Lessons learned running SSL at scale

Chris Down (cdown@fb.com)
Security Engineer, Facebook London
3 sections
1. Be ready to respond
OpenSSL Security Advisory [07 Apr 2014]

========================================

TLS heartbeat read overrun (CVE-2014-0160)

A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64k of memory to a connected client or server.

https://www.openssl.org/news/secadv/20140407.txt
Challenges
Which services need SSL reissue?
(and which have already been attacked?)
Who can fix them?
How?
Solutions
Store and issue certs centrally
Store associated data
Know what’s being attacked
2. Monitor everything
How should we monitor certs?
At the SSL vendor?
At the SSL terminator?
Somewhere else?
All three?
Google let root certificate for Gmail expire, causing e-mail hiccups
Issued by GeoTrust, expired cert broke trust for SMTP, other services.

by Sean Gallagher - Apr 6, 2015 3:40pm BST

Oops: Instagram forgot to renew its SSL certificate
by GwEN Williams — 30 Apr '15, 02:41pm in APPhs

Apple neglects to renew SSL certificate, breaks Software Update in the process
3. Misc recommendations
Use EC if you can
Use CT logs wisely
Use HPKP
Detect + report MITM from clients

Analyzing Forged SSL Certificates in the Wild

Lin-Shung Huang*, Alex Rice†, Erling Ellingsen†, Collin Jackson*
*Carnegie Mellon University, {linshung.huang, collin.jackson}@sv.cmu.edu
†Facebook, {arice, erling}@fb.com

Handshake optimisation
Early termination
OCSP stapling
facebook