

Thesis
M.Sc.

IDP, HiWi

Traceable Measurement Result Publication in Append-only Ledgers

Motivation

Many scientist and research institutes conduct regular Internet measurements. These measurements result in lots of data that can partially be accessed online^a. The data, however, is not interconnected and retroactive changes are non-detectable. To publish data in an integrated and traceable way, public ledgers such as Bitcoin's blockchain or certificate transparency logs can be used.



The goal of this thesis is to create a system for traceable publication of measurement results using public ledgers. The system will take results from Internet scans (e.g. TLS scans, SSH scans, traceroutes, latency measurements, routing data, WHOIS information, . . .) and store them in an append-only public ledger. Similar to certificate transparency, this ensures that the data can not be manipulated retroactively. Additionally, the integrated storage of measurement data allows to deep-dive into measurement anomaly analysis and uncover special network and device setups. Finally, clients (e.g. OpenSSH extension, Firefox add-on) can then consult this system to bootstrap trust in a remote system on first use.

^ascans.io, shodan.io, censys.io

Your Task

- Evaluate existing related work and identify relevant tools (e.g. [1, 2])
- Design architecture for traceable publication of measurement results
- Implement publication system
- Develop input interface and feed measurement data into it
- Develop output interface for client trust bootstrap on first-use
- Analyze measurement anomalies using integrated ledger system

Bibliography

- [1] S. Matsumoto, P. Szalachowski, and A. Perrig, "Deployment Challenges in Log-based PKI Enhancements," in *Proc. of the 8th European Workshop on System Security*. ACM, 2015.
- [2] D. Basin *et al.*, "Design, Analysis, and Implementation of ARPKI: an Attack-Resilient Public-Key Infrastructure," *IEEE Transactions on Dependable and Secure Computing*, 2016.

Contact

Oliver Gasser gasser@net.in.tum.de
Quirin Scheitle scheitle@net.in.tum.de

<http://go.tum.de/306574>

