A Secure Selection and Filtering Mechanism for the Network Time Protocol Version 4

Neta Rozen Schiff, Danny Dolev, Tal Mizrahi, Michael Schapira

draft-ietf-ntp-chronos-00

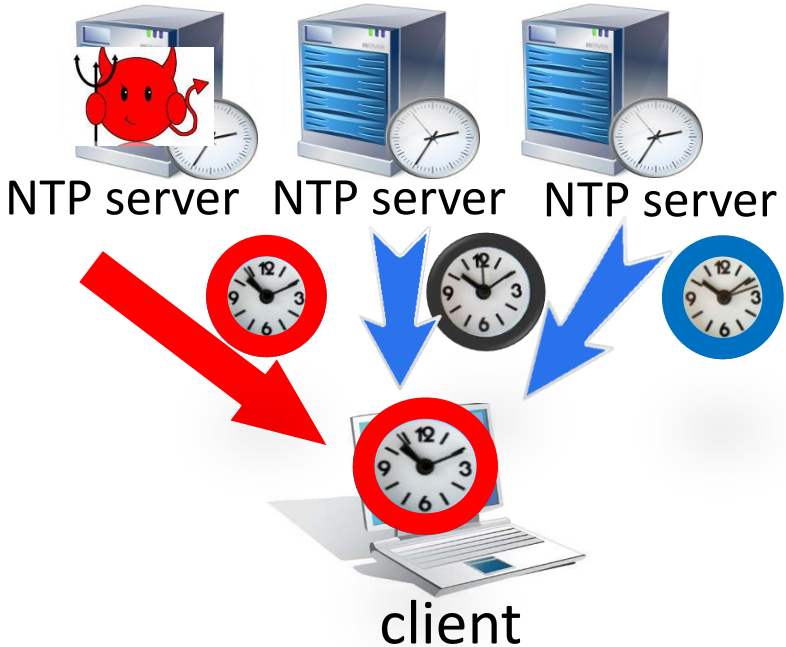
https://datatracker.ietf.org/doc/draft-ietf-ntp-chronos/

NTP, IETF 108, July 2020

Reminder: Threat Model

The attacker:

- Controls a large fraction of the NTP servers in the pool (say, ¼) or the paths between the servers and clients – MitM attacker.
- Capable of either deciding the content of NTP responses or timing when responses arrive at the client.



Reminder: Chronos Architecture

Chronos' design combines several ingredients:

- **Rely on many NTP servers (hundreds) per client**

- **In each poll interval**
  - Randomly choose a small fraction of the servers in the pool (e.g., r=4-10)
  - Avoids overloading NTP servers

- **Smart filtering**
  - Remove outliers via a technique used in approximate agreement algorithms

Chronos and NTPd

- Chronos compared to NTPv4:
  - Greater variety of sampled servers over time
  - Possible adverse effects on precision

Therefore, in the current draft Chronos is used as a "watchdog" alongside NTPv4, thus matching NTPv4's precision while significantly improving security against time shifting attacks

Chronos Watchdog Mechanism

- The NTPv4 conventional protocol periodically queries m servers in each poll interval.
- In parallel, a Chronos watchdog periodically queries a (variable) set of r servers in each Chronos poll interval.
- In each poll interval the Chronos virtual clock value is compared with the NTPv4 clock value.

If the difference between NTPv4 and Chronos offsets exceeds a predetermined value, an attack is detected and Chronos' offset is used to update the client's clock.
Otherwise, NTPv4's offset is used for updating the client’s clock.

Next Steps

- Working on implementing Chronos as a watchdog
- Continuing to evaluate the performance and security under different attack strategies and at different locations
- Looking for more feedback about the current version