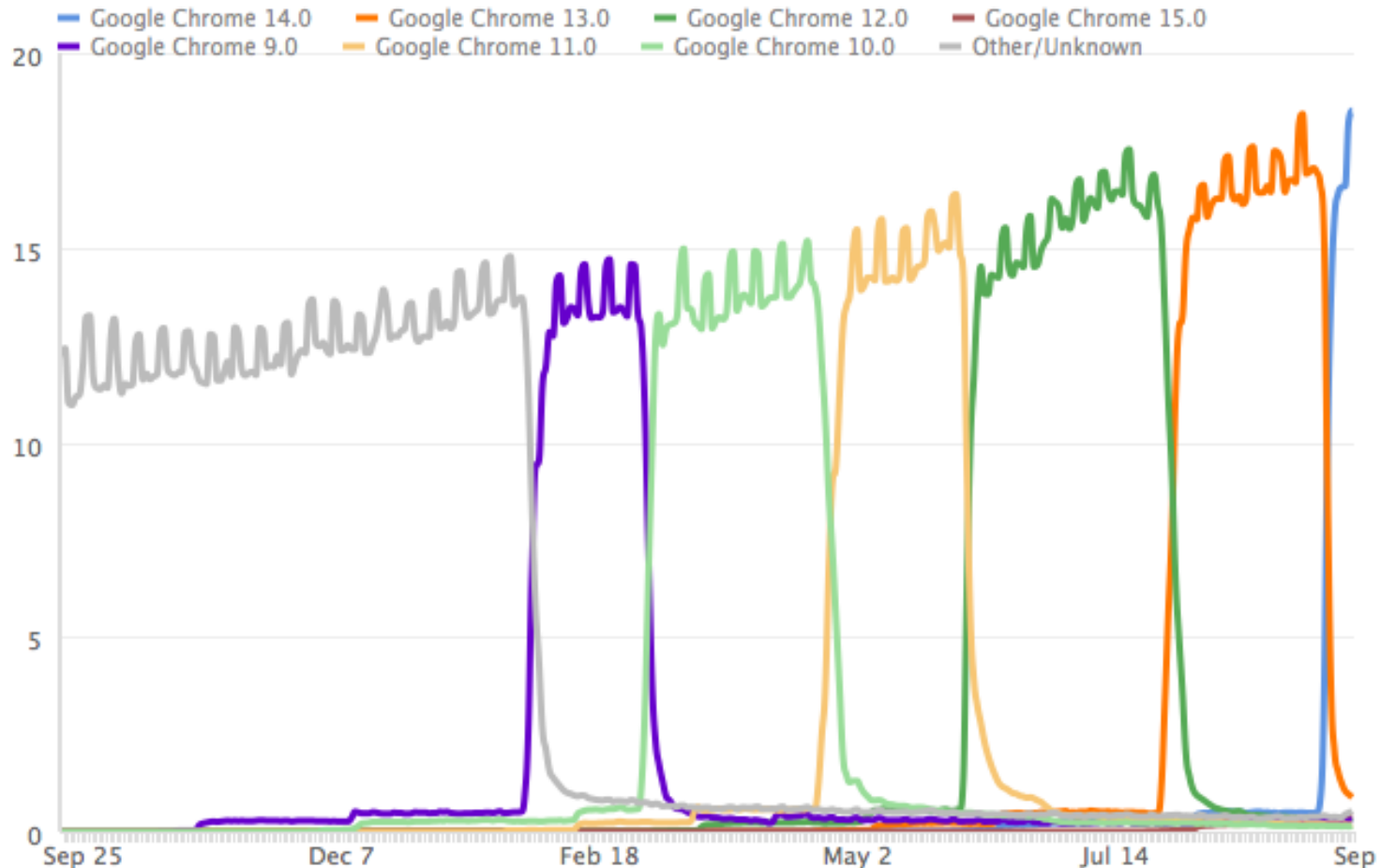
March 2013: Pwnium 3 and Pwn2Own

November 2013: Mobile Pwn2Own

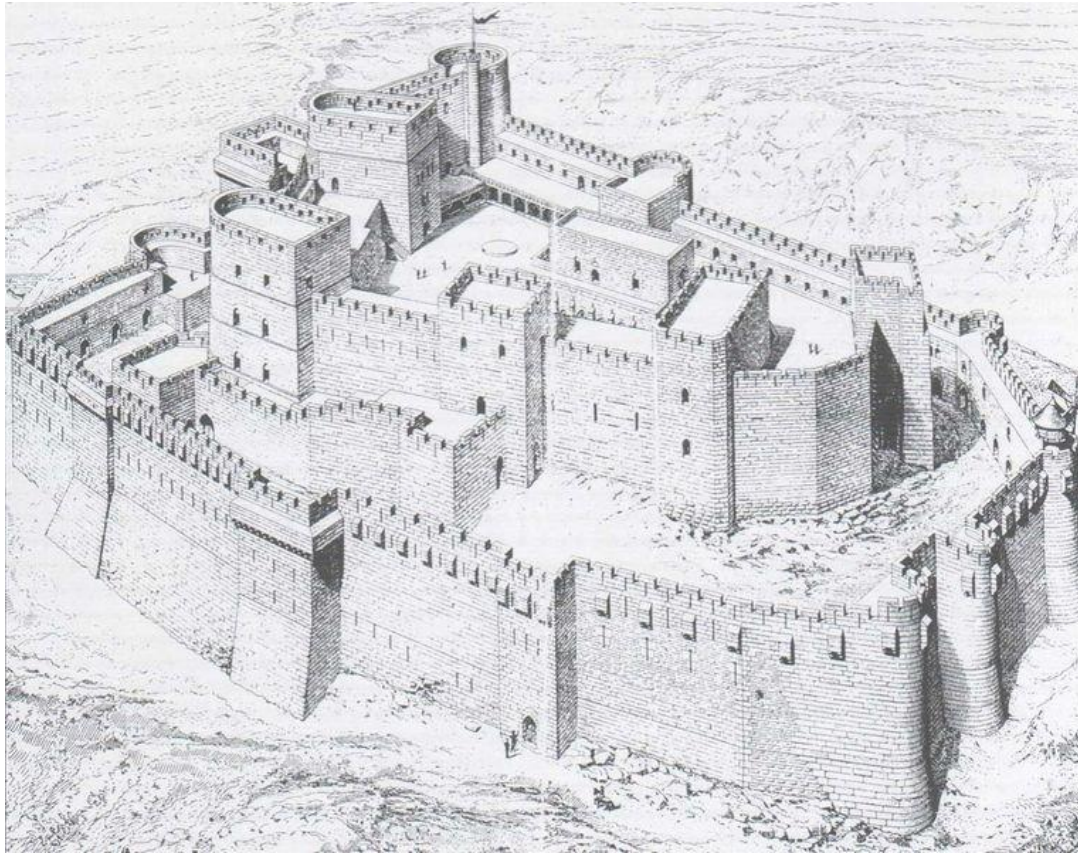


