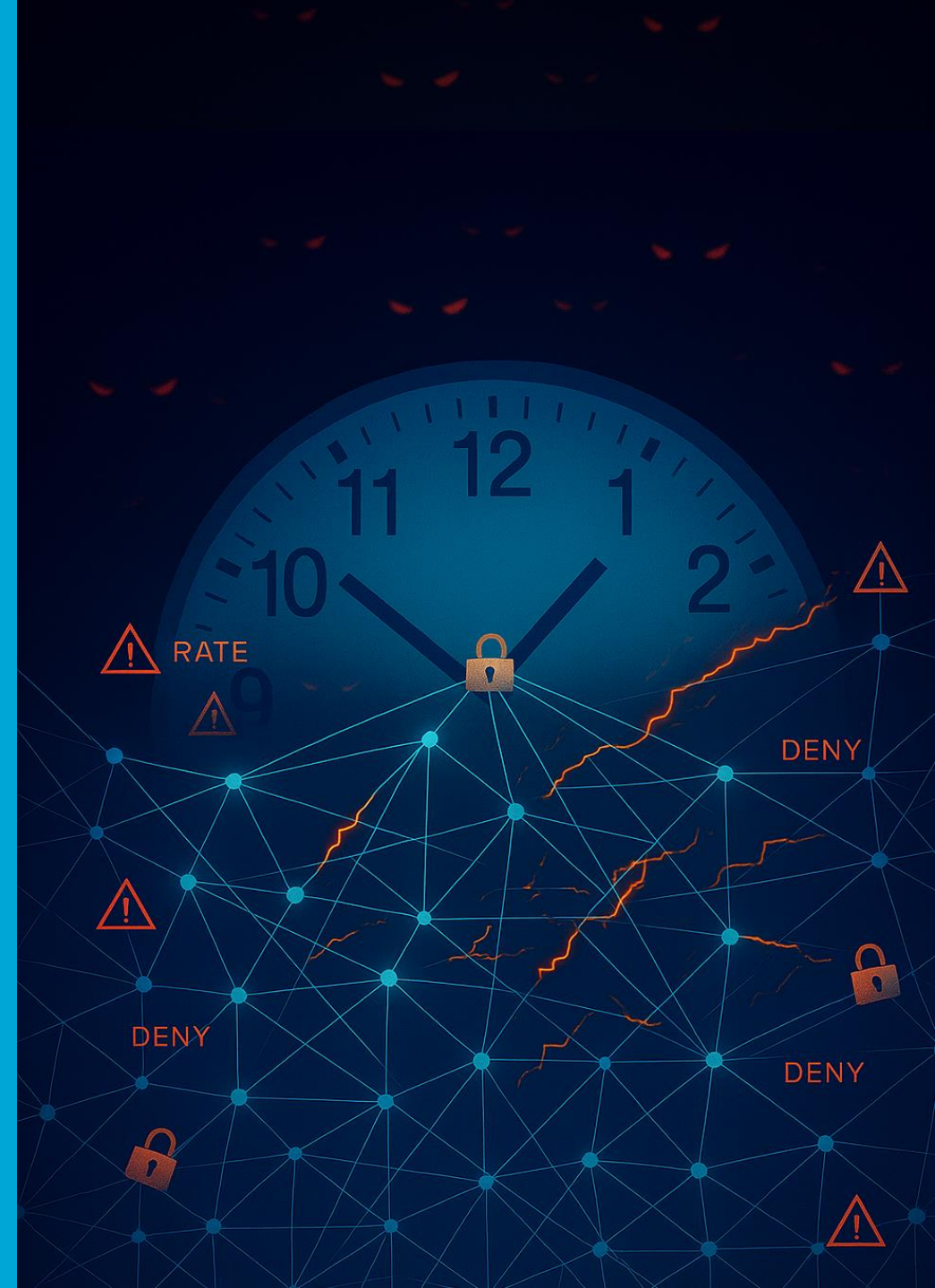


Are NTP clients Always right?

