X.509 in Practice
(It's worse than you think)*

* Unless you are immensely suspicious and possibly paranoid

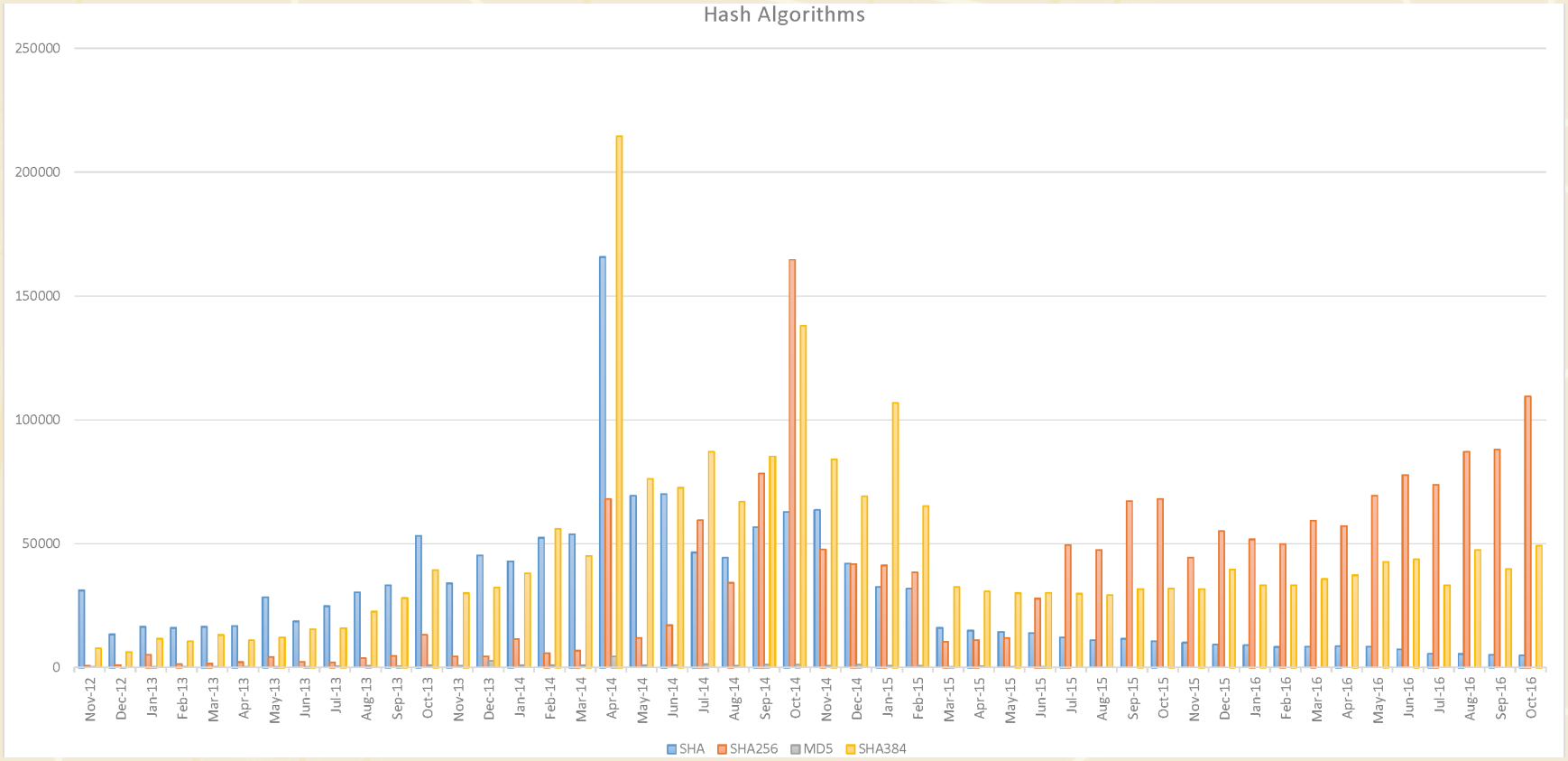
Outline

- Observing certificates in the wild
- Identify patterns
- Heartbleed Case Study
- Two Predictions

Certificates in the Wild

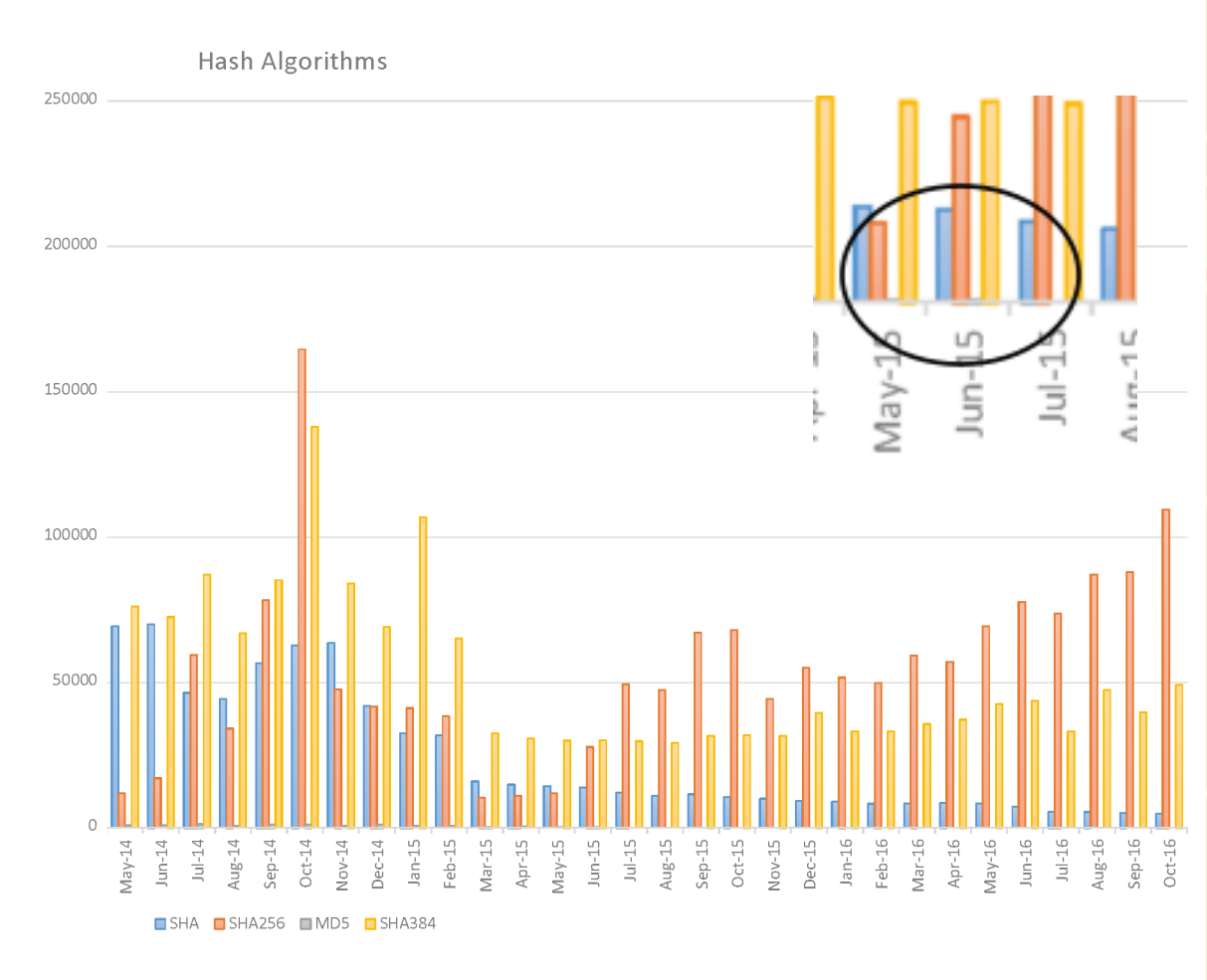
- Comprehensive data set of certificates people see on daily basis
  - Top million websites every day
  - Phishtank every hour
  - Banks as defined by FDIC (twice)

