Time: What happens if the world spins backwards?

Jerry Xu

Mentors: Prof. Ari Trachtenberg, Trishita Tiwari

Presented at MIT PRIMES October Conference

Sunday, October 20th, 2019

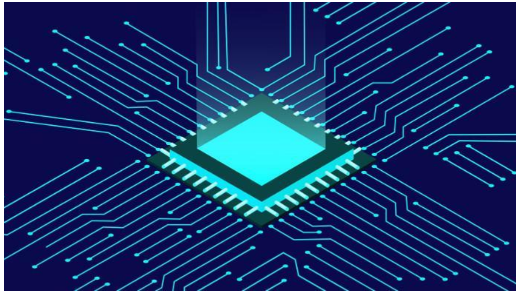
BU Department of Electrical & Computer Engineering

MIT PRIMES

Overview

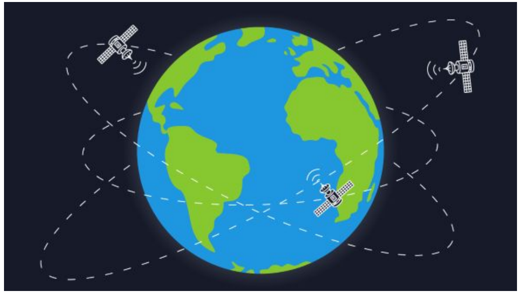
- Time on digital devices is synced across the internet
  - Protocol used to sync time is insecure
- Demonstrate a man in the middle attack
- Analyze results and explore possible malicious applications
  - Interfere with human interaction
  - Limit machines' abilities to self-maintain
  - Undermine security

Why is time important?

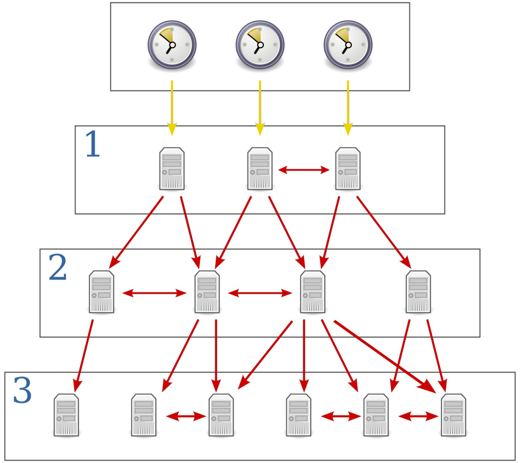


23:59:59
Dec 31 1999 Fri

ST3160815A



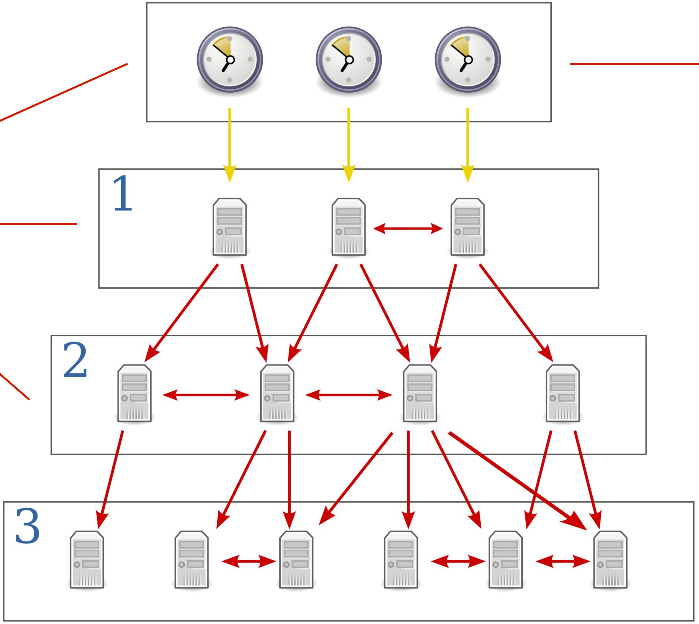
How do we sync time?



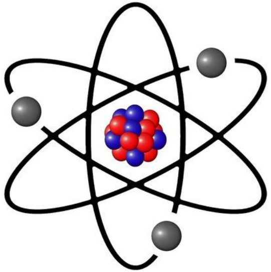
- Network Time Protocol (NTP; 1985)
- Fundamental Internet Protocol
- Operates on UDP
  - Fast, not reliable
- Designed for precision

How do we sync time?

Level = Stratum
(pl. strata)

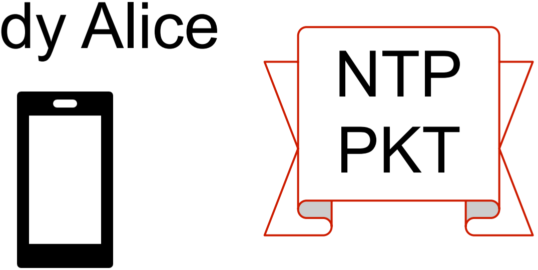


Stratum 0



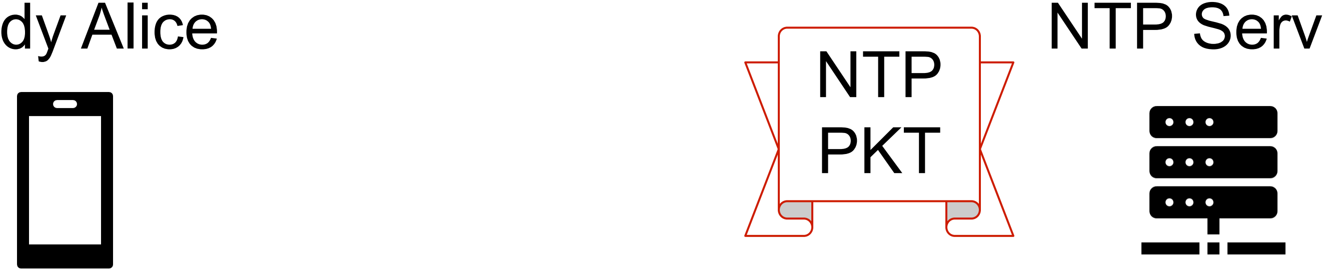
How do we sync time? – Latency mitigation

