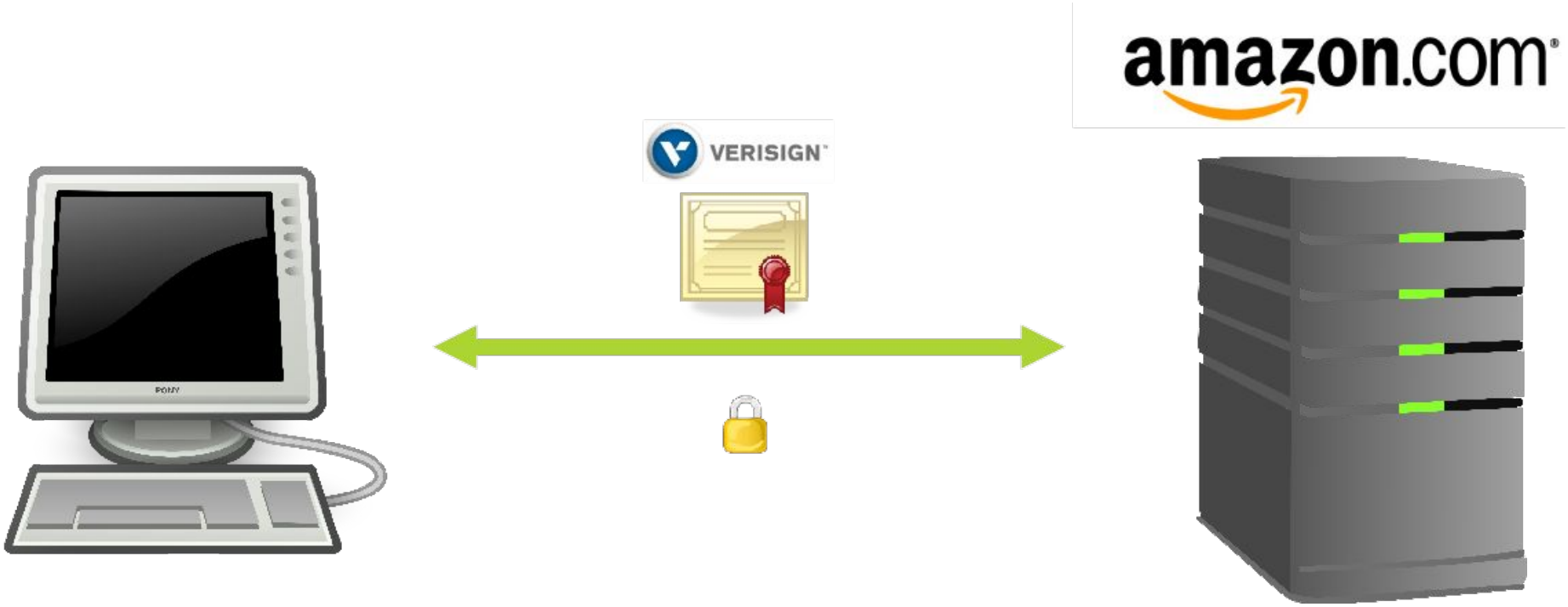
Certificate Measurements to Detect Man-in-the-Middle Attacks and Middleboxes