A Real Hash of the Standard



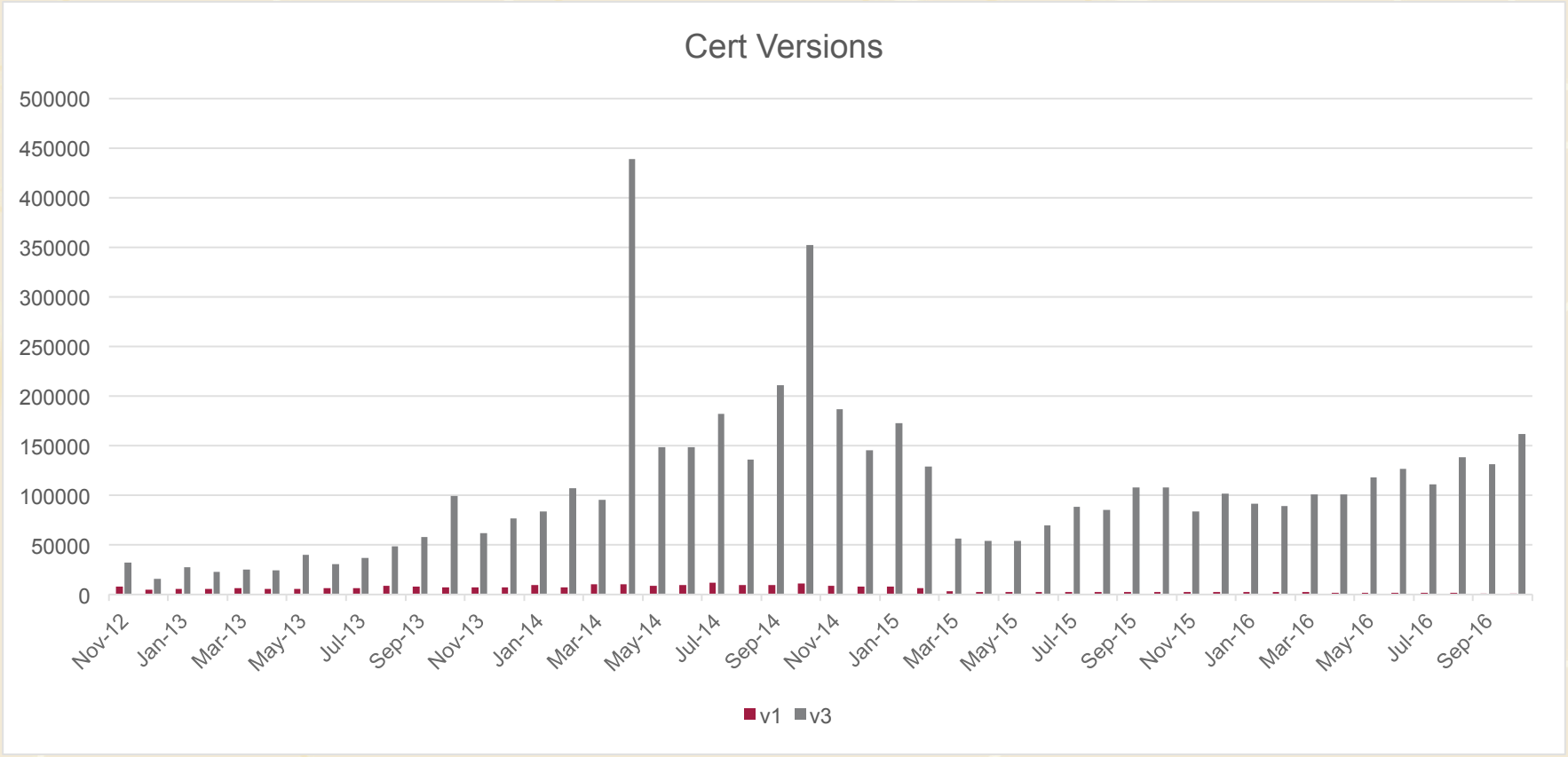
Last Seen in 2013?

