Preventing (Network) Time Travel with Chronos

Neta Rozen Schiff
The Hebrew University of Jerusalem
neta.r.schiff@gmail.com

Michael Schapira
The Hebrew University of Jerusalem
schapiram@huji.ac.il

Danny Dolev
The Hebrew University of Jerusalem
danny.dolev@mail.huji.ac.il

Omer Deutsch
The Hebrew University of Jerusalem
omermaya@gmail.com

ABSTRACT

The Network Time Protocol (NTP) synchronizes time across computer systems over the Internet. Unfortunately, NTP is highly vulnerable to "time shifting attacks", in which the attacker's goal is to shift forward/backward the local time at an NTP client. This has severe implications for the correctness and safety of time-sensitive applications and for security mechanisms. Importantly, time shifting attacks on NTP are possible even if all NTP communications are encrypted and authenticated.

We present Chronos, a new NTP client that achieves good synchronization even in the presence of powerful man-in-the-middle attackers. Chronos is backwards compatible with legacy NTP and involves no changes whatsoever to NTP servers. In addition, Chronos is carefully engineered to minimize communication overhead so as to avoid overloading NTP servers.

We evaluate Chronos' security and network efficiency guarantees via a combination of theoretical analyses and experiments with a prototype implementation. Our results indicate that to succeed in shifting time at a Chronos client by over 100ms from the UTC, even a powerful man-in-the-middle attacker requires over 20 years of effort in expectation. Based on work published at [1].

CCS CONCEPTS

• **Security and privacy** → **Network security**;

KEYWORDS

Chronos,; time synchronization,; Network Time Protocol (NTP),; provable security,; network security.

ANRW '18, July 16, 2018, Montreal, QC, Canada
© 2018 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-5585-8/18/07.
https://doi.org/10.1145/3232755.3232766

ACM Reference Format:
Neta Rozen Schiff, Michael Schapira, Danny Dolev, and Omer Deutsch. 2018. Preventing (Network) Time Travel with Chronos. In *ANRW '18: Applied Networking Research Workshop, July 16, 2018, Montreal, QC, Canada.* ACM, New York, NY, USA, 1 page. https://doi.org/10.1145/3232755.3232766