Shreyas **Konjerla**,
Giovane C. M. **Moura**,
Georgios **Smaragdakis**,
Tamme **Dittrich**,

TU Delft, **NL**
SIDN Labs & TU Delft, **NL**
TU Delft, **NL**
Tweede Golf, **NL**



Agenda

01

Introduction

02

Baseline
Behavior

03

Time-Shifting
Attacks

04

Denial of
Service
Attacks

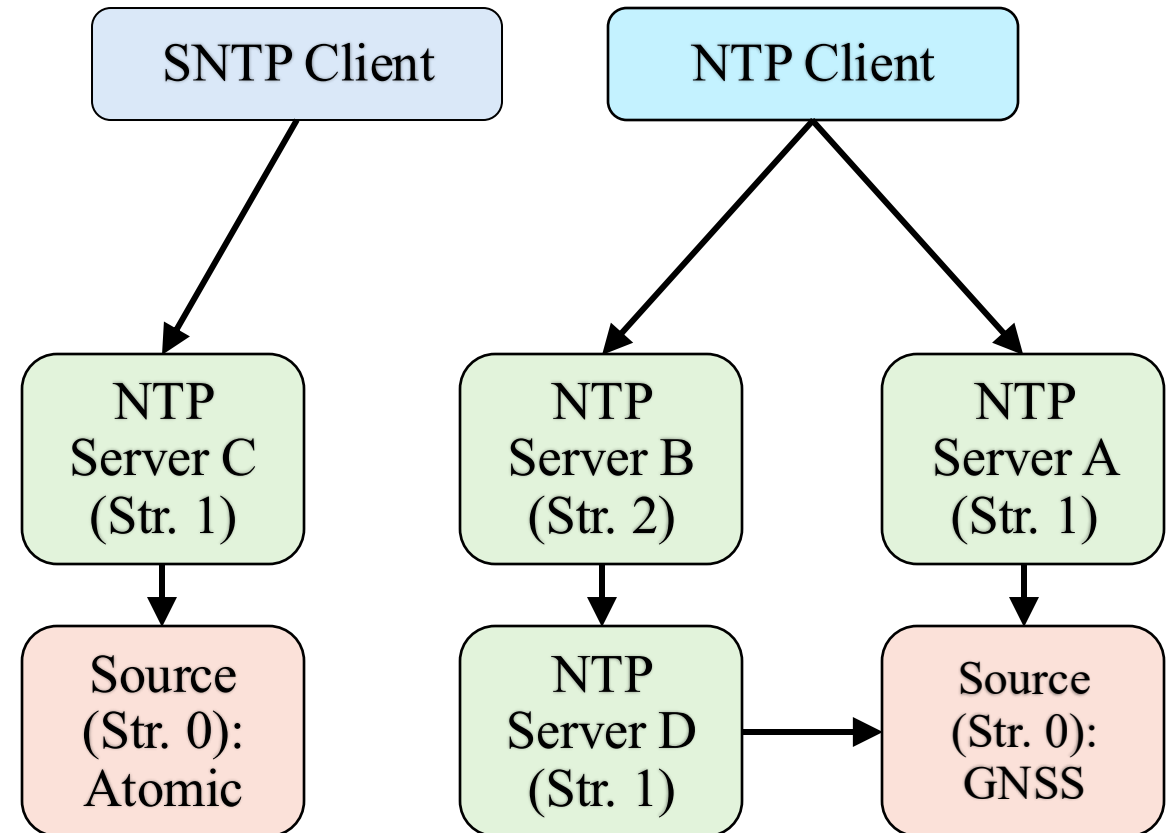


1

Introduction

Introduction

- Clock sync is essential for many applications.
- NTP is the **default** protocol for **timekeeping**.

