WSTS, 2019

Clock Sync Safety and Security for Enterprise in Depth

FSMLabs
Enterprise Real-Time®

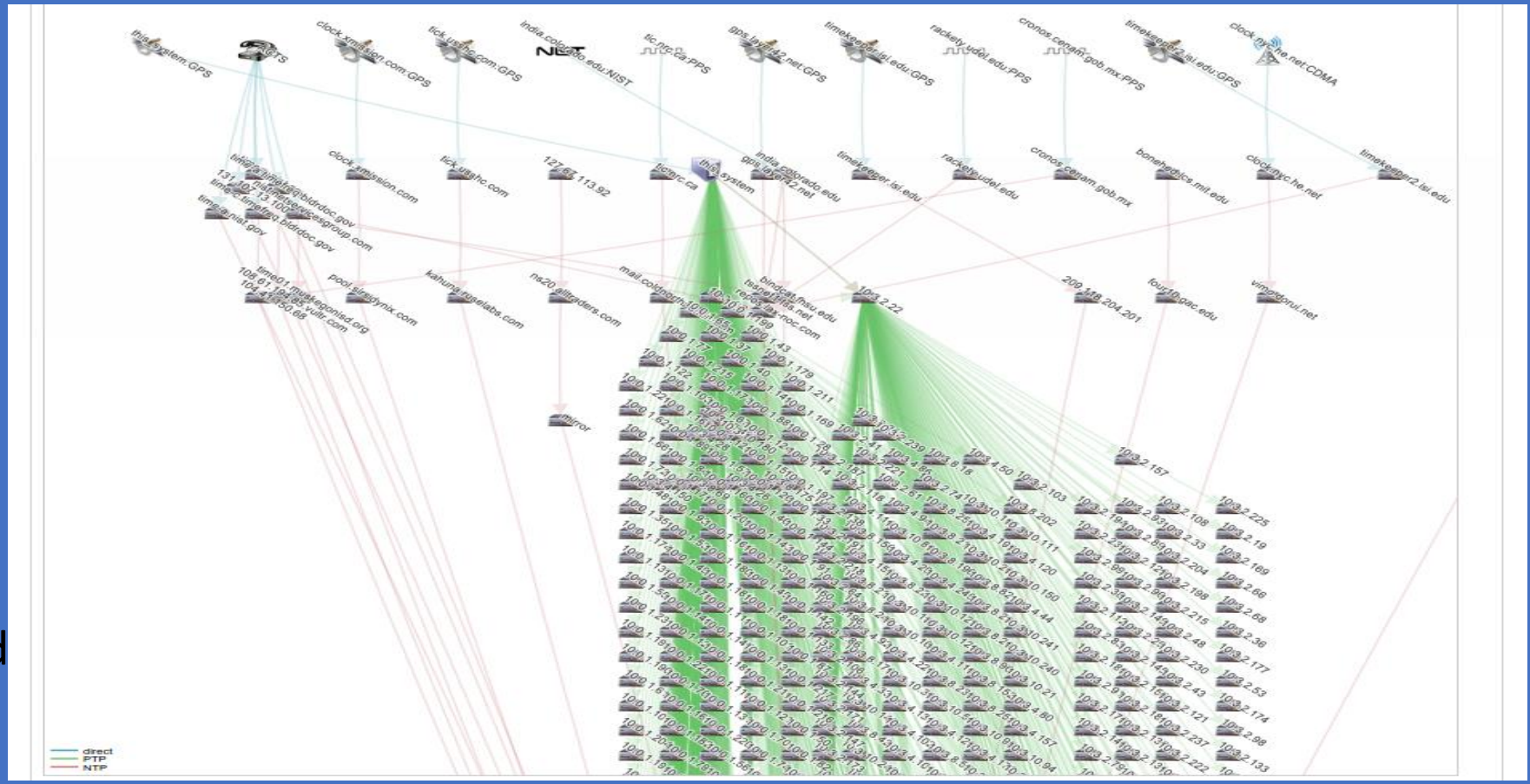
What is the threat profile?

- Protecting clock integrity in financial networks
- Using clock sync as a security mechanism

FSMLabs
Enterprise Real-Time

Clock sync distribution is inherently fragile

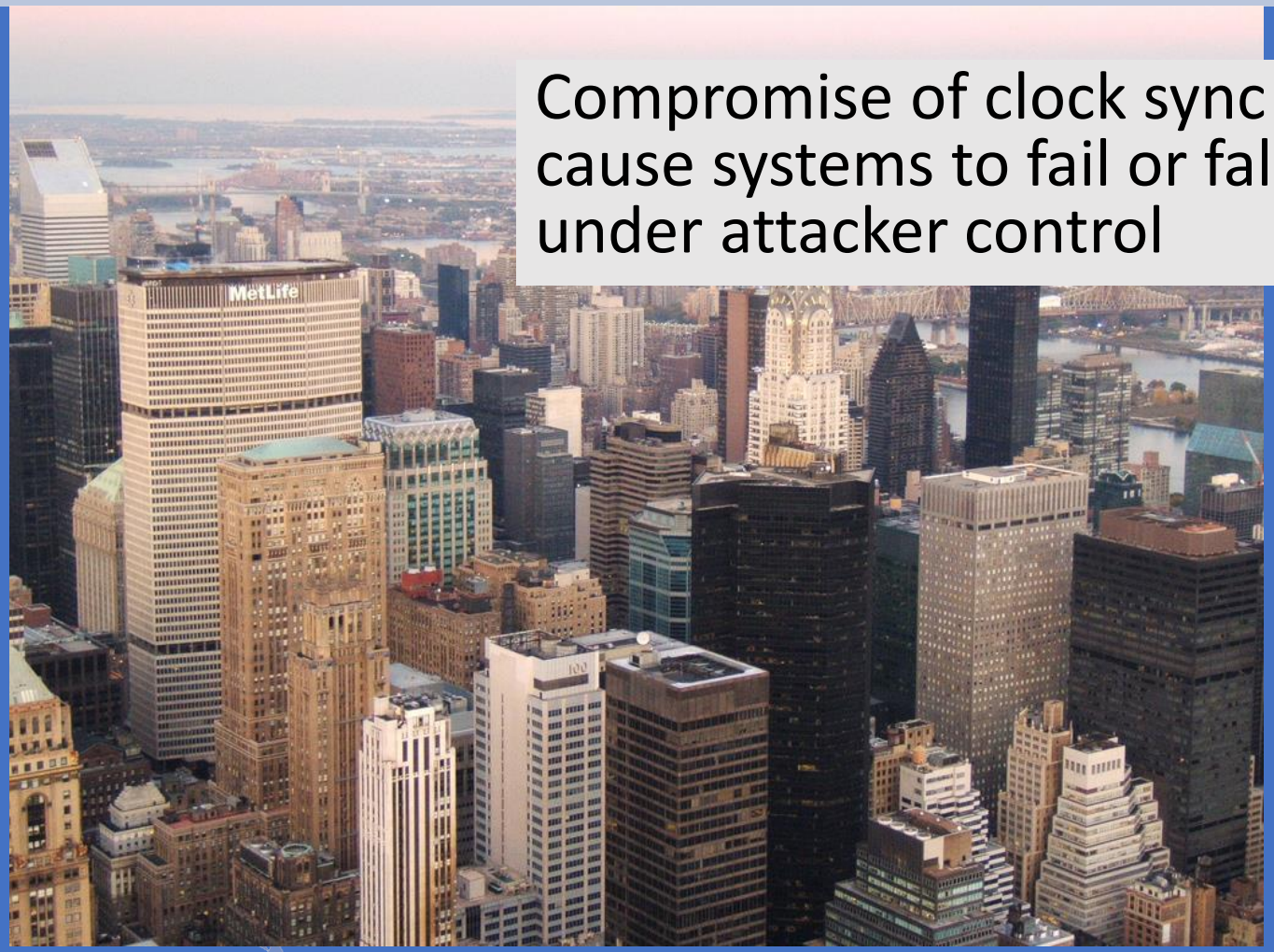
- GPS/GNSS can be jammed or spoofed
- Clock sources can be counterfeited or compromised.
- The network can be broken or interfered with
- Stratum servers & boundary clocks …
- Clients …
- Protocols are open and have little built in security