- MD5 last observation June 2015



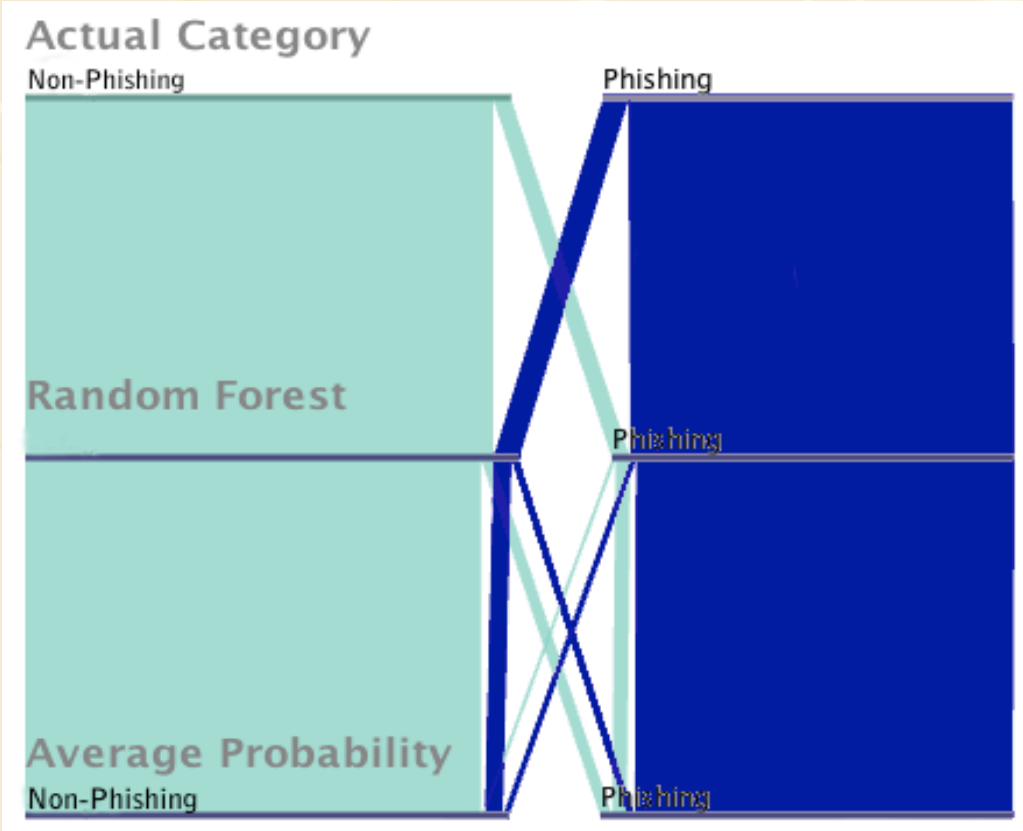
One

Version 3 Adoption



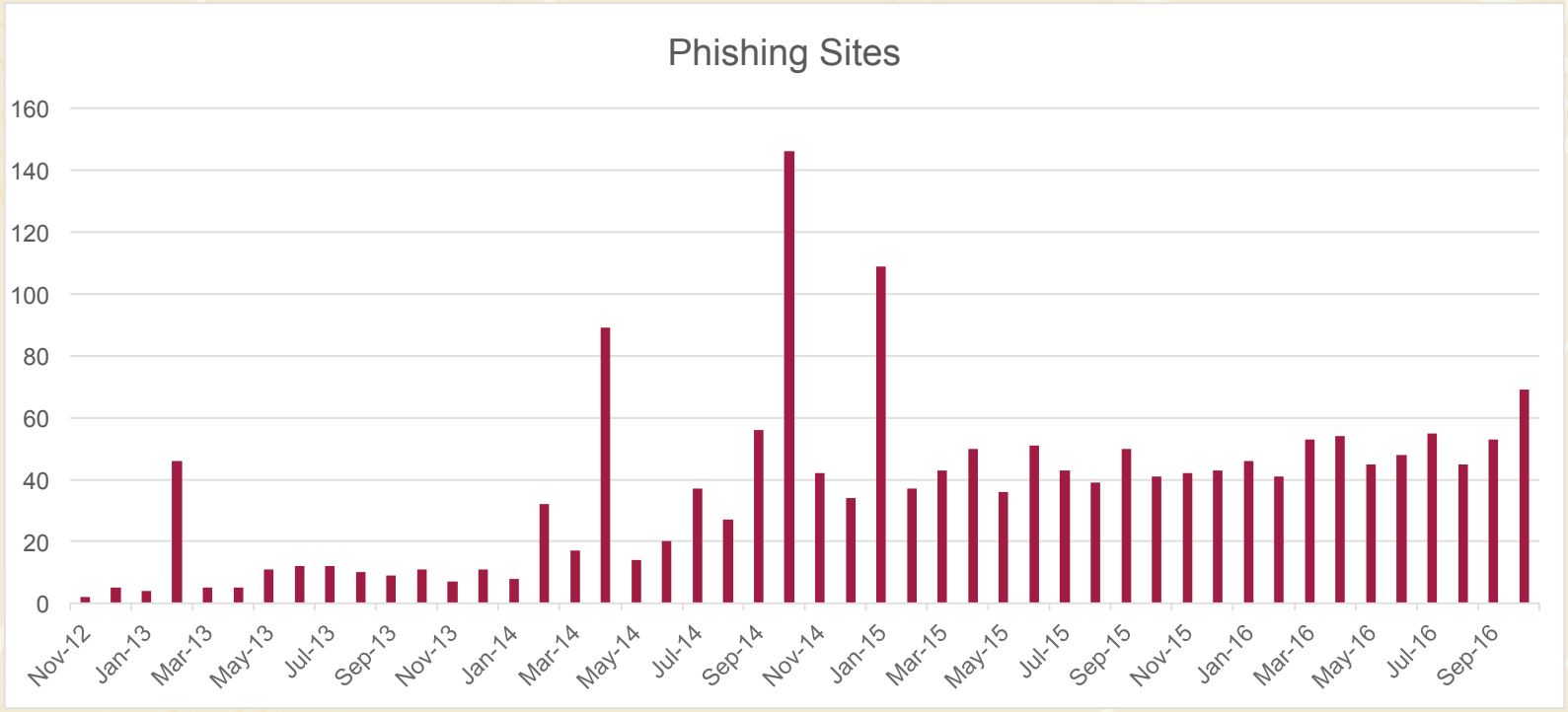
Distinguishing Phishing with TLS

- Increased TLS phishing but still very small
- TLS abuse dominates TLS issuance
  - Cloud Providers
- Differences
  - Different CAs represented
  - Date
    - date of issue
    - date seen
  - Lack of extensions
  - Other features

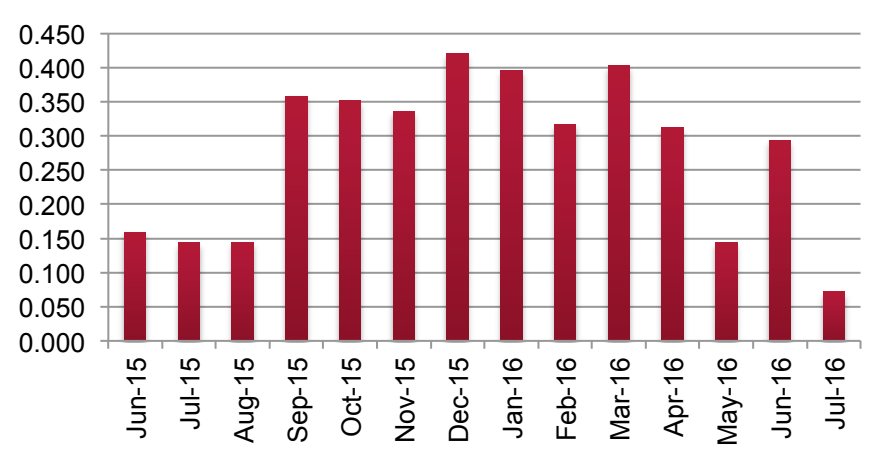


Phishing Trends – Absolute Number

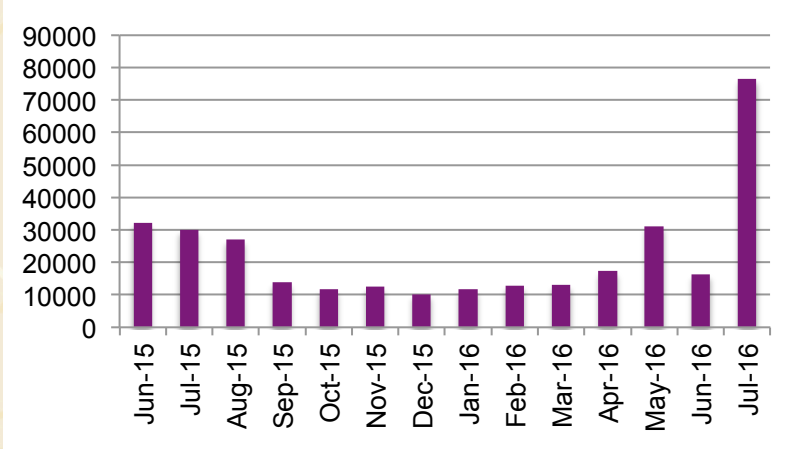
- Hit PhishTank every hour total TLS responses



Phishing Trends as a Percentage



Less than 1%



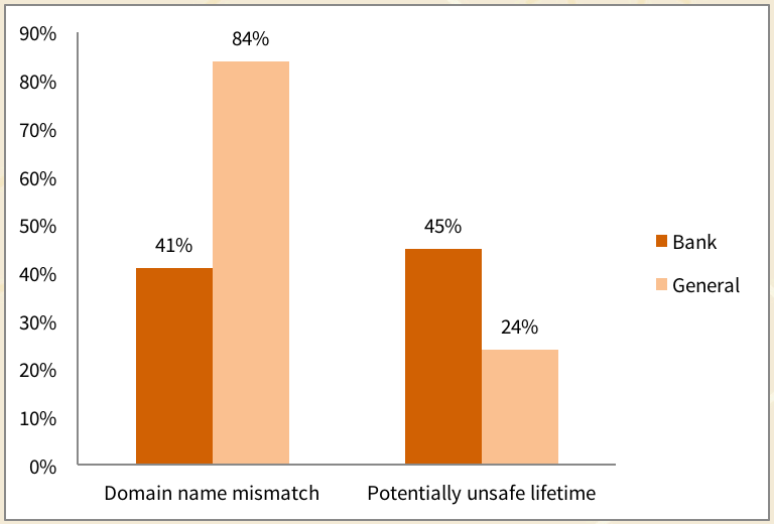
Larger variation in number of verified phishing sites

Summary of Depository Institutions

- FDIC lists 27,000 records
- These are savings & loans, banks, etc
- Each is supposed to report its domain name
- TLS phishing is small compared to overall payment fraud
  - but growing
- Low-expertise victims