Pinkie Pie has won \$60K, \$60k, \$40K across Pwniums...

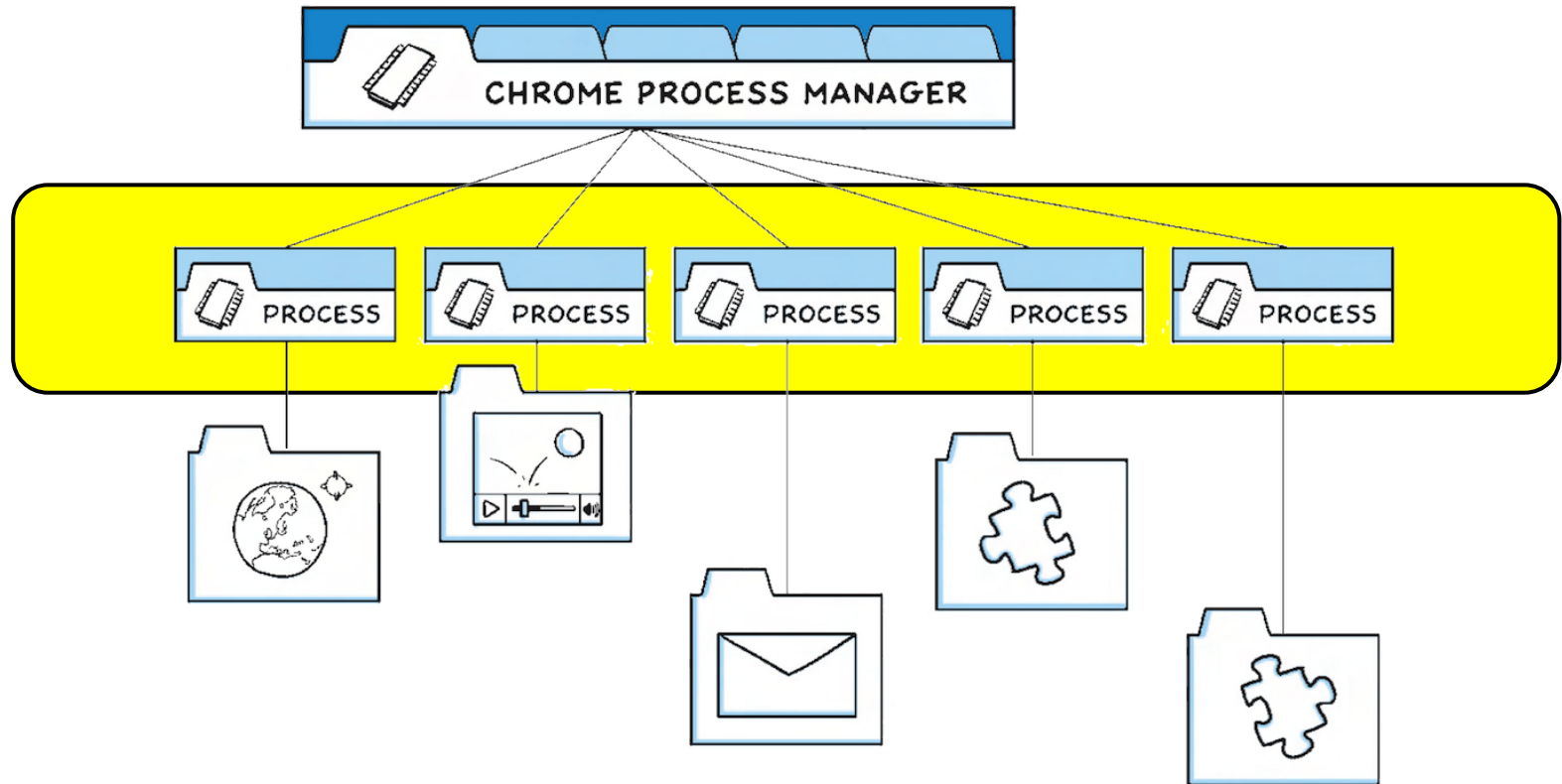
Fix Bugs, Update Users. Fast.