Timekeeper "Time map" showing clock distribution

FSMLabs
Enterprise Real-Time

Critical electronic networks are increasingly dependent on high quality clock sync



Compromise of clock sync can cause systems to fail or fall under attacker control

- Financial trading companies need high quality clock sync to meet regulatory requirements, prevent fraud, find “alpha”, validate SLAs …
- Cloud and distributed data depend on clock sync for data consistency
- Software defined networks need clock sync for analytics and efficiency
- …

FSMLabs
Enterprise Real-Time

Design principles

- Defense in depth
  - Any security method can be breached – plan for it
  - Have each component cross check and reinforce the other components
- Engineering analysis of threats
  - Identify a threat
  - Determine cost of compromise and probability of compromise
  - Determine cost of protection
  - Analyze tradeoffs

Compromise points

Jam or Spoof radio

GNSS Clock

Compromise or interfere

Block or tamper

Network Components
Boundary clocks

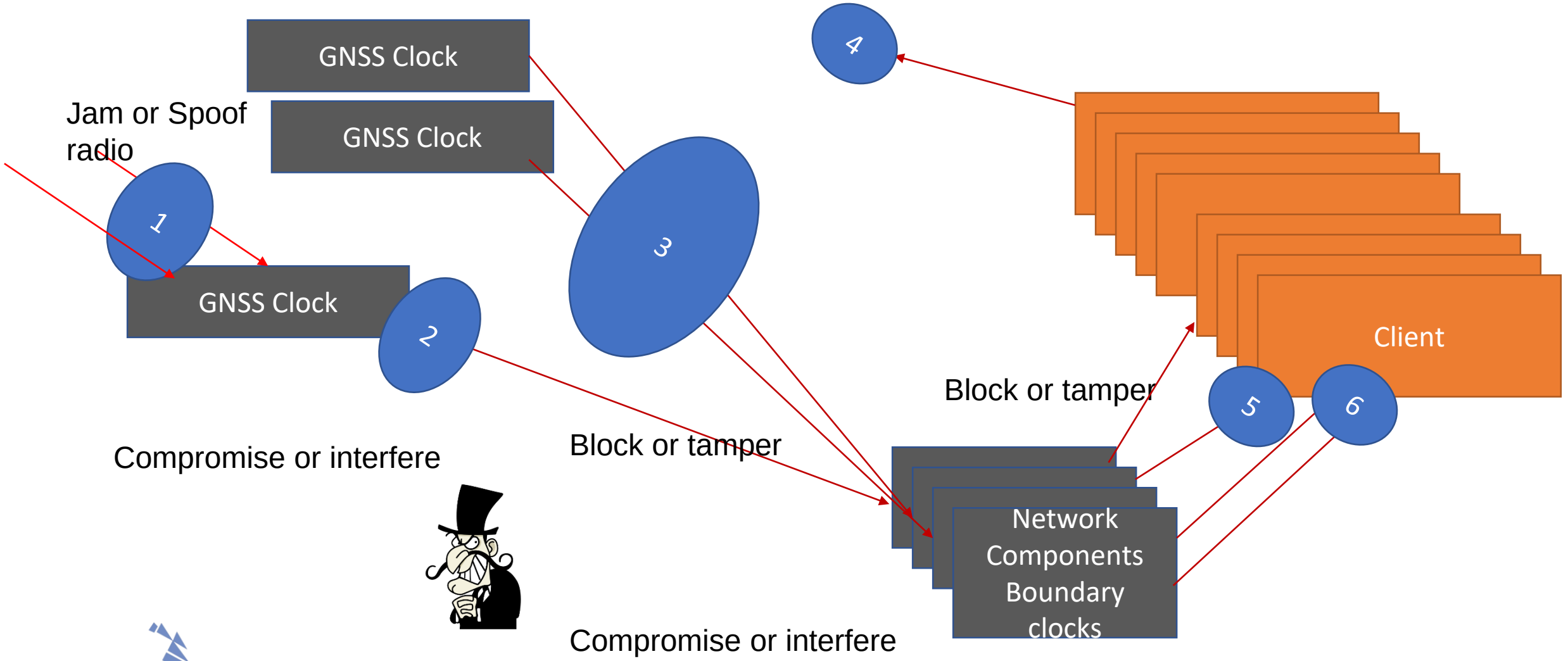
Compromise or interfere

Block or tamper

Client

FSMLabs
Enterprise Real-Time

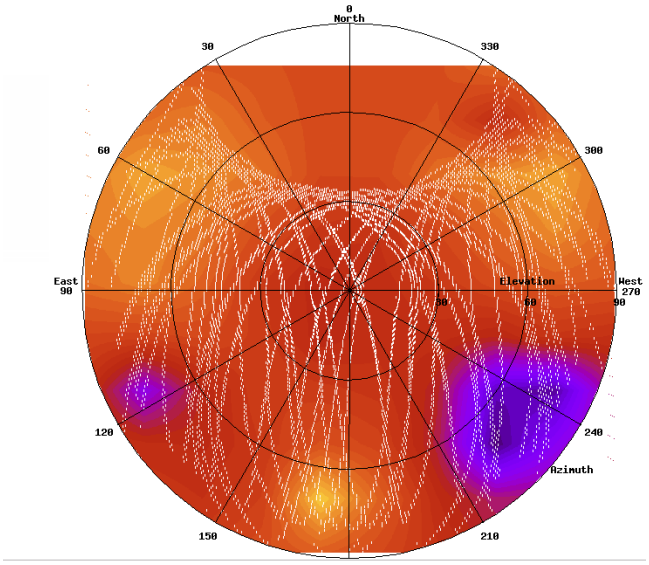
Security points



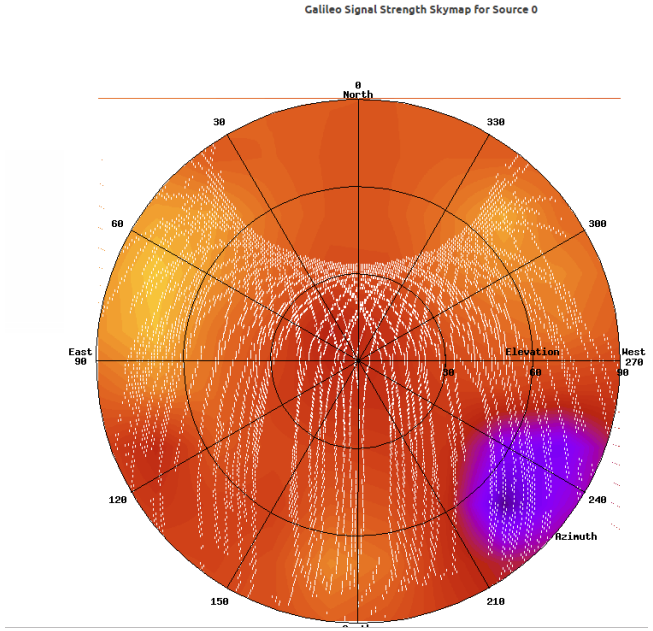
FSMLabs
Enterprise Real-Time®

1) Multiple constellations: Compare views of sky.

Sky view for different constellations should not differ radically. If one changes and the others don't – problem with that source.



