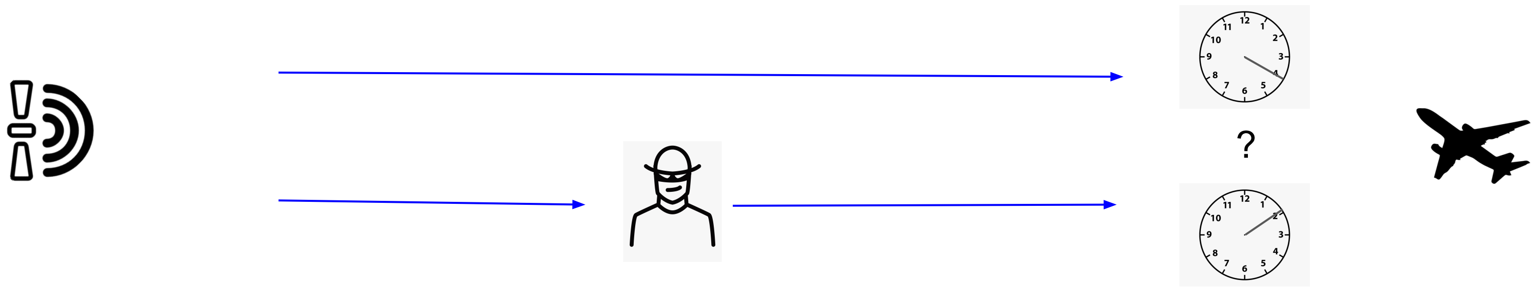
Addressing GNSS TESLA Synchronization Vulnerability

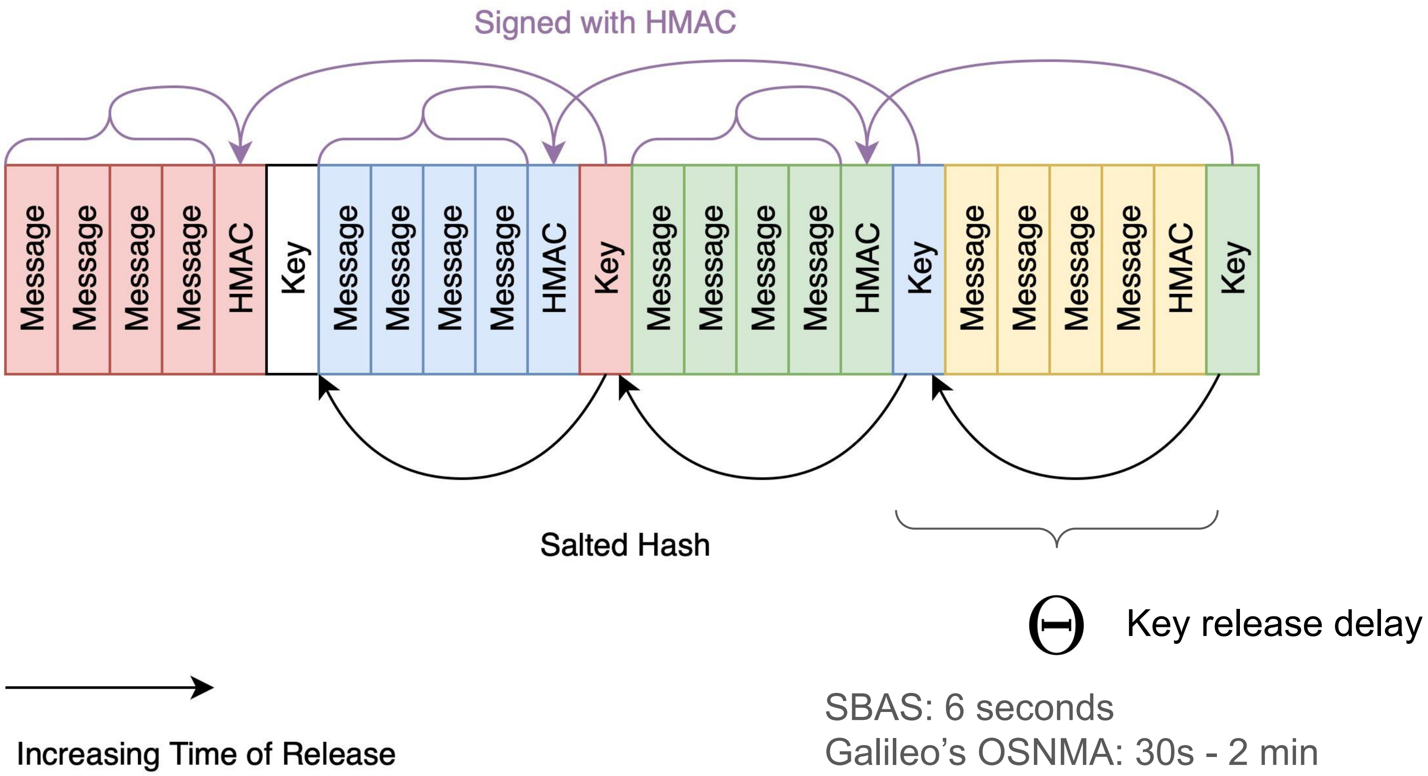
Jason Anderson, Sherman Lo, Todd Walter
Stanford University

