Distributed Domain Validation (DDV)

Markus Brandt Haya Shulman Michael Waidner
Fraunhofer SIT / Technische Universität Darmstadt

September 21, 2019

The security of Internet-based applications fundamentally relies on the trustworthiness of Certificate Authorities (CAs). One of the most popular approaches to prove ownership is Domain Validation (DV). Although efficient and cheap, DV is vulnerable to attacks. The security of Internet-based applications fundamentally rely on the trustworthiness of Certificate Authorities (CAs). One of the most popular approaches to prove ownership is Domain Validation (DV). Although efficient and cheap, DV is vulnerable to attacks [BDK+18, BLSE+18].

There are attempts to create alternative PKIs and proposals to use additional entities for storing and checking certificates. They require a complete change of the architecture, or they only identify already issued certificates. Due to these obstacles, the new proposals are not deployed.

To mitigate the threats without requiring changes to the existing PKI, we propose Distributed Domain Validation (DDV). DDV mitigates the vulnerabilities without the need for cryptography by making assumptions in distributed systems. DDV uses multiple vantage points while ensuring that the paths of each vantage point do not overlap to avoid possible hijacks from a single Autonomous System (AS). While retaining the benefits of DV (automation, efficiency and low costs) DDV is secure even against Man-in-the-Middle (MitM) attackers. Deployment of DDV is simple and does not require changing the existing infrastructure nor systems of the CAs. We demonstrate the security of DDV under realistic assumptions and provide open-source access to DDV implementation.

References

[BDK+18] Markus Brandt, Tianxiang Dai, Amit Klein, Haya Shulman, and Michael Waidner. Domain validation++ for mitm-resilient pki. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, pages 2060–2076, New York, NY, USA, 2018. ACM.

[BLSE+18] Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal. Bamboozling certificate authorities with BGP. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 833–849, Baltimore, MD, August 2018. USENIX Association.

crypto day matters 31 (2019)
Beiträge vom 31. Kryptotag, 17.-18.10.2019, Qualcomm, Berlin.
doi:10.18420/cdm-2019-31-21