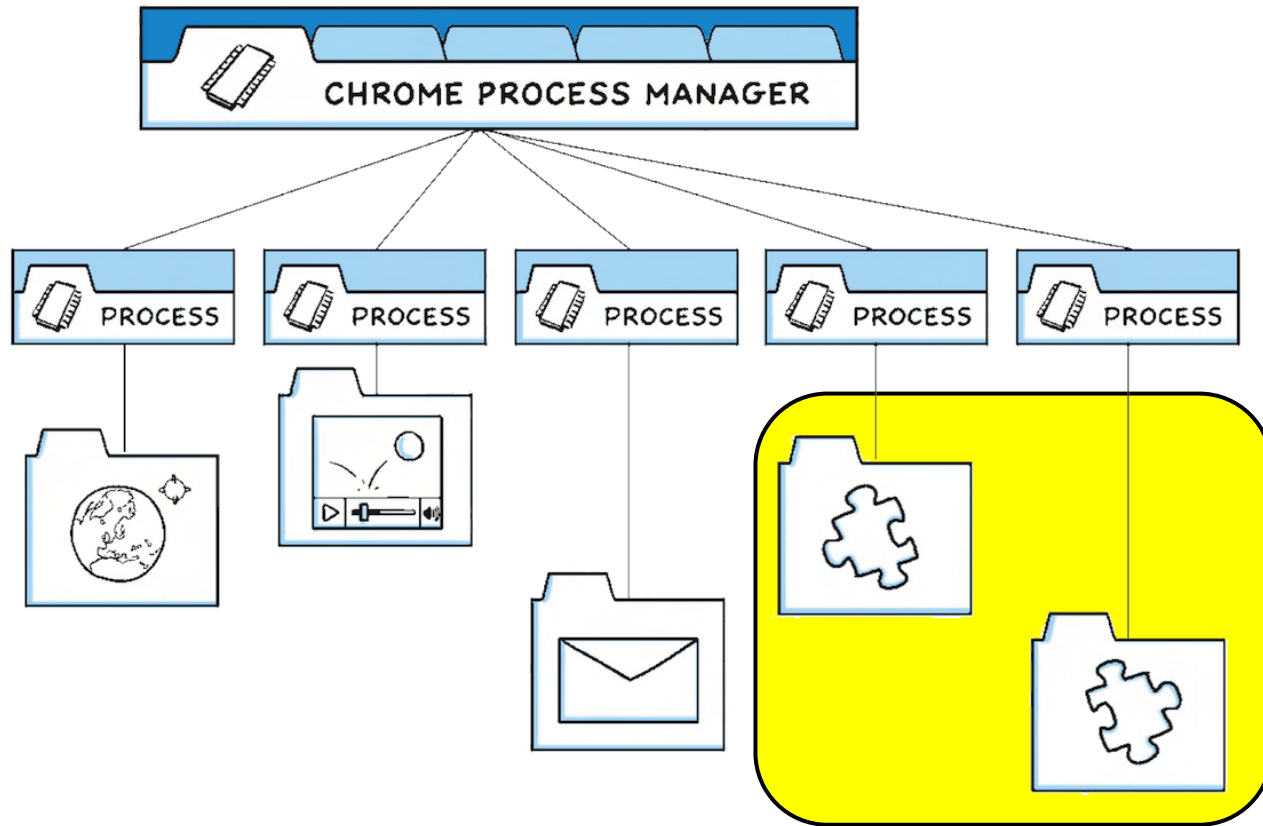
Defense in Depth



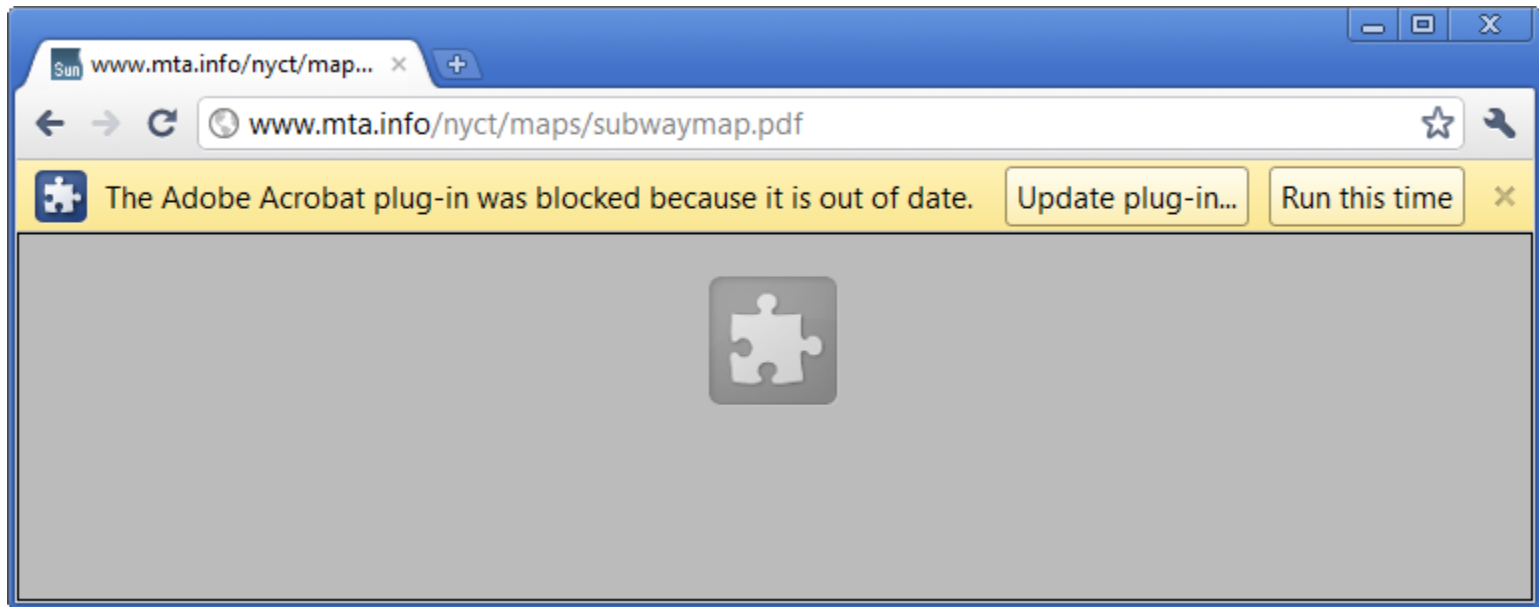
Process Sandboxing



Plugin Sandboxing



Plugin Blocking



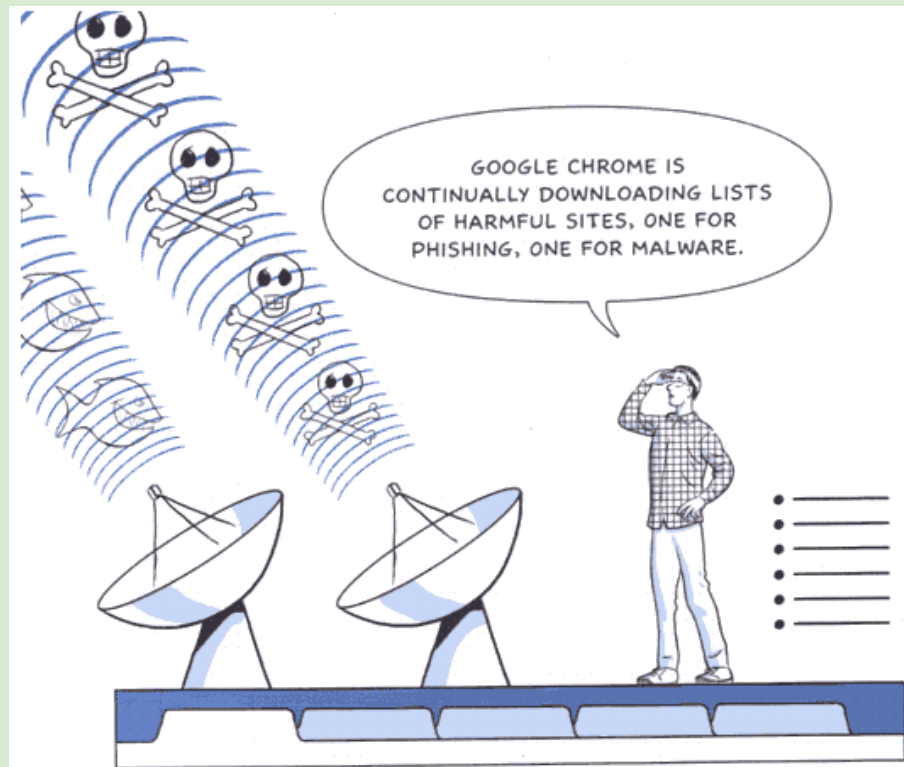
Phishing & Malware Sites

Get a user to visit or load a malicious website that either (a) phishes their personal data or (b) delivers some malicious payload (e.g. malware).

Methods:


- **Socially engineer someone to click on a link.**
- **Compromise a popular site people already visit.**

Counterthreat



Safe Browsing

Block Badness


 chrome

The Website Ahead Contains Malware!

Google Chrome has blocked access to _____ for now.

Even if you have visited this website safely in the past, visiting it now is very likely to infect your Mac with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. [Learn more](#)

