

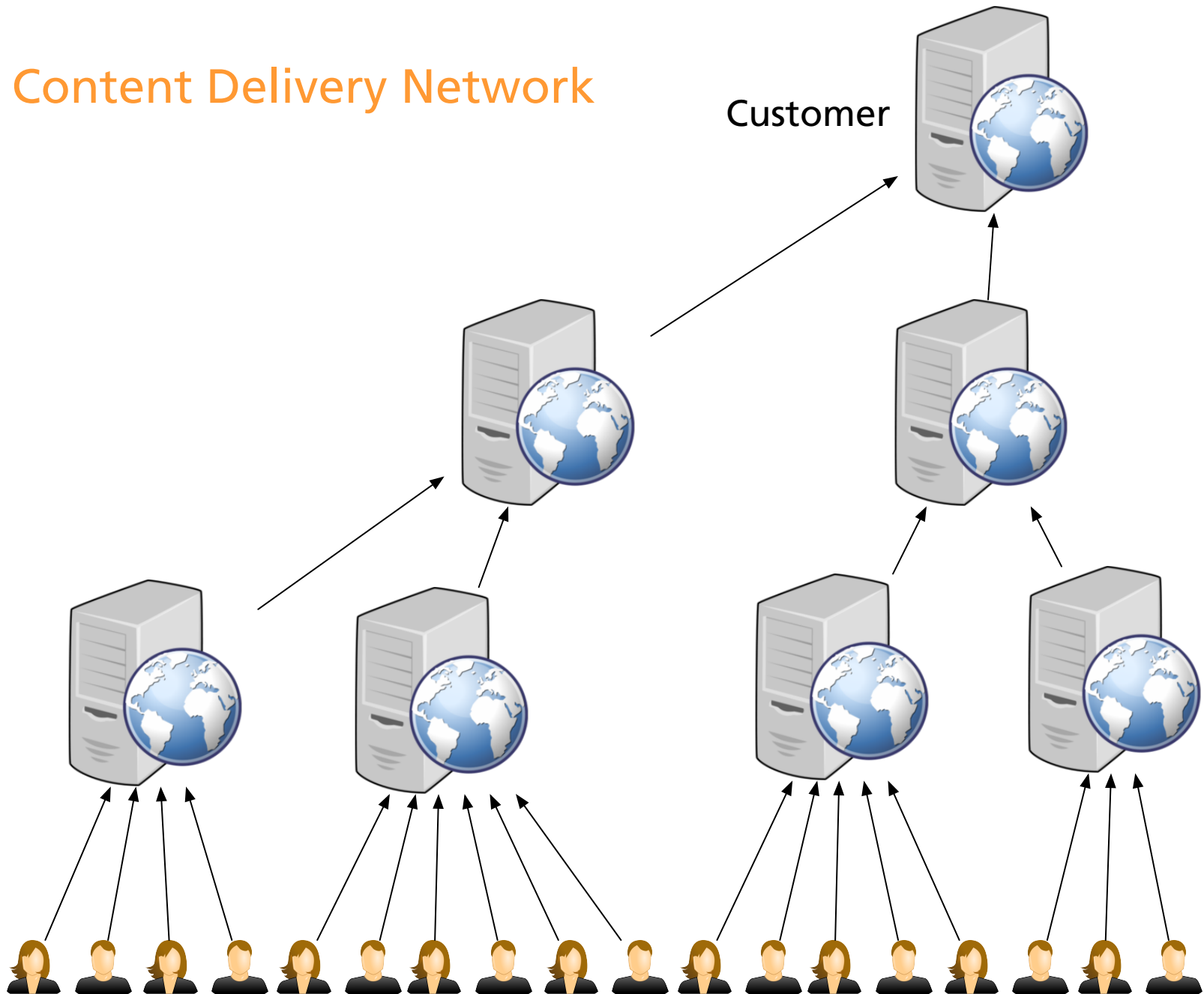


Crypto at Scale

Brian Sniffen

bsniffen@akamai.com

Content Delivery Network



“At Scale”