Why is Network Sync Needed for GNSS Security?

- GNSS is a one-way signal
  - Not possible to secure against delayed signals without an non-GNSS two-way sync
- Delayed signals will be perceived to cause the time estimate to lag

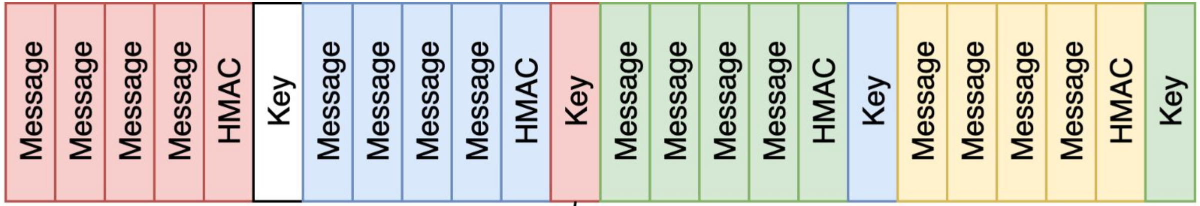


Typical Construction of GNSS TESLA



SBAS: 6 seconds
Galileo's OSNMA: 30s - 2 min
Chimera: 2-6 seconds and/or 2-3 minutes

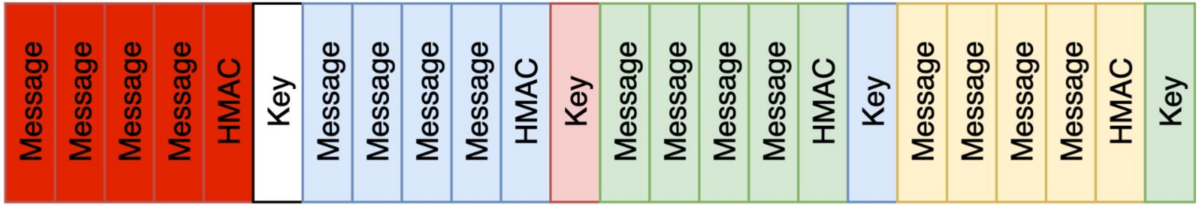
Problems with Clock Lag



If Signal is sufficiently delayed (6 seconds for SBAS/EGNOS) the spoofer can take key and forge authenticated messages.

Or clock offset θ

Delayed Signal



Insecure if $\theta < -\Theta$

Increasing Time of Release

Why do we have a Security Vulnerability?