Tardy Alice



T_A: Leaves client

How do we sync time? – Latency mitigation



Tardy Alice

NTP PKT

NTP Server

T_A: Leaves client

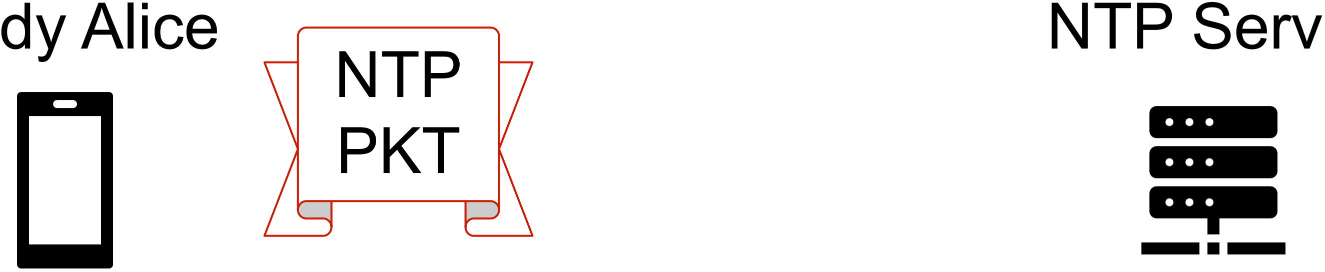
T_B: Arrives server

T_C: Leaves server

How do we sync time? – Latency mitigation

Tardy Alice

NTP Server



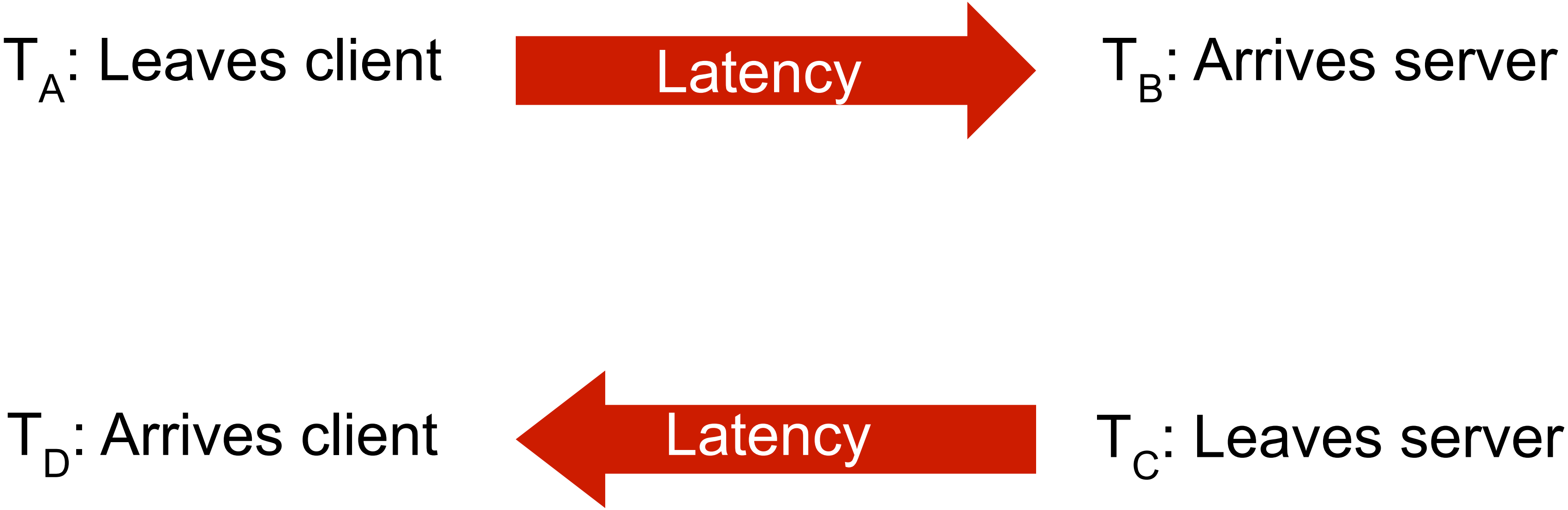
T_A: Leaves client

T_D: Arrives client

T_B: Arrives server

T_C: Leaves server

How do we sync time? – Latency mitigation



T_A: Leaves client

Latency

T_B: Arrives server

T_D: Arrives client

Latency

T_C: Leaves server

How do we sync time? – Latency mitigation

$$T_B - T_A = \text{offset} + \text{latency}$$

$$T_D - T_C = (\text{-offset}) + \text{latency}$$

$$\text{offset} = \frac{(T_b - T_a) - (T_d - T_c)}{2}$$

NTP “Safeguards” in Packet Structure

- Authentication field
- Panic threshold
- Checksum

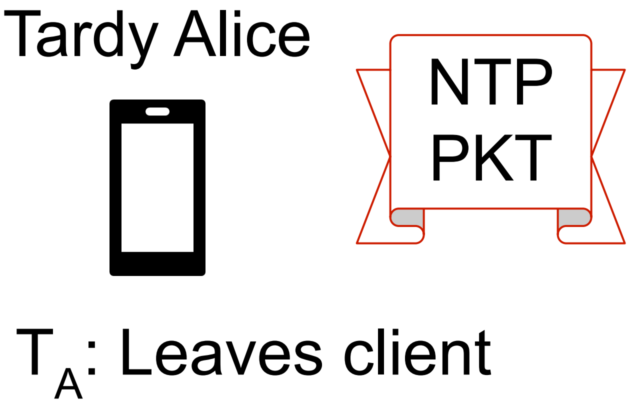
Conclusion → insecure as consequence of design

Can we modify a packet?
What will happen as a result?

