Measuring and Improving the Management of Today's PKI

Alan Mislove, Christo Wilson, David Choffnes
Northeastern University
http://securepki.org

Motivation

A SSL certificate is a signed attestation binding a subject to a public key

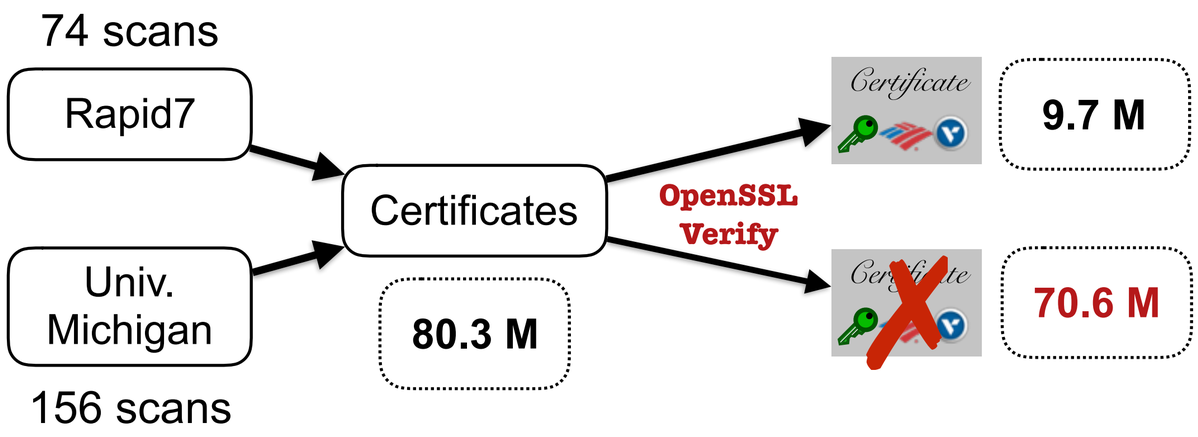
- Issued by a trusted Certificate Authority (CA)
- Forms a logical chain of certificates starting from a root certificates

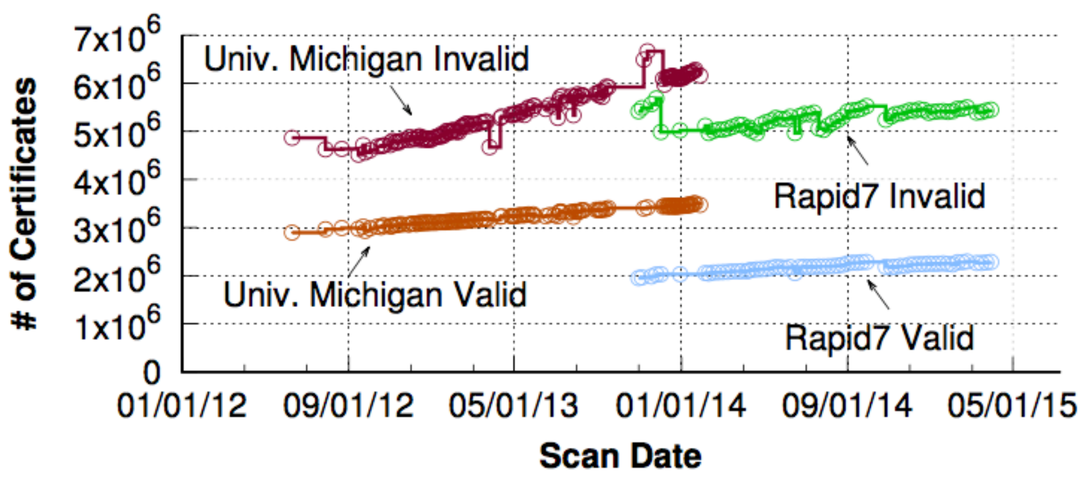
If a client is unable to validate a cert (due to sign by untrusted CA, self-signed, expired, or etc.), it is defined as invalid

- Prior studies focused **almost exclusively** on valid certificates

What's the rest of certificate ecosystem?