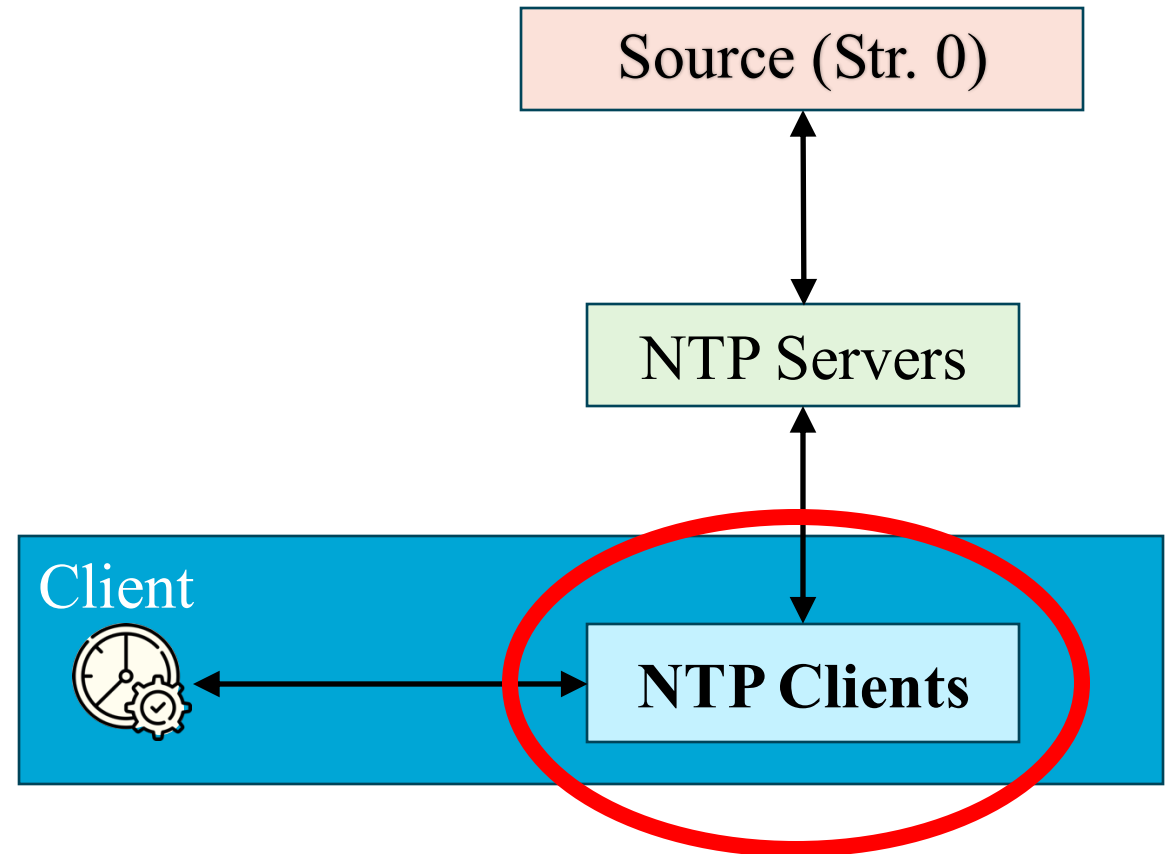


Introduction

- NTP Version 4 (RFC5905)
- Standardized in 2011.
- Added better algorithms
- Kiss-of-Death mechanism.
- NTS (extension added in 2020).

Introduction – NTP Security

- Very little work has been done on client side.
 - Vulnerable clients **undermine** the best of server networks.
- They are the final judge.



Introduction - Clients

Client	OS	Last Release
macOS	macOS	Sept 2024
w32t	Windows	April 2025
TimesyncD	Ubuntu	Sept 2024
NTPSec	Ubuntu	Nov 2024
NTPD-RS	Ubuntu	Jan 2025
NTPD	Ubuntu	June 2023
OpenNTPD	Ubuntu	Oct 2022
Chrony	Ubuntu	Oct 2024

Highlighted are **SNTP** clients.

Contributions

- Measure the behavior of (S)NTP clients under normal operation.
 - Large variations among clients.
- Exposed clients to 2 NTP attacks – Time shift and Kiss-of-Death.
 - All Oses' default clients vulnerable to time-shift attacks.

