# A Secure Selection and Filtering Mechanism for the Network Time Protocol

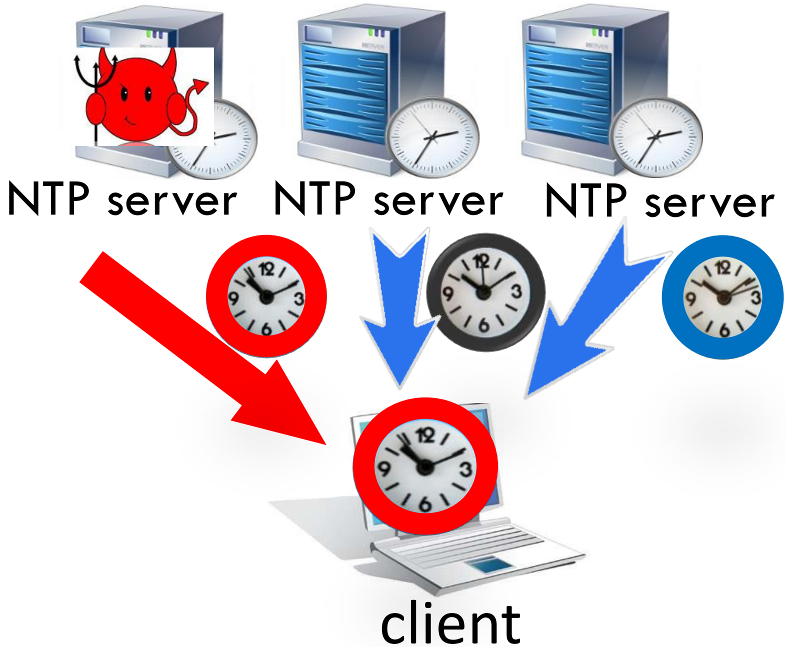
**draft-ietf-ntp-chronos-02**

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’ Design Goals

The **Chronos NTP client** is designed to achieve the following:

- **Provable security** in the face of fairly powerful MitM attacks
  - ➢ negligible probability for successful timeshifting attacks
- **Backwards-compatibility**
  - ➢ no changes to NTP servers
  - ➢ limited software changes to client
- **Low computational and communication overhead**
  - ➢ query few NTP servers