- With the original TESLA, the key release delay is set individually between provider and receiver
- If an adversary interferes with the sync bootstrap, then the key release delay increases
- DOS is possible, forgery is not

- With GNSS TESLA, the key release delay is system wide with the multicast context
- Individual clocks have stochastic drifts
- Knowledge of an insecure onboard clock reveal whether a receiver will accept forgeries
- There is a simple test to find insecure outliers

Forming a Test of Vulnerability to Find Outliers

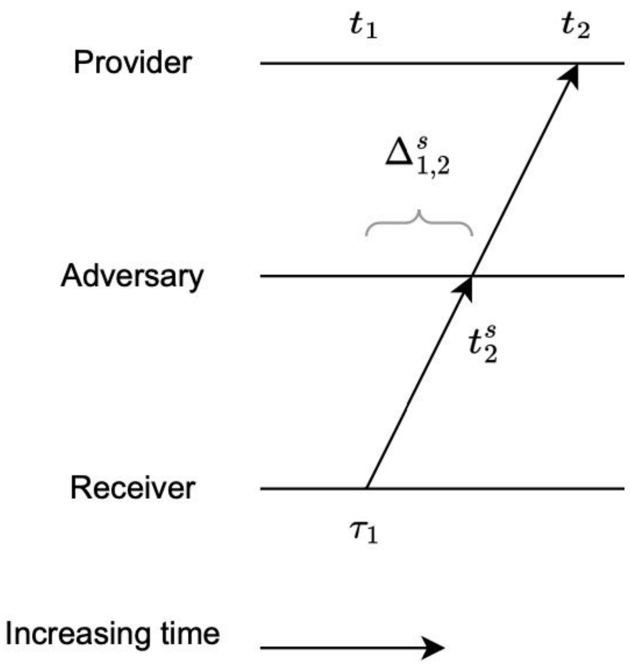
- A simple test to determine vulnerability

$$\Pr(\Delta_{1,2} < 100\text{ms}) > 0.99$$

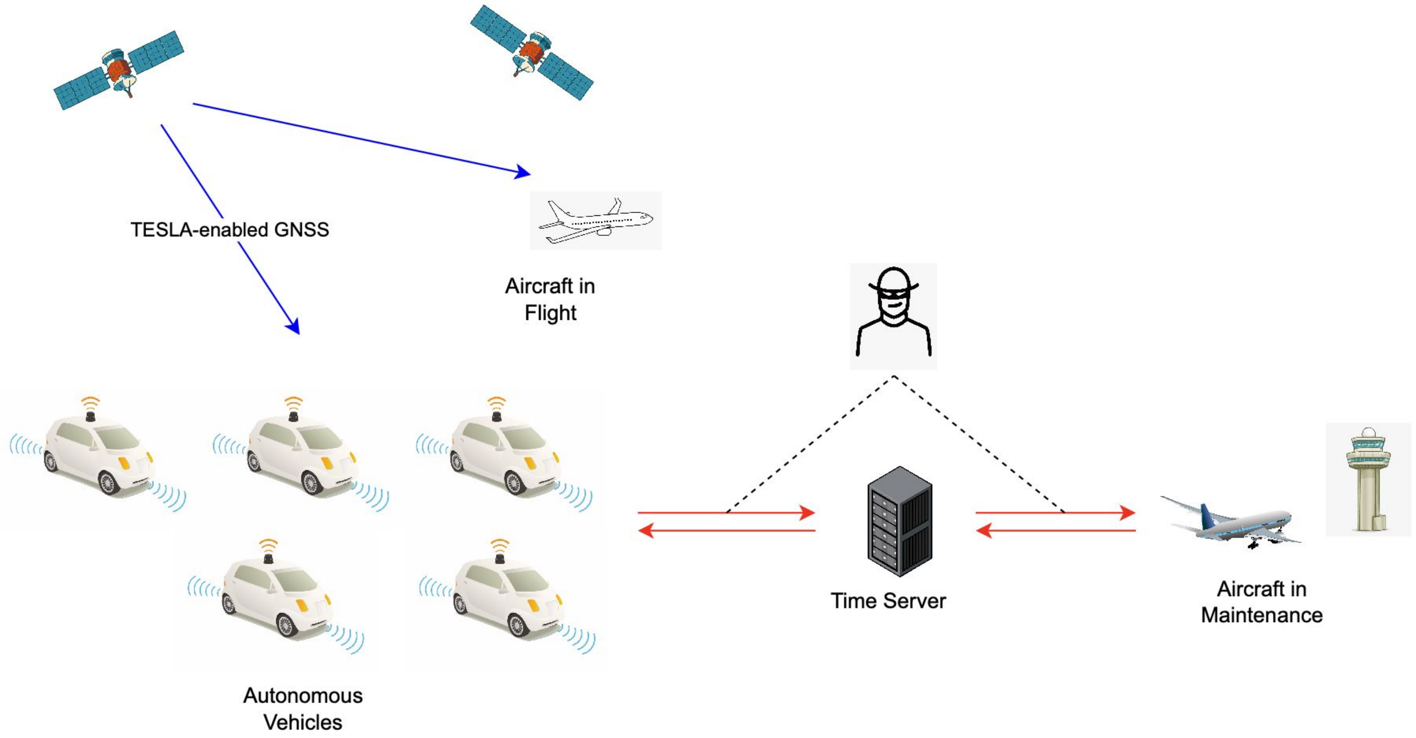
$$\Pr(\theta < -(t_2^s - \tau_1) + 100\text{ms}) > 0.99$$