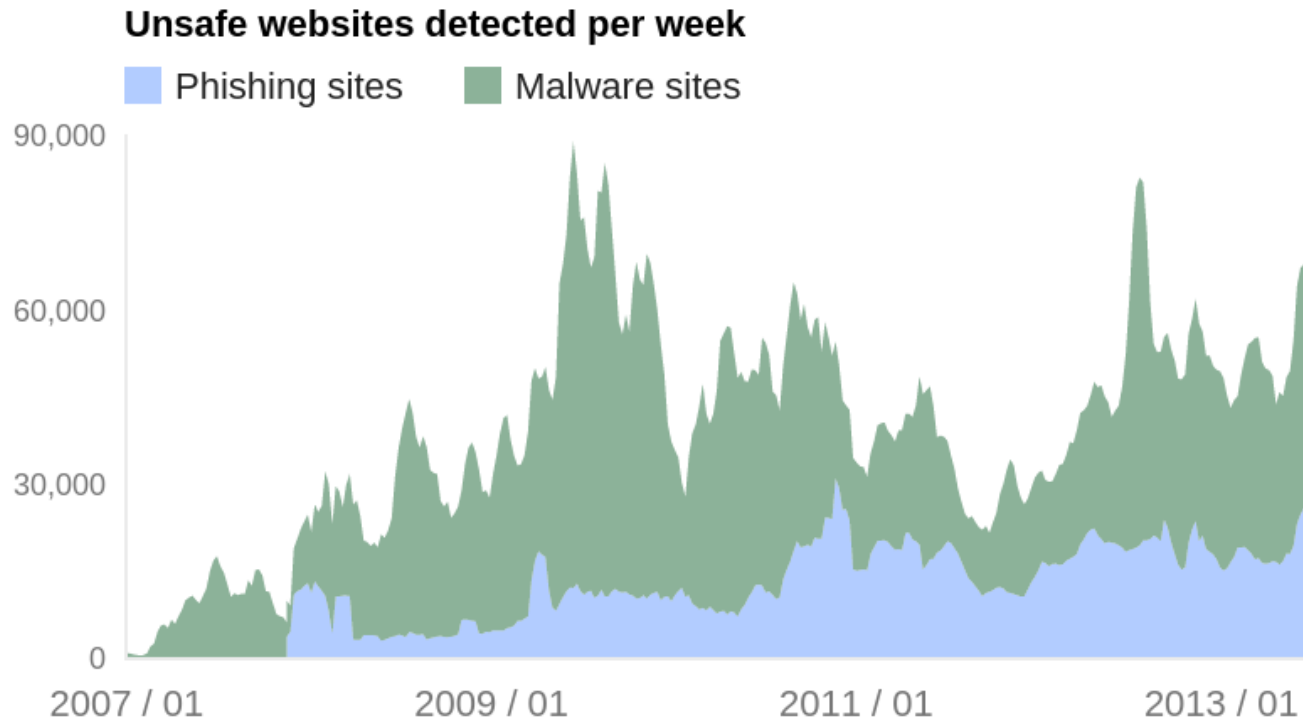


[Go back](#) [Advanced](#)

☐ Improve malware detection by sending additional data to Google when I encounter warnings like this. [Privacy policy](#)

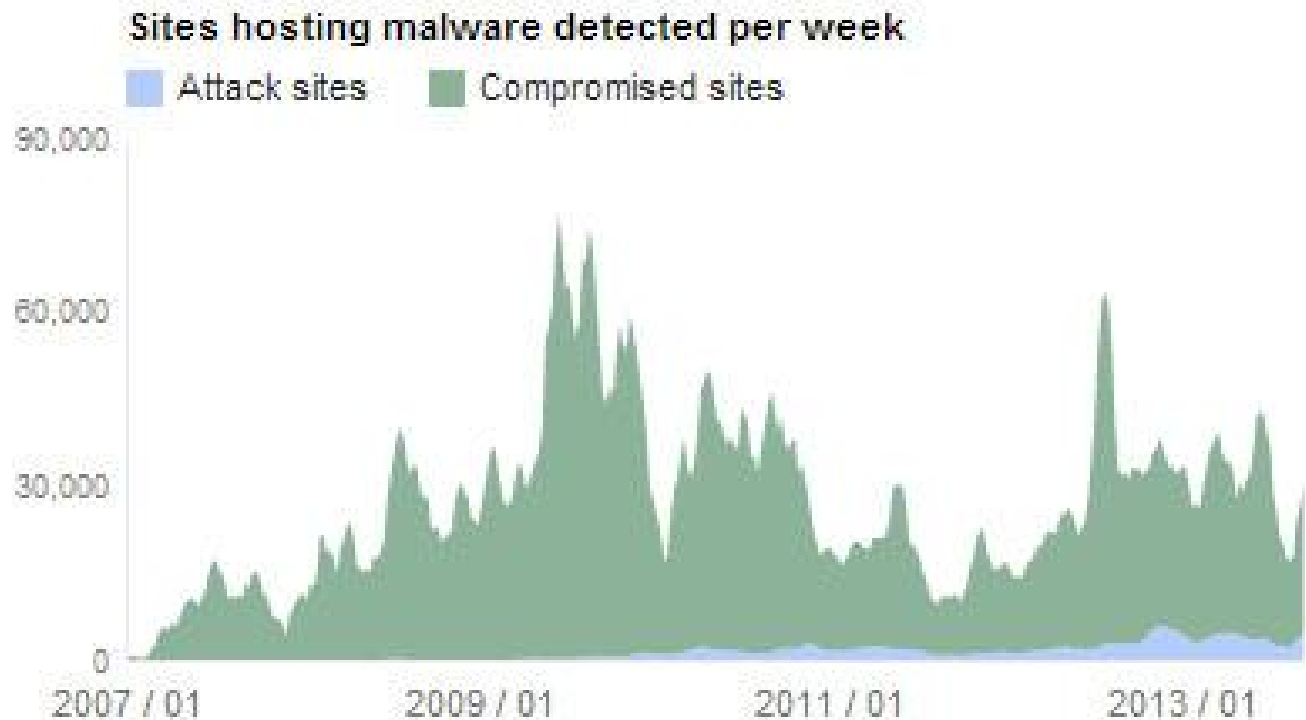


Find Badness



<http://www.google.com/transparencyreport/safebrowsing>

Notify of Badness



<http://www.google.com/transparencyreport/safebrowsing>

Attacks to SSL

Violate the security and privacy guarantees of SSL to steal user information.