2

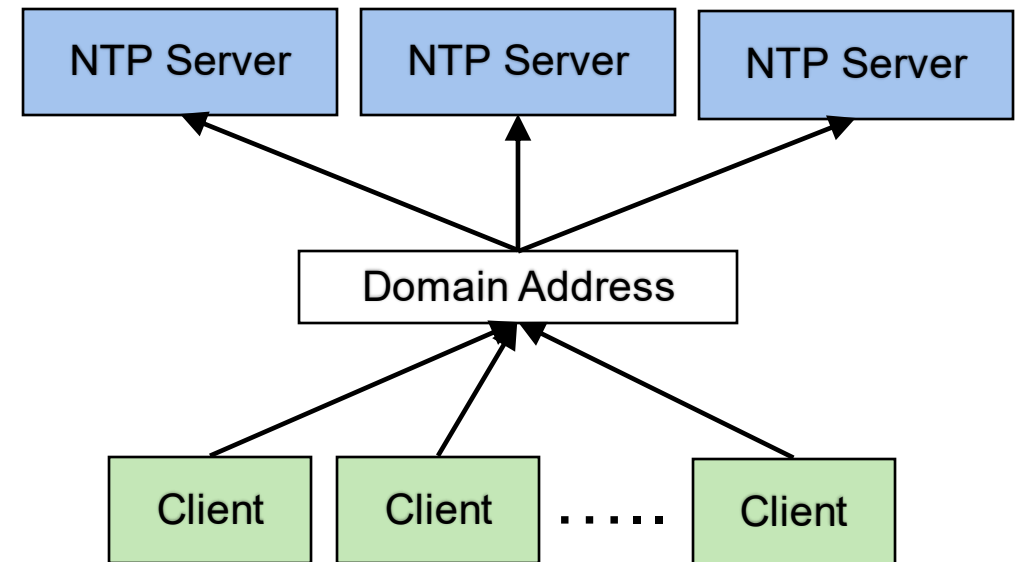
Analyzing Baseline Behavior

Baseline Behavior

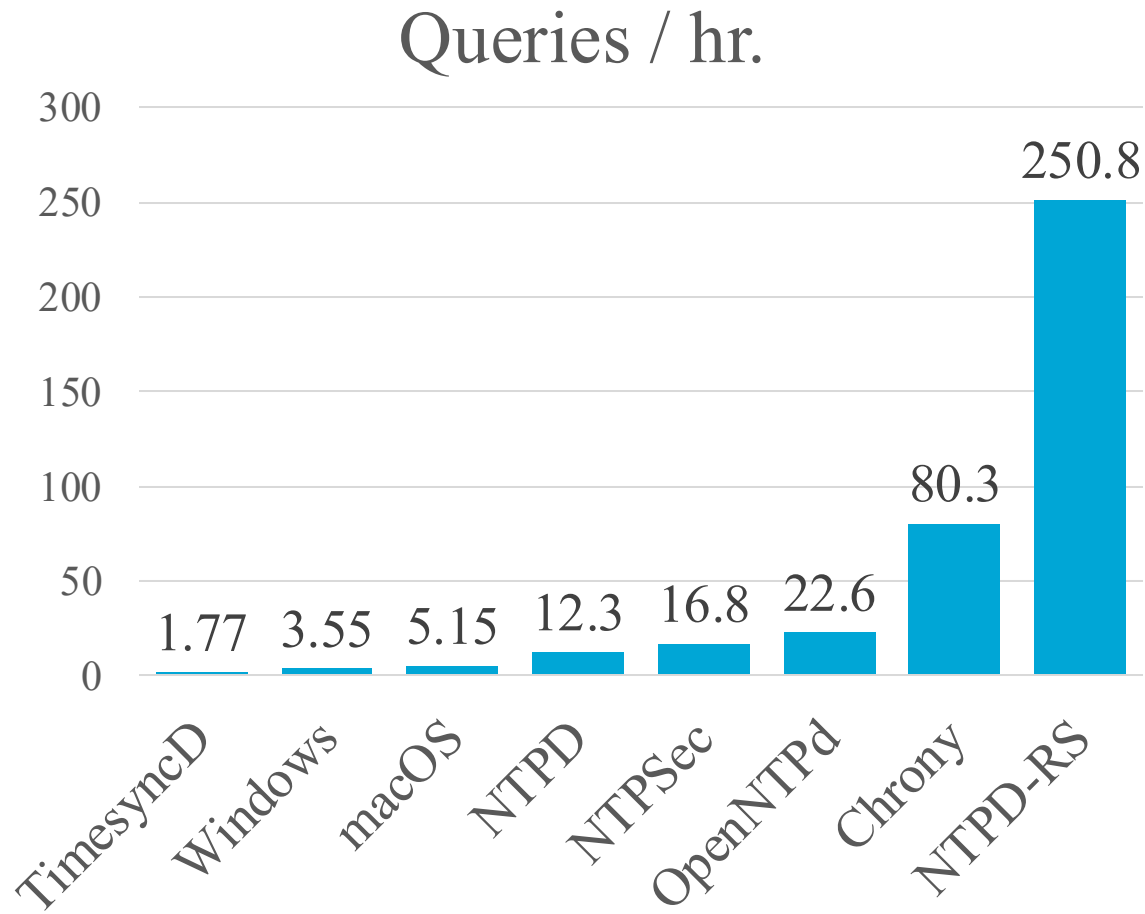
- We analyze the behavior of (S)NTP clients.
- What we analyze:
 - How often client query servers?
 - How many servers do they use?
 - How do they compare to the others?