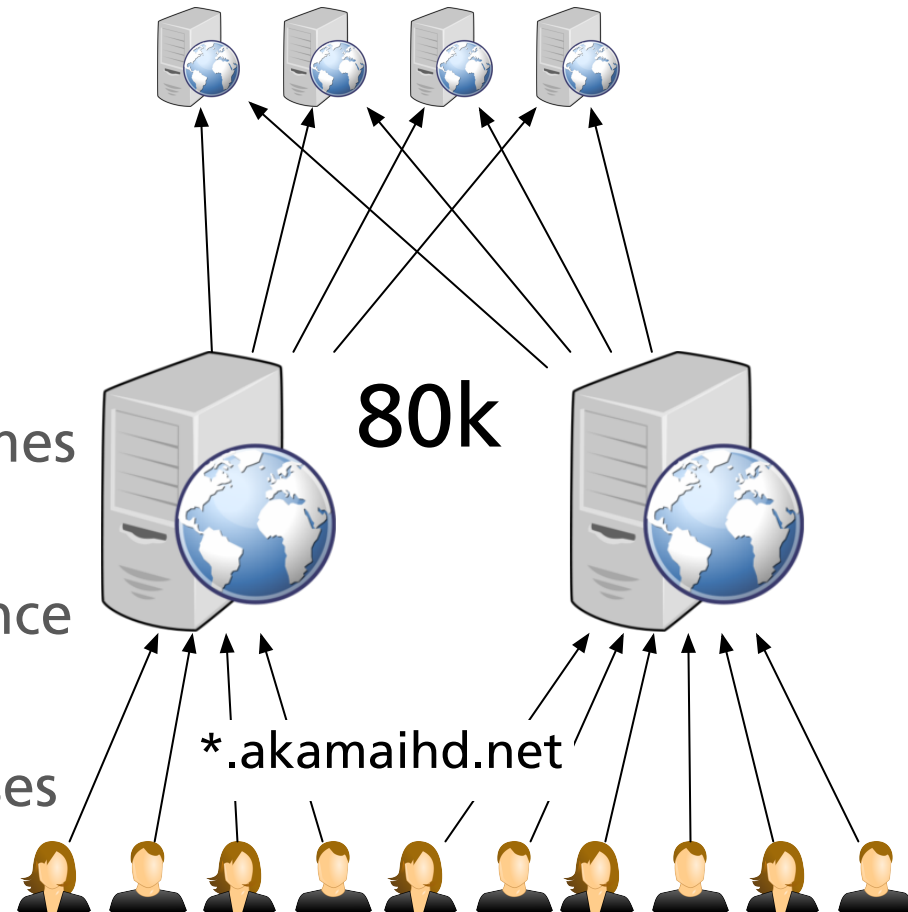
- 10^{15} requests in 2014
- 60 KB each

- 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

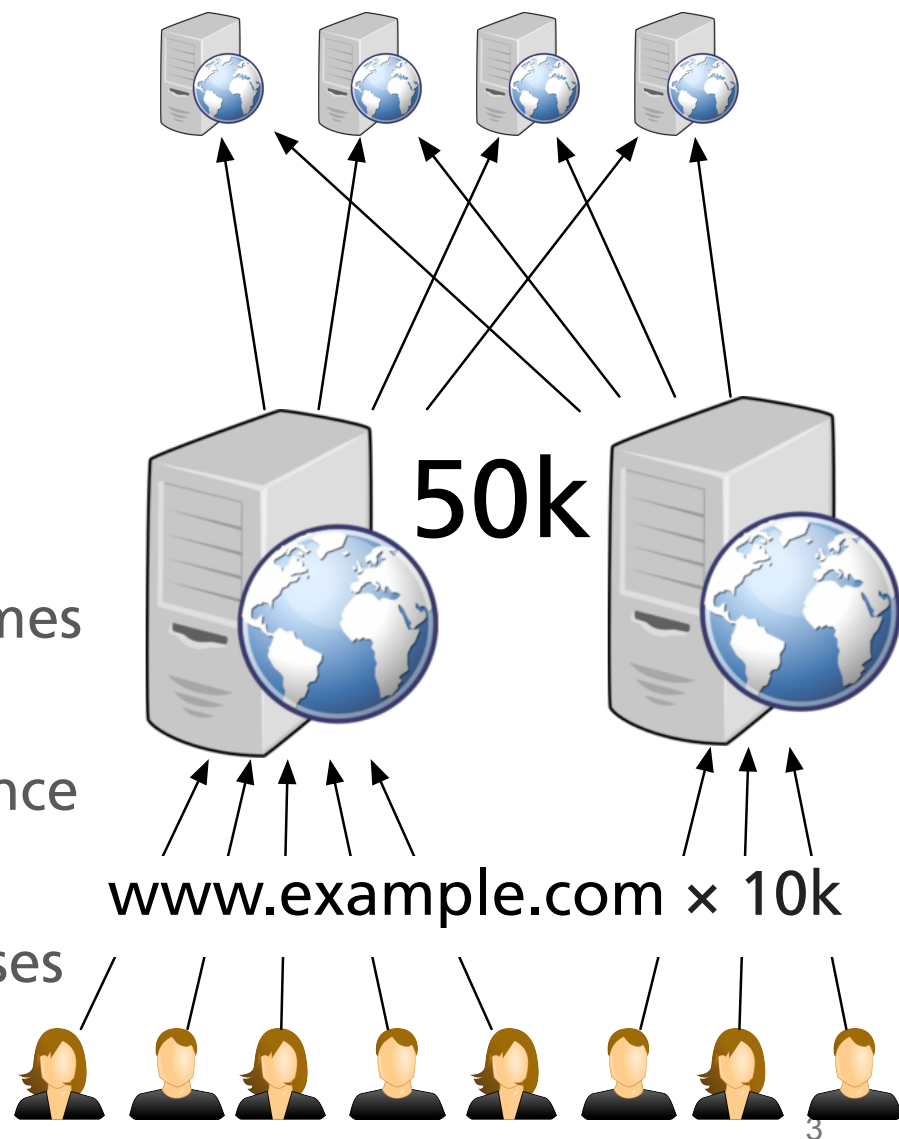
“At Scale”

