Key Sharing in the SSL Ecosystem

Frank Cangialosi[1], Taejoong Chung[2], David Choffnes[2], Dave Levin[1], Bruce M. Maggs[3], Alan Mislove[2], Christo Wilson[2]
[1]University of Maryland, [2]Northeastern University, [3]Duke University and Akamai Technologies

Problem

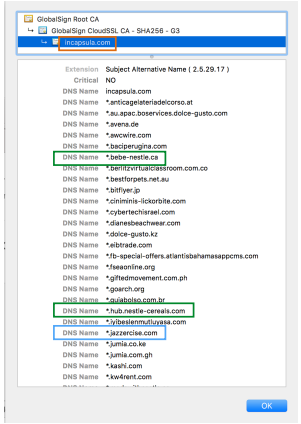
HTTPS content is often hosted by third parties like CDNs. To do this, **websites share their private keys** which:

- Violates the basic assumptions of the PKI
- Creates a centralized target for attackers

We seek to quantify the extent of key sharing and the implications it has on the management certificates

How are keys shared?

- **Upload** keys to provider (AWS)
- **Delegate** key generation to the provider (Akamai)



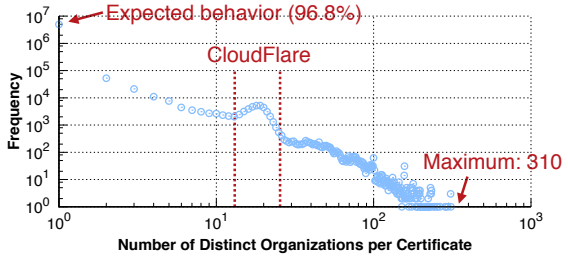
Some providers aggregate multiple customers onto **"cruiseliner certificates"** with large SAN lists

Spirit: One organization
Practice: Many organizations

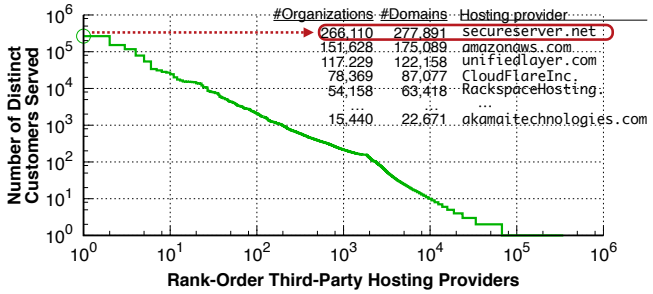
Data

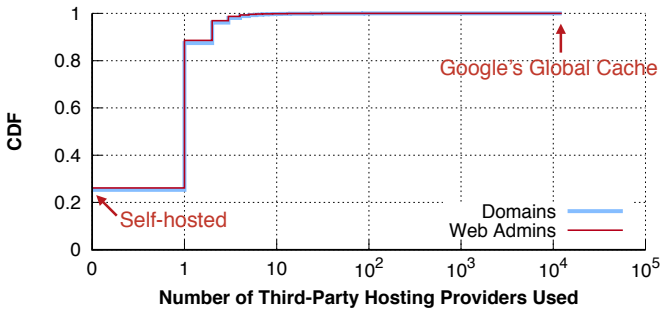
We draw from multiple datasets, including:
1. Full IPv4 certificate scans from Rapid7
2. WHOIS data to ascertain **domain ownership**

How often are organizations aggregated on a single certificate?

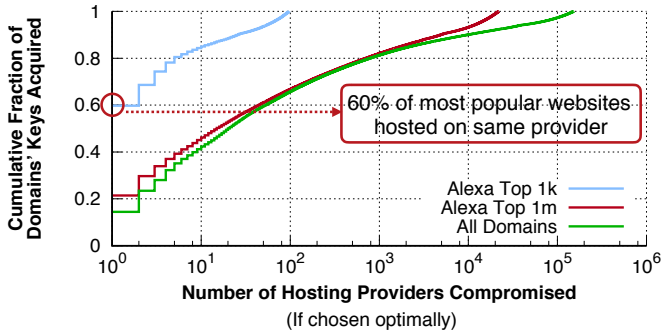


Trust: The Extent of Sharing





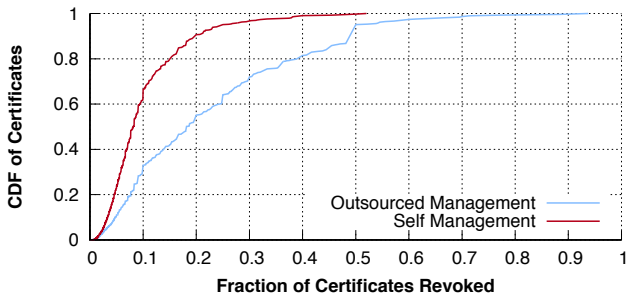
73.9% of companies share their private keys, some with thousands of third-party hosting providers.



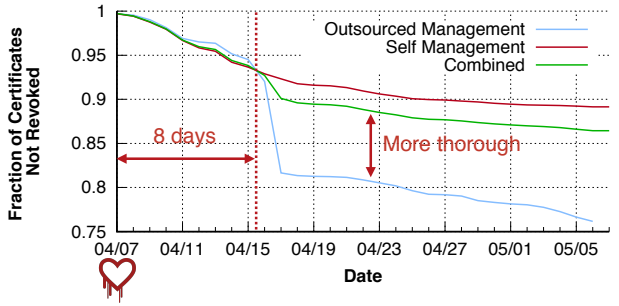
By compromising 10 hosting providers, attackers could gain access to 40-74% of all domains' private keys.

Management: The Implications

Natural experiment: reaction to Heartbleed



Certificates managed by third-party hosting providers tend to have slightly better revocation rates



Third-party hosting providers are *slower to react* to events, but ultimately more thorough

Conclusions

- Key sharing is rampant
- Hosting providers are prime targets for attack
- Future: new techniques that enable providers to serve content without access to private keys.

This work was supported in part by NSF awards CNS-1564143 and CNS-1563320, and by the NSA as part of a Science of Security lablet.