Baseline Behavior – Setup

- Configure 3 VMs as NTP Servers.
- All clients use these servers.
 - Domain address with 3 IPs.
- Collected 60hrs of traffic.



Baseline Behavior – Results



- SNTP client send much **less** queries.
- They have a **fixed** polling rate.
- NTP clients show **large** variations.
- More packets is **better** accuracy.

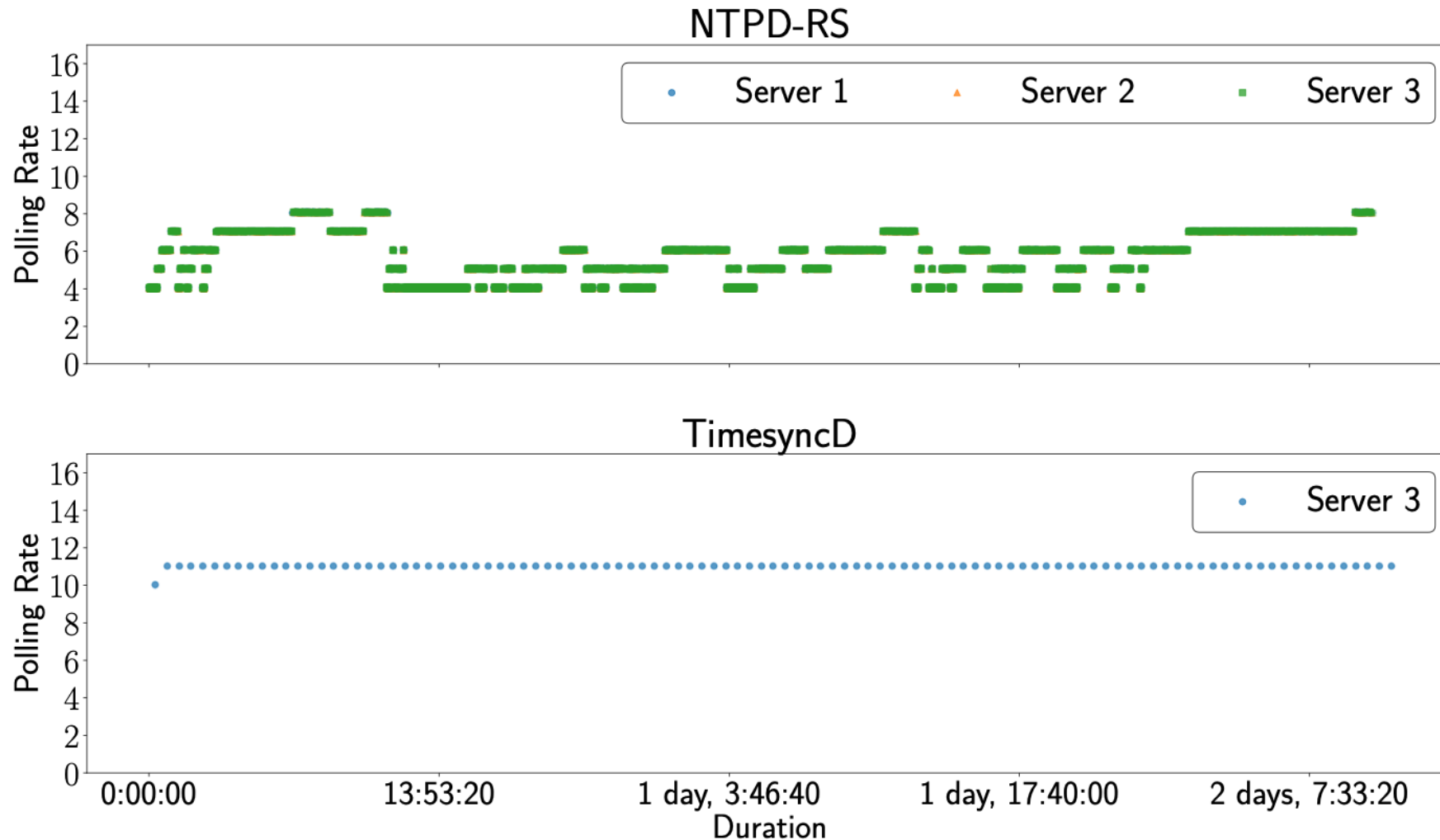
Baseline Behavior – Results

	Queries per Server		
	S1	S2	S3
Chrony	1643	1498	1681
macOS	102	101	106
NTPD	246	246	246
NTPD-RS	5012	5012	5026
OpenNTPd	425	473	463
NTPSec	336	336	337
Windows	80	77	56
TimesyncD	108	0	0