Exploiting NTP

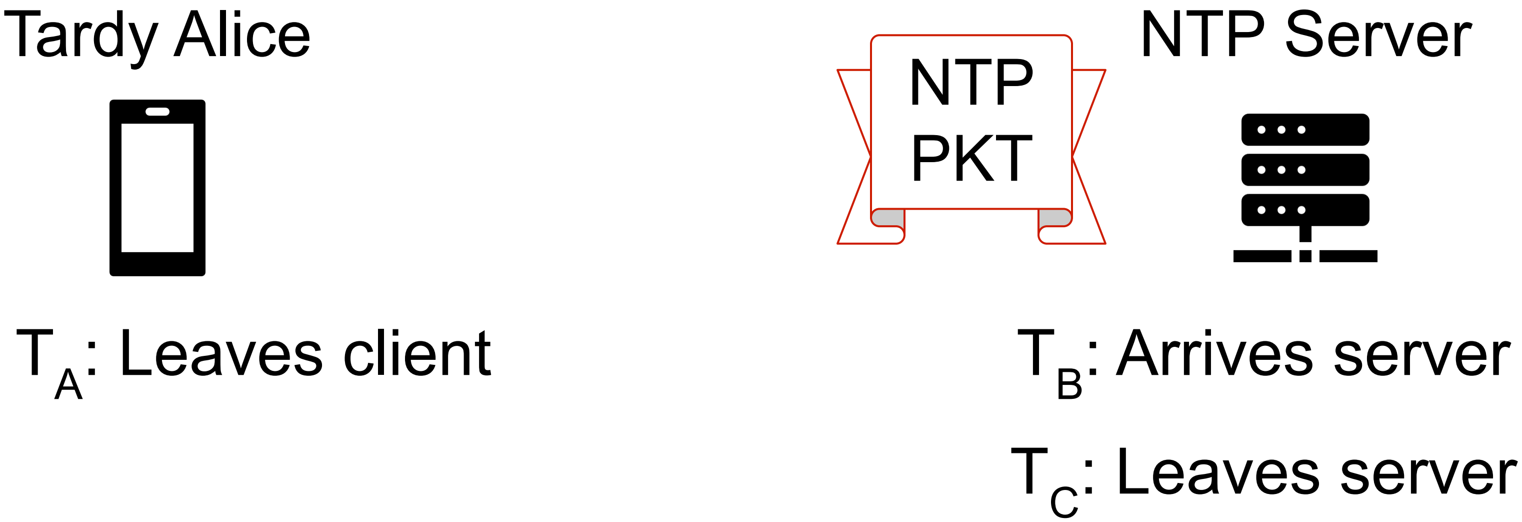
- Spoofing legitimate NTP server
  - Hard; limited scope
- Modifying packets in transport
  - Easier
  - Active vs passive
    - Active: requires access between target and NTP server
    - “On-path”
    - Passive: no direct access
    - “Off-path”