GPS

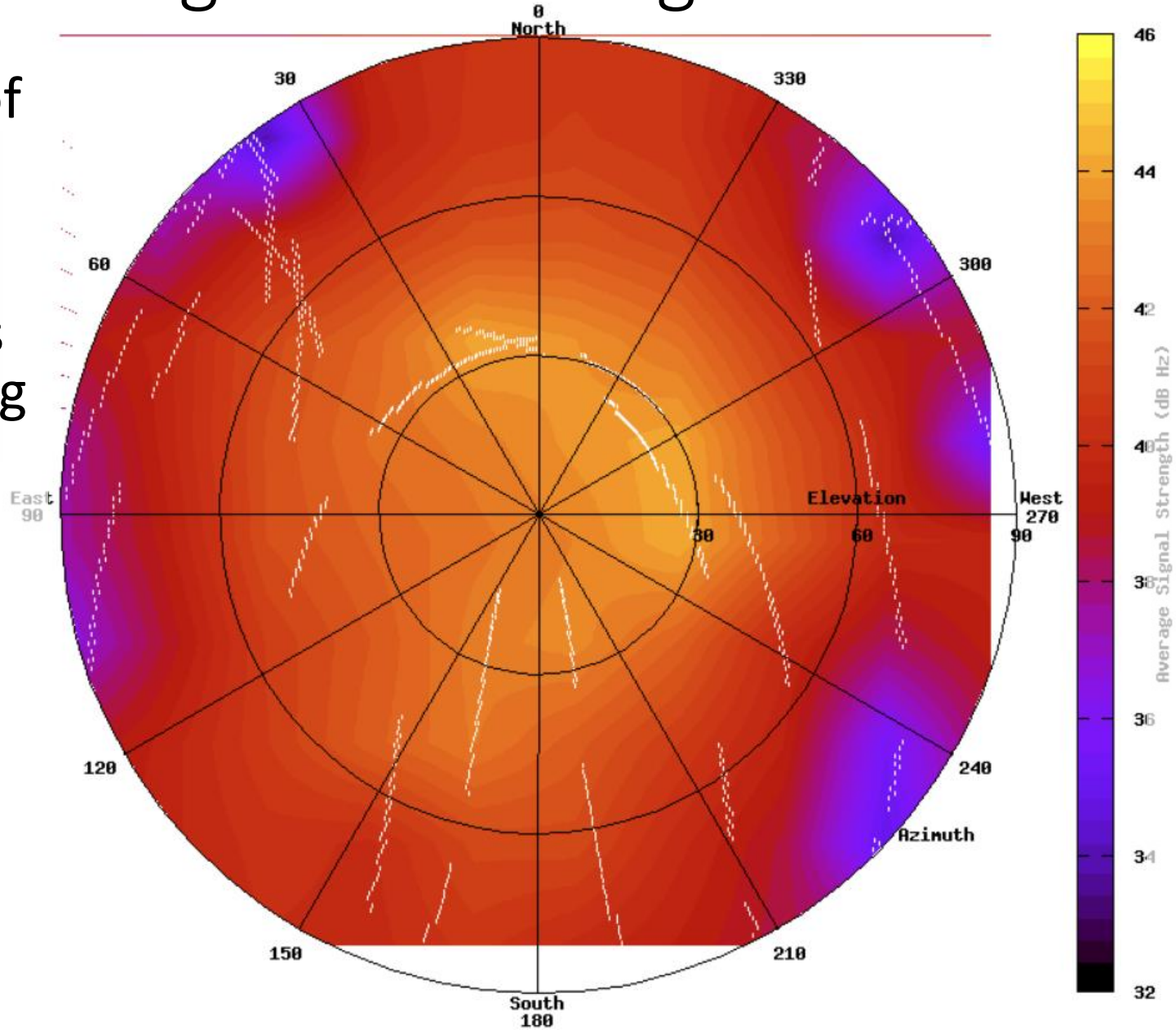


Galileo

FSMLabs
Enterprise Real-Time®

2) Second guess GNSS signal

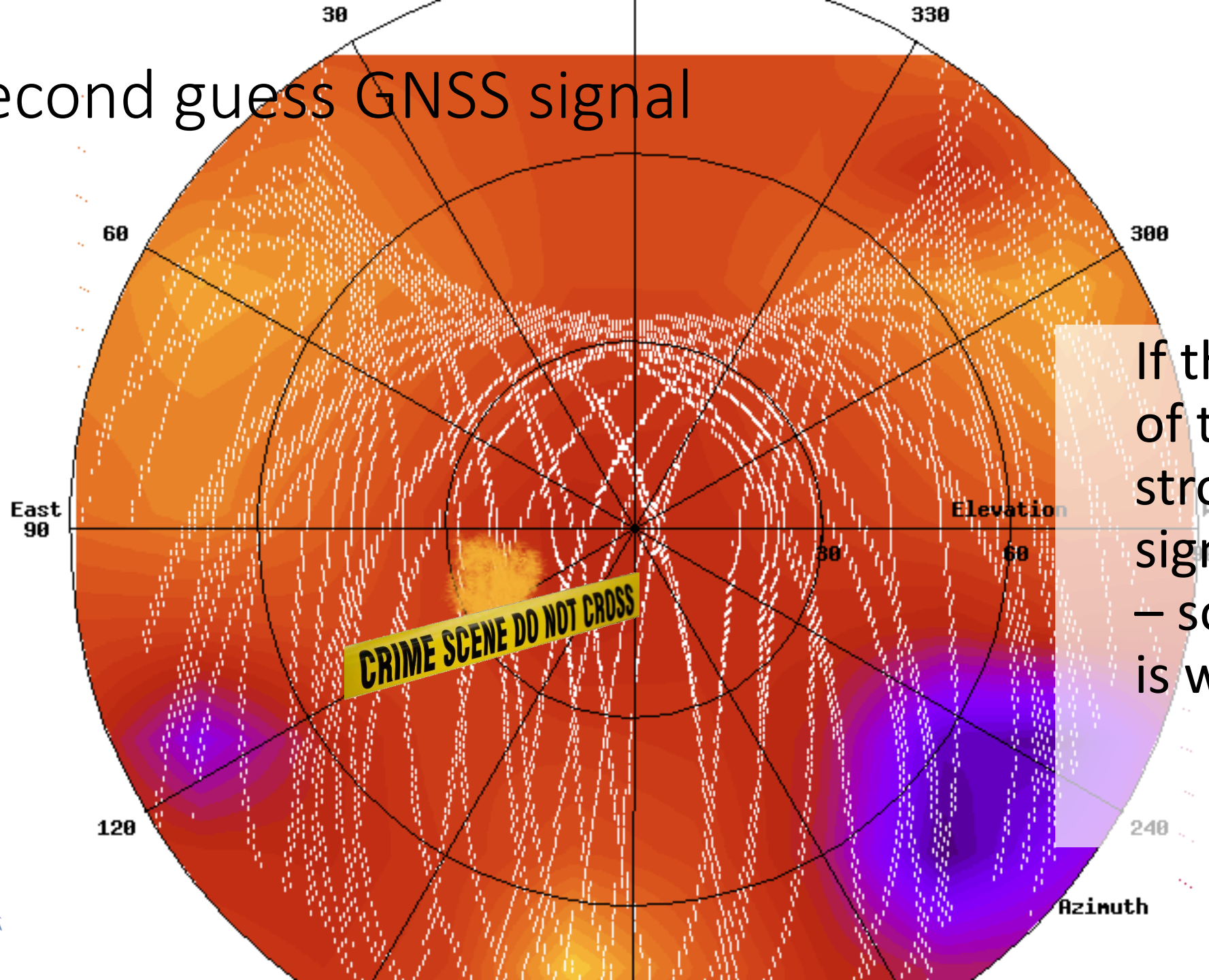
Heatmap of the signal quality permits early alerts for spoofing and jamming – as well as accidental failures.



