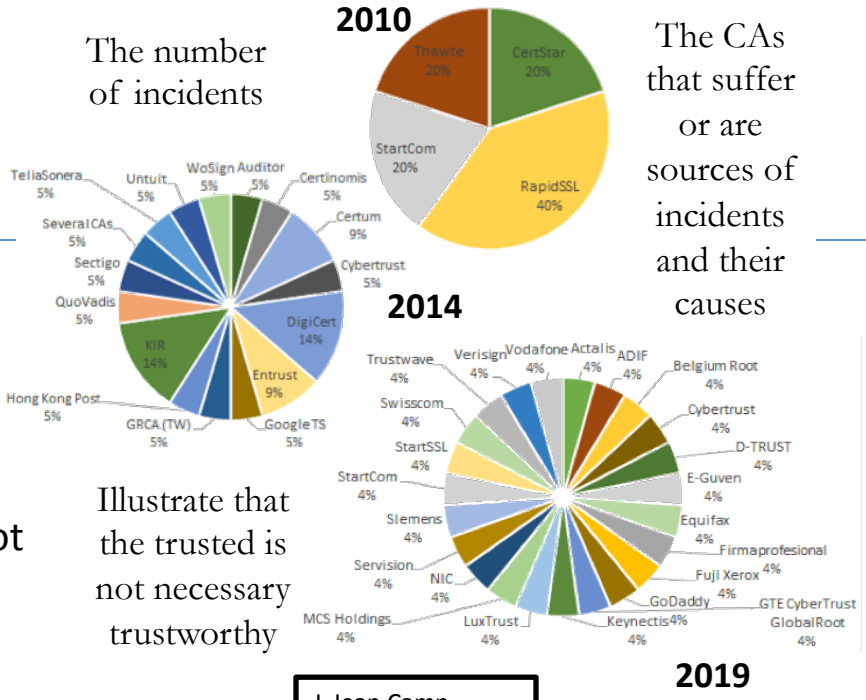
Understanding Socio-Technical Failure Modes in Public Key Infrastructures

Challenge:

- Certificate Authorities are the foundation of trust on the Internet
- The failures are often considered purely technical
- Understanding organizational, economic, and human factors of these failure modes
- Each incident may impinge very few to millions

As the Internet has expanded from the laboratory, throughout the academy, to global commerce and crime, into the infrastructure, out to the home, in clothing, embedded into automobiles, and even into the body the underlying trust infrastrutue is still managed by a few root program operators and the CA Browser Forum. The risks of this are not understood.

The number of incidents



The CAs that suffer or are sources of incidents and their causes

Illustrate that the trusted is not necessary trustworthy

Solution:

- Investigation of CA failures
- Evaluate perceptions of trust provided by signed certificates
- Remove roots that do not align with human trust models
- Multilevel warning systems when the alignment is lacking

Scientific Impact:

- Classification of failure modes of CAs identified failures from large number of CAs
- Many of the failures were a result of purposeful business practice
- User perceptions of the meaning of certificates is far from what they offer
- Evaluation of failures indicates the trust of current CAs is not a match for the technologies being constructed upon it

Broader Impact:

- Include diverse stakeholders in investigation of perceptions of PKI
- Publication at policy as well as computer science events
- Outreach to leaders in cryptography at root program owners

L Jean Camp
Indiana University

CNS 1814518