How do we sync time? – On-path attack



T_A: Leaves client

How do we sync time? – On-path attack



Tardy Alice

NTP PKT

NTP Server

T_A: Leaves client

T_B: Arrives server

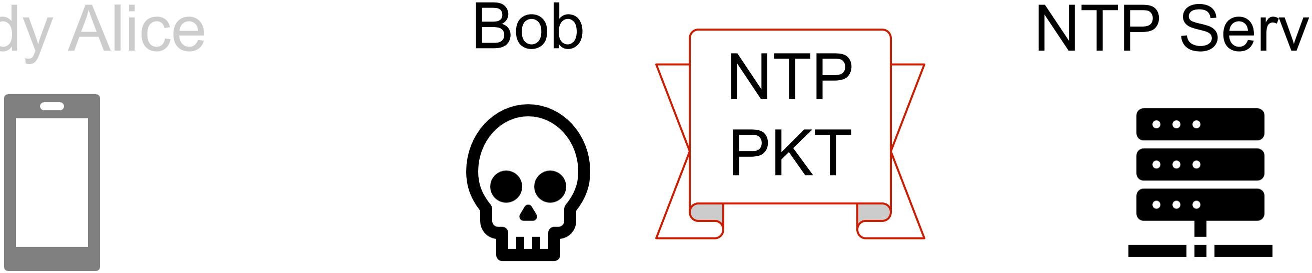
T_C: Leaves server

How do we sync time? – On-path attack

Tardy Alice

Adversarial Bob

NTP Server

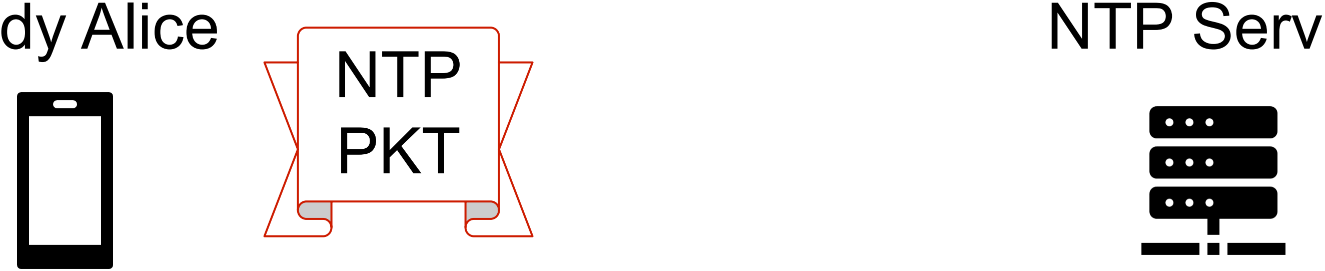


T_A: Leaves client

Changed T_B

Changed T_C

How do we sync time? – On-path attack



Tardy Alice

NTP Server

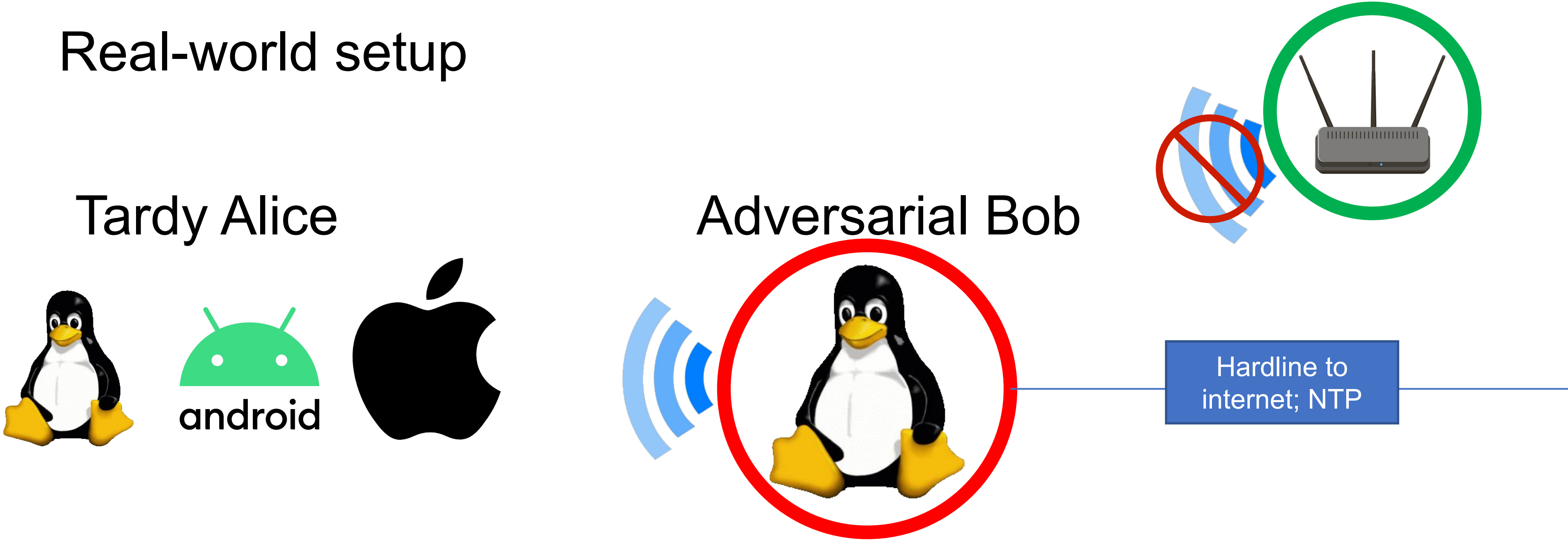
T_A: Leaves client

T_D: Arrives client

Changed T_B

Changed T_C

Real-world setup

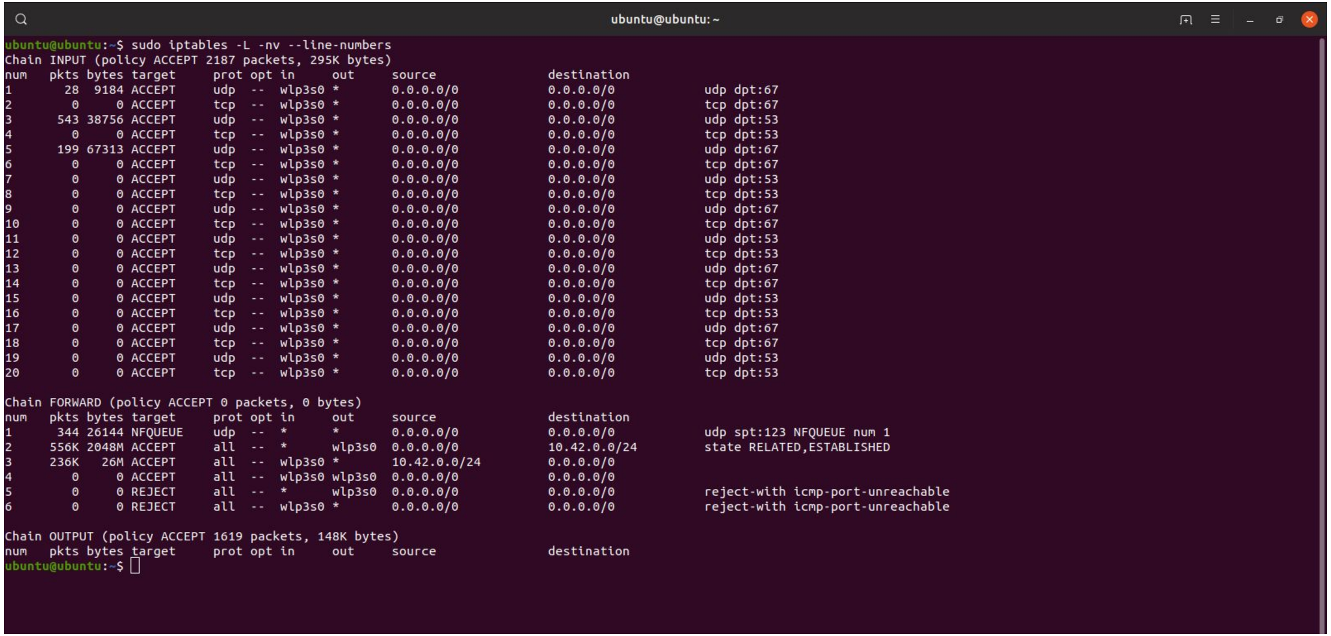


Tardy Alice

Adversarial Bob

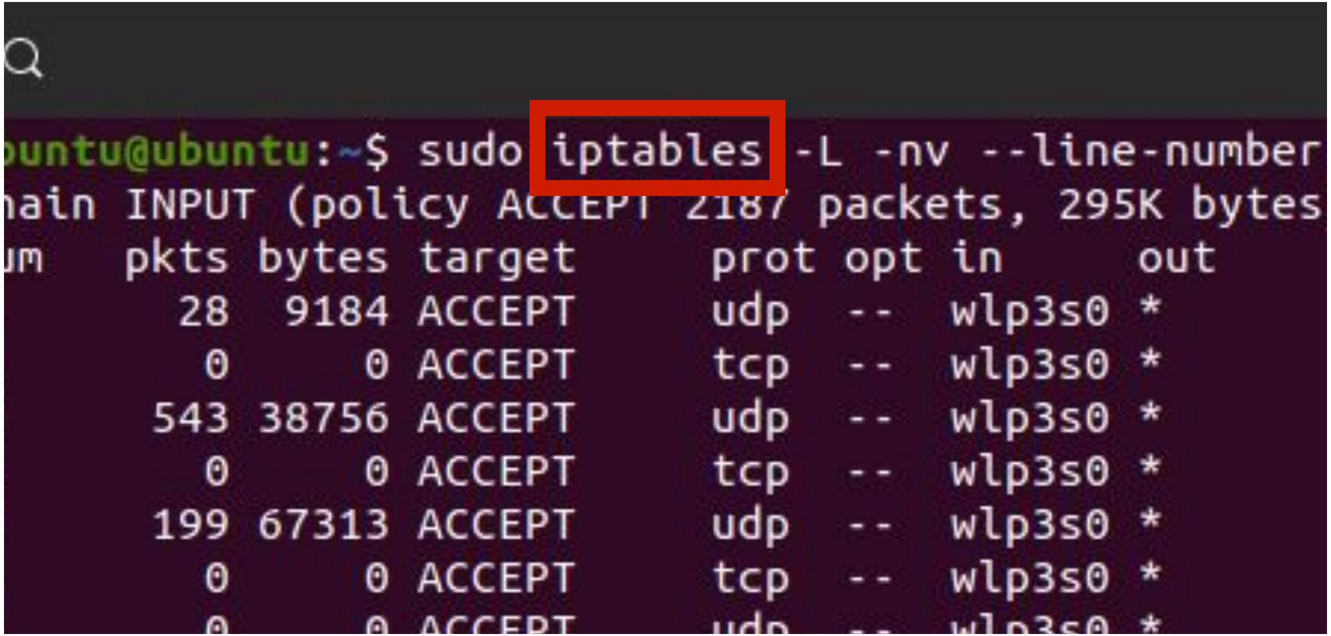
Hardline to internet; NTP

Real-world setup – what does Bob see?