TimeKeeper Skymap with darker colors for low reception and showing satellite movements.

FSMLabs
Enterprise Real-Time®

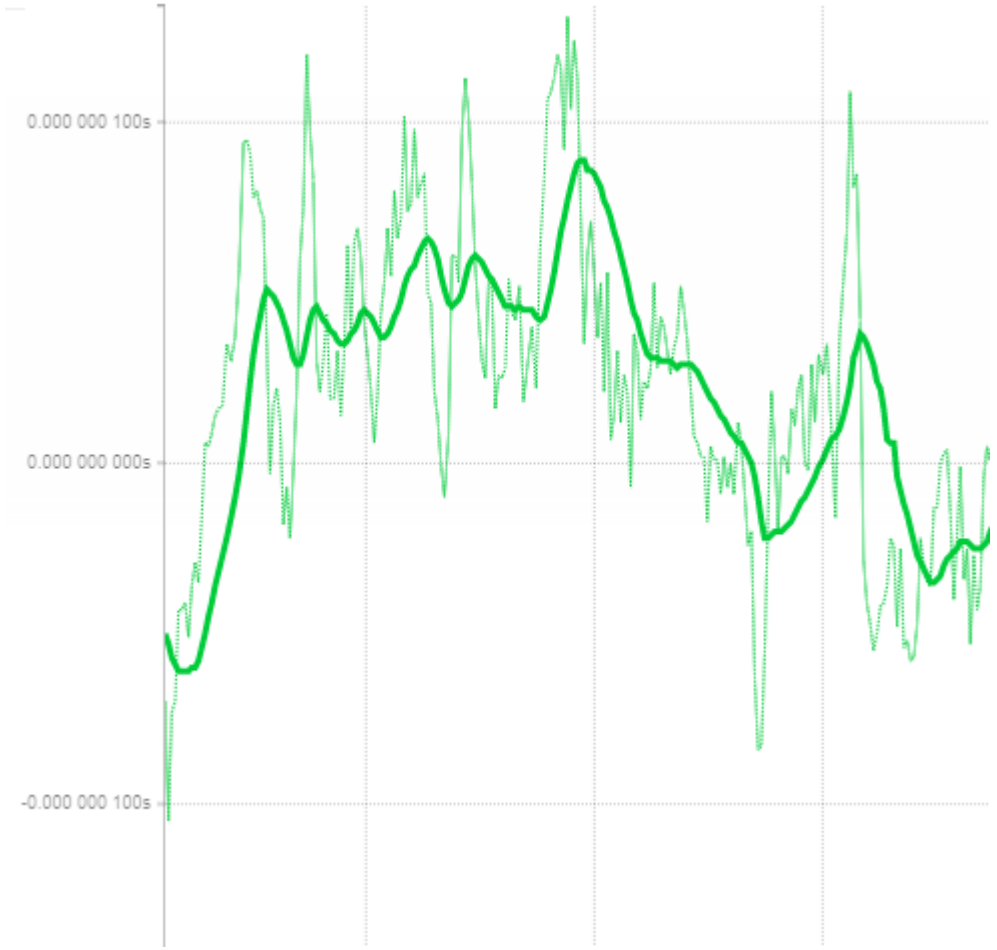
Second guess GNSS signal



If the location of the strongest signals moves – something is wrong.