Methods:

- **Exploit flaws in SSL implementation**
- **Exploit the Certificate Authority trust chain**

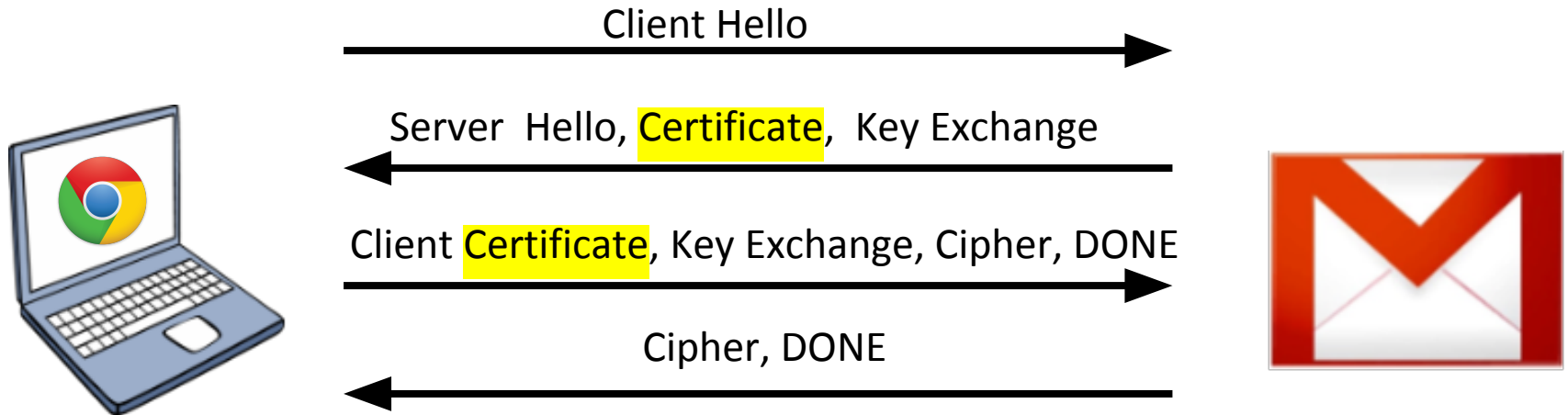
Gimme some SSL!