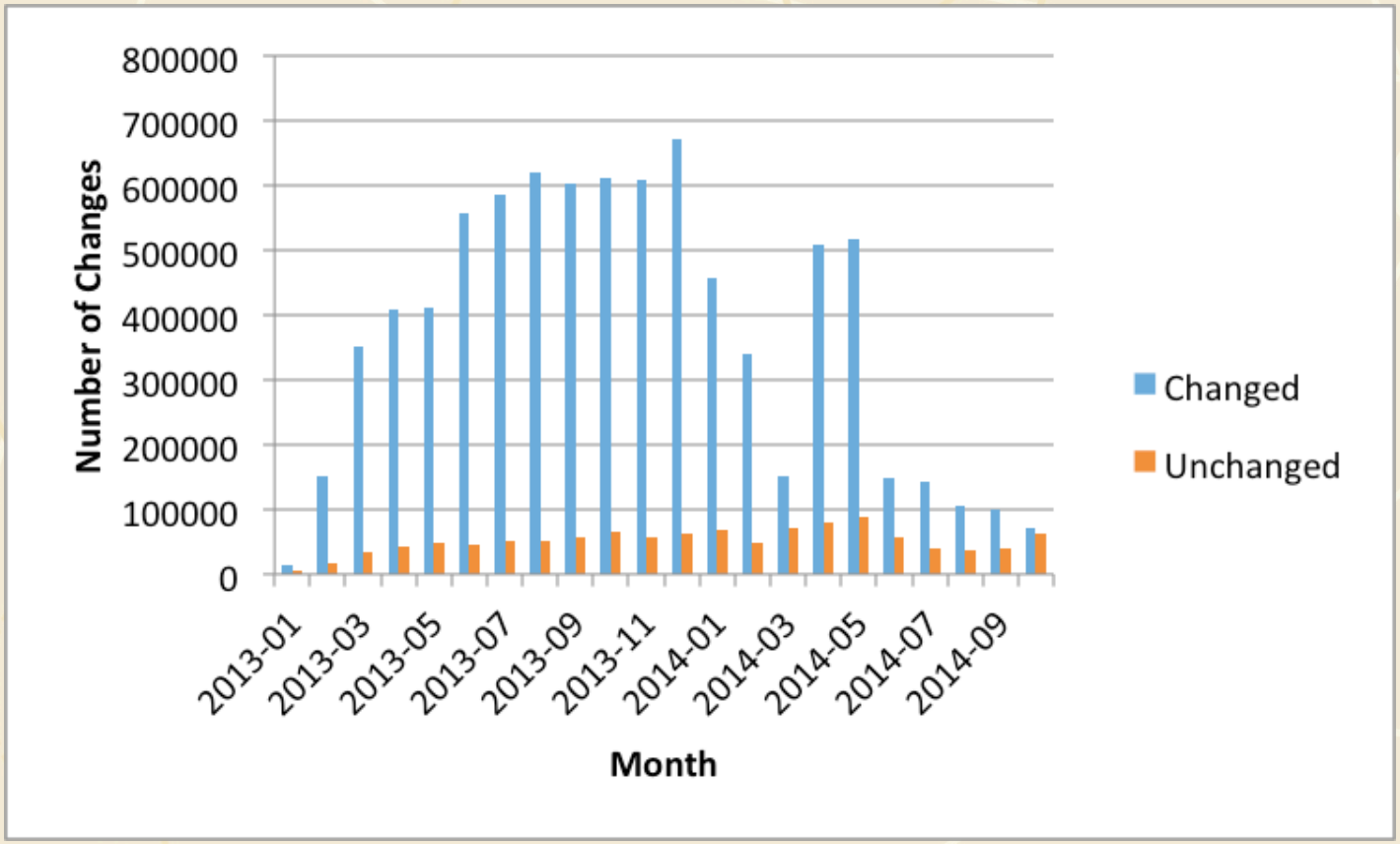
Summary of Banking Analysis

- Certificate sharing *only in banks*
  - sinkdns.org used by 51 different HTTPS bank domains
  - webaccess1.com used by 43 different banks
  - virtualization company Parallels shared by 37
- Is bad *but* better than average

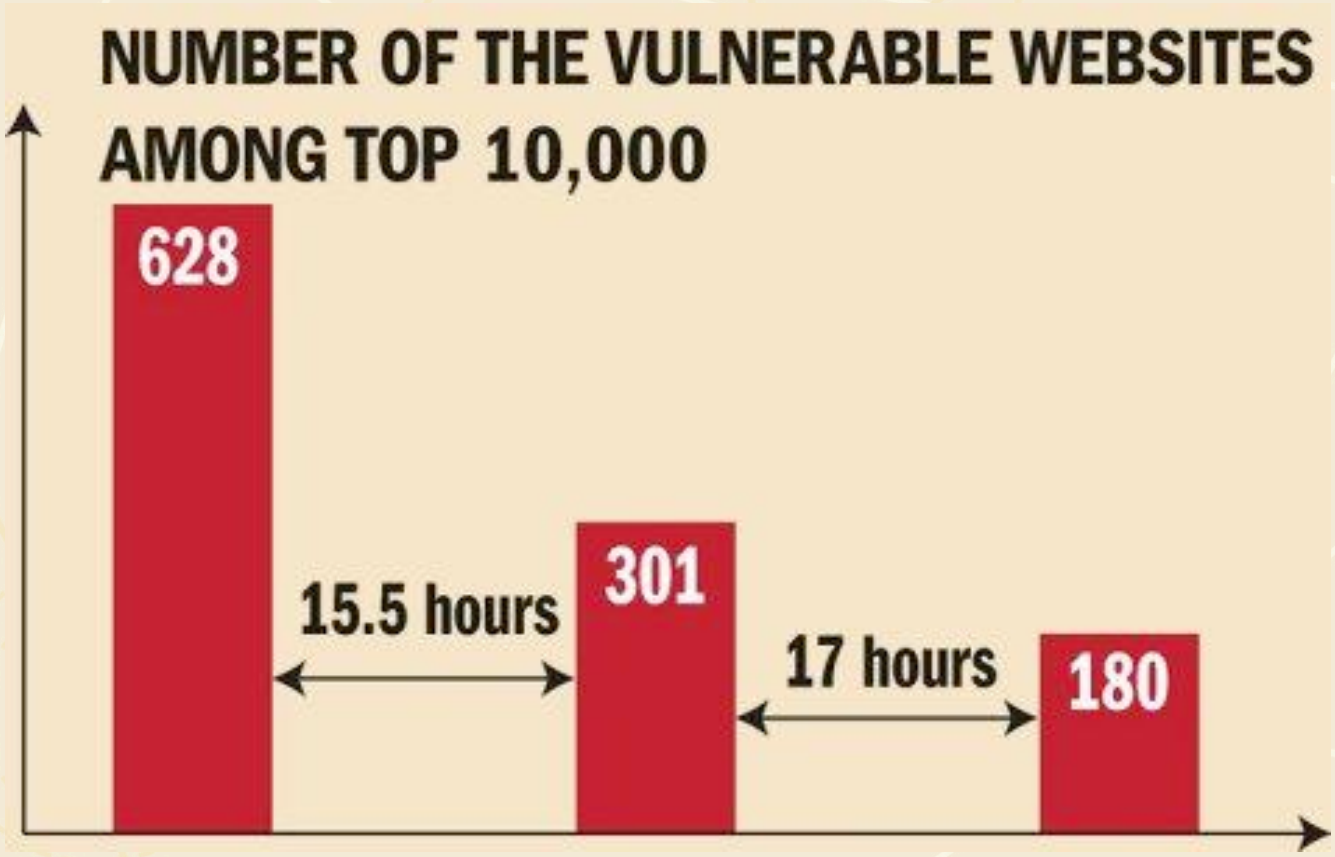


And What About in an Emergency?