- 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

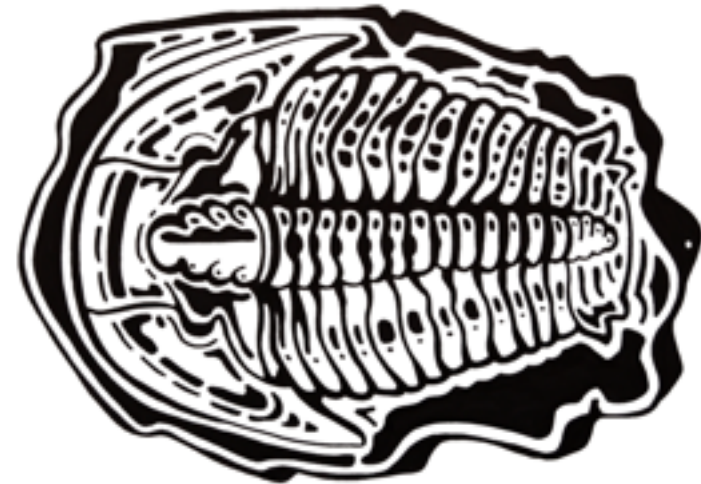
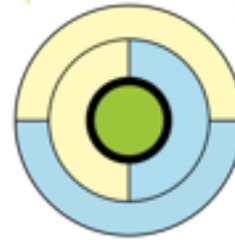


“Crypto” at scale

TLS is a tool for making fewer Web connections work.