•••

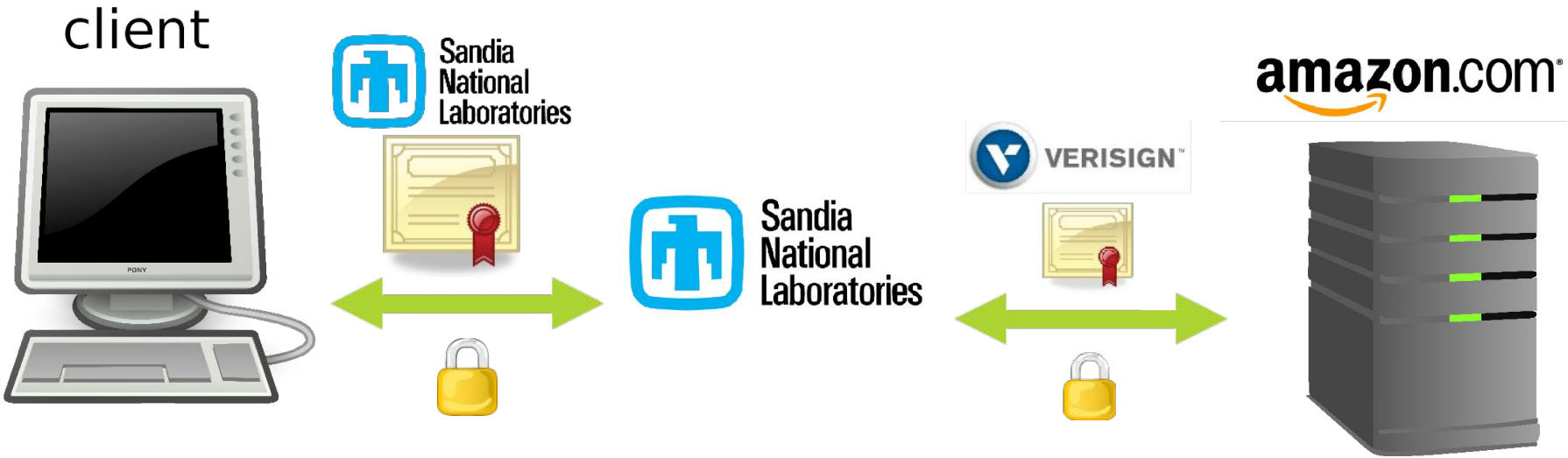
Mark O'Neill, Scott Ruoti, Kent Seamons, Daniel Zappala
Internet Research Lab & Internet Security Research Lab
Brigham Young University

Certificate validation



Man-in-the-middle attack

Middlebox


client
Sandia National Laboratories
Sandia National Laboratories
VERISIGN
amazon.com

How do they fool you?

- Add a new root cert to your system
- A company may...
  - Use private PKI infrastructure
  - Deploy a software image with new root certs
- A government may...
  - Find a CA willing to delegate signing authority to them
  - Own a CA
  - Coerce a company into signing a fake cert
- A hacker may...
  - Break into a CA and issue fake certs
  - Use malware to install a fake cert

How can we measure this?

- Own a major web site, give Flash detection tool to your users
  - Detect proxied connections to Facebook (millions)
  - Prevalence is 1/500, possibly missing those proxies that whitelist Facebook
  - Find some malware, based on self-identification in Issuer field

L.-S. Huang, A. Rice, E. Ellingsen, and C. Jackson. Analyzing forged ssl certificates in the wild. IEEE Symposium on Security and Privacy, 2014.

- Ask mobile users to install an app: Netalyzer
  - Prevalence is 1/1500, much smaller sample size (100s/1000s), requires opt in
  - No malware (yet)

N. Vallina-Rodriguez, J. Amann, C. Kreibich, N. Weaver, and V. Paxson. A tangled mass: The android root certificate stores. 10th ACM International on Conference on emerging Networking Experiments and Technologies, pages 141–148. ACM, 2014.

How can we measure this?

- Use Google Adwords to deliver Flash detection tool to users
  - Detect proxied connections to 17 sites (millions)
  - Prevalence is 1/250, varies by country
  - Find some additional malware (8%), self-identified in Issuer field

M. O'Neill, S. Ruoti, K. Seamons, D. Zappala. TLS Proxies: Friend or Foe? Internet Measurement Conference, 2016

- Observe traffic at major sites, fingerprint clients, identify middleboxes
  - Measure at Firefox update servers, Cloudflare, popular e-commerce sites
  - Prevalence is 1/25 to 1/10, malware is 1%
  - Lots of broken middleboxes

Z. Durumeric, Z. Ma, D. Springall, R. Barnes, N. Sullivan, E. Bursztein, M. Bailey, J. A. Halderman, V. Paxson. The Security Impact of HTTPS Interception, NDSS 2017

Classification of claimed Issuer Organization

- Based on self-reporting of Issuer Organization field
- Majority are business or personal firewalls (84%)
- **8% malware**
- **7% unknown (null)**