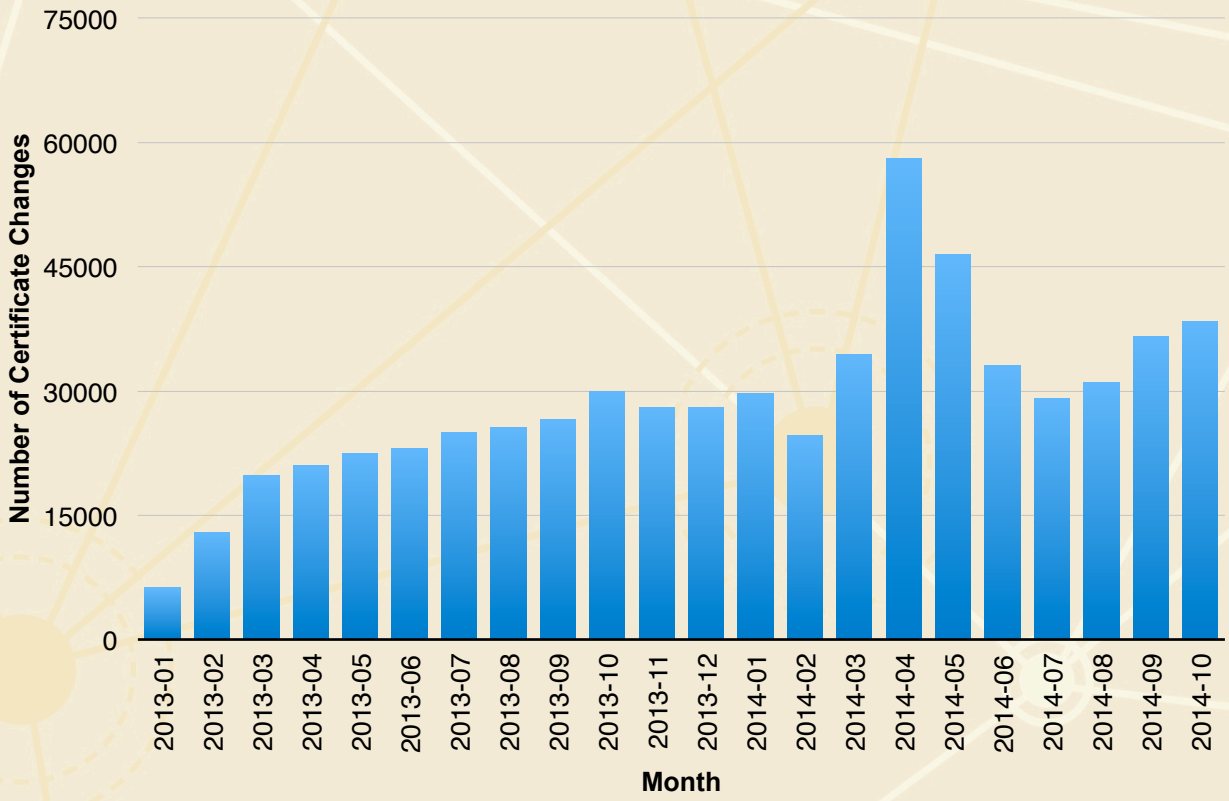
A For Effort? Updated Signature Without Changing the Key