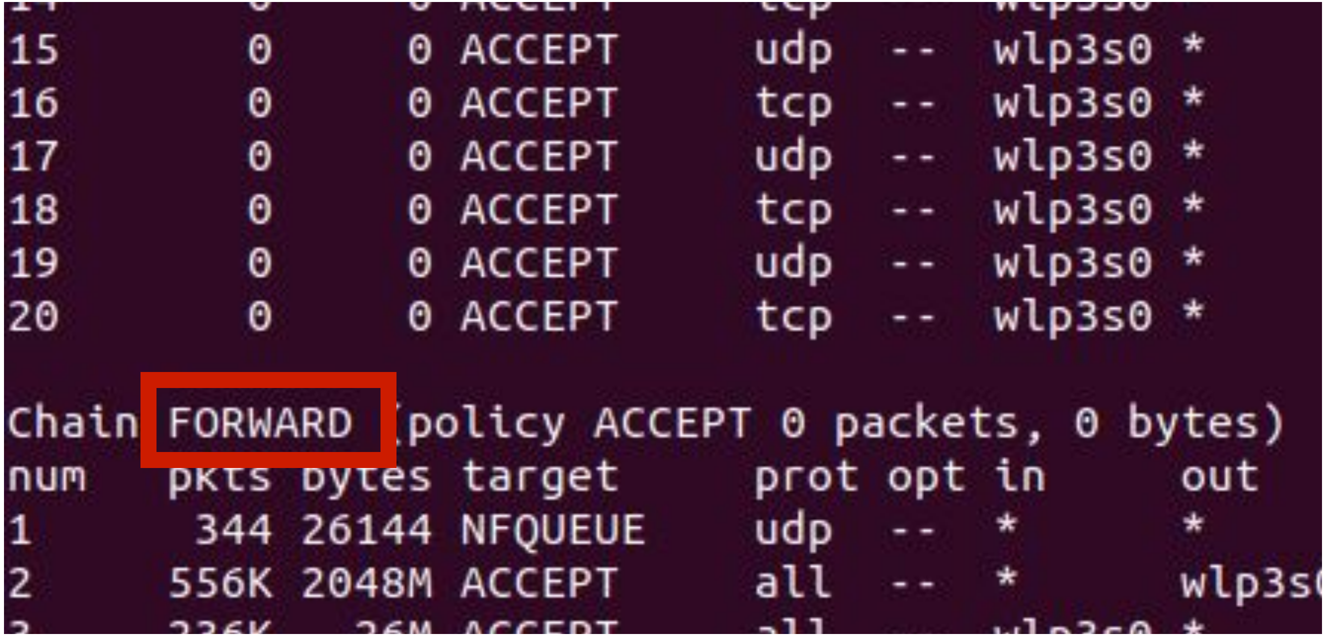
```
ubuntu@ubuntu:~$ sudo iptables -L -nv --line-numbers
Chain INPUT (policy ACCEPT 2187 packets, 295K bytes)
num   pkts bytes target     prot opt in     out     source               destination
1       28  9184 ACCEPT     udp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            udp dpt:67
2        0     0 ACCEPT     tcp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:67
3      543 38756 ACCEPT     udp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
4        0     0 ACCEPT     tcp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
5      199 67313 ACCEPT     udp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            udp dpt:67
6        0     0 ACCEPT     tcp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:67
7        0     0 ACCEPT     udp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
8        0     0 ACCEPT     tcp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
9        0     0 ACCEPT     udp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            udp dpt:67
10       0     0 ACCEPT     tcp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:67
11       0     0 ACCEPT     udp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
12       0     0 ACCEPT     tcp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
13       0     0 ACCEPT     udp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            udp dpt:67
14       0     0 ACCEPT     tcp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:67
15       0     0 ACCEPT     udp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
16       0     0 ACCEPT     tcp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53
17       0     0 ACCEPT     udp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            udp dpt:67
18       0     0 ACCEPT     tcp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:67
19       0     0 ACCEPT     udp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            udp dpt:53
20       0     0 ACCEPT     tcp  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            tcp dpt:53

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out     source               destination
1      344 26144 NFQUEUE    udp  --  *      *       0.0.0.0/0            0.0.0.0/0            udp spt:123 NFQUEUE num 1
2     556K 2048M ACCEPT     all  --  *      wlp3s0  0.0.0.0/0            10.42.0.0/24         state RELATED,ESTABLISHED
3     236K   26M ACCEPT     all  --  wlp3s0 *       10.42.0.0/24         0.0.0.0/0
4        0     0 ACCEPT     all  --  wlp3s0 wlp3s0  0.0.0.0/0            0.0.0.0/0
5        0     0 REJECT     all  --  *      wlp3s0  0.0.0.0/0            0.0.0.0/0            reject-with icmp-port-unreachable
6        0     0 REJECT     all  --  wlp3s0 *       0.0.0.0/0            0.0.0.0/0            reject-with icmp-port-unreachable

Chain OUTPUT (policy ACCEPT 1619 packets, 148K bytes)
num   pkts bytes target     prot opt in     out     source               destination
ubuntu@ubuntu:~$ 
```

Real-world setup – what does Bob see?