FSMLabs
Enterprise Real-Time®

Second guess satellite time

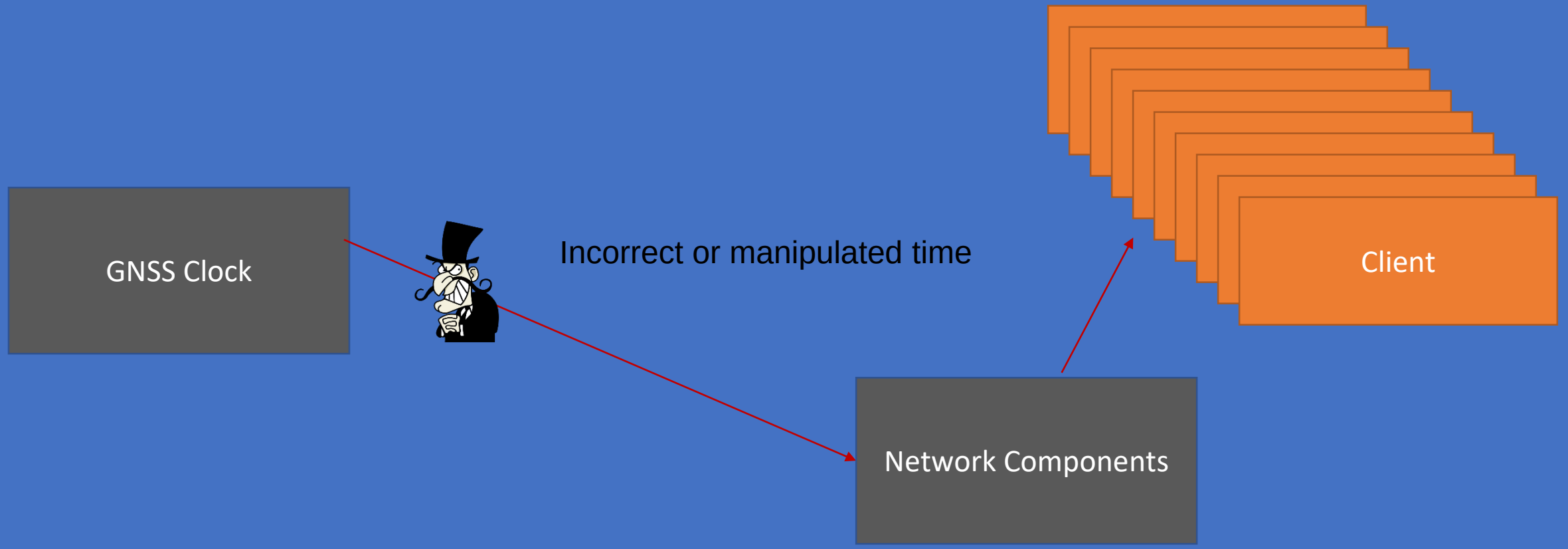


If the frequency changes or offset jumps possible problem (also a good way to catch spurious leap seconds).

To the left: time is as expected within 100ns.

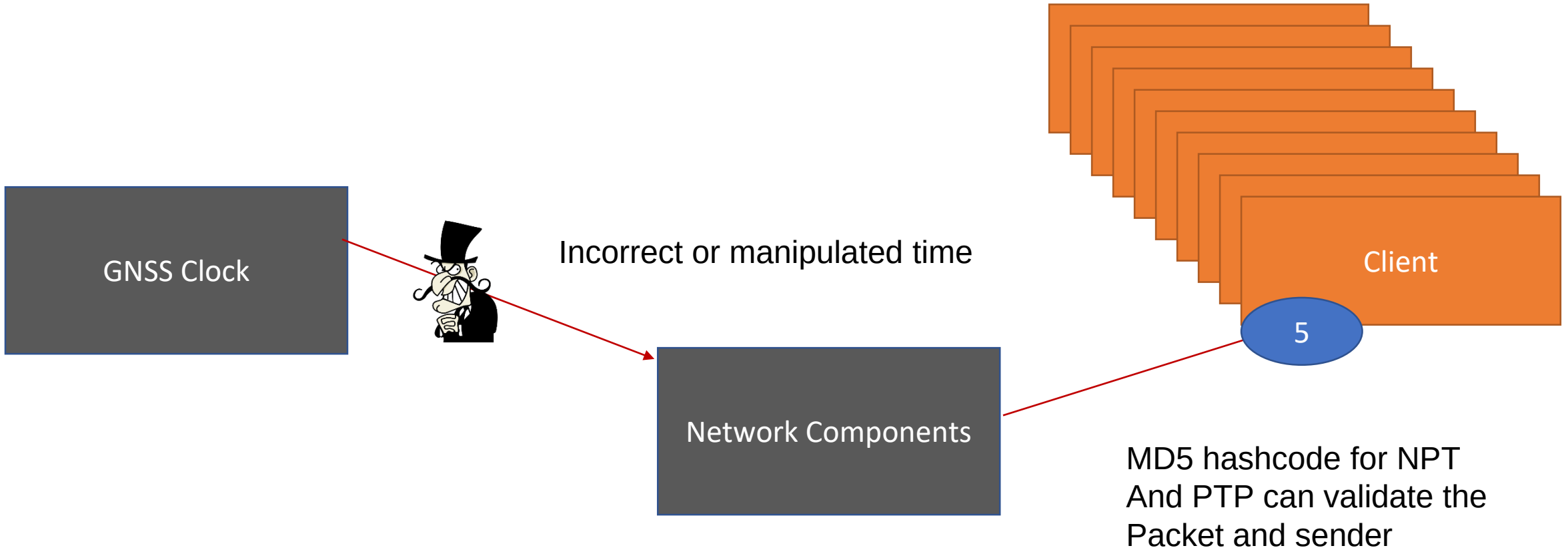
FSMLabs
Enterprise Real-Time®

If time depends on a single source – it is particularly vulnerable.