# 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

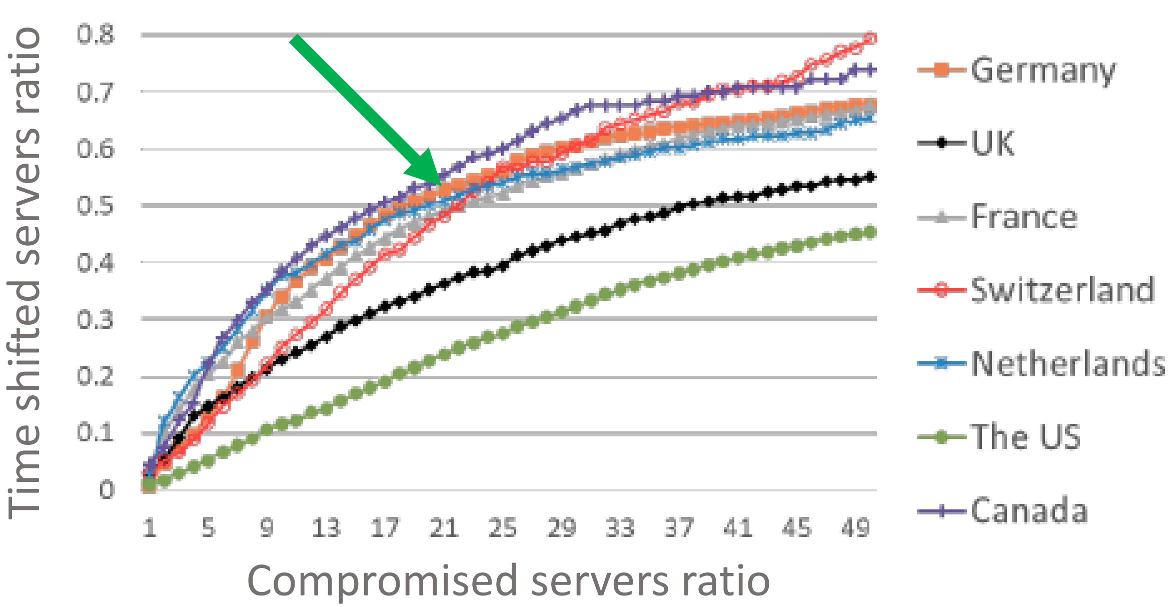
# Chronos' Limitations

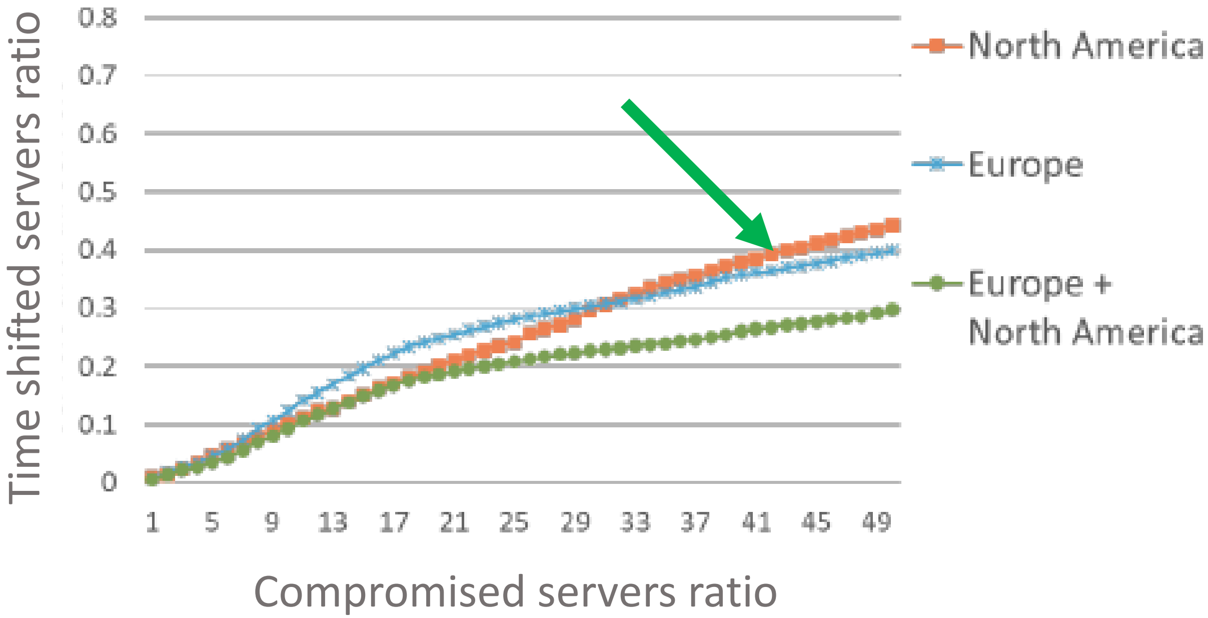
- **Relying on many servers**
  - There are regions with only few NTP servers.

- **Many servers might be compromised by few servers**
  - NTP servers are hierarchically dependent.
  - Lowers the bar for an attacker; influence many servers while using few servers.

# Chronos Limitations – Inter-Server Dependencies

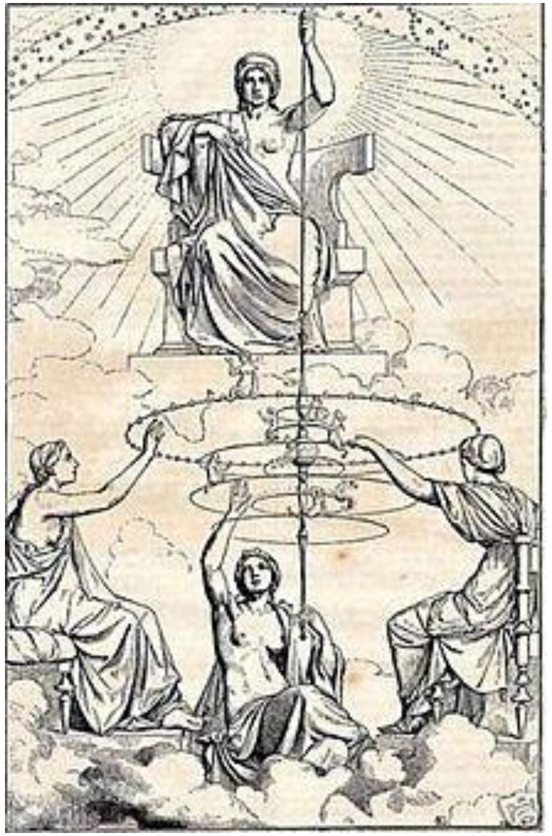
- We evaluate server-dependency by querying NTP timeservers.
- **An attacker can timeshift the majority of timeservers in a region by compromising fairly few timeservers.**





# Extending Chronos with Ananke

- Maintain a trusted pool of timeservers
    - ➢**100s servers**
    - ➢**Stratum 1 only**
    - ➢Belonging to a **reputable organization**
    - ➢In the future, **audited** (e.g., by authorities like IANA)