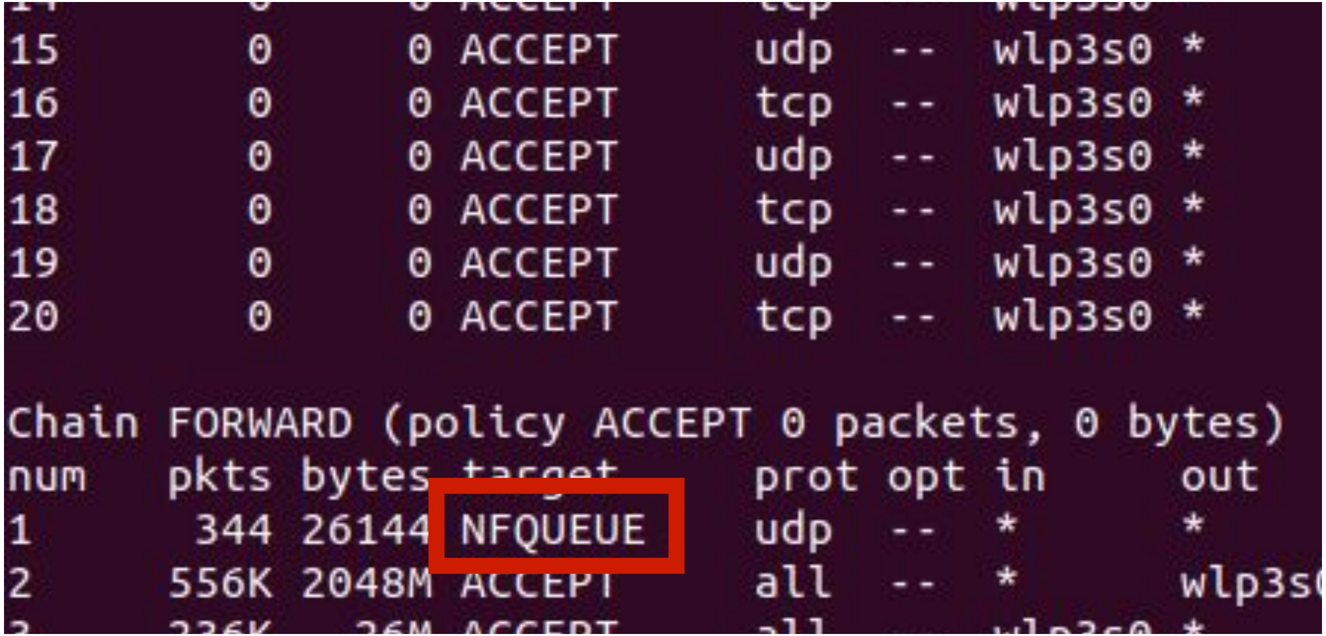
```
untu@ubuntu:~$ sudo iptables -L -nv --line-number
ain INPUT (policy ACCEPT 2187 packets, 295K bytes
um    pkts bytes target     prot opt in     out
        28  9184 ACCEPT     udp  --  wlp3s0 *
         0     0 ACCEPT     tcp  --  wlp3s0 *
       543 38756 ACCEPT     udp  --  wlp3s0 *
         0     0 ACCEPT     tcp  --  wlp3s0 *
       199 67313 ACCEPT     udp  --  wlp3s0 *
         0     0 ACCEPT     tcp  --  wlp3s0 *
         0     0 ACCEPT     udp  --  wlp3s0 *
```

Real-world setup – what does Bob see?



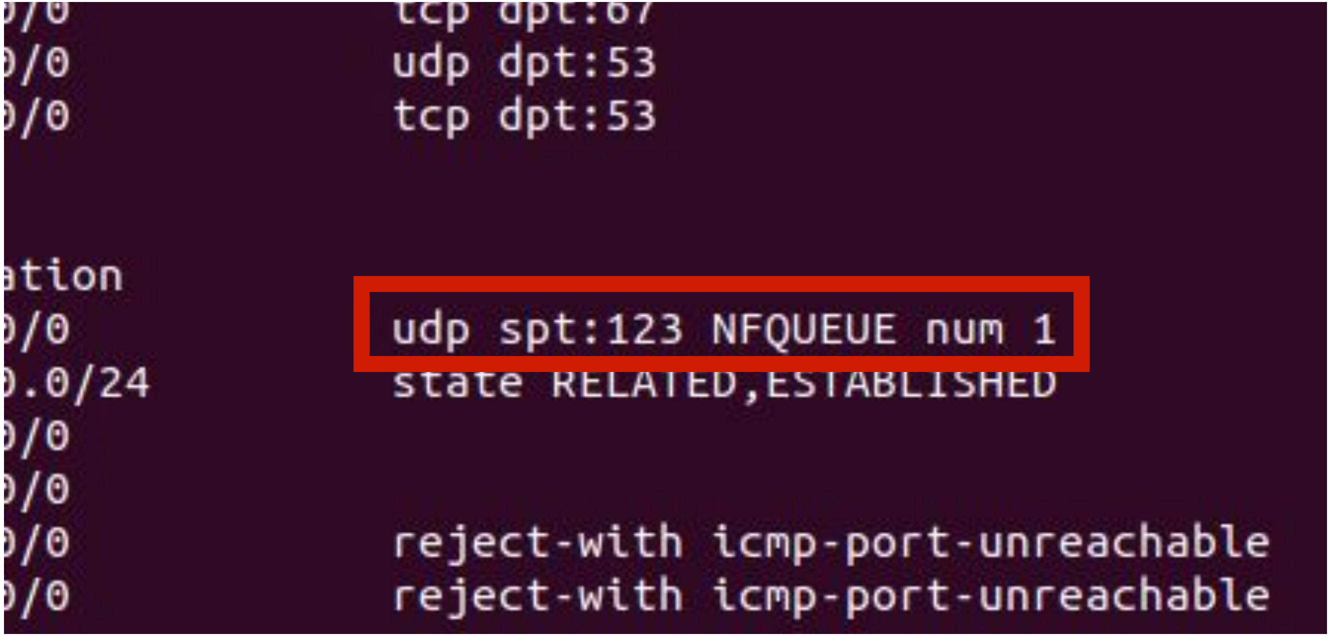
```
14          0         0 ACCEPT      tcp  --  wlp3s0 *
15          0         0 ACCEPT      udp  --  wlp3s0 *
16          0         0 ACCEPT      tcp  --  wlp3s0 *
17          0         0 ACCEPT      udp  --  wlp3s0 *
18          0         0 ACCEPT      tcp  --  wlp3s0 *
19          0         0 ACCEPT      udp  --  wlp3s0 *
20          0         0 ACCEPT      tcp  --  wlp3s0 *

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out
1      344 26144 NFQUEUE    udp  --  *      *
2     556K 2048M ACCEPT     all  --  *      wlp3s
3     236K   26M ACCEPT     all  --  wlp3s0 *
```

Real-world setup – what does Bob see?



```
14           0       0 ACCEPT      tcp  --  wlp3s0 *
15           0       0 ACCEPT      udp  --  wlp3s0 *
16           0       0 ACCEPT      tcp  --  wlp3s0 *
17           0       0 ACCEPT      udp  --  wlp3s0 *
18           0       0 ACCEPT      tcp  --  wlp3s0 *
19           0       0 ACCEPT      udp  --  wlp3s0 *
20           0       0 ACCEPT      tcp  --  wlp3s0 *

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
num   pkts bytes target     prot opt in     out
1      344 26144 NFQUEUE    udp  --  *      *
2     556K 2048M ACCEPT     all  --  *      wlp3s
3     336K   36M ACCEPT     all  --  wlp3s0 *
```

Real-world setup – what does Bob see?

