
I WANT
YOUR
COOKIES!!!!

SSLv3 is dead

- draft-thomson-sslv3-diediedie
- Long litany of attacks on SSLv3
- POODLE removed the last
- Padding oracle attack, like BEAST
  - Similar risks with regard to cookies
  - Especially bad for the web, because JS

Can we kick SSLv3 off the web?

Before & After Measurements

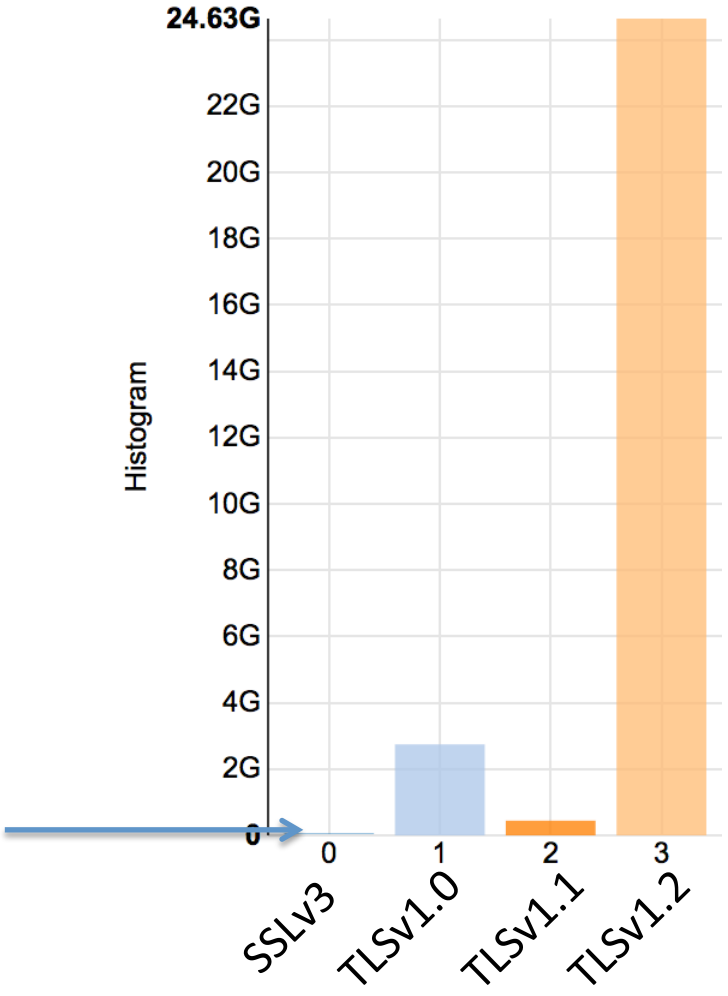
- Before: How much of the web relies on SSLv3?
- After: Are people responding?

- Methodologies:
  - Firefox Telemetry
  - Scanning

Telemetry

- Firefox reports on which versions actually get used
- SSLv3 before: 0.26%
- SSLv3 after: 0.19%

20.86M txns over 4 weeks

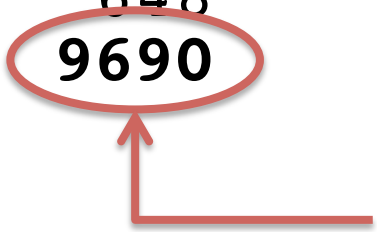


Scanning

30,992,616	Hosts completed a handshake (443)
927,330	Hosts required SSLv3 (3%)
731,535	Hosts provided a well-formed cert
274,008	Unique names collected from CN/SAN
63,834	Unique FQDNs with valid TLDs
22,669	Unique names matching Alexa top 1M
1,196	Exact matches to Alexa 1M domains
21,473	Proper subdomains
10,923	Responded with a valid TLS message
551	TLS 1.2
34	TLS 1.1
648	TLS 1.0
9690	SSL 3.0

