To Trust, or not to Trust, that is the Question: Structural Properties of X.509 Certificates

Johanna Amann[1], Robin Sommer[1,3], Matthias Vallentin[2], Seth Hall[1]
[1]International Computer Science Institute [2]UC Berkeley
[3]Lawrence Berkeley National Laboratory

ABSTRACT

The SSL/TLS protocol suite constitutes the key building block of today's Internet security, providing encryption and authentication for end-to-end communication with its underlying X.509 certificate infrastructure. However, the system remains brittle due to its liberal delegation of signing authority: a single compromised certification authority undermines trust globally. Several recent high-profile incidents have demonstrated this shortcoming. A striking example is the 2012 breach of the DigiNotar Certificate Authority (CA) where 30 CA certificates were compromised. The perpetrators used these certificates, e.g., to carry out man-in-the-middle-attack attacks against users in Iran accessing Google [3]. Over time, the security community has proposed a number of countermeasures to increase the security of the certificate ecosystem; examples include DANE, which supports certificate pinning through DNS, TACK which pins certificates to server keys, or HPKP which instructs web-clients to pin certificates for future connections [2].

We set out to understand to which degree benign changes to the certificate ecosystem share structural properties with attacks, based on a large-scale data set of more than 17 billion SSL/TLS sessions [1]. We find that common intuition falls short in assessing the maliciousness of an unknown certificate, since their typical artifacts routinely occur in benign contexts as well. Examples include certificates being signed by intermediate CA certificates that were not encountered before (e.g. for `delaware.gov`); sites starting to use certificates signed by different CAs while continuing to use their old certificates (e.g. for `americanexpress.com`); and new certificates being issued while the current ones are still valid for a significant time.

BODY

Even for a human observer with full knowledge it is impossible to decide if a new certificate is legitimate without out-of-band context.

REFERENCES

[1] Johanna Amann, Robin Sommer, Matthias Vallentin, and Seth Hall. No Attack Necessary: The Surprising Dynamics of SSL Trust Relationships. In *Proc. Annual Computer Security Applications Conference*, 2013.

[2] Jeremy Clark and Paul C. van Oorshot. SoK: SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements. In *Proc. IEEE Security and Privacy*, 2013.

[3] Ronald Prins. DigiNotar Certificate Authority Breach "Operation Black Tulip". Interim Report, Fox-IT, September 2012.

Volume 3 of Tiny Transactions on Computer Science