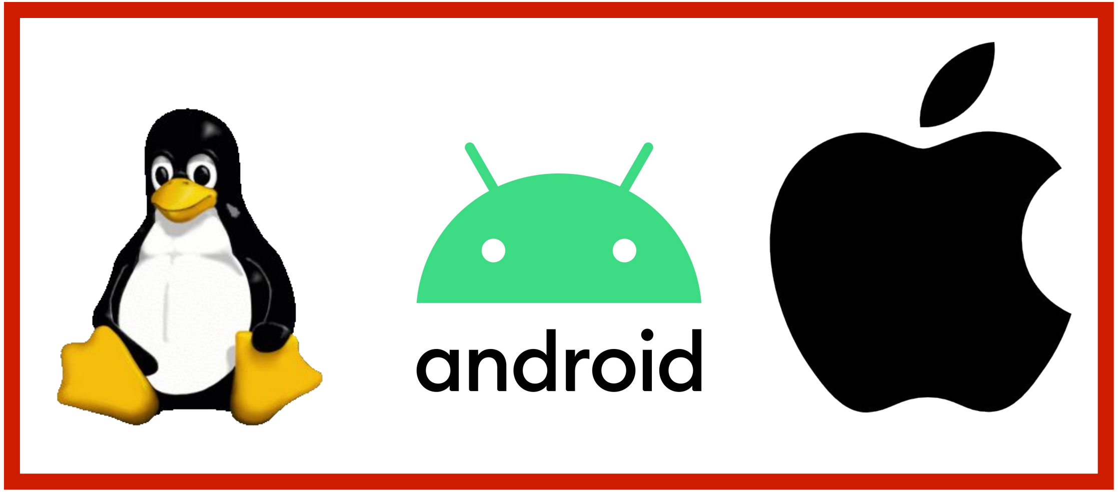


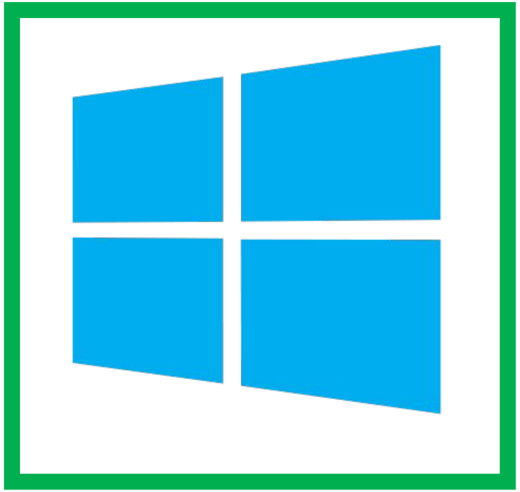
```
0/0           tcp dpt:67
0/0           udp dpt:53
0/0           tcp dpt:53


ation
0/0           udp spt:123 NFQUEUE num 1
0.0/24        state RELATED,ESTABLISHED
0/0
0/0
0/0           reject-with icmp-port-unreachable
0/0           reject-with icmp-port-unreachable
```

Types of modifications – what can Bob do?

- Direct – a precise time
  - Difficult to implement; needs guessing at latency
- Offset – a fixed deviation from the correct time
  - Easier to implement, but less useful

Platforms Affected





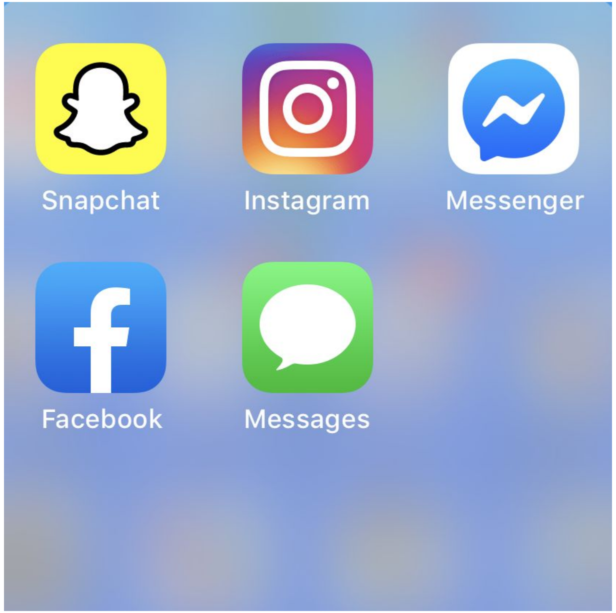
Effects of changing time

- Superficial changes
  - No data changed; only user-facing GUI
- Noncritical changes
  - Insensitive data changed
- Critical/Theoretical issues
  - Forcing computer to perform detrimental actions
  - Sensitive data changed

Effects of changing time

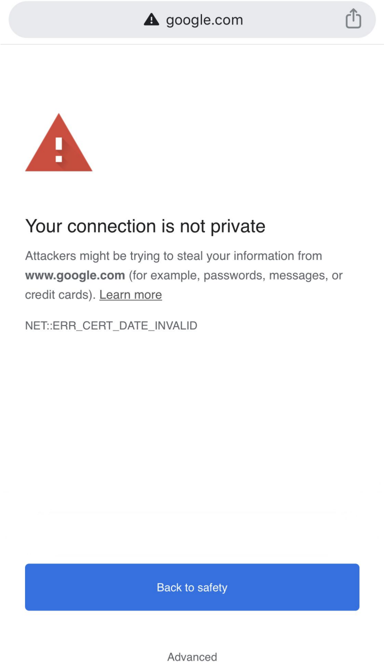
- Superficial changes
  - No data changed; only user-facing GUI
- Noncritical changes
  - Insensitive data changed
- Critical/Theoretical issues
  - Forcing computer to perform detrimental actions
  - Sensitive data changed

Superficial



- Social media
  - Time-centric
- Does not change actual data
  - Comparison of local time to server
- Graceful handling
  - Use absolute time
  - Use pre-existing timezone strategy
  - Calculate times off-device

Noncritical



Your connection is not private

Attackers might be trying to steal your information from **www.google.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_DATE_INVALID

- Injection of user-facing data
  - Incorrect sorting by time
  - Change critical metadata
  - Insertion of data where desired