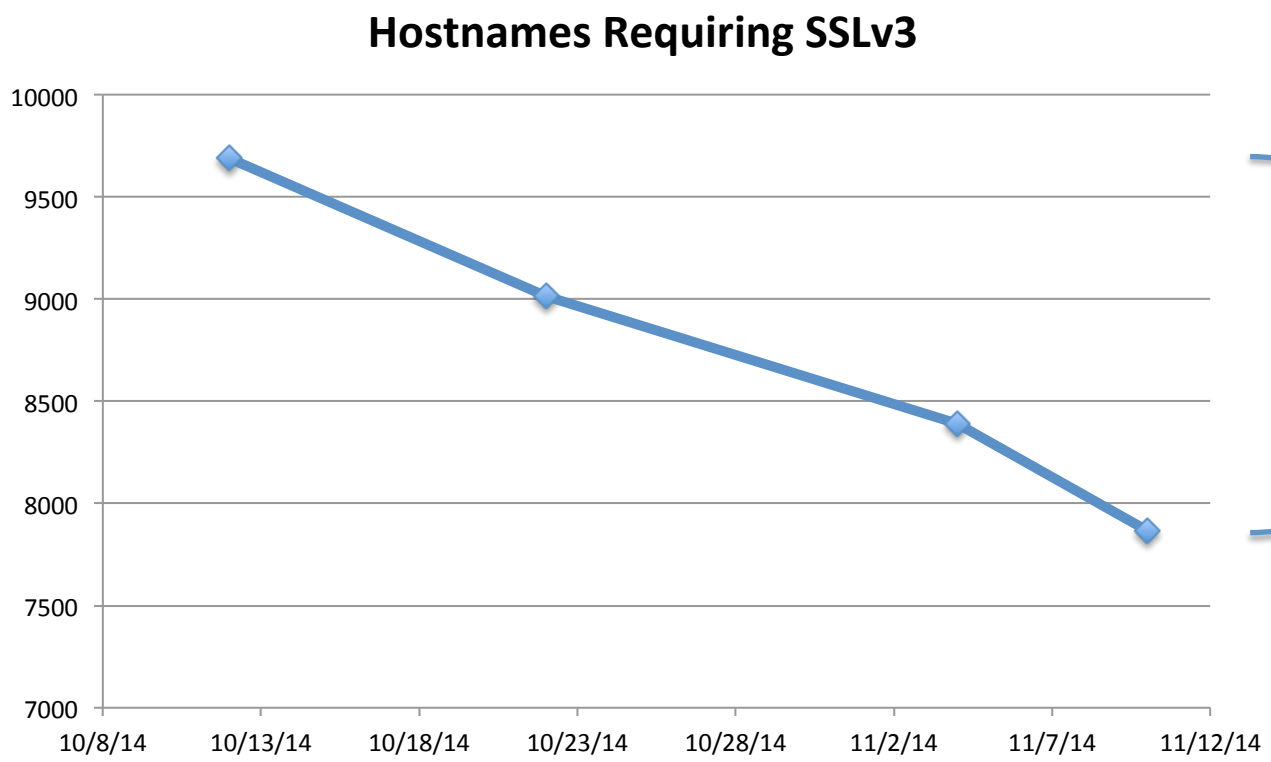
Scanning: Before

```
30,992,616  Hosts completed a handshake (443)
   927,330  Hosts required SSLv3 (3%)
   731,535  Hosts provided a well-formed cert
   274,008  Unique names collected from CN/SAN
    63,834  Unique FQDNs with valid TLDs
    22,669  Unique names matching Alexa top 1M
     1,196    Exact matches to Alexa 1M domains
    21,473    Proper subdomains
    10,923  Responded with a valid TLS message
       551    TLS 1.2
        34    TLS 1.1
       648    TLS 1.0
      9690    SSL 3.0
```



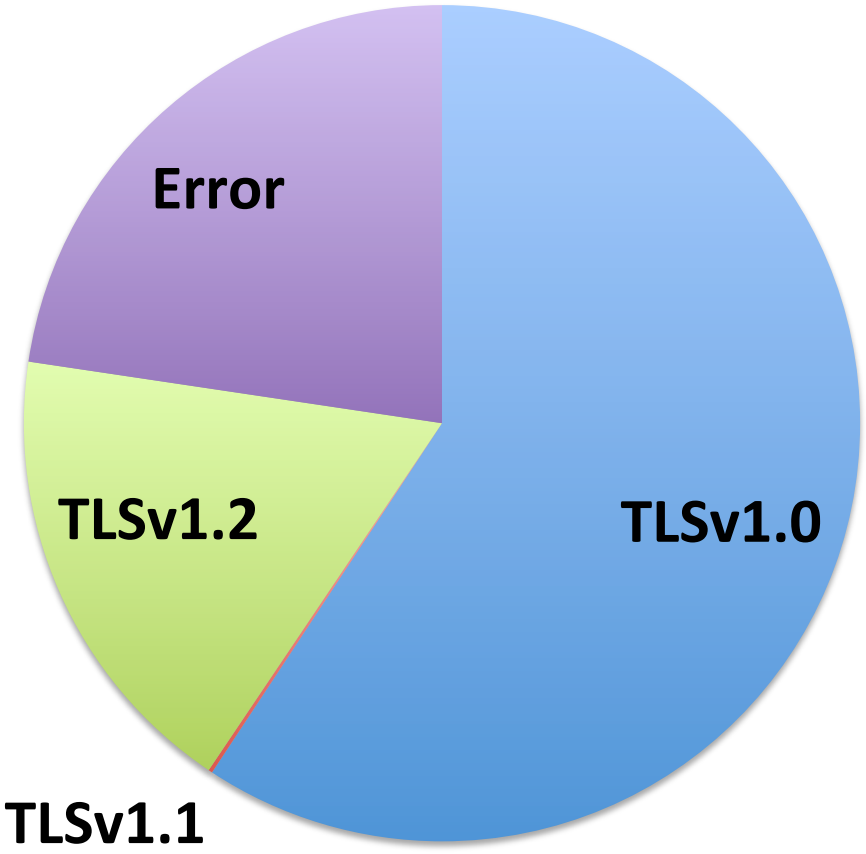
Subdomains of 0.4% of the Alexa Top 1M
How will they react to the announcement?

Scanning: After



~4 weeks
1823 sites fixed
18.8%

What did they upgrade to?



Lessons

- Protocols can die
- Publicity can move the needle
  - Sometimes quite quickly
- Even big companies have old stuff
  - Apple, Mozilla, Verizon, IBM, Citibank, …
- There are still lots of embedded devices that need attention

Epilogue: RC4

Epilogue: RC4