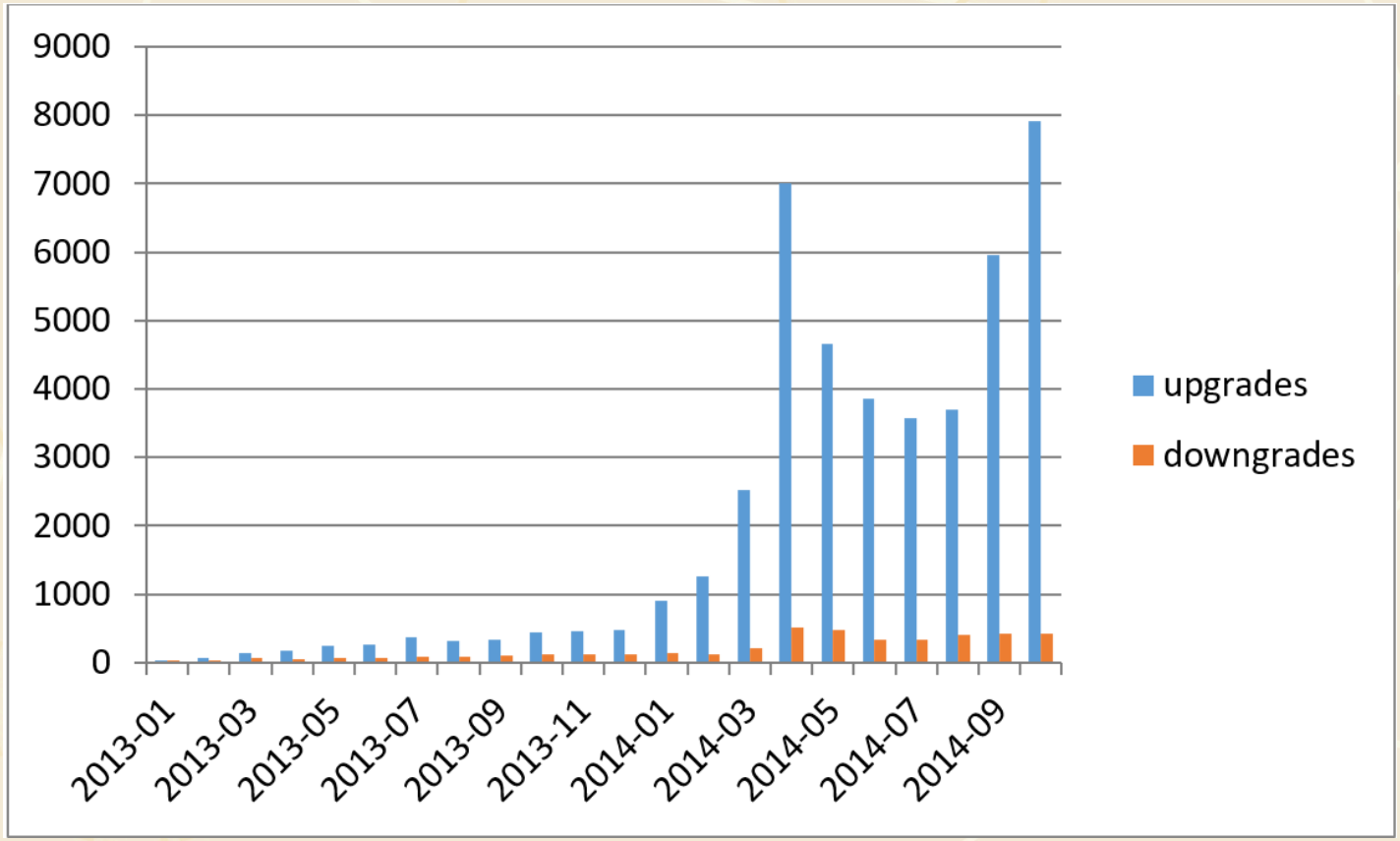
When Patching is Not Enough



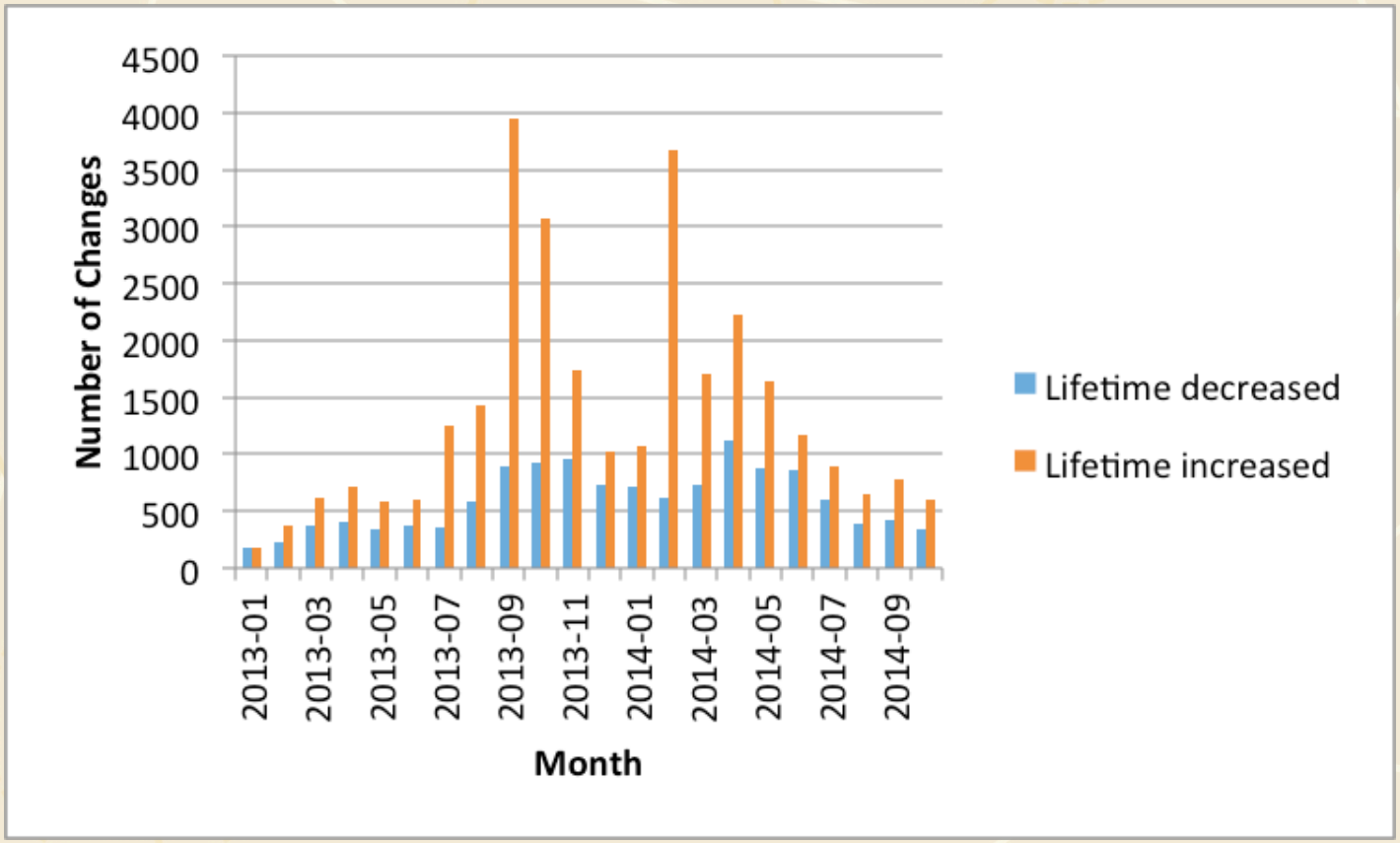
Early Replacement of Non-expired Certificates



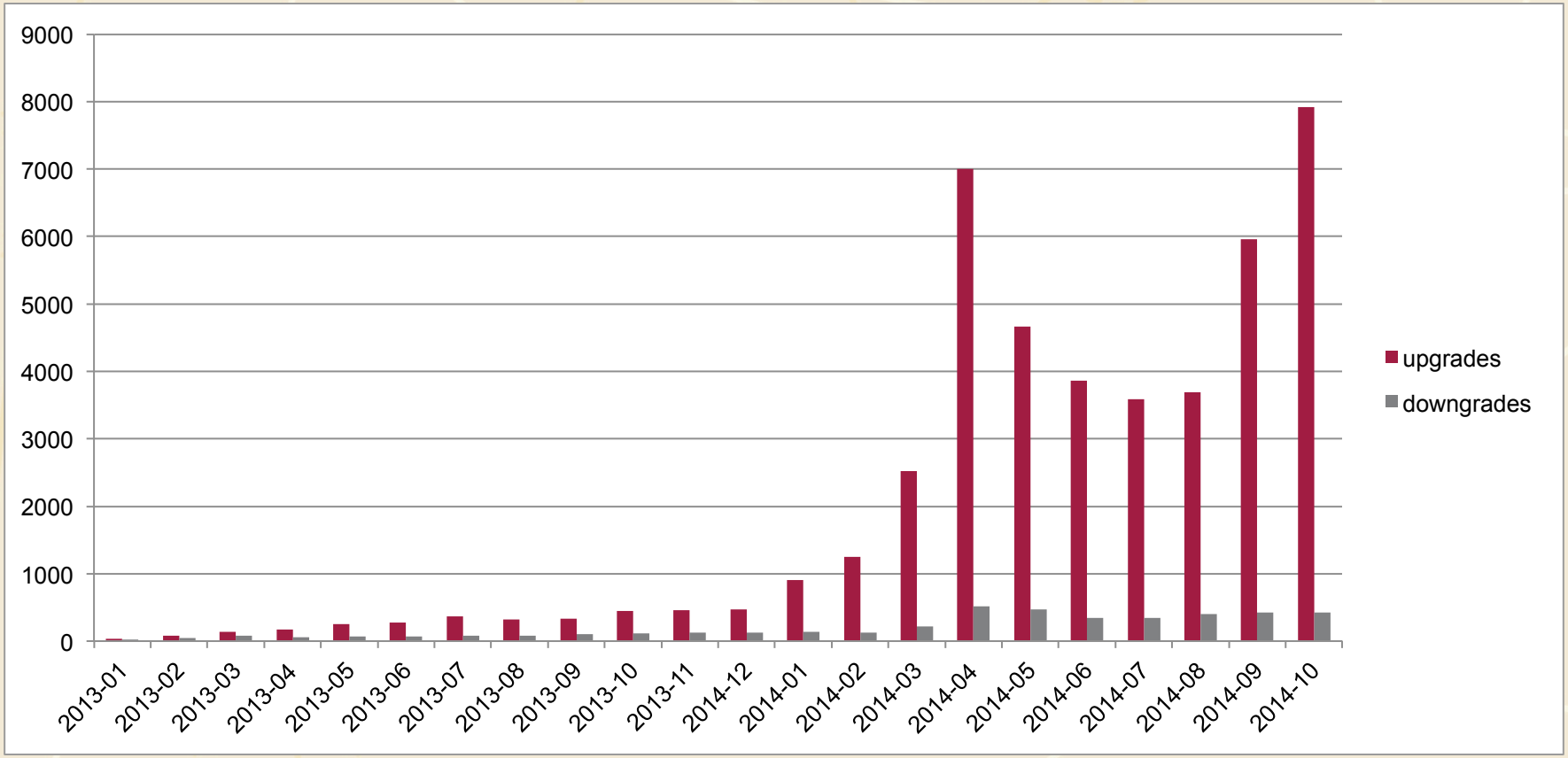
For Those Changed in Reponse to Heartbleed