- TimesyncD uses only **one** server.
- Single point of failure.
- macOS, Windows rotate between through all servers.

Highlighted are **SNTP** clients.

Baseline Behavior – Results

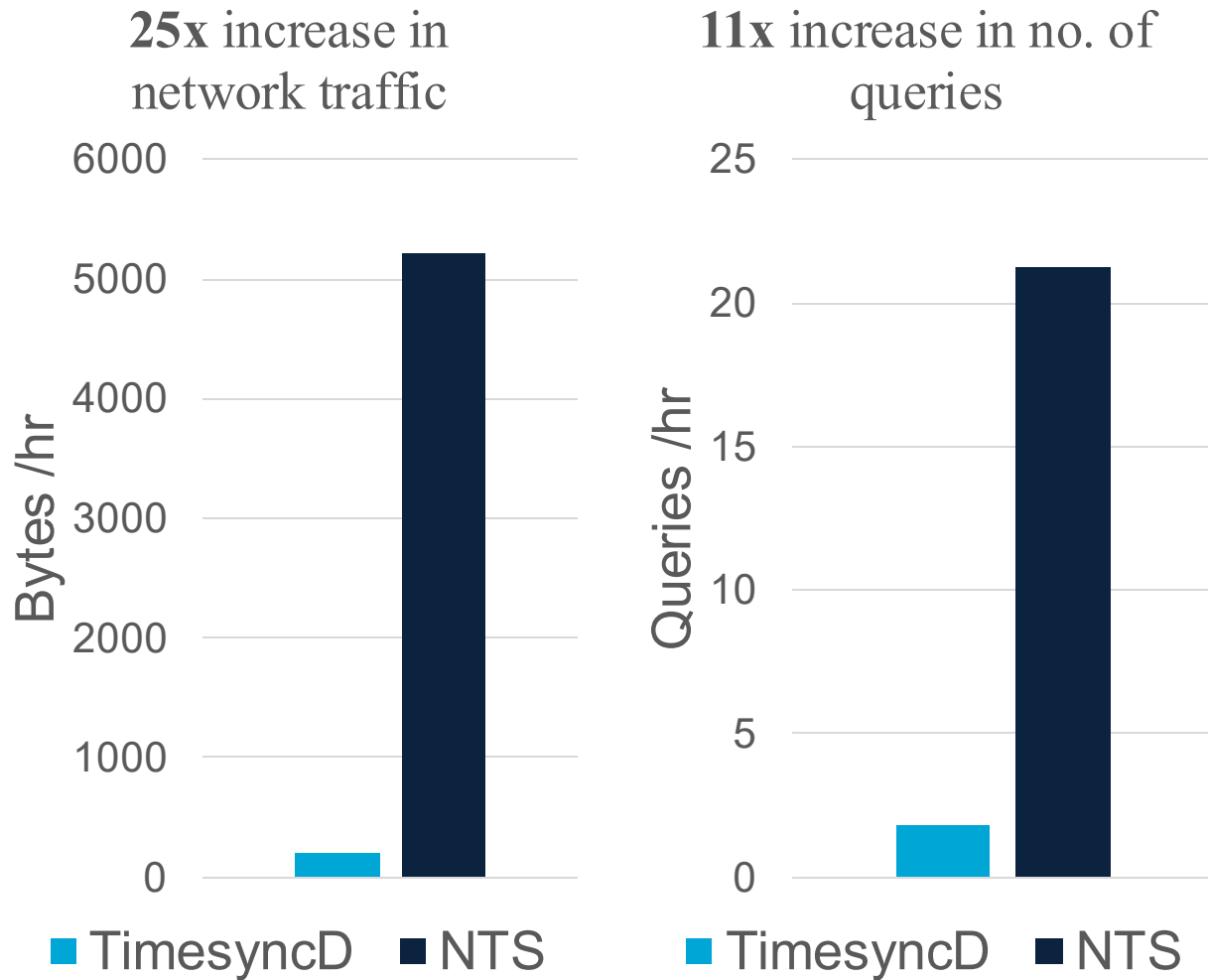


Timeseries for NTP and SNTP Clients.
Highlights the differences in behavior and server utilization.