$$-(t_2^s - \tau_1) + 100\text{ms} < -\Theta$$

SBAS: 6 seconds
Galileo’s OSNMA: 30s - 2 min
Chimera: 2-6 seconds and/or 2-3 minutes

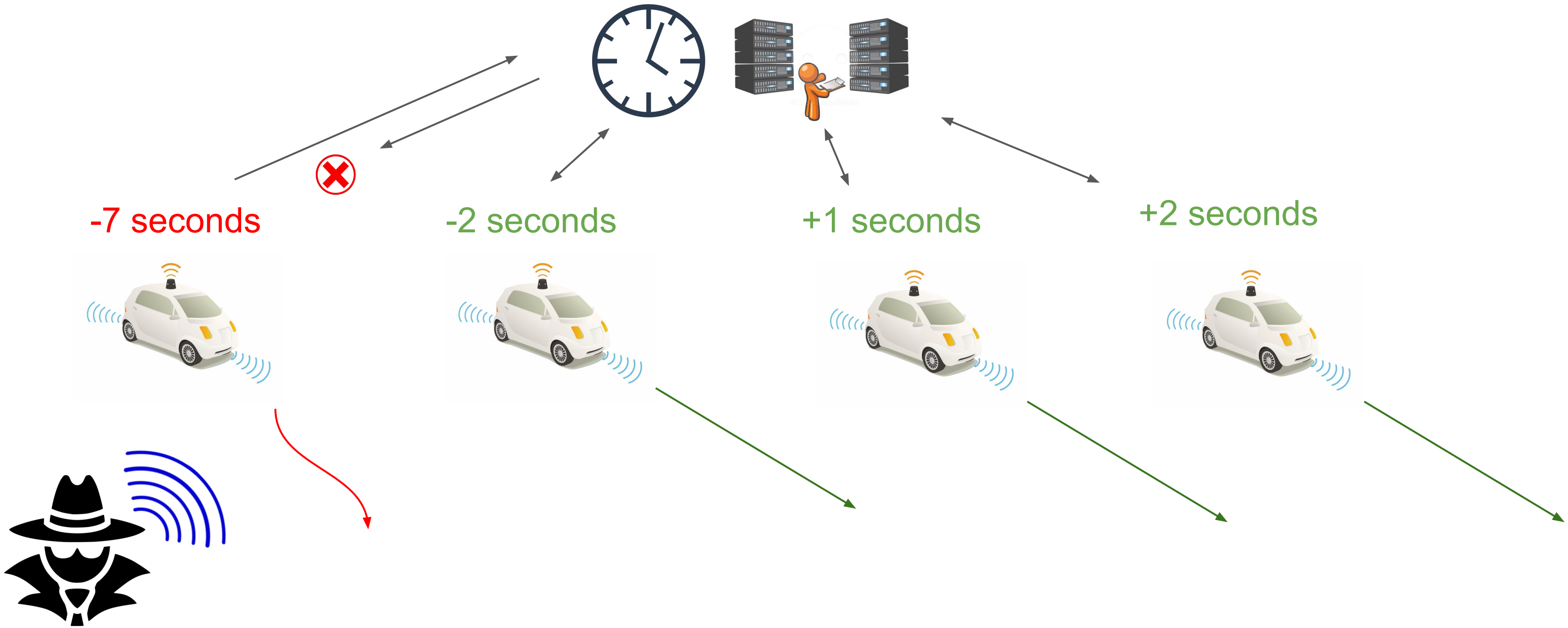


A Vision for the Future



An Attacker can wait to find a lagging clock

An adversary may not care which specific vehicle serves its nefarious purpose.