Proxy Type	Connections	Percent
Business/Personal Firewall	8,101	68.86%
Business Firewall	69	0.59%
Personal Firewall	11	0.09%
Parental Control	156	1.33%
Organization	1,394	12.66%
School	32	0.27%
Malware	1,112	8.65%
Unknown	840	7.14%
Telecom	0	0%
Certificate Authority	49	0.42%

Adware and malware

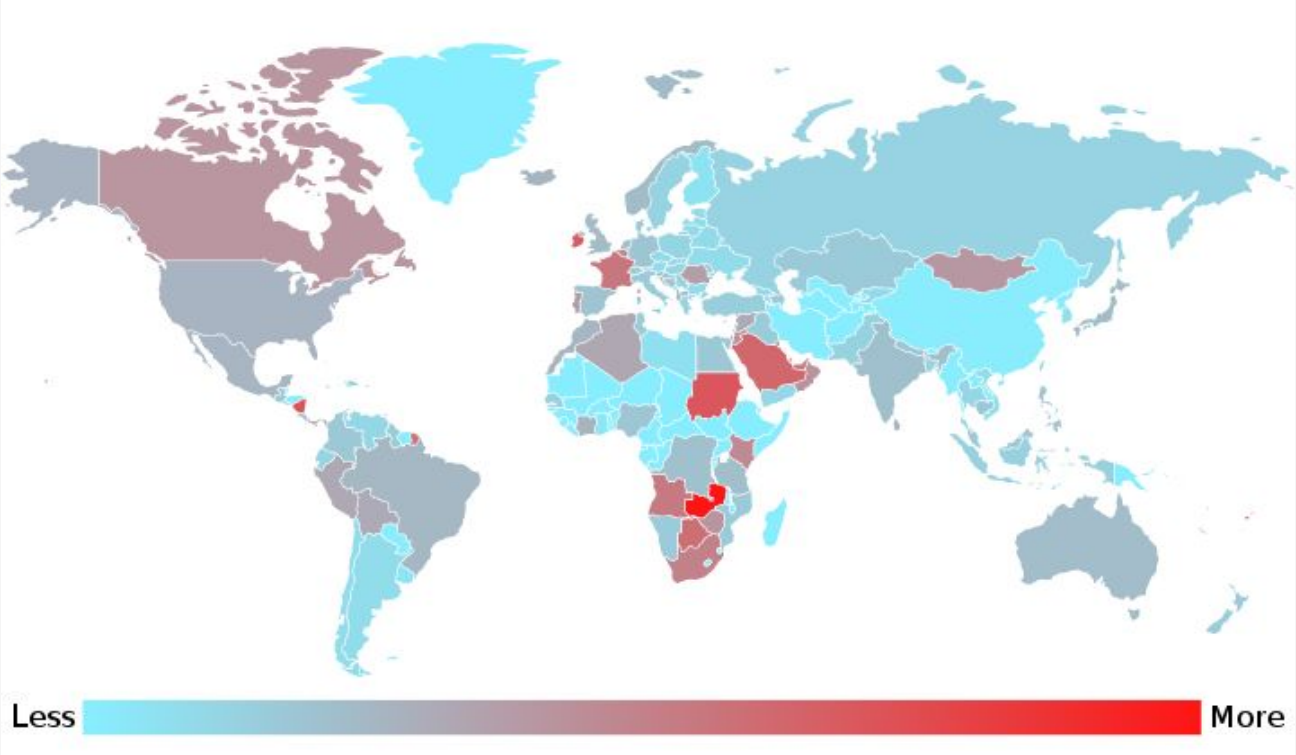
- Sendori: compromises DNS lookup
- WebMakerPlus: inserts ads in encrypted pages
- Sweesh, AtomPark: spam
- IopFailZeroAcccessCreate: malware
- Typically add a root cert to avoid browser warnings