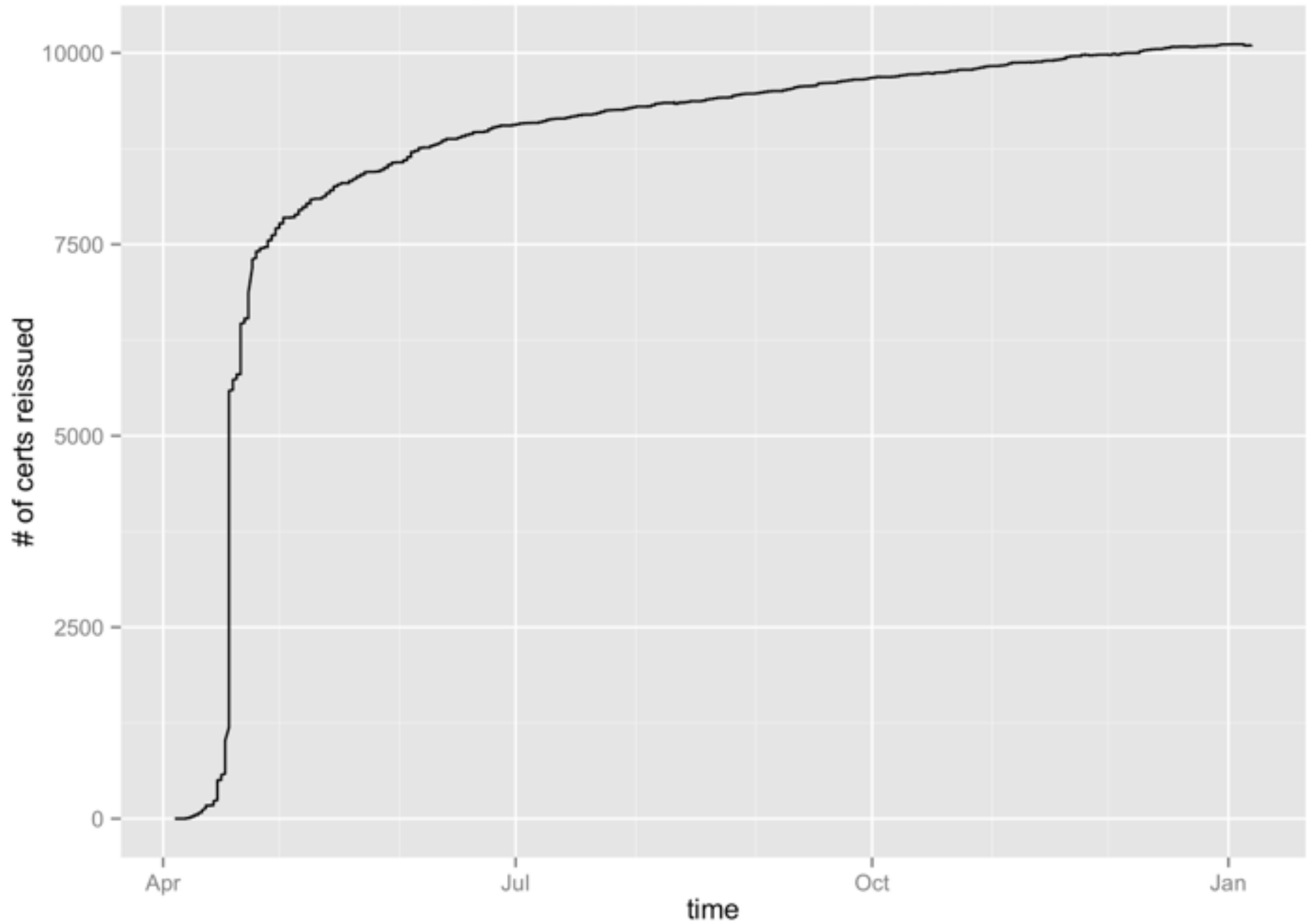


2014 Crises

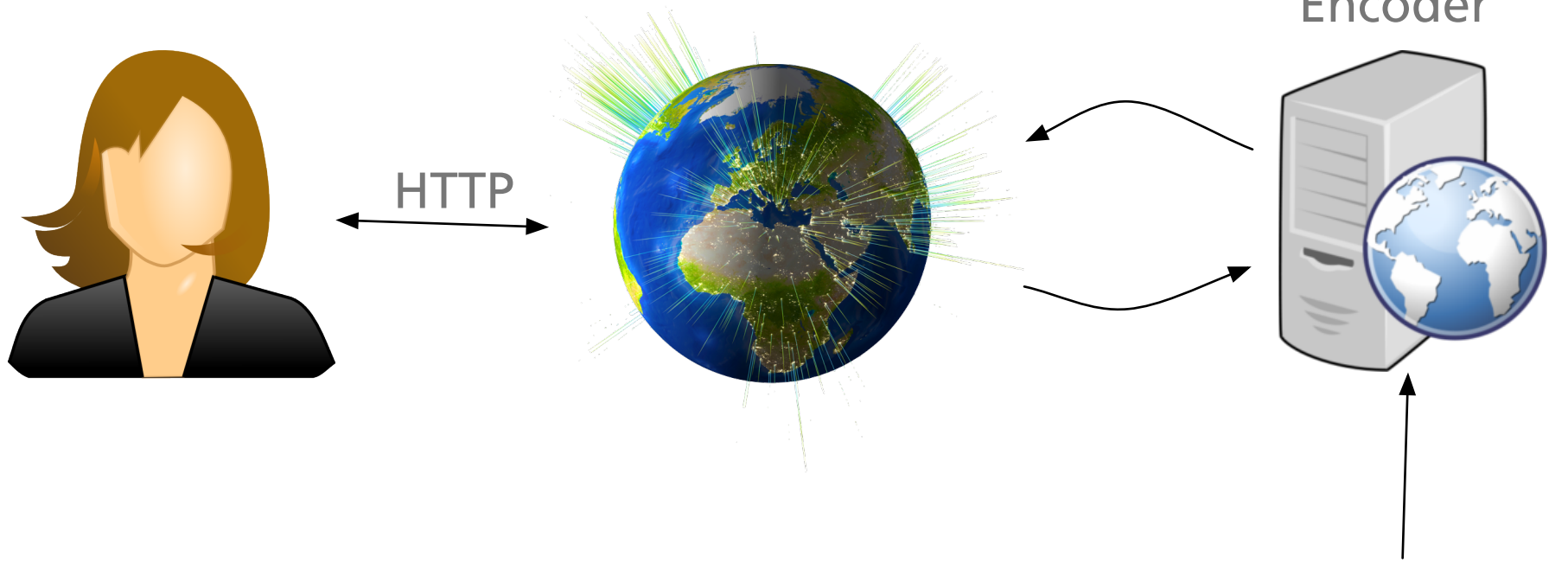




Cert Reissuance after Heartbleed



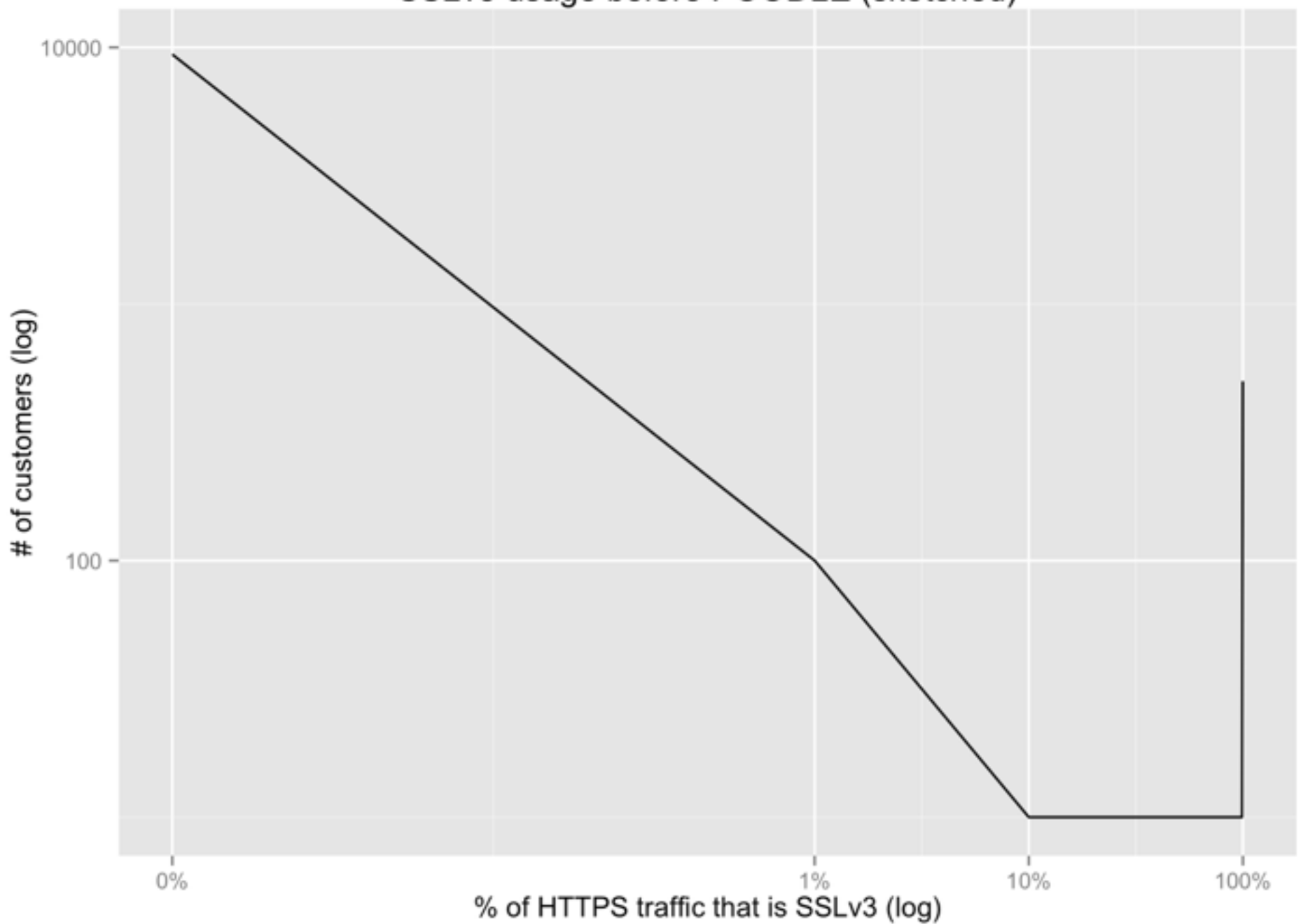
