What's Happening in **TLS**?

Mark Nottingham, 

@mnot

John Allsopp
@johnallsopp

#heartbleeding? Come hear two of the worlds leading web security experts @mnot and @creativemisuse at Code melbourne. webdirections.org/code14/

Reply Retweet Favorite More

RETWEETS	FAVORITE
6	1

9:53 AM - 10 Apr 2014

Mark Nottingham
@mnot

@johnallsopp Oh, I am so not a “leading security expert” — I just drink with some of them :)

Reply Delete Favorite ••• More

10:01 AM - 10 Apr 2014

John Allsopp
@johnallsopp

@mnot that'll do ;-)

Reply Retweet Favorite More

10:09 AM - 10 Apr 2014

http://lmgtfy.com/?q=heartbleed

: Some Lessons Learned

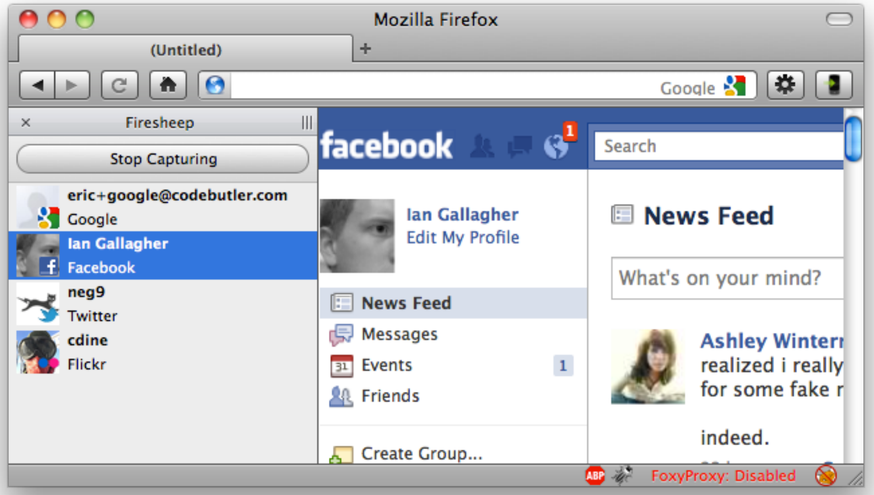
- TLS is wicked complex
- Dangerously close to a monoculture (OpenSSL)
- Open Source is not magical (but it’s not the problem here)
- Incident handling is really important
  - Assume compromised keys / infrastructure

Recent Goals in the TLS Community

1. More **TLS**
2. Better **Trust**
3. More **Speed**

More TLS

http://tools.ietf.org/html/draft-farrell-perpass-attack/


Mozilla Firefox
(Untitled)
Google
Firesheep
Stop Capturing
eric+google@codebutler.com
Google
Ian Gallagher
Facebook
neg9
Twitter
cdine
Flickr
facebook
Search
Ian Gallagher
Edit My Profile
News Feed
Messages
Events
1
Friends
Create Group...
News Feed
What's on your mind?
Ashley Winter
realized i really
for some fake r
indeed.
FoxyProxy: Disabled


Google™
Street View

More TLS: HTTP/2

- HTTP/2 doesn't *require* TLS, but Firefox and Chrome engineers say: "**We will only support HTTP/2 over TLS**."
- They position this as a "carrot."
- Network operators aren't happy about this

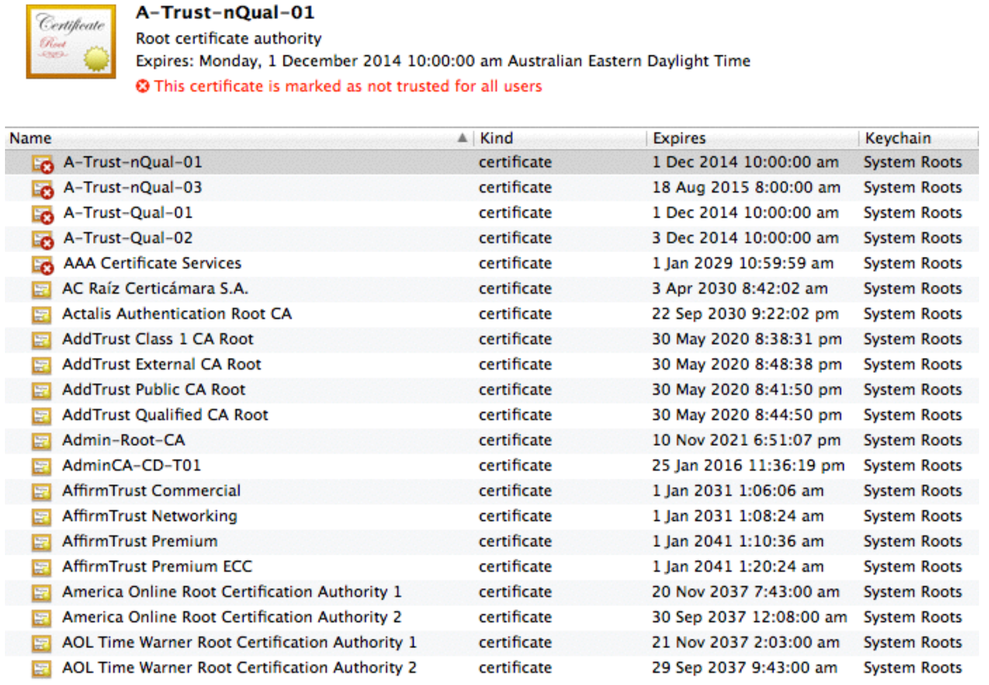
IE	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Blackberry Browser	IE Mobile
11.0	28.0	34.0	7.0	20.0	7.0	5.0-7.0	4.4	10.0	10.0

http://http2.github.io/

HTTP:// over TLS

- Mozilla is interested in **transparently** using TLS for http:// URIs
  - No change in security context, browser UI
  - Makes protocol upgrades easier
  - Defeats purely **passive** attacks
- This is controversial; some feel it “cheapens” TLS

