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

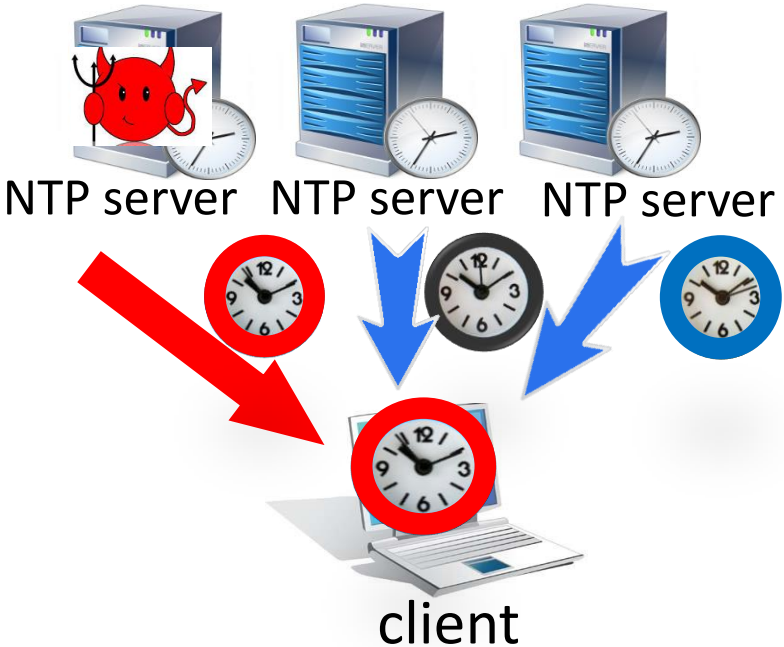
draft-schiff-ntp-chronos-02

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

Reminder: Threat Model

The attacker:

- Controls a large fraction of the NTP servers in the pool (say, ¼)
- Capable of both deciding the content of NTP responses **and** timing when responses arrive at the client
- Malicious



Reminder: Chronos Architecture

Chronos' design combines several ingredients:

- **Rely on many NTP servers**
  - Generate a large server pool (hundreds) per client
    - E.g., by repeatedly resolving NTP pool hostnames and storing returned IPs
  - Sets a very high threshold for a MitM attacker
- **Query few servers**
  - Randomly query a small fraction of the servers in the pool (e.g., 10-20)
  - Avoids overloading NTP servers
- **Smart filtering**
  - Remove outliers via a technique used in approximate agreement algorithms
  - Limits the MitM attacker's ability to contaminate the chosen time samples

Comments for Chronos

Use Chronos externally to enhance the security of NTPv4 (or within the NTP)

- In draft 01 - we added a hybrid approach, when precision and accuracy are critical:
  - By default NTPv4 updates the local clock
  - When a threat or evidence of attack is detected (based on Chronos' samples), Chronos time is considered instead.

Chronos use greater variety of sampled servers over time, and it may cause adverse effects on precision and accuracy

- In draft 02 - we evaluate the effects on precision and accuracy:
  - Chronos has fair precision (around 3ms)
  - Chronos updates are close on average to NTP (2-3ms gap)

Next Steps

- We have updated the draft based on the comments
- We are continuing to evaluate Chronos's performance and security for different attack strategies and at different locations
- We believe Chronos draft is ready for WG adoption