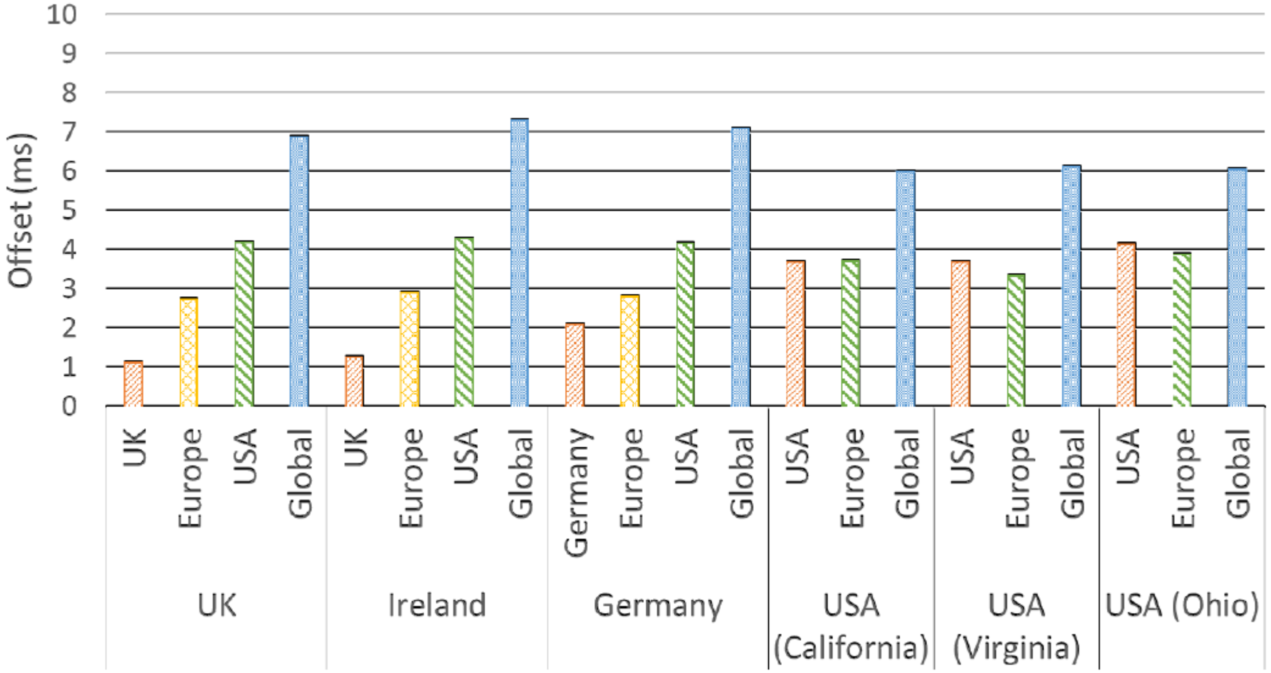


# Extending Chronos with Ananke – Cont.

- The NTP client runs two parallel synchronization processes
  - **Primary**: A default NTPv4 (or NTPv5) client, which synchronizes with pool-assigned servers in its region.
  - **Watchdog**: the secure Chronos client, which synchronizes with the Ananke server pool.
- If the primary process' time deviates by "too much" from the watchdog's time, the watchdog updates the local time at the client.

# Preserving today's time accuracy/precision and load balancing

- **Preserve NTP's time accuracy and precision**
  - ➢NTPv4 is used as long as not under attack.
  - ➢Even when forced to use ex-region servers, the offset can be bounded by few milliseconds.



# Preserving today's time accuracy/precision and load balancing

- **Preserve NTP's time accuracy and precision**
  - ➢NTPv4 is used as long as not under attack.
  - ➢Even when forced to use ex-region servers, the offset can be bounded by few milliseconds.

- **Respect today's load distribution across timeservers**
  - ➢ In primary process: NTPv4 load-balancing is used as is.
  - ➢ In watchdog process: query rate of Ananke servers is very low.

# Security Guarantees

- Shifting time at a client by at least 1.1 seconds from the UTC will take the attacker at least 26 years in expectation.

- Where:
  - Ananke consists of 200 servers, 1/7 controlled by an attacker
  - 12 (random) servers in Ananke queried once every 10 hours (10x less frequent than in the primary process).
  - Good samples are within 50ms from UTC.

# Conclusion

- We presented attacks by malicious NTP timeservers that can harm even security-enhanced NTP clients like Chronos.
- We empirically quantified the impact of such attacks, showing that it can induce significant harm.
- We outlined a path for improving NTP’s security by coupling Chronos with Ananke.

# New comments for draft 02

We updated the draft based on the comments by the NTP WG members regarding the watchdog mechanism, Chronos’ default parameters, etc.

We thank Ulrich Windl and Watson Ladd for useful discussions!

# Next Steps

- We will update the draft to incorporate Ananke.
- We are working on implementing Chronos as a watchdog, alongside NTPv4.
- We are continuing to evaluate Chronos' performance and security guarantees under different attack strategies and at different locations.