Crypto at Scale

Brian Sniffen
bsniffen@akamai.com
Avoid data theft and downtime by extending the security perimeter outside the data-center and protect from increasing frequency, scale and sophistication of web attacks.
"At Scale"

- 10^{15} requests in 2014
- 60 KB each

- About 250 \cdot 10^3 machines
- About 150 \cdot 10^3 web servers
- About 80 \cdot 10^3 share one cert
- About 50 \cdot 10^3 have vanity names
- About 10 \cdot 10^3 vanity names
- About 5 \cdot 10^3 points of presence

- About 50 \cdot 10^6 (2^{24}) IPv4 addresses
- About 20% of Web traffic
"At Scale"

- $10^{15}$ requests in 2014
- 60 KB each

- About $250 \cdot 10^3$ machines
- About $150 \cdot 10^3$ web servers
- About $80 \cdot 10^3$ share one cert
- About $50 \cdot 10^3$ have vanity names
- About $10 \cdot 10^3$ vanity names
- About $5 \cdot 10^3$ points of presence

- About $50 \cdot 10^6$ ($2^{24}$) IPv4 addresses
- About 20% of Web traffic
“At Scale”

- $10^{15}$ requests in 2014
- 60 KB each

- About $250 \cdot 10^3$ machines
- About $150 \cdot 10^3$ web servers
- About $80 \cdot 10^3$ share one cert
- About $50 \cdot 10^3$ have vanity names
- About $10 \cdot 10^3$ vanity names
- About $5 \cdot 10^3$ points of presence

- About $50 \cdot 10^6$ ($2^{24}$) IPv4 addresses
- About 20% of Web traffic
“At Scale”

- $10^{15}$ requests in 2014
- 60 KB each

- About $250 \cdot 10^3$ machines
- About $150 \cdot 10^3$ web servers
- About $80 \cdot 10^3$ share one cert
- About $50 \cdot 10^3$ have vanity names
- About $10 \cdot 10^3$ vanity names
- About $5 \cdot 10^3$ points of presence

- About $50 \cdot 10^6$ ($2^{24}$) IPv4 addresses
- About 20% of Web traffic
“Crypto” at scale

TLS is a tool for making fewer Web connections work.
Avoid data theft and downtime by extending the security perimeter outside the data-center and protect from increasing frequency, scale and sophistication of web attacks.

2014 Crises
Avoid data theft and downtime by extending the security perimeter outside the data-center and protect from increasing frequency, scale and sophistication of web attacks.

Cert Reissuance after Heartbleed

- # of certs reissued vs. time
- Graph shows the increase in cert reissuance after the Heartbleed vulnerability was disclosed.
- A sharp increase in April followed by a steady increase until January.
Avoid data theft and downtime by extending the security perimeter outside the data-center and protect from increasing frequency, scale and sophistication of web attacks.

**Streaming encoder protocol**

0. Client sends A, Server accepts A
1. Client sends A, Server accepts A|B
2. Client sends B, Server accepts A|B
3. Client sends B, Server accepts B
Fix Origin SSL

- Four year project
- 99.4% done
- Pinned keys
- Short CA list $\subset$ Firefox
- PFS
- No TLS fallback
Reasons for availability > integrity at origin

• “I’d have to pay for that software module”  
  • Lotus Domino  
  • F5

• “My assessor only says it has to be SSL, not that it has to be good.”

• “Our next change window is in 2016.”

• “Surprise, we have another origin server.”

• “But I’m paying you to not have to deal with security!”  
  ...or my IT department.
How much would you pay not to talk to IT?
Hello
your name is

a248.e.akamai.net
SNI: What took so long?

2001: SNI designed.
2004: Patch for OpenSSL (3rd party)
2006: Many clients (Opera, FF, IE on Vista).
2007: OpenSSL, Mac
2010: Android
2014: Python, Java

Never in Windows XP.
Never in Android 2.2 Froyo.
Avoid data theft and downtime by extending the security perimeter outside the data-center [https://security.akamai.com/heartbleed/historical_counts.svg](https://security.akamai.com/heartbleed/historical_counts.svg) and protect from increasing frequency, scale and sophistication of web attacks.
What do we need?

Overlapping windows of safety across a decade.

Better a change a year than a crisis every five.

Client branches on protocol version. SRV records?

Design for obsolescence: terminal handshakes.
What do we need?

Overlapping windows of safety across a decade.

Better a change a year than a crisis every five.

Client branches on protocol version. SRV records?

Design for obsolescence: terminal handshakes.

Interested? I’m hiring.
bsniffen@akamai.com