Estimating Clock Bound

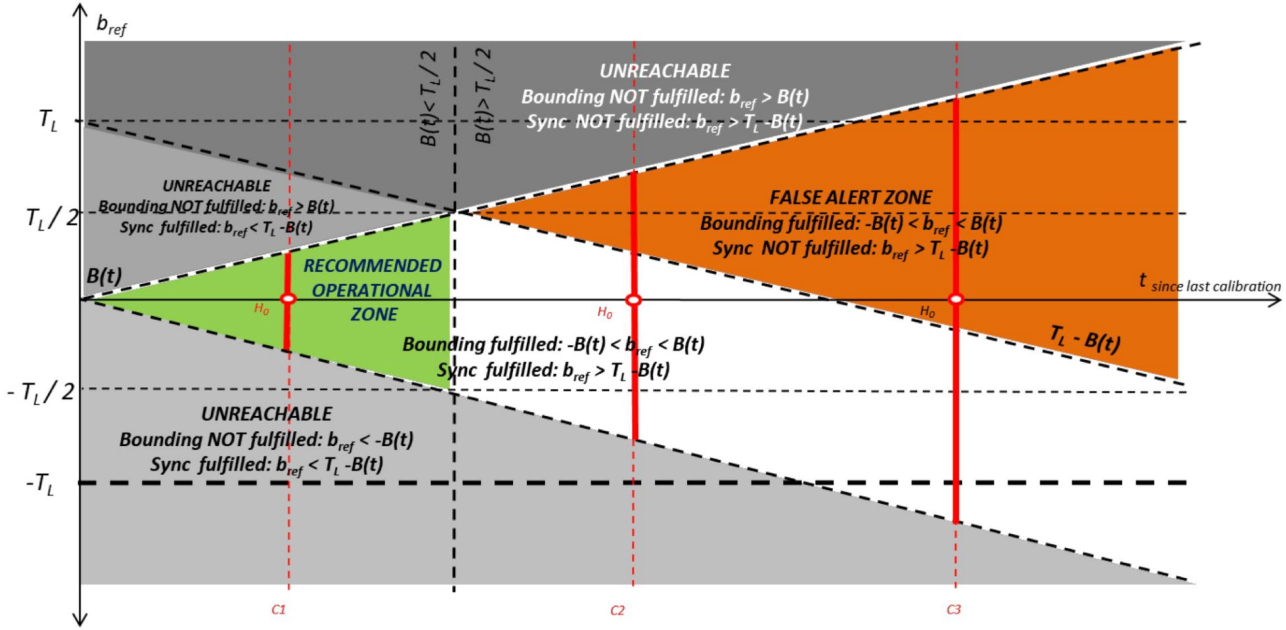


Figure from
Fernandez-Hernandez, Ignacio, et al. "Independent time synchronization for resilient gnss receivers." Proceedings of the 2020 International Technical Meeting of The Institute of Navigation. 2020.

How to address this?

- Do not reveal t1 in NTP protocol, Non-Predictable Queries
  - Already existing draft NTP Data minimization
- Enforce Time Synchronization with quick Round Trip Time
  - Might spontaneously require a vehicle to go out of service
  - This requirement is likely not palatable to current aviation stakeholders

How to Communicate Security Requirements?