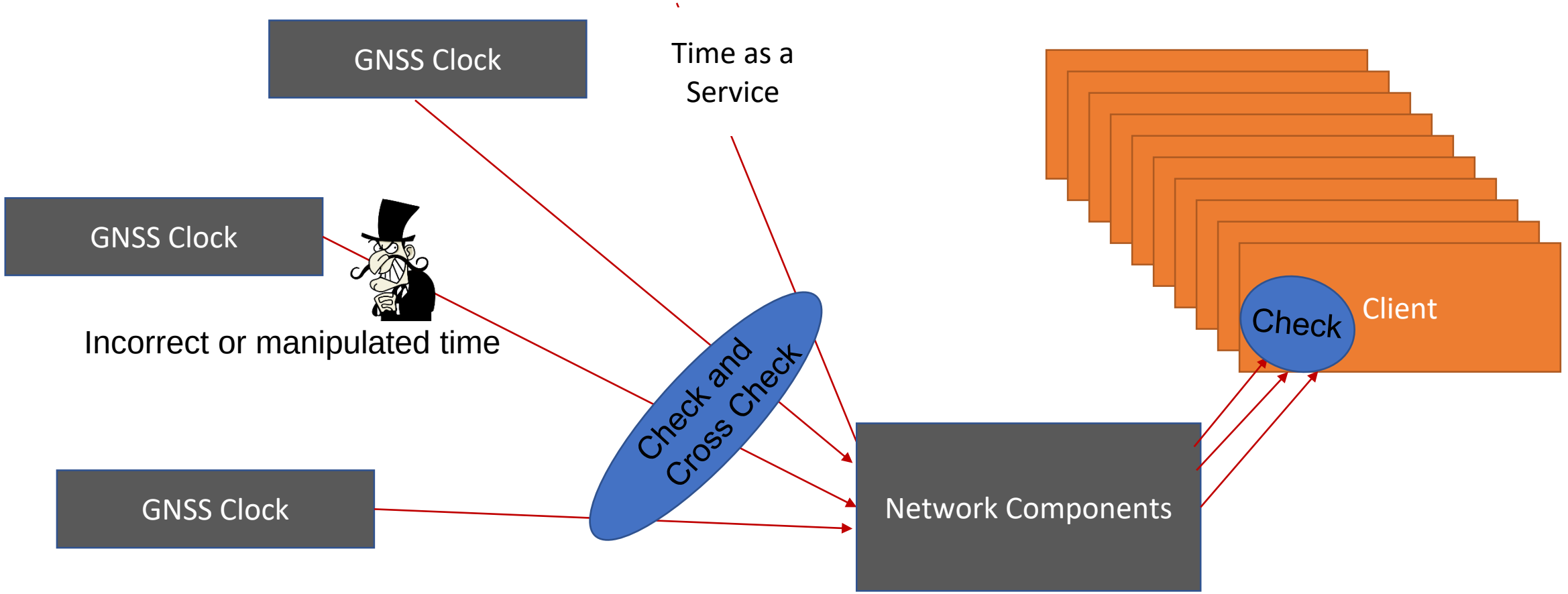
FSMLabs
Enterprise Real-Time

hash-code can validate time source



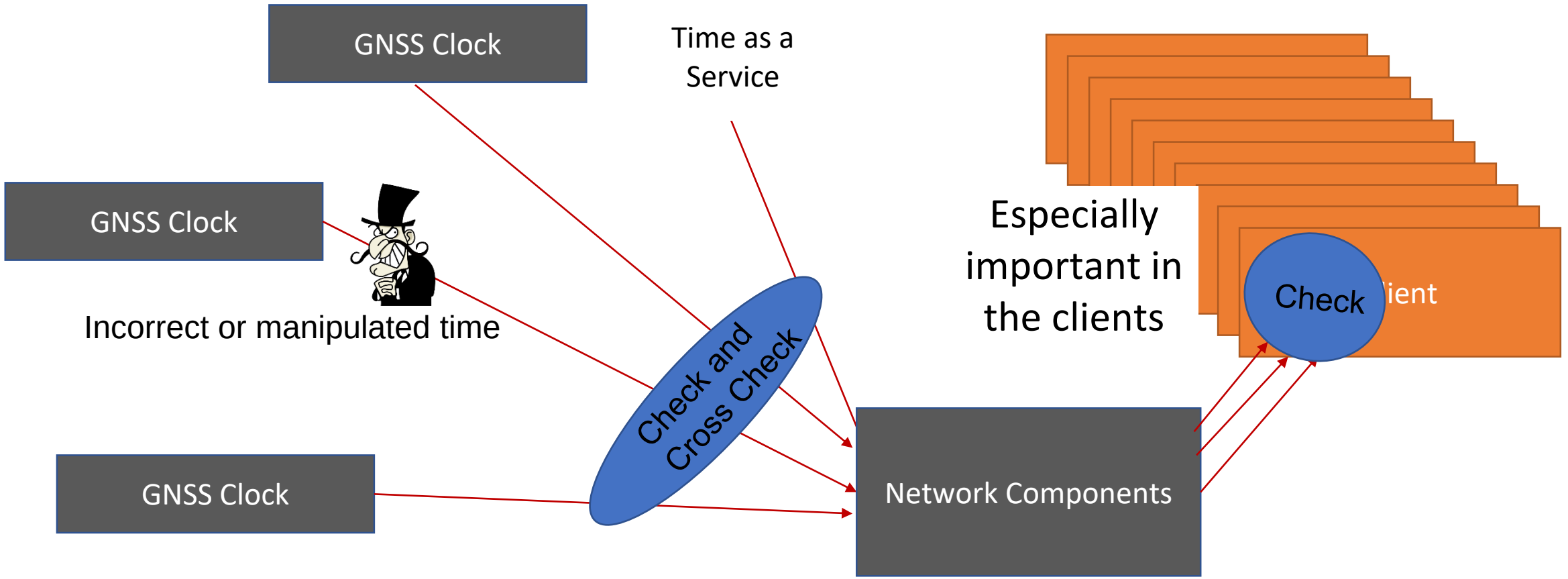
FSMLabs
Enterprise Real-Time®

3&6) Multi-source, multi-protocol analysis is more robust in detecting compromise or failure.



