The Boon and Bane of Cross-Signing

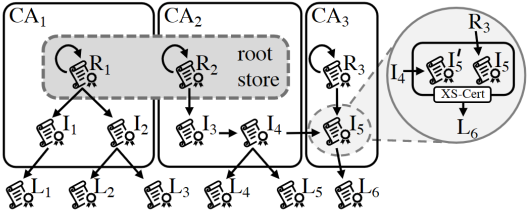
Shedding Light on a Common Practice in Public Key Infrastructures

Presenter: Ken Fang

September 26, 2021

Crossing-Signing: Motivation, Overview, Related work

- PKIs provide trust infrastructure for today's internet
  - Web shopping, online banking, mobile apps, health systems, industry, etc.



- Related Work
  - Certificate Validation Errors [CCS'17]
  - Non-XS revocation issues [IMS'15, S&P'13]
  - Crossing related
    - Observed many XS certificates
    - XS cause intransparency
    - Check CA policy compatibility for XS

Shredding Light on Cross-signing

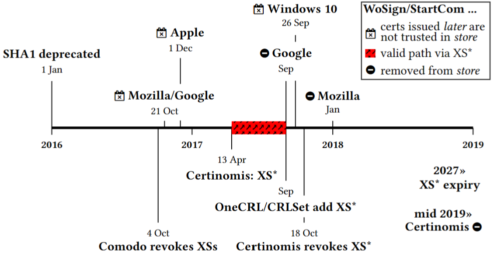
- Datasets
  - Passive Dataset (ICSI Notary)
    - Certificates from real user traffic
  - CA Certificate from CT
  - Root stores of Mozilla, Google, Apple, Microsoft, and state PKIs
- Cross-signing Certificate
  - 322 Cross-signed CAs
    - 86 Cross-signed Root CAs
    - 236 Cross-signed intermediates
  - 47221 leaf XS-certs

- Results Overview

⚠	Valid after revocation	16	*
⚠	PKI barrier breaches	7	*
✓	Bootstrapping	57	
+/−	Expanded trust (new stores / longer time)	64 / 46	
+/−	Alternative paths	155	
+/−	Support of multiple signature algorithms	23	
+/−	Ownership change	35	*
🐞	Backdating	7	*
🐞	Missing transparency	2	*

The Bad: Undesired trust paths

- Valid paths after revocation
  - CA CRLs
  - Vendor-controlled CRLs
- Bypassing special Rules
  - Certinomis of cross-sign of Startcom
- PKI barrier breaches
  - US FPKI: not accepted by Mozilla
    - But cross-signed by Identrust and Verisign



WoSign/StartCom ...

☒ certs issued *later* are not trusted in *store*

🟥 valid path via XS*

⊖ removed from *store*

SHA1 deprecated 1 Jan

☒ **Apple** 1 Dec

☒ **Windows 10** 26 Sep

⊖ **Google** Sep

☒ **Mozilla/Google** 21 Oct

⊖ **Mozilla** Jan

2016 **2017** **2018** **2019**

13 Apr **Certinomis: XS***

Sep **OneCRL/CRLSet add XS***

4 Oct **Comodo revokes XSs**

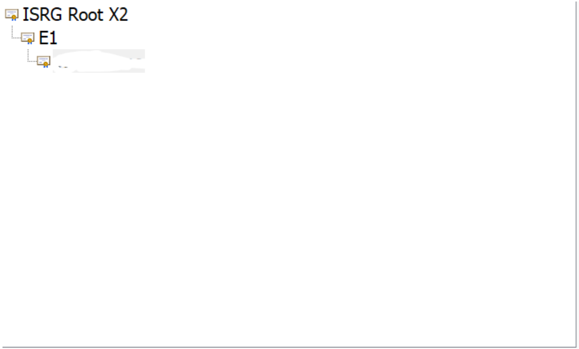
18 Oct **Certinomis revokes XS***

2027» XS* expiry

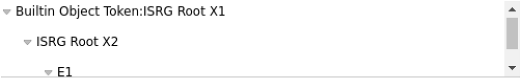
mid 2019» Certinomis ⊖

The Good: Bootstrapping CAs

- Let's Encrypt
  - Bootstrapped by using cross-sign by Identrust
  - Finally don't need cross-signed at end of this month
- Many other examples like: Amazon, CNNIC, etc



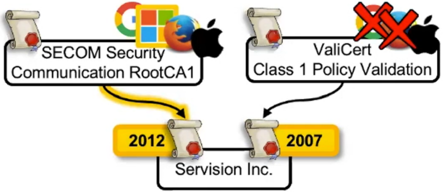
ISRG Root X2
E1



Builtin Object Token:ISRG Root X1
ISRG Root X2
E1

Controversial Benefits & Pitfalls

- Other Controversial Benefits
  - Expand trust
    - More root store
    - Longer validity
  - Fall-back Paths



Migrating risks of Cross-signing

- Short Validity Periods
  - Quick Phase out needless cross-sign.
- XS certificate extension
  - Shed light on motivation
  - Limit cross-sign to intended effect

Conclusion

- Cross-signing is common in web PKI
- The Bad: Undesired trust paths
- The Good: Bootstrapping CAs
- Limit Risk while keep benefits
  - Short Validity Periods
  - certificate extension
  - Improve transparency: have report on revocations

Issues

- No clearly measurement result.
- TLS certificate is only a subset of Certificate. (Data may biased)

The End