



Empirical Security Analysis & Engineering

‘Any security technology whose effectiveness can’t be empirically determined is indistinguishable from blind luck.’ (Dan Geer)

- There are countless examples where security failed in real-world deployment



Empirical Security Analysis & Engineering

‘Any security technology whose effectiveness can’t be empirically determined is indistinguishable from blind luck.’ (Dan Geer)

- There are countless examples where security failed in real-world deployment, sometimes spectacularly.
- Often: too hard, complex, or uneconomical to do right



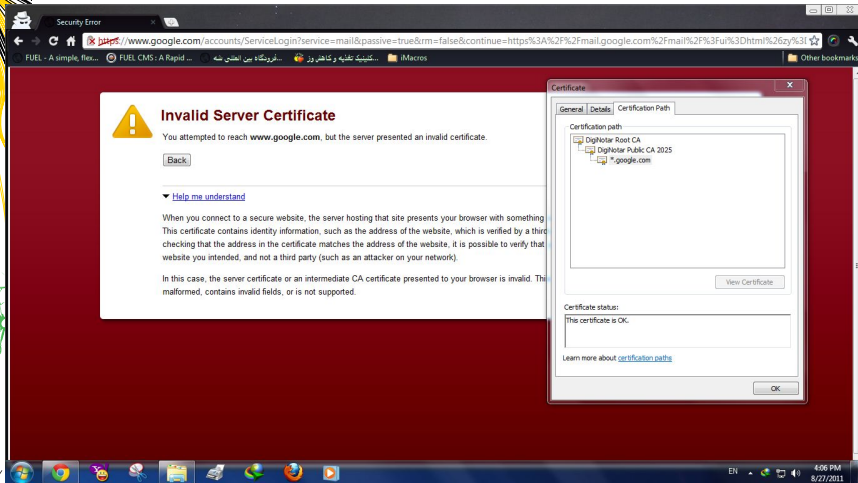
Empirical Security Analysis & Engineering

‘Any security technology whose effectiveness can’t be empirically determined is indistinguishable from blind luck.’ (Dan Geer)

- There are countless examples where security failed in real-world deployment, sometimes spectacularly.
- Often: too hard, complex, or uneconomical to do right
- We look at lessons learnt and some hands-on practice
- We learn from *empirical measurement*



Web PKI: DigiNotar meltdown



What happened here?



Massively broken crypto

Widespread Weak Keys in Network Devices

We performed a large-scale study of RSA and DSA cryptographic keys in use on the Internet and discovered that significant numbers of keys are insecure due to insufficient randomness. These keys are being used to secure TLS (HTTPS) and SSH connections for hundreds of thousands of hosts.

- We found that 5.57% of TLS hosts and 9.60% of SSH hosts share public keys in an apparently vulnerable manner, due to either insufficient randomness during key generation or device default keys.
- We were able to remotely obtain the RSA private keys for 0.50% of TLS hosts and 0.03% of SSH hosts because their public keys shared nontrivial common factors due to poor randomness.
- We were able to remotely obtain the DSA private keys for 1.03% of SSH hosts due to repeated signature randomness.

Nearly all the vulnerable hosts are headless and embedded network devices, such as routers, firewalls, and server management cards. These types of devices often generate keys automatically on first boot, and lack many of the physical sources of randomness used by traditional PCs to generate random numbers. We identified apparently vulnerable devices and software from 54 manufacturers and notified these companies about the problems.

In experiments with several popular open-source software components, we were able to reproduce these vulnerabilities and show how such weak keys can arise in practice. Most critically, we found that the Linux random number generator can produce predictable output at boot under certain conditions, although we also observed compromised keys on BSD and Windows-based systems.

Learn more:

[Research Paper](#)[FAQ](#)



Broken operations: DNS/DNSSEC

Understanding the Role of Registrars in DNSSEC Deployment

Taejoong Chung
Northeastern University

Roland van Rijswijk-Deij
University of Twente and SURFnet

David Choffnes
Northeastern University


Dave Levin
University of Maryland

Bruce M. Maggs
Duke University and
Akamai Technologies

Alan Mislove
Northeastern University

Christo Wilson
Northeastern University

ABSTRACT



The Domain Name System (DNS) provides a scalable, flexible name resolution service. Unfortunately, its unauthenticated architecture has become the basis for many security attacks. To address this, DNS Security Extensions (DNSSEC) were introduced in 1997. DNSSEC's deployment requires support from the top-level domain (TLD) registries and registrars, as well as participation by the organization that serves as the DNS operator. Unfortunately, DNSSEC has seen poor deployment thus far: despite being proposed nearly two decades ago, only 1% of .com, .net, and .org domains are properly signed.

In this paper, we investigate the underlying reasons *why* DNSSEC adoption has been remarkably slow. We focus on registrars, as most TLD registries already support DNSSEC and registrars often serve as DNS operators for their customers. Our study uses large-scale, longitudinal DNS measurements to study DNSSEC adoption, cou-

CCS CONCEPTS

- **Security and privacy** → **Public key (asymmetric) techniques;**
- **Networks** → **Application layer protocols; Security protocols; Naming and addressing;**

KEYWORDS

DNS; DNSSEC; DNS Security Extension; PKI; Public Key Infrastructure; Registrar; DNS Operator

ACM Reference format:

Taejoong Chung, Roland van Rijswijk-Deij, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. 2017. Understanding the Role of Registrars in DNSSEC Deployment. In *Proceedings of IMC '17, London, United Kingdom, November 1–3, 2017*, 15 pages. <https://doi.org/10.1145/3131365.3131373>

Measuring privacy leaks

BMJ

[WHO WE ARE](#) [WHAT WE DO](#) [PRODUCTS & SERVICES](#) [NEWSROOM](#) [WORK AT BMJ](#) [CONTACT US](#) [Q](#)

Data sharing by popular health apps is routine and far from transparent

[BMJ](#) / [Newsroom](#) / [Newsroom](#) / [Data sharing by popular health apps is routine and far from transparent](#)



Details

- Course code: 202100073
- 5 ECTS
- **Completely online in 2021**
- Mon 10:45-12:30 (lecture), Wed 08:45-12:30 (tutorial)