Datasets

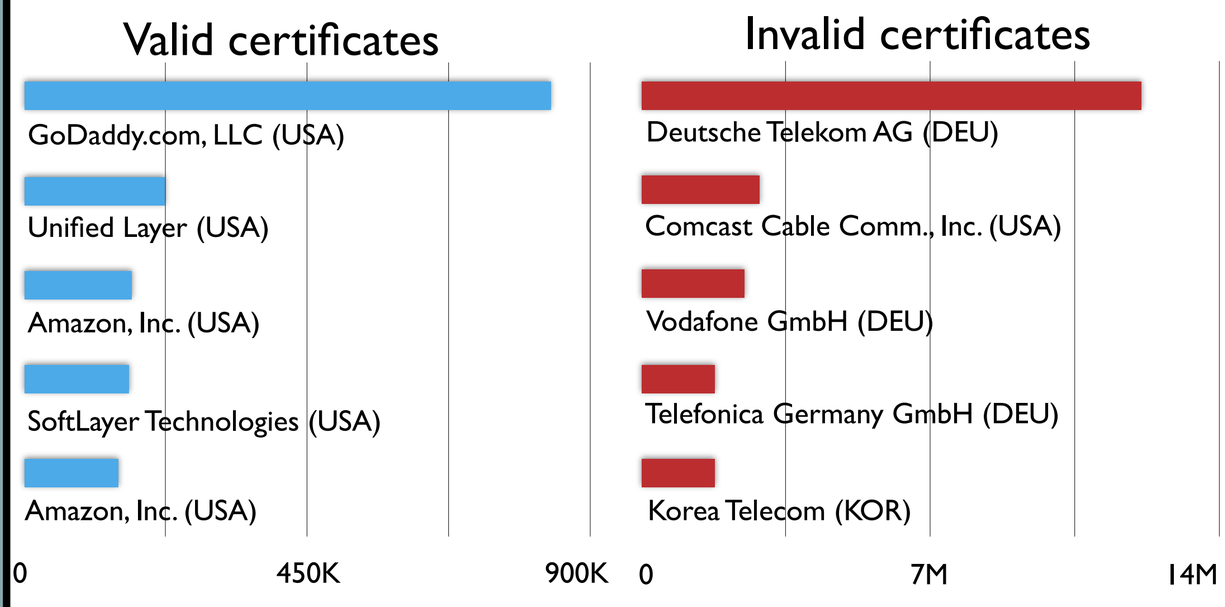




Invalid certificates are the **vast majority**
(87.9% across all scans, 65% daily scans)

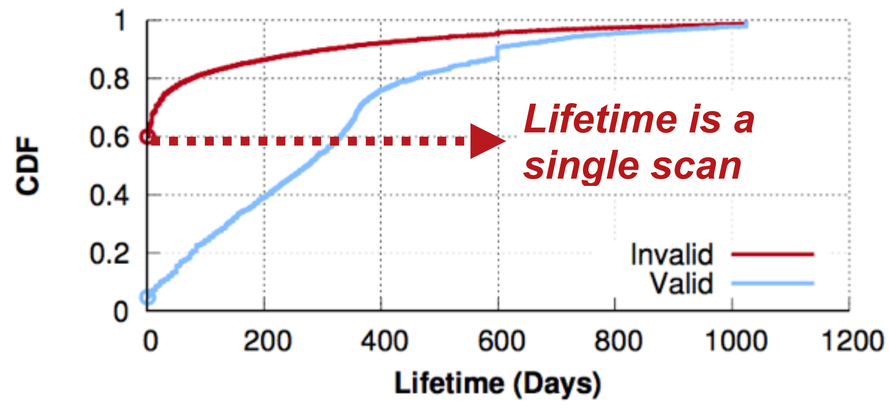
Analysis

Advertised AS (and organization) of Certificates



Invalid certificates (1) are geographically dispersed and (2) hosted with end-user home ISPs

Lifetime of Certificates

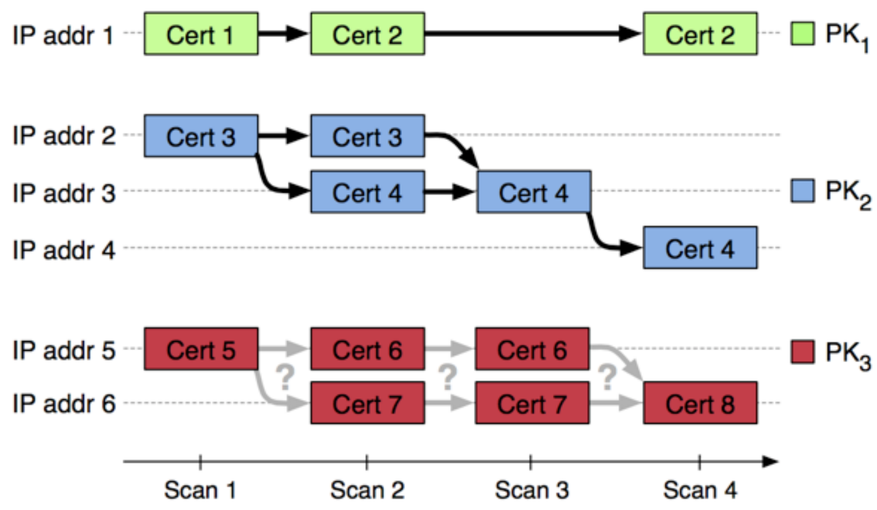


60% of invalid certificates are ephemeral and they are likely to be reissued on a regular basis

Linking Invalid Certificates

Goal: Linking Certificates across scans

1. Filter certificates advertised multiple IP address
2. Group certificates by shared field value (e.g., public key, common name, and etc.)
3. Filter certificates having overlapping lifetime



Apply above linking process for each linkable features (e.g., public key, common name, SANs, and etc.)

We're able to link 27 M certificates (39.4%)

Application

Inferring ISP IP Assignment policy

We can observe how a given ISP reassigns IP addresses to its customers by monitoring patterns of advertised IP addresses from certificates

Policy	ISP Lists
Static	Comcast Cable Communications, AT&T Internet Services, and etc. (90% of their devices are static)
Dynamic	Deutsche Telekom, Telefonica Venezolana, Tim Celular, and etc. (75% of their hosts change IP between every scan)

Conclusions

- Invalid certificates are the vast majority
- They are ephemeral and hosted by end-user devices
- They can be linked using latent features, giving us insight to (1) infer ISP IP assignment policy and (2) track end-user devices

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF SaTC Principal Investigator Meeting
Jan 9-11, 2017
Alexandria, VA