Streaming encoder protocol

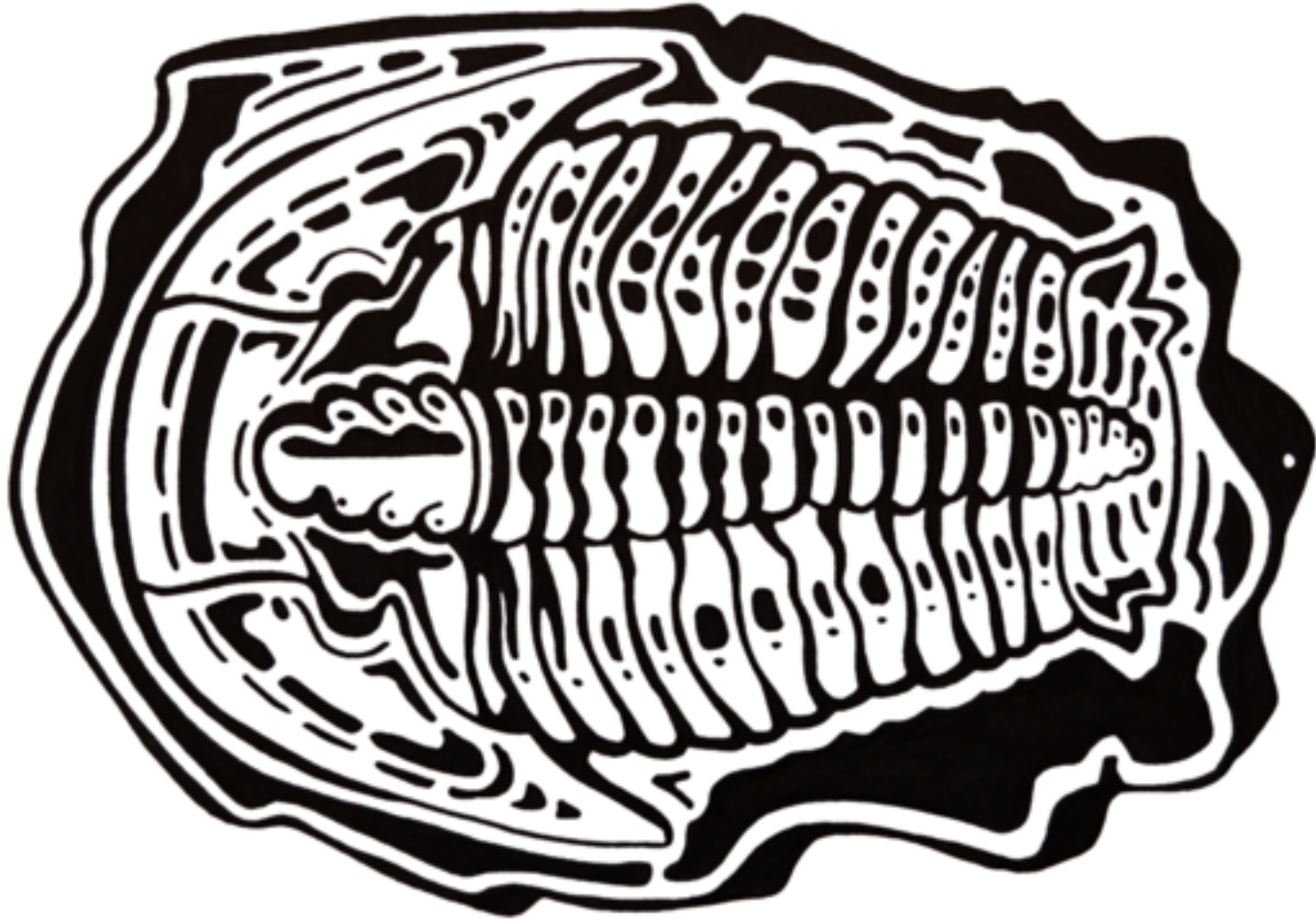


0. Client sends A, Server accepts A
1. Client sends A, Server accepts **A|B**