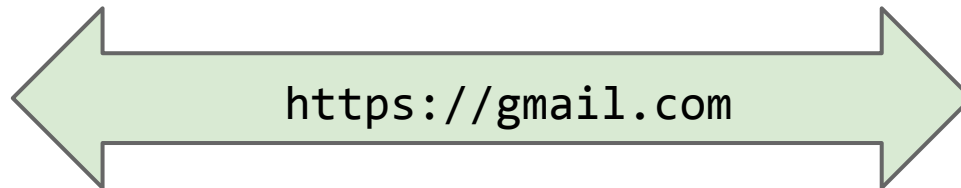
`https://gmail.com`



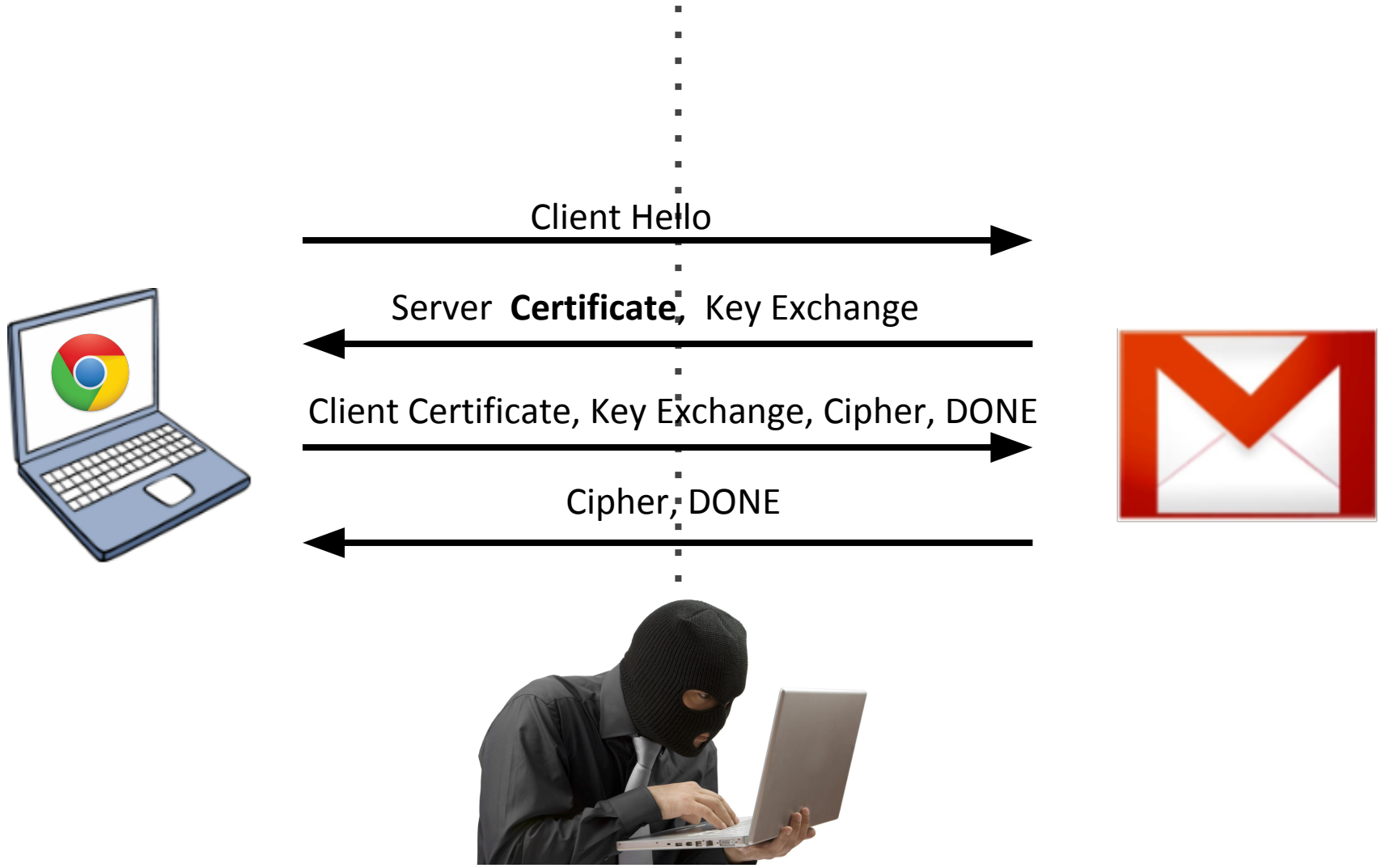
SSL Protocol Handshake



SSL Protocol Handshake



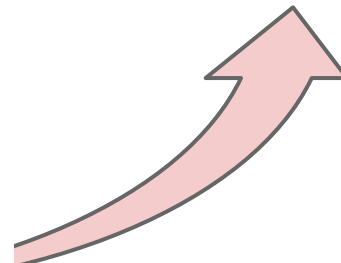
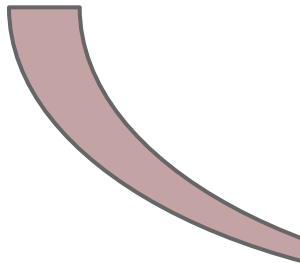
Man-in-the-Middle Attack



SSL Protocol Handshake



`https://gmail.com???`



Certificate Pinning

Chrome comes pre-loaded with the certificates it expects to see for Google-owned websites, and if it does not see one of those when it visits a Google-owned website, it shows an error page to the user and will not let the user continue.

Certificate Pinning FTW!

“Today we received **reports of attempted SSL man-in-the-middle (MITM) attacks against Google users**, whereby someone tried to get between them and encrypted Google services. The people affected were primarily located in Iran. The