Rank	Issuer Organization	Connections
1	Bitdefender	4,788
2	PSafe Tecnologia S.A.	1,200
3	Sendori Inc	966
4	ESET spol. s r. o.	927
5	Null	829
6	Kaspersky Lab ZAO	589
7	Fortinet	310
8	Kurupira.NET	267
9	POSCO	167
10	Qustodio	109
11	WebMakerPlus Ltd	95

Negligent Behavior

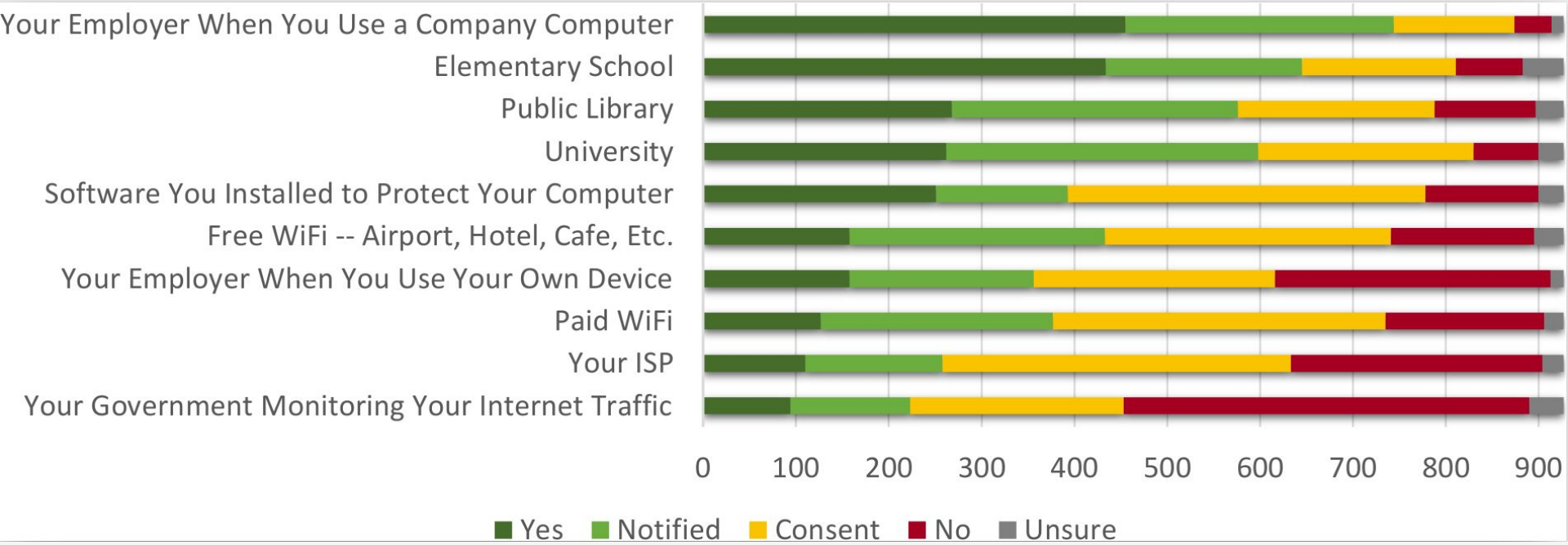
- One in parental filter (Kurupira) replaced our untrusted certificate for google.com and gmail.com with a trusted certificate signed by its own root cert
  - Allows transparent man-in-the-middle attacks
- Over half of substitute certificates have weak keys (1024 or 512 bits)
- A small percent use MD5 for signing
- A small percent claim to be signed by Digicert, though none actually are
- A small percent modify the subject field

Proxied connections by country



Highest = 12% proxy rate, Lowest = 0%

User attitudes survey: scenarios



Strong opinions on notification and consent

“If I encrypt something no one has the right to unencrypt it unless I give them the right to - simple as that.”

Now what?

- Flash measurements no longer feasible
  - Going away, no longer accept ads with active probing
- Server-side measurements
  - How do we get enough measurement locations?
  - Attackers can mimic browser or AV fingerprints — miss the attack
- Client-side measurements
  - How do we get certs that user devices (including mobile) actually see?
  - Attackers can masquerade as AV program in Issuer field — but at least see the attack
  - How can we measure this at scale?