ICRC: Instant Certificate Revocation Checking using Blockchain-backed Bloom Filters

Vinothkumar Nagasayanan, Elias Rohrer, and Florian Tschorsch
Distributed Security Infrastructures
Technical University Berlin

30th Crypto Day, March 28/29, 2019

TLS-based protocols, such as HTTPS, are relying on certificates to enable authenticated communications. Currently, most web browsers use the Online Certificate Status Protocol (OCSP) to verify the revocation status of each individual certificate. However, OCSP introduces a significant delay during the TLS handshake and leaks unnecessary information to the OCSP providers. While OCSP Stapling and OCSP Must-Staple are designed to mitigate these issues, they are far from global deployment, as shown by Chung *et al.* (2018).

In our work, we introduce *ICRC*, a new blockchain-based architecture that manages certificate revocation data and allows clients to retrieve the revocation status efficiently. To this end, browsers periodically retrieve updates from a consortium blockchain (e. g., consisting of all major CAs) holding global certificate revocation data. Clients verify the certificate status based on their local state, which mitigates the delay overhead and privacy concerns. In order to minimize the data and therefore being able to maintain tight update cycles, we exchange revocation data using Bloom filters.

To show the feasibility of our approach, we implemented a proof of concept of ICRC. It consists of a working client prototype based on Mozilla Firefox that connects to a consortium blockchain based on Hyperledger Sawtooth. Moreover, we conducted a pilot study that confirmed the significant issues of OCSP: the OCSP response delays varied heavily depending on the client's geographical location. However, we found that around a third of the average TLS handshake's delay can be attributed to the OCSP induced delay. Moreover, we found that a large number of OCSP providers were entrusted with the requests, leaking possibly private information. The pilot study clearly shows the potential merits of our approach, which simply does not introduce additional delay or privacy concerns.

References

Taejoong Chung, Jay Lok, Balakrishnan Chandrasekaran, David R. Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, John P. Rula, Nick Sullivan & Christo Wilson (2018). Is the Web Ready for OCSP Must-Staple? In *IMC: '18: Proceedings of the Internet Measurement Conference*, 105–118.

crypto day matters 30 (2019)
Beiträge vom 30. Kryptotag, 28.-29.03.2019, Mozilla, Berlin.
doi:10.18420/cdm-2019-30-10