2. Client sends **B**, Server accepts A|B
3. Client sends B, Server accepts **B**



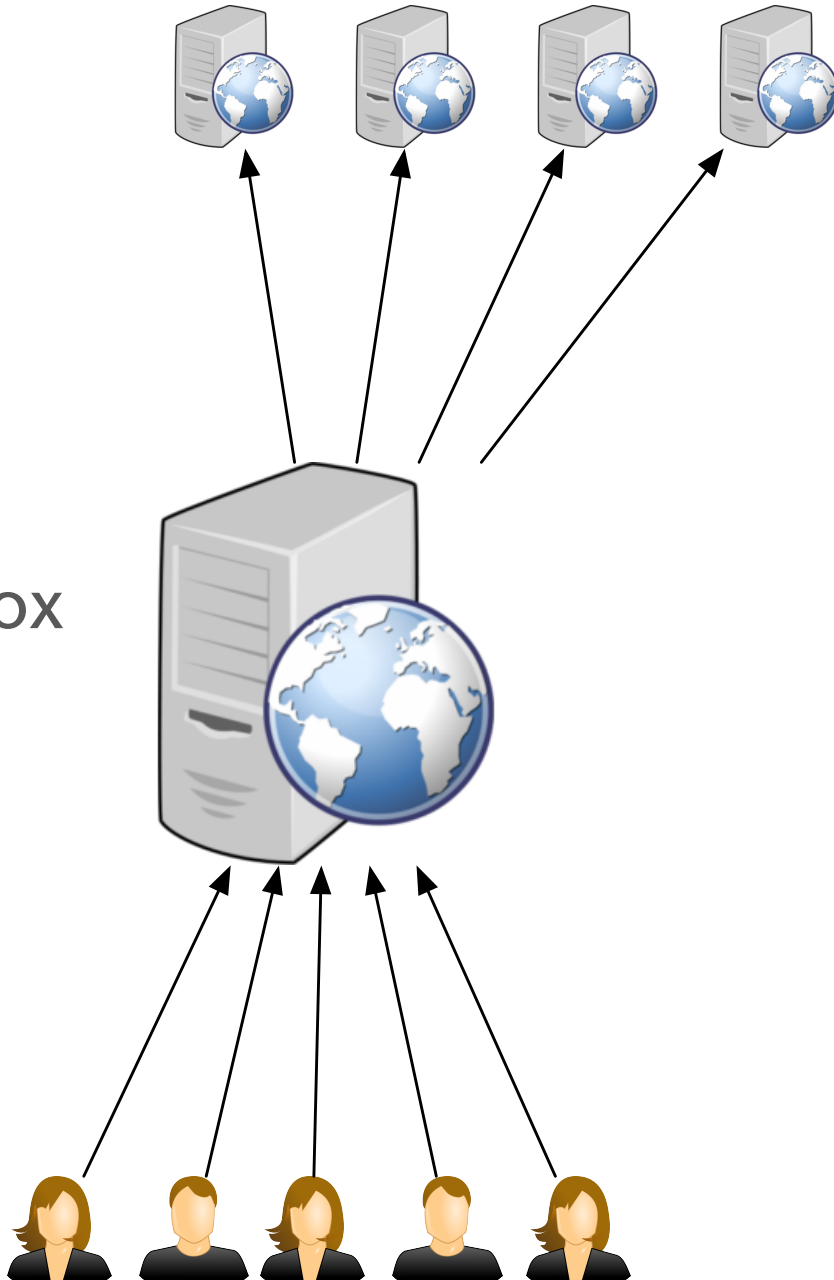
SSLv3 usage before POODLE (sketched)





