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

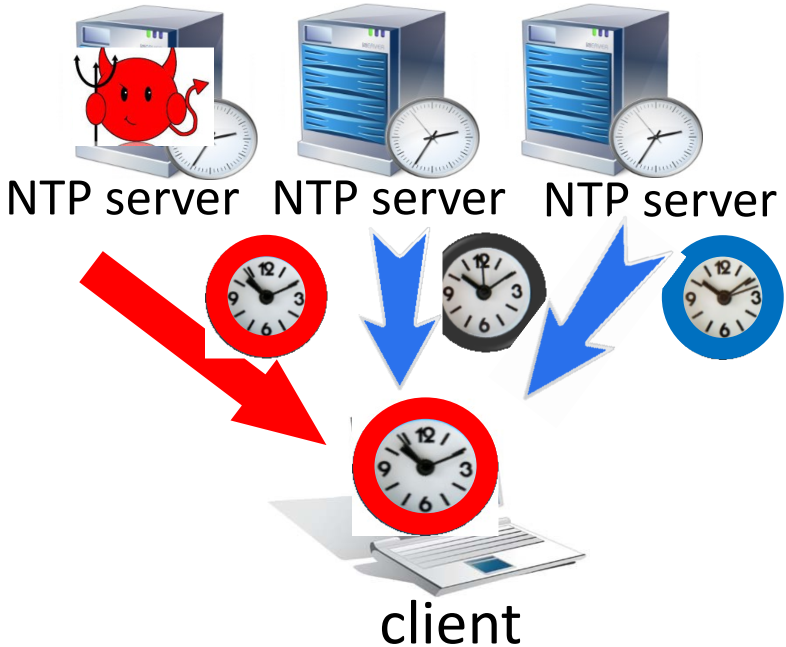
draft-schiff-ntp-chronos-01

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 **<u>and</u>** 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

New in draft 001: Precision Vs. Security

- Chronos compared to NTPv4:
  - Greater variety of sampled servers over time
  - Avoids (NTPv4) source quality filters
  - Provable security guarantees

- Possible adverse effects on precision and accuracy.
  - Bounded by Chronos' ω parameter (25ms)
  - Insignificant for many applications of interest

- 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.

New comments for draft 001

- Use Chronos externally to enhance the security of NTPv4

- Use Chronos as a new filter (or verification step) within NTPv4

We thank Dieter and Greg for useful discussions!

Thank You

See full draft (@IETF):
https://tools.ietf.org/id/draft-schiff-ntp-chronos-01.html