IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, November 2022
Impact Factor: 6.252

Blockchain-based Certificate Verification

Harshada S. Nichit[1], Mitali J. Gadge[2], Pallavi S. Sonawale[3], Sneha S. Gadekar[4], Prof. Rote R.[3]
Students[1,2,3,4] and Guide[5]
Samarth Group of Institution College of Engineering Belhe, Maharashtra, India

Abstract: *Traditional public key infrastructures (PKIs) depend on trusted certification authorities (CAs) to issued certificates, used in SSL/TLS to verified web servers and establish secure channels. However, recent security incidents shows that CAs may issue fake certificates. In this paper, we suggest blockchain-based certificate transparency (CT) and revocation transparency (RT) to balance the complete authority of CAs. Our scheme is suitable to PKIs but significantly reinforces the security guarantees of a certificate. The CA-issues certificates and their cancellation status information of an SSL/TLS web server are published by the subject (i.e., the web server) as a transaction in the global certificate blockchain. The certificate blockchain acts as add only public logs to monitor CAs' certificate issues and revocation operations, and an SSL/TLS web server is permits with the cooperative control on its certificates. A browser compares the certificate received in SSL/TLS negotiations with the ones in the public certificate blockchain, and accepts it only if it is published and not cancelled. We apply the prototype system with Firefox and Nginx, and the trial results show that it establishes reasonable overheads.*

Keywords: Blockchain; Certificate transparency; Certificate revocation; Public key infrastructure; Trust management.

REFERENCES

[1]. M. Abadi, A. Birrell, I. Mironov, T. Wobber, and Y. Xie, "Global authentication in an untrustworthy world," in 14th USENIX Conference on Hot Topics in Operating Systems (HotOS), 2013.
[2]. M. Alicherry and A. Keromytis, "Doublecheck: Multi-path verification against man-in-the-middle attacks," in 14th IEEE Symposium on Computers and Communications (ISCC), 2009, pp. 557–563.
[3]. R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose, "IETF RFC 4033 - DNS security introduction and requirements," 2005.
[4]. C. Arthur. (2011) Rogue web certificate could have been used to attack Iran dissidents. [Online]. Available: https://iranian.com/main/news/2011/08/30/
[5]. rogue-web-certificate-could-have-been-used-attack-iran-dissidents. html
[6]. G. Ateniese and S. Mangard, "A new approach to DNS security (DNSSEC)," in 8th ACM Conference on Computer and Communications Security (CCS), 2001, pp. 86–95.
[7]. J. Braun, F. Volk, J. Classen, J. Buchmann, and M. Mu¨ hlha¨user, "CA trust management for the Web PKI," Journal of Computer Security, vol. 22, no. 6, pp. 913–959, 2014.
[8]. M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in 3rd Symposium on Operating Systems Design and Implementation (OSDI), 1999, pp. 173–186.
[9]. Censys. (2016) Censys public reports. [Online]. Available: https://censys.io/
[10]. M. Chase and S. Meiklejohn, "Transparency overlays and applications," in 13th ACM Conference on Computer and Communications Security (CCS), 2016, pp. 168–179.