System: EGNOS
Manager: ESA
Timing Standard

System: Galileo
Manager: EUSPA & ESA
Timing Standard

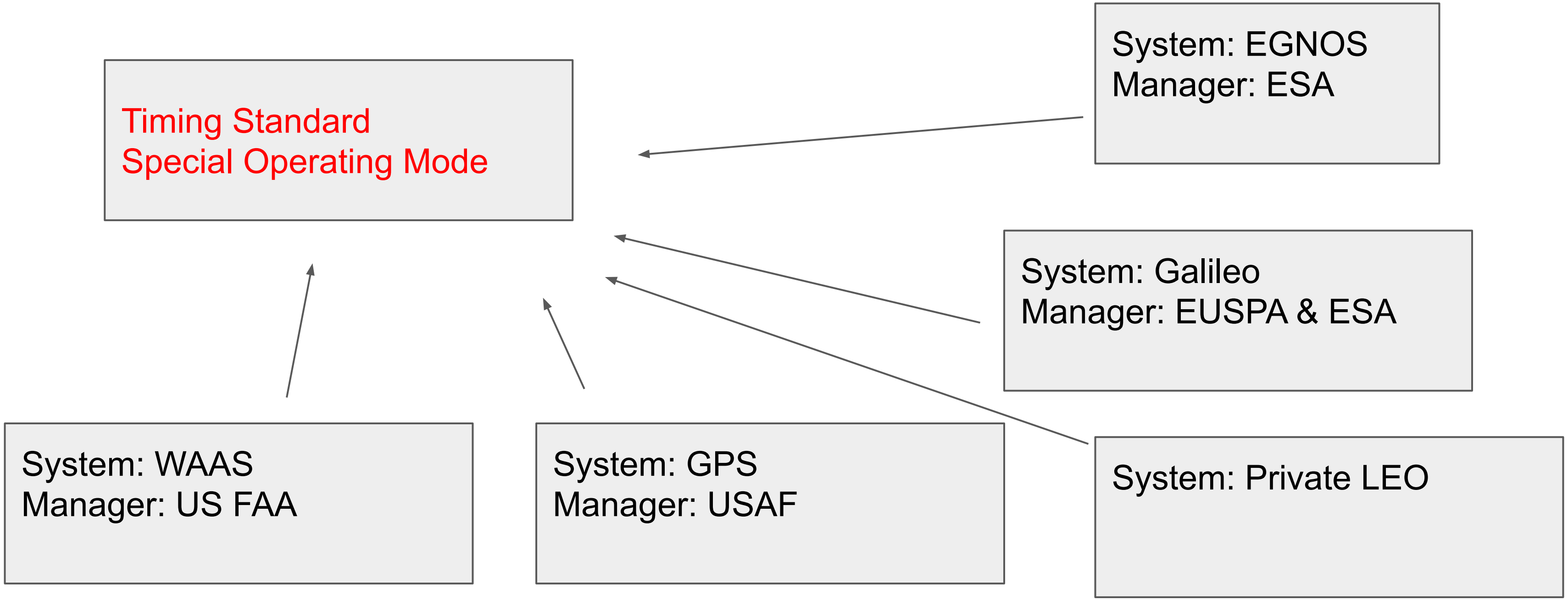
System: WAAS
Manager: US FAA
Timing Standard

System: GPS
Manager: USAF
Timing Standard

System: Private LEO

Timing Standard

How to Communicate Security Requirements?



Final Thoughts

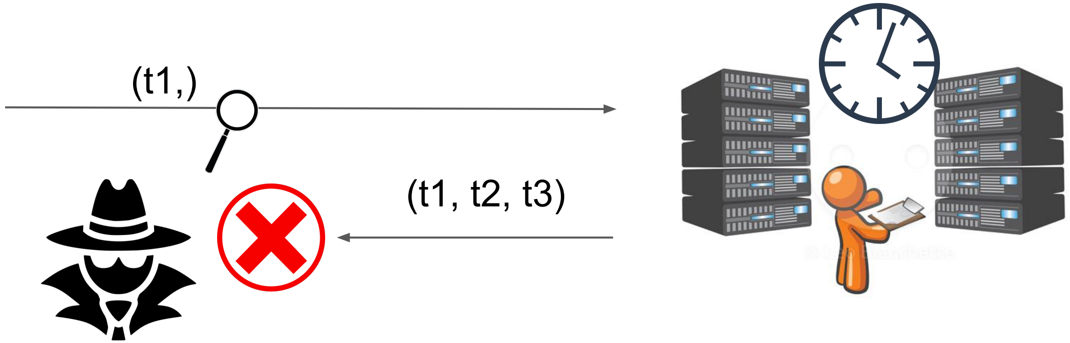
- Hoping to get support to incorporate these ideas to NTP so that I can cite one standard in future stakeholders among
  - Aviation Receivers Manufacturers
  - Aviation Manufacturers
  - Autonomous Cars
  - Regulators
  - Navigation System