FSMLabs
Enterprise Real-Time®

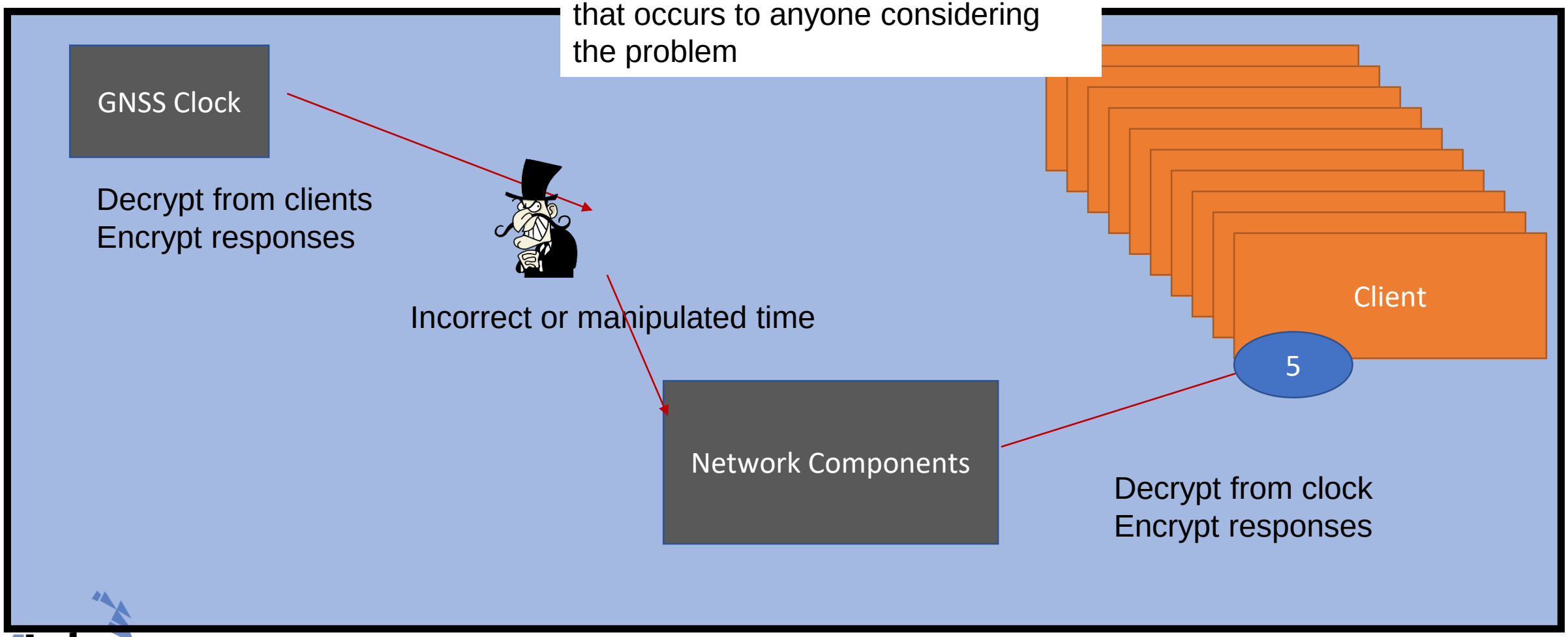
The IEEE PTP 1588 standard has been recently revised to permit this for PTP domains: we can use a mix of PTP, multiple PTP profiles, and NTP



FSMLabs
Enterprise Real-Time®

Full encryption is not a compelling solution

Although it is perhaps the first idea that occurs to anyone considering the problem



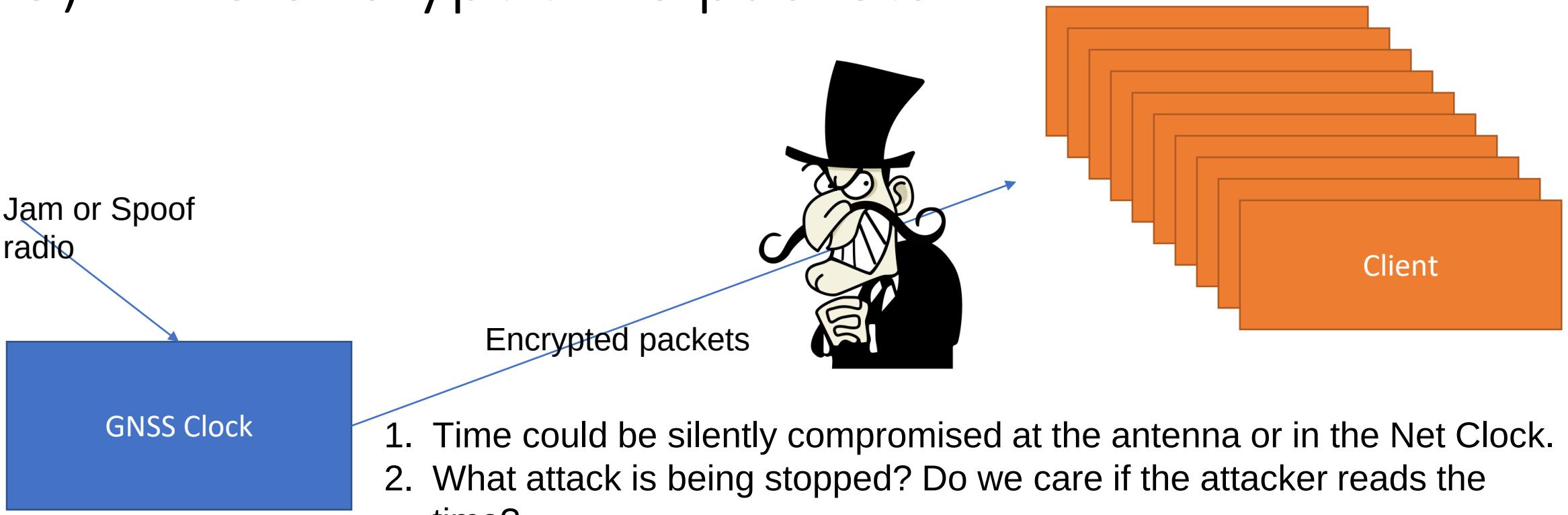
FSMLabs
Enterprise Real-Time®

Engineering analysis

All solutions have a cost and need careful consideration of effectiveness in the particular environment.

FSMLabs
Enterprise Real-Time

5) If we encrypt time packets



1. Time could be silently compromised at the antenna or in the Net Clock.
2. What attack is being stopped? Do we care if the attacker reads the time?
3. How expensive is encrypt/decrypt – does the solution cause failure?
4. Does encryption increase packet size too much?
5. If the attack depends on attacker getting past a firewall – is anything helped by the solution?

