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

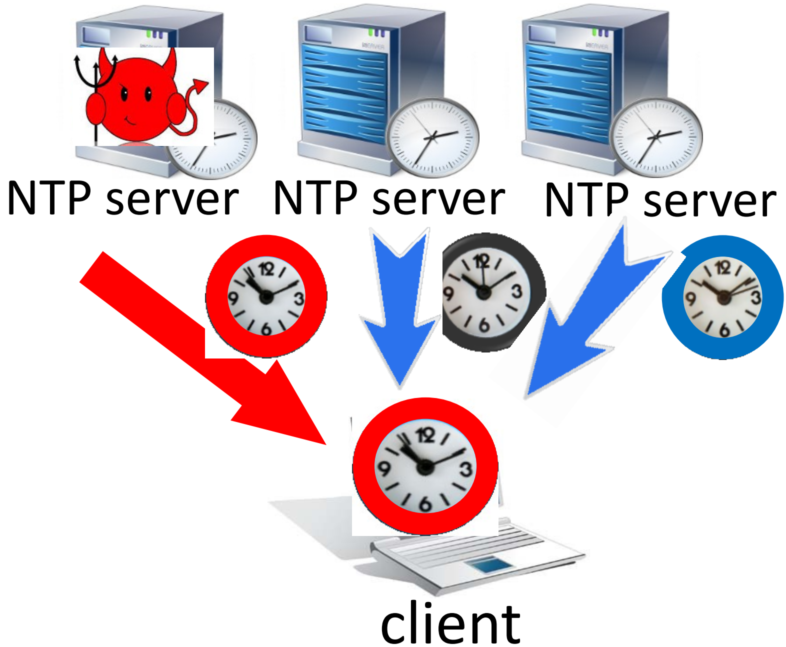
draft-schiff-ntp-chronos-02

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

Chronos and NTPd

- 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.

New in draft 002: Precision Evaluation

- We evaluated Chronos precision in different locations in Europe and US.

- Preliminary results:
  - Chronos has fair precision, up to several ms from NTP
  - Chronos updates are close on average to NTP (several ms gap)

- We considered smoothing mechanisms in order to improve Chronos precision

New in draft 002: Smoothing algorithms for Chronos

- Two smoothing mechanism were tested:
  - Return the offset with minimal absolute value unless its distance from the average offset is larger than a predefined value. Yielded improvements.
  - Use the same set of servers as in the previous sample, unless the difference between their offset and the offset of new servers is larger than a predefined value. Didn’t yield a significant improvement.