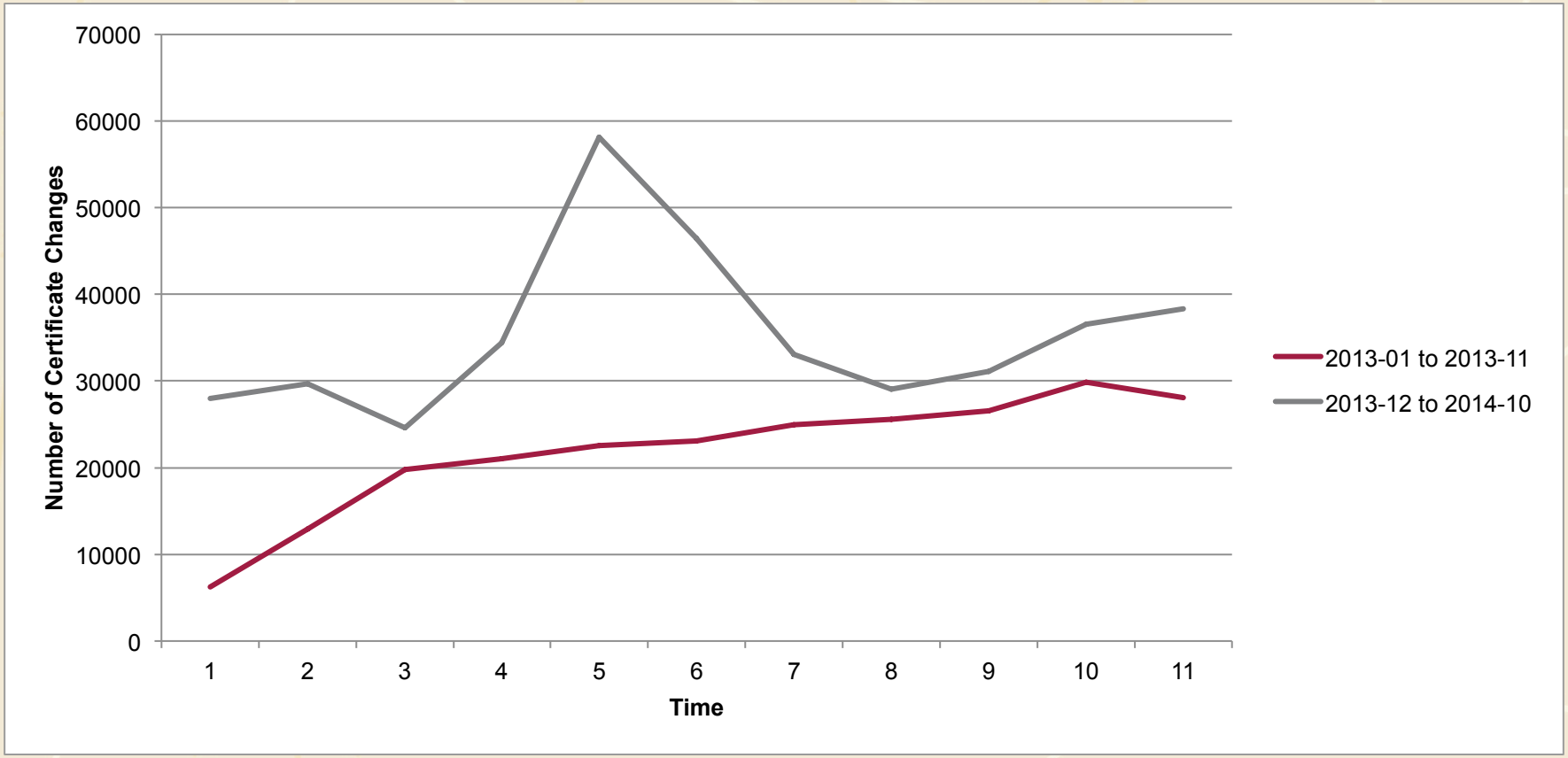
One Life to Live: Heartbleed Changes



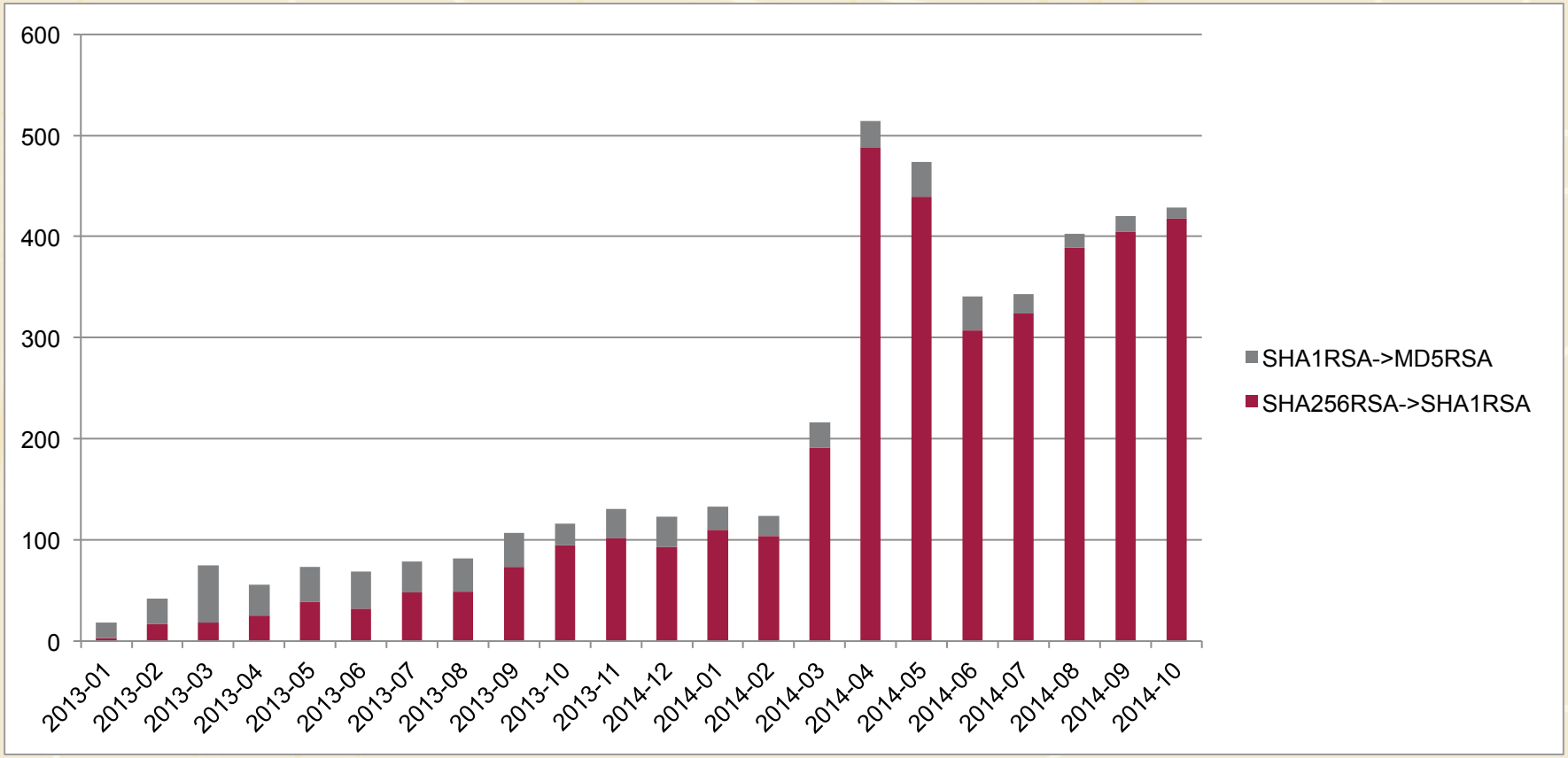
Change in Signature Algorithm



Two Year Comparisons



For Updated Non-expired



IoT Hubs?

SmartThings

Mother Sen.se

SmartThings Siemens Hub

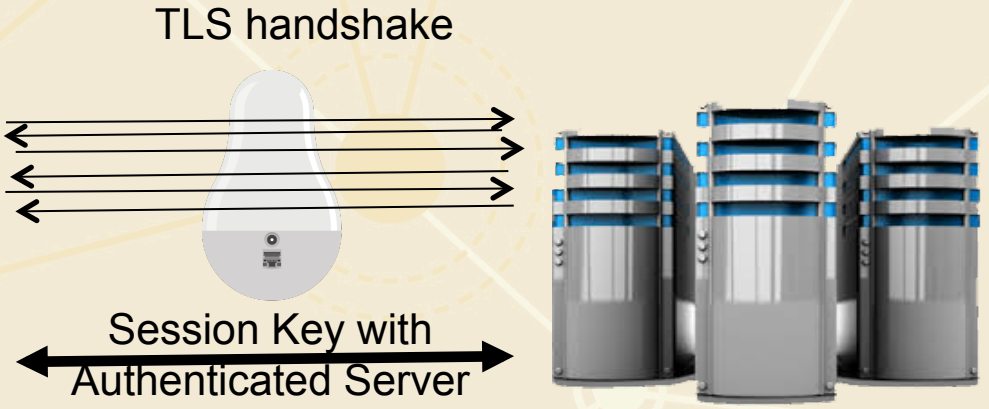
- Version V3
- Serial Number 05
- Signature Algorithm sha1RSA
- Signature Hash Algorithm sha1
- Issuer admin@smartthings.com
- Valid from Wednesday, January 14, 2015
- Valid to Saturday, January 11, 2025
- Subject admin@smartthings.com
- Public Key RSA(1024 Bits)