We gratefully acknowledge the support of the FAA Satellite Navigation Team for funding this work under Memorandum of Agreement #: 693KA8-19-N-00015.

Backups

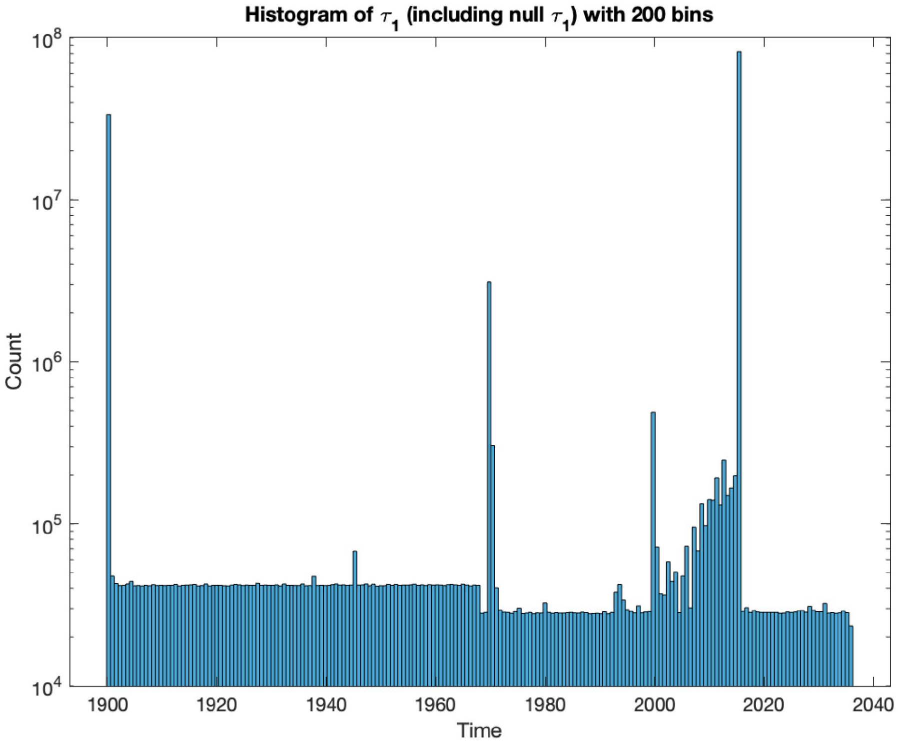
The Attack

1. An attacker listens to NTS (or NTP) traffic ingoing the server
2. An attacker uses the originator timestamp to estimate the receiver's clock lag
3. Once the attacker observes a receiver with substantial clock lag, the attacker blocks the NTS traffic outgoing from the server to the vulnerable receiver so the receiver cannot know its clock is vulnerable
4. An attacker broadcasts forged GNSS signals to the vulnerable receiver



How vulnerable are we now?

- From 2015 NIST 18-hour long Study on NTP servers,
  - Some clocks transmit null tau1
  - Some clocks transmit random tau1
  - Some clocks transmit a coarse tau1
- Many clocks transmit the actual tau1, and among those, we find many clocks would be vulnerable if they were being synchronized for TESLA-based GNSS under our attack model
- Credit Dr. Jeff Sherman from NIST



How vulnerable are we now?

- After accounting for a reasonable NTP transit time, assuming the SBAS 6-second security requirement, we observe clocks that would accept forgeries.
- Many receivers with -(t2-tau1) < -6