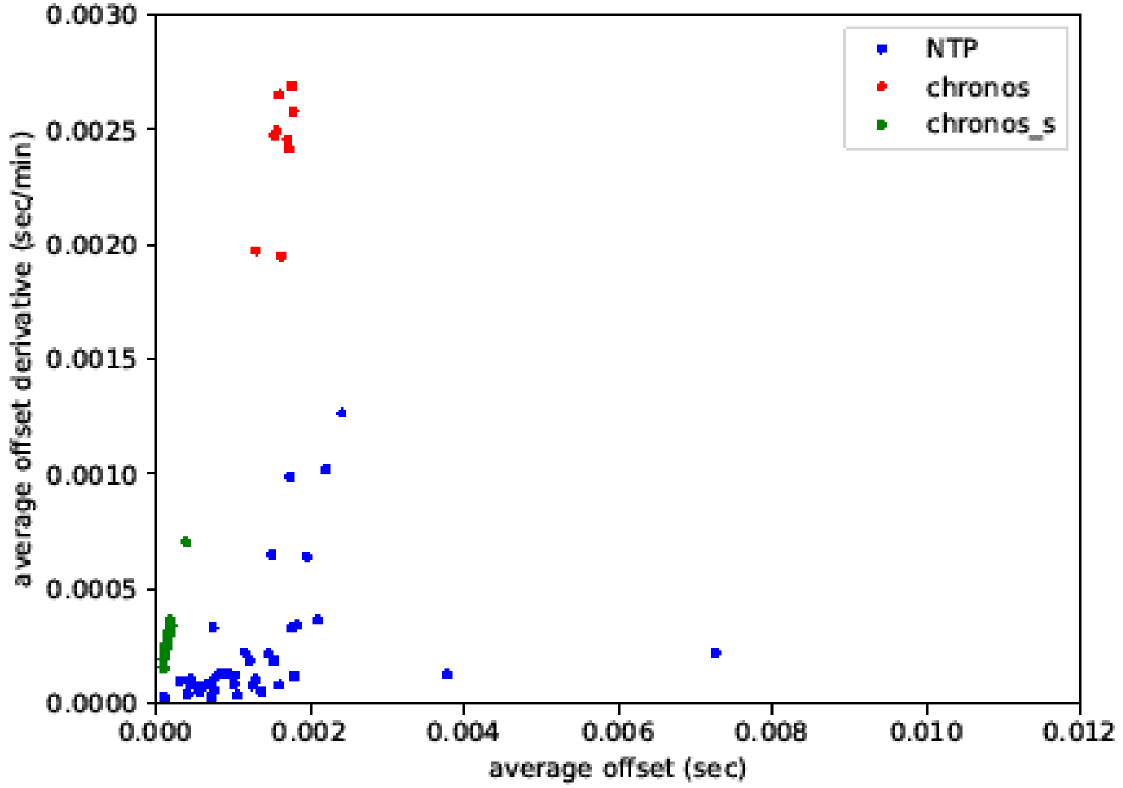
Average offsets and derivatives

- Chronos usually has more fluctuations compares to NTP, in non-attacking scenarios
- The smoothing algorithm, decrease them and reduce its offsets (in absolute values)
- We verified it on several locations:

Average offsets and derivatives

- Chronos usually has more fluctuations compares to NTP, in non-attacking scenarios
- The smoothing algorithm, decrease them and reduce its offsets (in absolute values)
- We verified it on several locations:

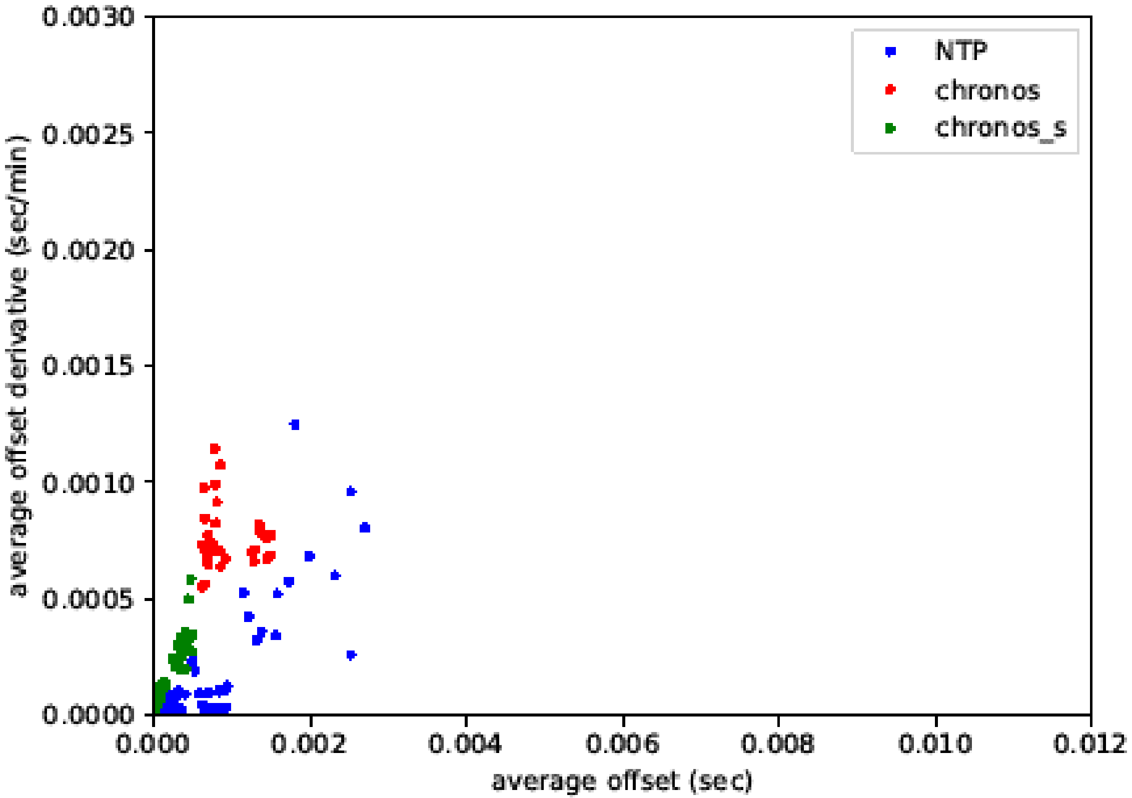
Oregon



Average offsets and derivatives

- Chronos usually has more fluctuations compares to NTP, in non-attacking scenarios
- The smoothing algorithm, decrease them and reduce its offsets (in absolute values)
- We verified it on several locations:

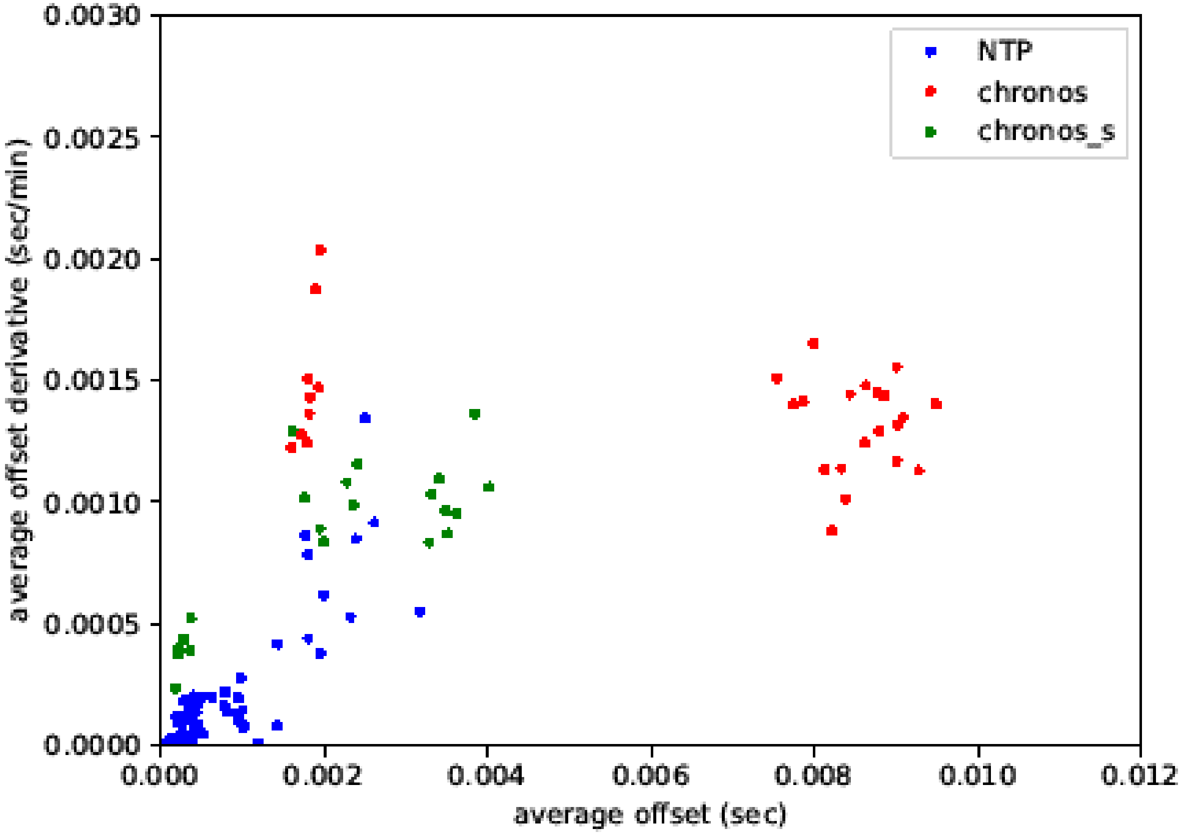
Frankfurt



Average offsets and derivatives

- Chronos usually has more fluctuations compares to NTP, in non-attacking scenarios
- The smoothing algorithm, decrease them and reduce its offsets (in absolute values)
- We verified it on several locations:

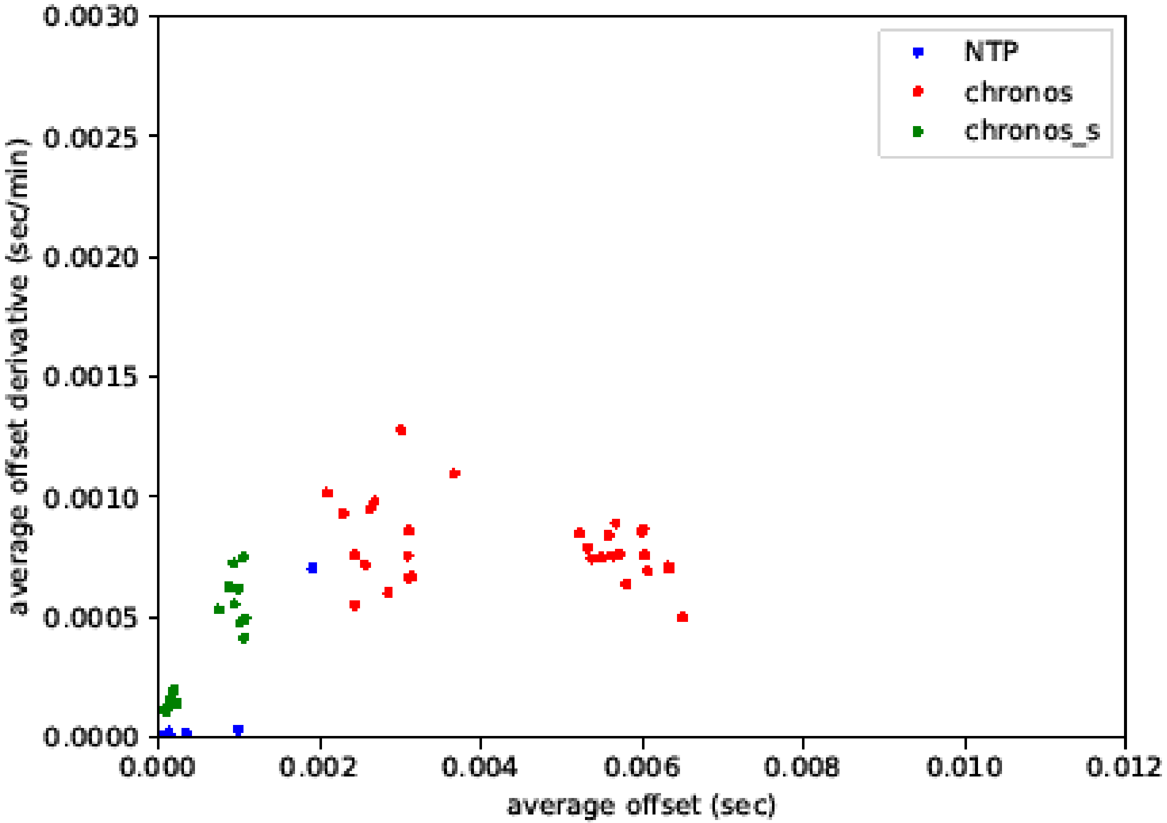
Virginia



Average offsets and derivatives

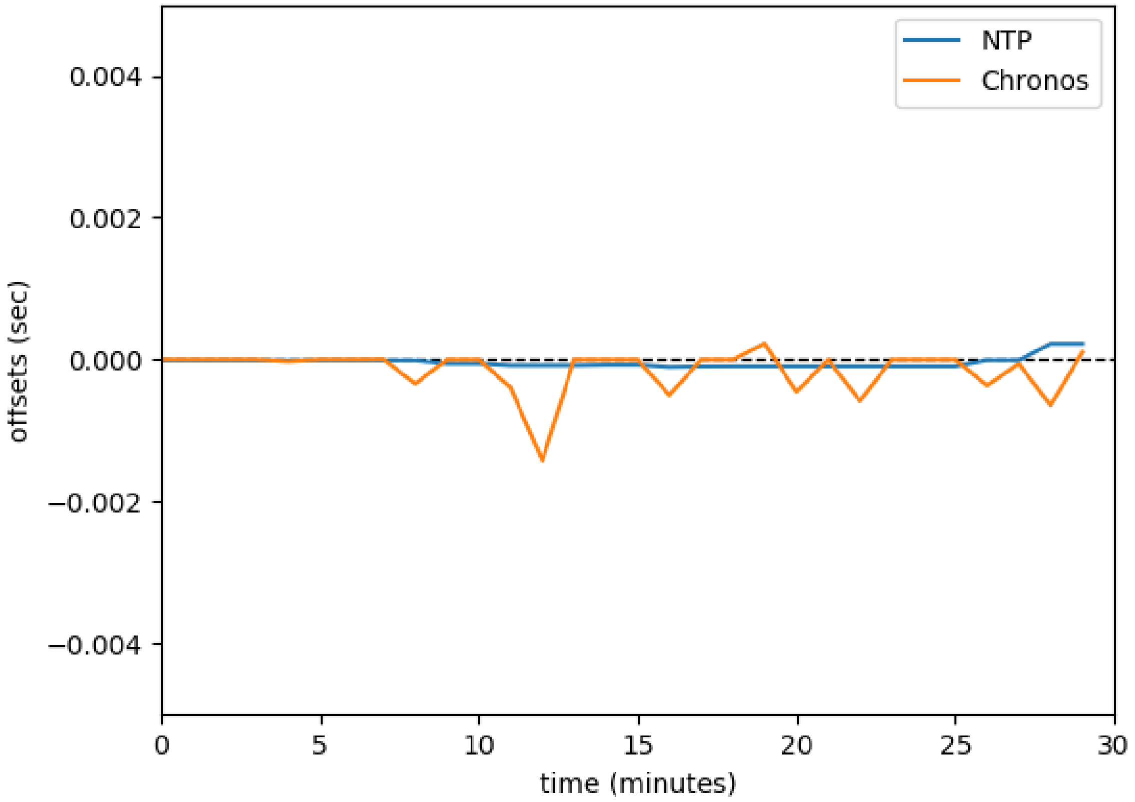
- Chronos usually has more fluctuations compares to NTP, in non-attacking scenarios
- The smoothing algorithm, decrease them and reduce its offsets (in absolute values)
- We verified it on several locations:

London



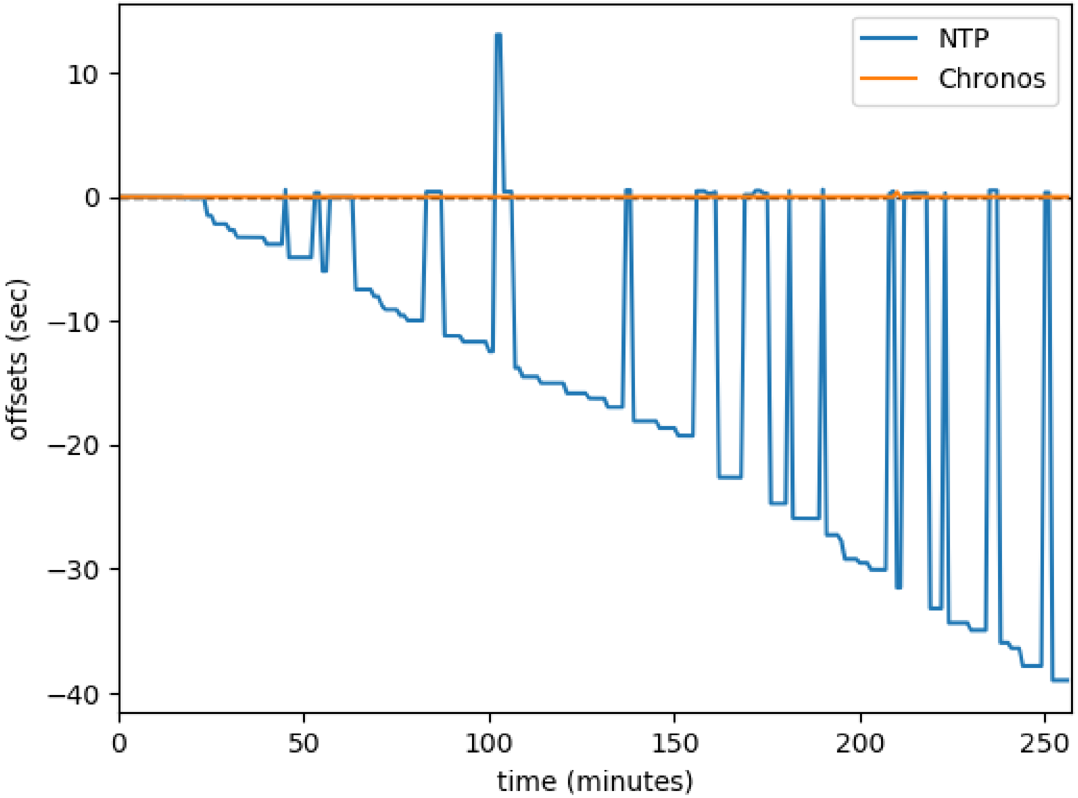
Preliminary results under attack

- Attack type: **rapidly** increasing shift + fake stratum 1
- Both Chronos and NTP remain accurate



Preliminary results under attack – cont.

- Attack type: **slowly** increasing shift + fake stratum 1
- Chronos precision remains while NTP is shifted



Conclusions

- We tested POC Chronos implementation under non attacking scenarios and under attacks
- Chronos precision is closer to NTP than expected (several ms instead of w=25ms), while the smoothing algorithm yields even better results
- Chronos is secured even facing slowly increasing shift, while NTP doesn’t. Smoothing didn’t affect Chronos security.
- We will continue to evaluate Chronos performance under different attacks, in different locations