Fix Origin SSL

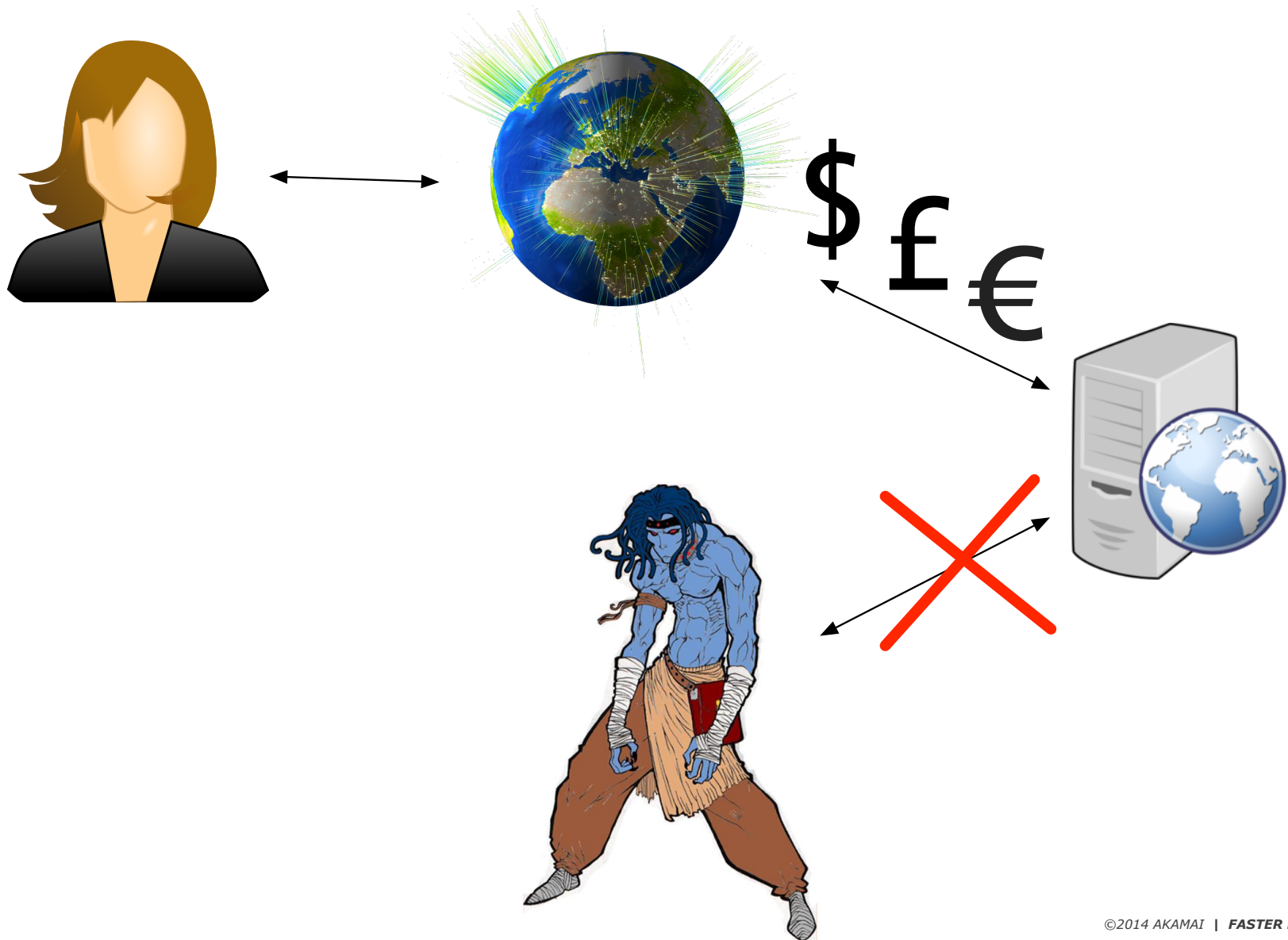
- Four year project
- 99.4% done
- Pinned keys
- Short CA list \subset Firefox
- PFS
- No TLS fallback



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.

2003: Specified in RFC 3546.

2004: Patch for OpenSSL (3rd party)

2006: Many clients (Opera, FF, IE on Vista).