Answer: Encrypting time packets is a solution looking for a problem

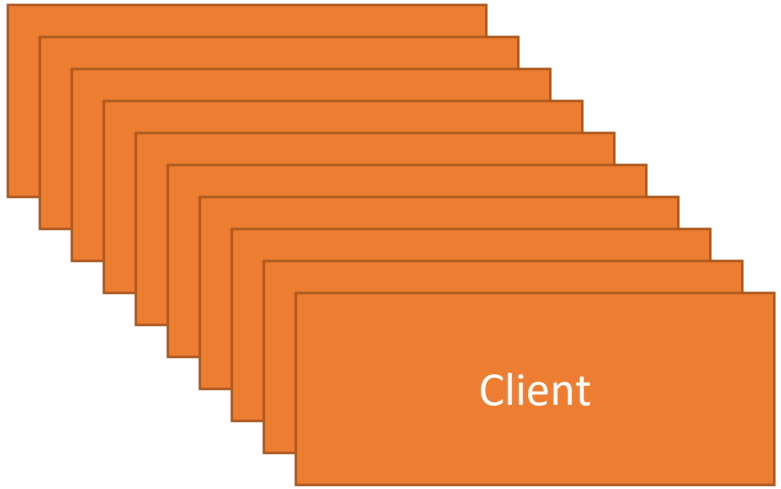
FSMLabs
Enterprise Real-Time®

If we encrypt time packets

Jam or Spoof radio

GNSS Clock

Hash key validated packets



Simplest version uses secret password

1. Simplest method is hashed value $hash(Message, password, [nonce])$
2. NTP already has a couple of standard uses
3. We added the same method to PTP
4. Allows validation that a clock message came from a trusted clock (or client) and that the data has not been tampered with
5. Can be made to be very lightweight

FSMLabs
Enterprise Real-Time®

Bonus method: comprehensive record keeping and aggregation: for forensics

Download yearly audit 'FINRA amazon hosts (report 2)' for 2018-01-01

Synchronization report for 2018-01-01

Report start:	Mon, 01 Jan 2018 00:00:00 GMT (1514764800)
Report end:	Tue, 01 Jan 2019 00:00:00 GMT (1546300800)
Report title:	FINRA amazon hosts (report 2)
Report type:	yearly
Client set:	10.10.2.*
End to end accuracy:	disabled
Min gap length:	180(s)
Warning threshold:	0.000 500 000
Min warning length:	0(s)
Time > warning:	**1.48% client/source time in warning**
Alert threshold:	0.001 000 000
Min alert length:	0(s)
Time > alert:	**1.88% client/source time out of compliance**

FSMLabs
Enterprise Real-Time®

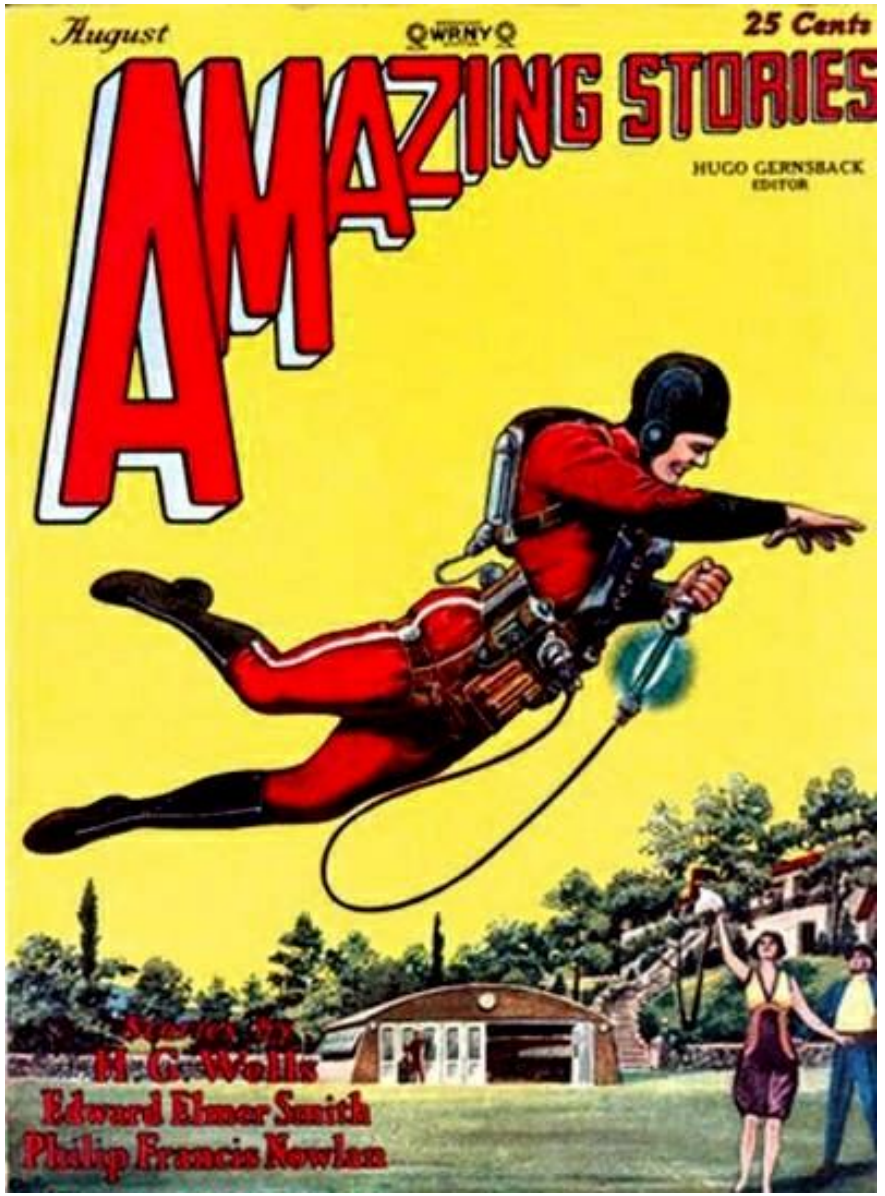
Using Clock sync to protect against cyber-threats - new work.

- Clock sync data can expose “man-in-the-middle” attacks by showing changes in one-way and RTT.
- Additional data collected with clock sync logs like temperature and system load provide early warnings.
- With tightly synchronized time: challenge/response can be qualified by response time.

FSMLabs
Enterprise Real-Time®

Future

- More dynamic cross check between different methods: multi-source+ sky map.
- Smarter analysis of clock sync logs and related information to deduce system problems and security issues.



FSMLabs
Enterprise Real-Time®

Contact info

FSMLabs, Inc.
11701 Bee Caves Road, Suite 200
Austin, TX 78738
USA
info@fsmlabs.com

Telephone: 1-512-263-5530

- TimeKeeper Client Software
- TimeKeeper Server Software
- TimeKeeper Compliance Software
- TimeKeeper GrandMaster Gen 2

FSMLabs
Enterprise Real-Time®