Better Trust



http://nakedsecurity.sophos.com/2013/01/08/the-turktrust-ssl-certificate-fiasco-what-happened-and-what-happens-next/

http://www.secureworks.com/cyber-threat-intelligence/threats/transitive-trust/

Http **S**trict **T**ransport **S**ecurity

```
Strict-Transport-Security: max-age=7776000
```

- “I’m only available over HTTPS. Don’t let users click through errors.”
  - Can include subdomains
  - Talk to browsers about “preloading”

IE	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Blackberry Browser	IE Mobile
11.0	28.0	34.0	7.0	20.0	7.0	5.0-7.0	4.4	10.0	10.0

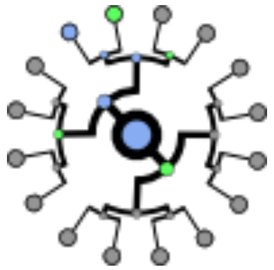
http://tools.ietf.org/html/rfc6797

Public-Key-Pins

```
Public-Key-Pins: max-age=31536000;
        pin-sha1="4n972HfV354KP560yw4uqe/baXc=";
        pin-sha256="LPJNul+wow4m6DsqxbninhsWHlwfp0JecwQzYpOLmCQ="
```

- “Pins” specific certs in the browser to avoid Rogue CAs
- May or may not catch MITMs
- Risk of locking your users out of your site; be careful…

http://tools.ietf.org/html/draft-ietf-websec-key-pinning



Certificate Transparency

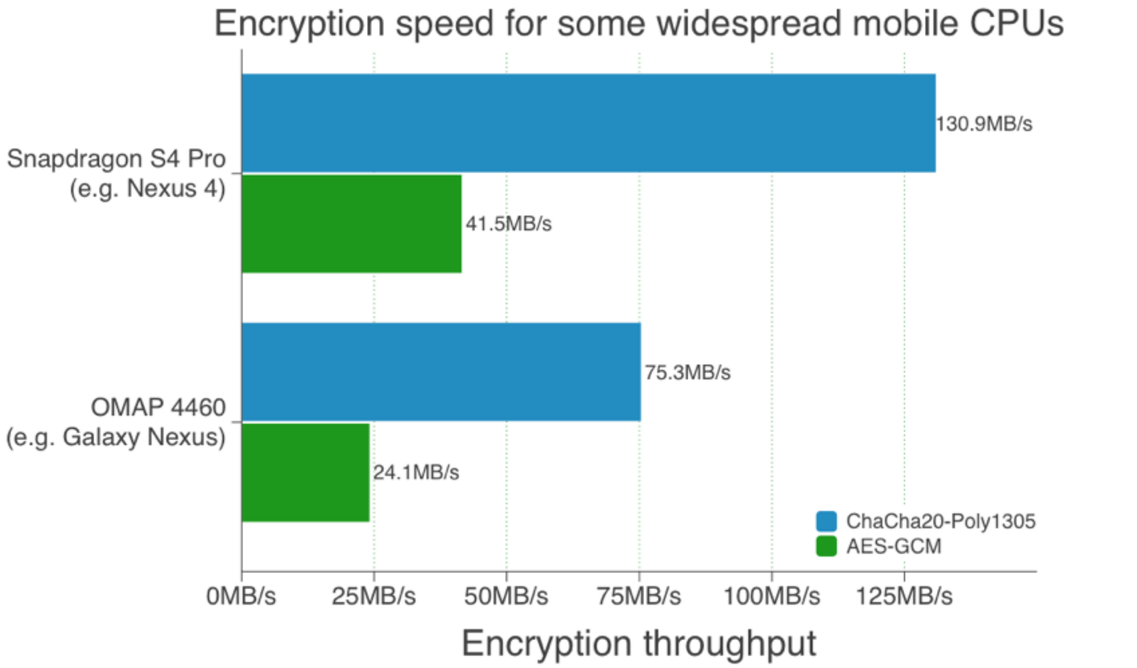
- “Notaries” as public cryptographic logs of CA activity
- Logs can then be monitored for rogue CAs
- Browsers can audit specific certs to make sure they show up in logs
  - Chrome will require for EV certs soon

http://www.certificate-transparency.org/

More Speed

ChaCha20 Poly1305

- New Cipher Suite from DJB
- **AEAD** = Authentication and Encryption Concurrently
  - Easier to optimise
- Fast on mobile hardware (i.e., w/o AES acceleration)
- Constant time
- < 100 LoC



http://googleonlinesecurity.blogspot.com/2014/04/speeding-up-and-strengthening-https.html

http://tools.ietf.org/html/draft-agl-tls-chacha20poly1305

TLS 1.3

- **Goals**:
  - Encrypt the Handshake
  - Reduce Handshake Latency
    - **0RT** or **1RT**
  - Improve the Crypto
    - Better cipher suites
    - Ditch Compression, Renegotiation?
- Starting now, done by EOY (?)

https://github.com/tlswg/tls13-spec/

MOAR

- https://www.howsmyssl.com/
- https://isTLSfastyet.com/
- https://bettercrypto.org/