2007: OpenSSL, Mac

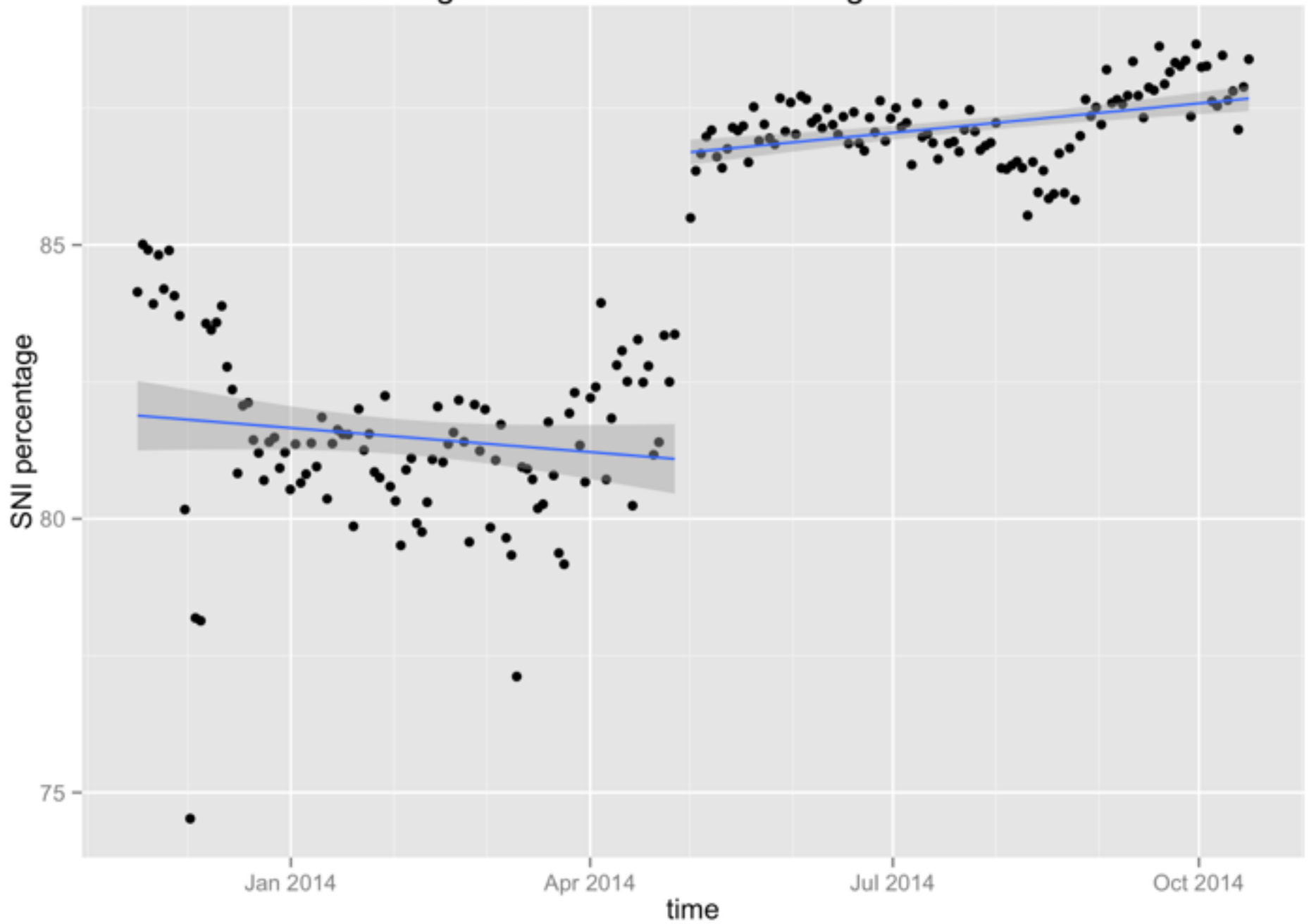
2010: Android

2014: Python, Java

Never in Windows XP.

Never in Android 2.2 Froyo.

Percentage of all ESSL traffic offering SNI extension



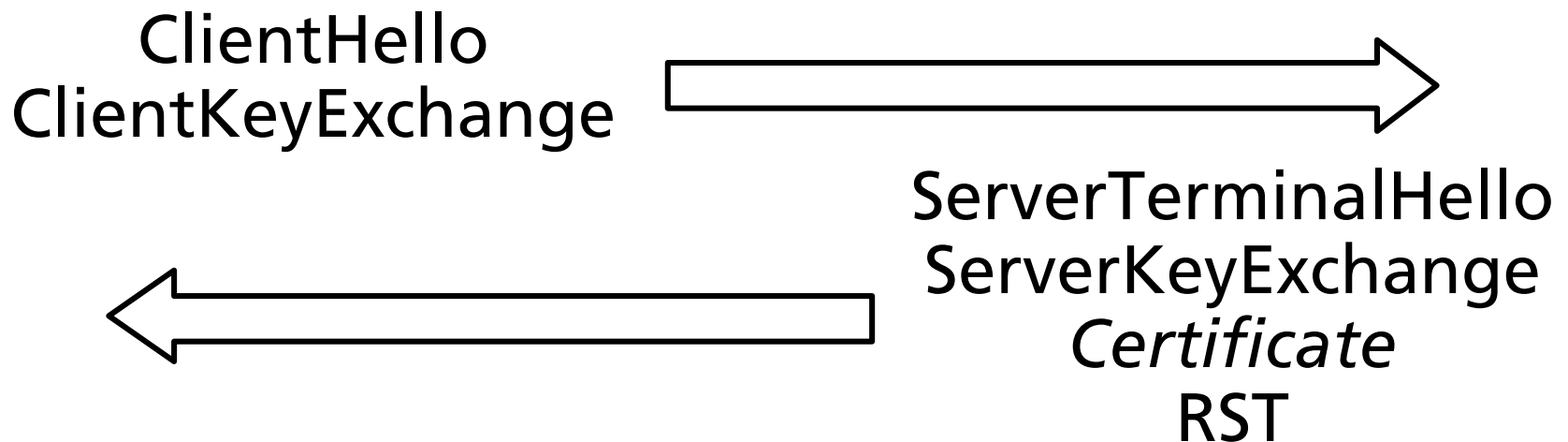
What do we need?

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