Baseline Behavior – Results

- Ubuntu will move to NTS (chrony) by **default**.
- They operate their own NTP server pool.
- We worked with them to measure network traffic increase.

Baseline Behavior - Results



- Significant rise in number of queries and network traffic.
- Notified them of the expected surge.

3

Time Shifting Attacks

Time Shift

- Attacker tries to manipulate the client into changing time.
- US Naval Observatory's NTP servers had an incident.
- Most feared situation for operators.



Time Shift – Expected Behavior

- NTP specifies a “*panic threshold*” in which defines the maximum allowed offset.
 - Recommended value is 1000s.
- We aim to force the client to change its time and see if it resists it.

Time Shift – Threat Model

- We control the malicious NTP servers.
- Clients are redirected to attackers' services.
 - Feasible by adding **malicious** servers in NTP Pool, DNS Hijacking, etc.

Time Shift - Results

Client	Offset Added					
	900s	1W	1M	3M	1Y	2Y
macOS	✓	✓	✓	✓	✓	✓
TimesyncD	✓	✓	✓	✓	✓	✓
Windows	✓	✓				

✓ shows successful attack

- All SNTP clients are **vulnerable** to time shifting.
- These are the **default** clients for major OSes.
 - **Billions** of devices affected.
- None of the NTP clients are vulnerable.

4

Kiss-of-Death (KoD) Attacks

Kiss of Death (KoD)

- Introduced to **protect** servers from aggressive clients.
- Used by **servers** to send control messages to clients.
- Can be **abused** to cause Denial-of-Service.
 - Spoofed packets cause clients to stop querying.

KoD – Expected Behavior

- Best practices for NTP (RFC8633) recommends honoring KoD packets.
 - Only up to a **certain** value.
- We try to manipulate clients into stopping synchronization.

KoD – Experiments

- Clients configured to use attackers' servers.
- Then servers responded with KoD packets.
 - RATE and DENY.

KoD – Results

	RATE	DENY
chrony	Ignored	Ignored
ntpd	Stopped	Too many queries
ntpd-rs	Increased query rate	Too many queries (bug)
OpenNTPd	Ignored	Ignored
NTPSec	Ignored	Ignored

- Most clients ignore KoD packets and are unaffected.
 - Developers deviating from standards.
- ntpd-rs sent 500k queries in 5 minutes for DENY.
- ntpd stopped for RATE and sent too many for DENY.

5

Conclusions

Recommendations and Findings

Conclusions

- 3 major OSes use vulnerable SNTP clients
 - Ubuntu will switch to NTS.
- Recommend both macOS and Windows deploy stronger NTP clients.
 - Alternatively, add sanity checks.
- Every SystemD-based Linux distros should reconsider using TimesyncD, and switch to more robust alternatives.

Findings

	Software	Issue	Vendor Response
1	NTPD-RS	Queries surge to nearby servers	Feature, not a bug
2	Ubuntu	Traffic growth by using Chrony and NTS	Acknowledged
3	macOS	Vulnerable to time shift	<i>“Not a bug”</i>
4	TimesyncD	Vulnerable to time shift	Acknowledged
5	W32Time	Vulnerable to time shift	
6	Debian Linux	Vulnerable to time shift	Waiting
7	NTPD-RS	Crashes during time shift attacks	Notified
8	NTPD-RS	KoD Bug (too many queries)	Bug patched
9	ntpd	Stops operating when responded with RATE	Acknowledged
10	ntpd	Keeps sending queries after receiving DENY	Acknowledged

Takeaways

- NTP lurks in the background of *all* modern computer systems.
 - Plays a key role in its well functioning.
- The defaults for major OSes are vulnerable.
 - Creates unnecessary risk for billions.



Full tech report can be found here.
You can contact me on: k.shreyas@gmail.com

Thank you for your attention!

Are NTP Clients Always Right? | Shreyas Konjerla