- Invalidating SSL
  - Annoyance to user
  - Kill Email Sync

Critical Issues

- Logging/scheduling (Linux)
  - Cronjobs
    - Scheduled tasks
    - Rely on system time
  - Logging
    - Rotating logs
    - Keeping logs forever
    - Premature removal
  - Multithreaded applications
    - Scheduling tasks
    - Interrupt functionality

Theoretical Issues

- Manipulating SSL
  - Reusing expired certificates
  - HTTP Downgrading
- If direct-time shifting
  - Predicting pseudorandom number generation

Shortcomings/limitations of threat model

- Windows is not exploitable by default
- Needs man in the middle access
  - Limited scope of targets
- Precise time shifting
  - Extremely unreliable
- “Helper” attack
  - Real consequences come when used in conjunction w/ other attacks

Resolving this issue

- Fix needs to start with developers of apps and OSes
  - Keep time calculations server-side
  - Use a “time zone” system like iMessage

- Re-implementing time sync
  - Use secondary, harder to spoof services: GPS, cell
    - Still vulnerable in general to nation-state attackers
  - Expanding Windows-like authentication system to other platforms

Conclusions/Future Work

- Fundamental protocol’s inherent flaw will be exploited
- Scope of attack is limited but significant
- Big issue: human loss of trust in tech

- Work on implementations of higher-level trust-based attacks
- Target more IoT devices
- Implement **security** or **replace** NTP

Special thanks to:

- Prof. Ari Trachtenberg and Trishita Tiwari
- Dr. Aanchal Malhotra
- Prof. Mayank Varia

- My parents
- MIT PRIMES

Any questions?

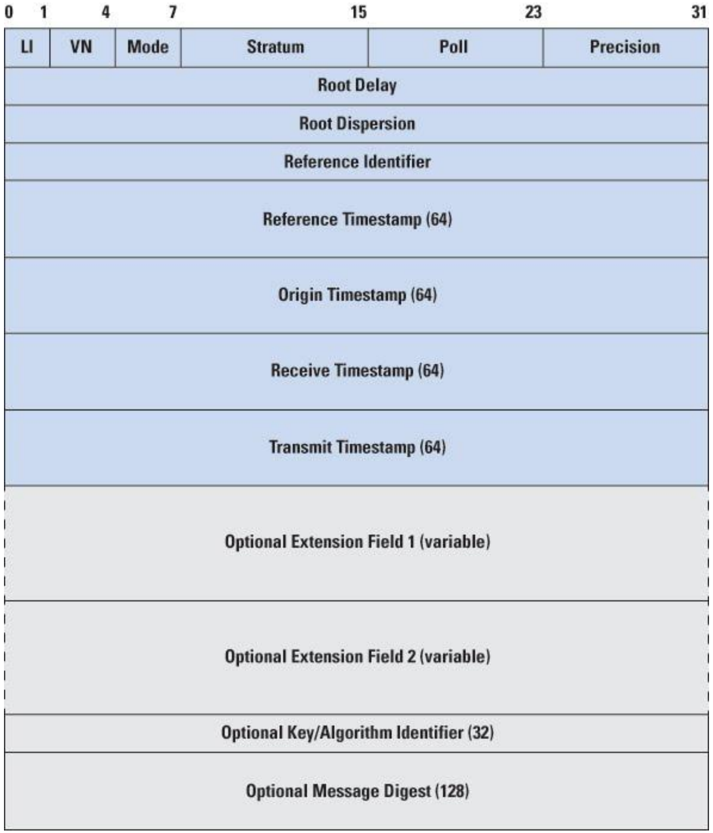
Academic Credits

- A Malhotra et al. *Attacking the Network Time Protocol*. Boston University. http://www.cs.bu.edu/~goldbe/papers/NTPattack.pdf
- G. Huston. *Protocol Basics – The Network Time Protocol.* Asia-Pacific Network Information Centre. https://labs.apnic.net/?p=462
- ubuntu documentation. *Time Synchronization*. Canonical Support. https://help.ubuntu.com/lts/serverguide/NTP.html
- Linode. *Control Network Traffic with IPTables*. Linode. https://www.linode.com/docs/security/firewalls/control-network-traffic-with-iptables/

Image Credits

- Moon animation: https://media.giphy.com/media/QIlf7zcBVJuak/giphy.gif
- FedEx plane: https://3acujq5da9i3we40i1od3kl1-wpengine.netdna-ssl.com/wp-content/uploads/2018/06/fedx_freighter_order3_960x600-696x435.jpg
- CPU clock: https://hsto.org/getpro/habr/post_images/9d4/ede/bb8/9d4edebb8a0253cb1b973bd5df46a9a9.jpg
- Logging: https://www.amlogging.com/wp-content/uploads/2019/08/am_logging_background_update.jpg
- SSL certificates: https://www.iconsdb.com/icons/preview/green/ssl-badge-2-xxl.png
- Y2K: https://i.ytimg.com/vi/Q85jerrwBc4/maxresdefault.jpg
- GPS: https://www.geotab.com/geoimages/blog/what-is-gps.png
- Stratum Diagram https://en.wikipedia.org/wiki/Network_Time_Protocol#/media/File:Network_Time_Protocol_servers_and_clients.svg
- Lock Breaking http://4.bp.blogspot.com/-Laasnybm00c/TbmmgZTIuiI/AAAAAAAAAC4/uRHCV3CBP3Q/s1600/breakingLock.jpg
- Wave https://azpng.com/png/2019/06/26/wave-clipart-wifi-waves-blue-transparent-x-free.png
- Tux the Linux Penguin https://upload.wikimedia.org/wikipedia/commons/a/af/Tux.png
- Android https://zdnet3.cbsistatic.com/hub/i/2019/08/22/5e05c9d9-27a7-4691-93fa-257717df6582/b96f965a7dee5ea340da1f48eb61a146/android-logo-stacked-rgb.jpg
- Apple Logo
- NTP Packet Structure: https://www.cisco.com/c/dam/en_us/about/ac123/ac147/images/ipj/ipj_15-4/154_ntp_fig01_lg.jpg

Additional Information – NTP Packet Structure



LI | VN | Mode | Stratum | Poll | Precision

Root Delay

Root Dispersion

Reference Identifier

Reference Timestamp (64)

Origin Timestamp (64)

Receive Timestamp (64)

Transmit Timestamp (64)

Optional Extension Field 1 (variable)

Optional Extension Field 2 (variable)

Optional Key/Algorithm Identifier (32)

Optional Message Digest (128)