Of Course Compared to the App…

- Google Play requires lifetime of **25** years
- Does not require revocation information
- **25** year Twilight Zone Marathons

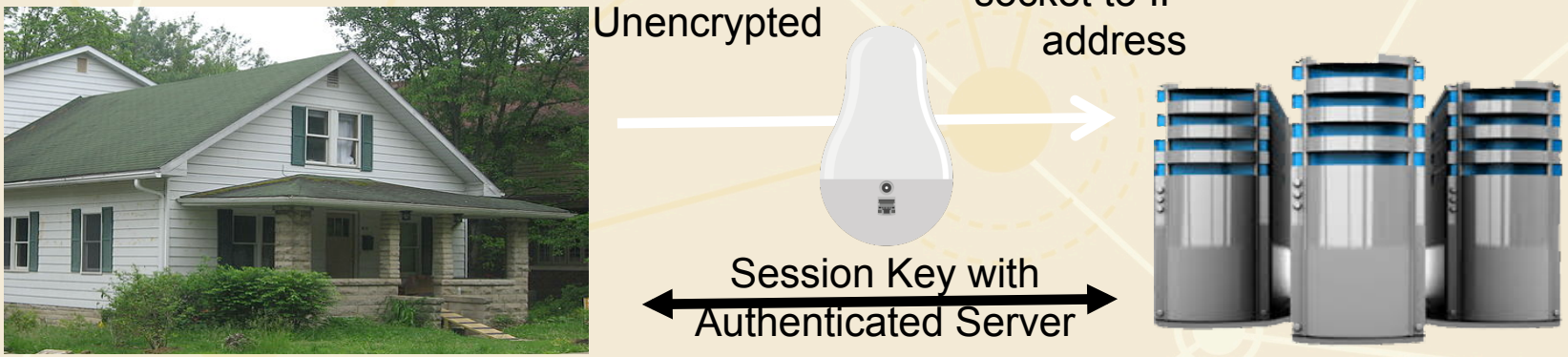
Sen.se

- Connects through any hub
- All sensor data that is received by the Mother, from the USB devices (“cookies”), is sent to the cloud
- Cookies send data through closest Mother



Sen.se

- Verifies connection to server
- Then sends data through second unsecured web socket



Testable Predictions

- Last observation of a traditional web server using SHA1: 2020
- SHA1 certificates by definition will remain at least until 2025
- Last observation of SHA1 mobile (including IoT apps): 2030

- Wildcards will continue unless made unusable and non-interoperable

Related Publications

- Zheng Dong, Kevin Kane, Siyu Chen, and L. Jean Camp, “The New Wildcats: High-Risk Banking From Worst-Case Certificate Practices Online”, *Journal of Technology Science*, April 2016, http://techscience.org/a/2016041501/
- Zheng Dong, Kevin Kane, and L Jean Camp, “Detection of Rogue Certificates from Trusted Certificate Authorities Using Deep Neural Networks”, *ACM Transactions on Privacy and Security (was TISSEC)*, 19:2, (2016)
- Zheng Dong, Apu Kapadia, Jim Blythe and L. Jean Camp, “Beyond the Lock Icon: Real-time Detection of Phishing Websites Using Public Key Certificates”, *eCrime* 2015 APWG (Barcelona, SP) 26-29 May 2015. Best Paper Award.
- S. Chen, Timothy Kelley, Zheng Dong, and L. Jean Camp, “The Effects of HeartBleed on Certificate Change: Meh”, *ACSAC* (Los Angeles, CA) 7 – 11 December 2015.

Indiana U

Faculty
L Jean Camp
www.ljean.com

Post Doctoral Fellow
Tim Kelley
www.linkedin.com/in/timothykelley

Students
Jacob Abbott: MS Secure Computing
www.linkedin.com/in/jacob-abbott-74b33b14

Siyu Chen (Alumni, at Amazon)
www.linkedin.com/in/syc404

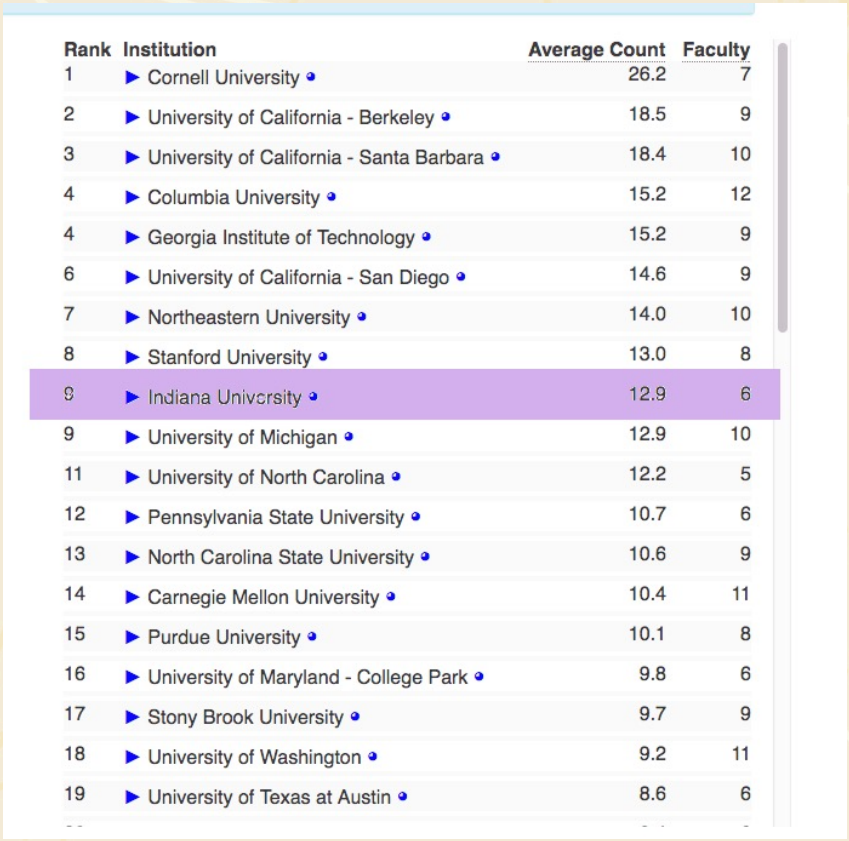
David Cooper: MBA
www.linkedin.com/in/dacooper1

Microsoft

Microsoft Research
Kevin Kane
www.microsoft.com/en-us/research/people/kkane/

Microsoft Corporation
Zheng Dong
www.linkedin.com/in/zhdong

IU. Visitors & speakers welcome.



Rank	Institution	Average Count	Faculty
1	Cornell University	26.2	7
2	University of California - Berkeley	18.5	9
3	University of California - Santa Barbara	18.4	10
4	Columbia University	15.2	12
4	Georgia Institute of Technology	15.2	9
6	University of California - San Diego	14.6	9
7	Northeastern University	14.0	10
8	Stanford University	13.0	8
9	Indiana University	12.9	6
9	University of Michigan	12.9	10
11	University of North Carolina	12.2	5
12	Pennsylvania State University	10.7	6
13	North Carolina State University	10.6	9
14	Carnegie Mellon University	10.4	11
15	Purdue University	10.1	8
16	University of Maryland - College Park	9.8	6
17	Stony Brook University	9.7	9
18	University of Washington	9.2	11
19	University of Texas at Austin	8.6	6

Remarkably Ranked.

CS Rankings Security
Dec. 2016

Ask Me About My Workshop on PKI IoT.