Some observations of TLS in the web
Thanks, Hubert and Netcraft

- Hubert Khario does monthly scans of the Alexa top 1M sites (reaches about 50%)
- Visit his website: https://securitypitfalls.wordpress.com
- Netcraft has good scans: https://news.netcraft.com
Milestones, I

• May 2014: SHA2 doubles from 4 to 8%
  – Why? Heartbleed recertification

• May 2014: TLS 1.2 reaches 50% adoption
  – Seven years after RFC 5246
Milestones, II

• September, 2014: CA’s and TLS certs are mostly 2KRSA (99% and 96%); 88% support RC4

• January, 2015: 70% of servers pick the cipher; ECDHE with NIST-P 256 is at 50% (78% total)

• June, 2015: RSA with SHA256 up to over 60%
Stats from a CDN: % of SSL traffic
More from a CDN: SNI %
More from a CDN: % of SNI
More from a CDN: SSLv3
Lesson to be learned

• If it ain’t broke, don’t fix it
  – Or
• Nobody updates anything unless forced