Poster: Monogamous relationships with short-term commitment are the best (for certificate management)

Carl Magnus Bruhner, *Linköping University, Sweden*

Title	Changing of the Guards: Certificate and Public Key Management on the Internet
Authors	Carl Magnus Bruhner[1], Oscar Linnarsson[1], Matus Nemec[1], Martin Arlitt[2], and Niklas Carlsson[1]
Affiliations	[1]Linköping University, Sweden; [2]University of Calgary, Canada
Date	March 28-30, 2022
Venue	Passive and Active Measurement (PAM) Conference 2022, Virtual event
Published in	Hohlfeld, O., Moura, G., Pelsser, C. (eds) Passive and Active Measurement. PAM 2022. Lecture Notes in Computer Science, vol 13210. Springer, Cham.

Abstract

Certificates are the foundation of secure communication over the internet. However, not all certificates are created and managed in a consistent manner and the certificate authorities (CAs) issuing certificates achieve different levels of trust. Furthermore, user trust in public keys, certificates, and CAs can quickly change. Combined with the expectation of 24/7 encrypted access to websites, this quickly evolving landscape has made careful certificate management both an important and challenging problem. In this paper, we first present a novel server-side characterization of the certificate replacement (CR) relationships in the wild, including the reuse of public keys. Our data-driven CR analysis captures management biases, highlights a lack of industry standards for replacement policies, and features successful example cases and trends. Based on the characterization results we then propose an efficient solution to an important revocation problem that currently leaves web users vulnerable long after a certificate has been revoked.

Acknowledgment

This work was partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP) funded by the Knut and Alice Wallenberg Foundation.

DOI/Links

DOI	10.1007/978-3-030-98785-5_3
Accepted	https://www.ida.liu.se/~nikca89/papers/pam22.pdf https://urn.kb.se/resolve?urn=urn:nbn:se:liu:diva-184851
Presentation	https://www.youtube.com/watch?v=2ekFrDxLn6c

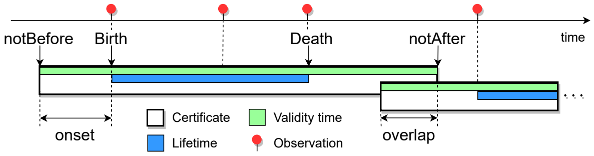
Monogamous relationships with short-term commitment are the best*

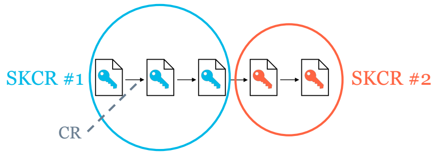
Changing of the Guards: Certificate and Public Key Management on the Internet (Proc. Passive and Active Measurement Conference, PAM 2022)

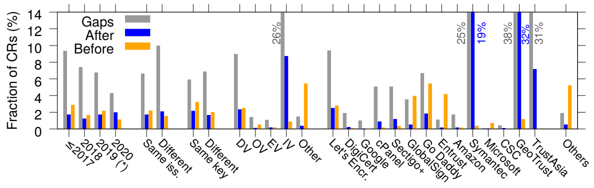
- We present a novel server-side characterization of certificate replacement (CR) relationships in the wild, including the reuse of public keys.
- We capture management biases, highlight a lack of industry standards for replacement policies, and feature successful example cases and trends.
- We propose an efficient solution with short-lived certificates to address the current risk of web users being vulnerable long after a certificate has been revoked.

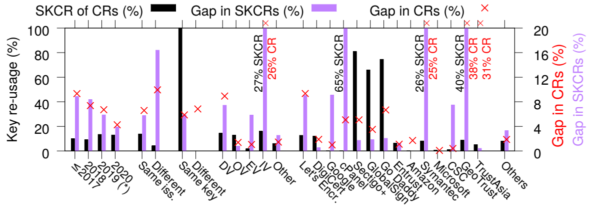
Method

- We parse and process certificates from Rapid7 Project Sonar dataset, extracting birth and death of certificates.
- We identify certificate replacements (CRs) and chains of CRs that reuse the same public key (SKCR).
- We perform an analysis of CR relationships and SKCR chains to characterize CR relationships in the wild.







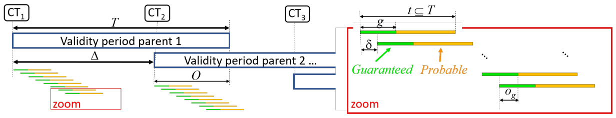


Results

- CR gaps and overlaps are decreasing over time.
- Changing CA more frequently results in more gaps.
- EV and OV certificates have the fewest gaps.
- Long-lived certificates have more gaps after expiry.
- Long SKCR chains are dominated by automation.

A case for short-lived certificates

We propose an efficient solution of parent–child certificates, limiting the cost of short-lived certificates. With this proposal, short validity can replace the need of timely revocation checks.



Carl Magnus Bruhner, Oscar Linnarsson, Matus Nemec, Martin Arlitt, and Niklas Carlsson (2022).
Changing of the Guards: Certificate and Public Key Management on the Internet. In: Hohlfeld, O., Moura, G., Pelsser, C. (eds) Passive and Active Measurement. PAM 2022. Lecture Notes in Computer Science, vol 13210. Springer, Cham. DOI: 10.1007/978-3-030-98785-5_3

Full paper

* for certificate management