attacker used a fraudulent SSL certificate issued by DigiNotar, a root certificate authority that should not issue certificates for Google (and has since revoked it).” - August 2011

HTTP Strict Transport Security

```
HTTP 1.1 301 Moved Permanently
```

```
...
```

```
Strict-Transport-Security: max-  
age=31536000; includeSubDomains
```

```
...
```

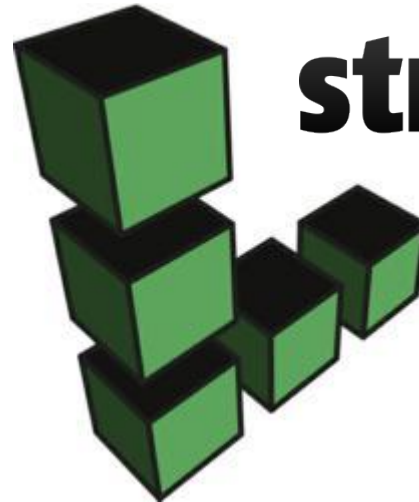
HTTP Header

HSTS Whitelisted Services



*PayPal*TM

Google



stripe

Only contact us
over HTTPS!

OK!



Closing Thoughts

Browser security matters. It should be a factor in choosing the software you use.

Chrome does some neat things to combat current security threats.

I'm hungry. Let's lunch! (Feedback welcome.)

Questions? Complaints?

**parisa@{google.com, chromium.org}
@laparisa**

www.chromium.org/Home/chromium-security