Securing Time Delivery in Enterprise and Financial Networks

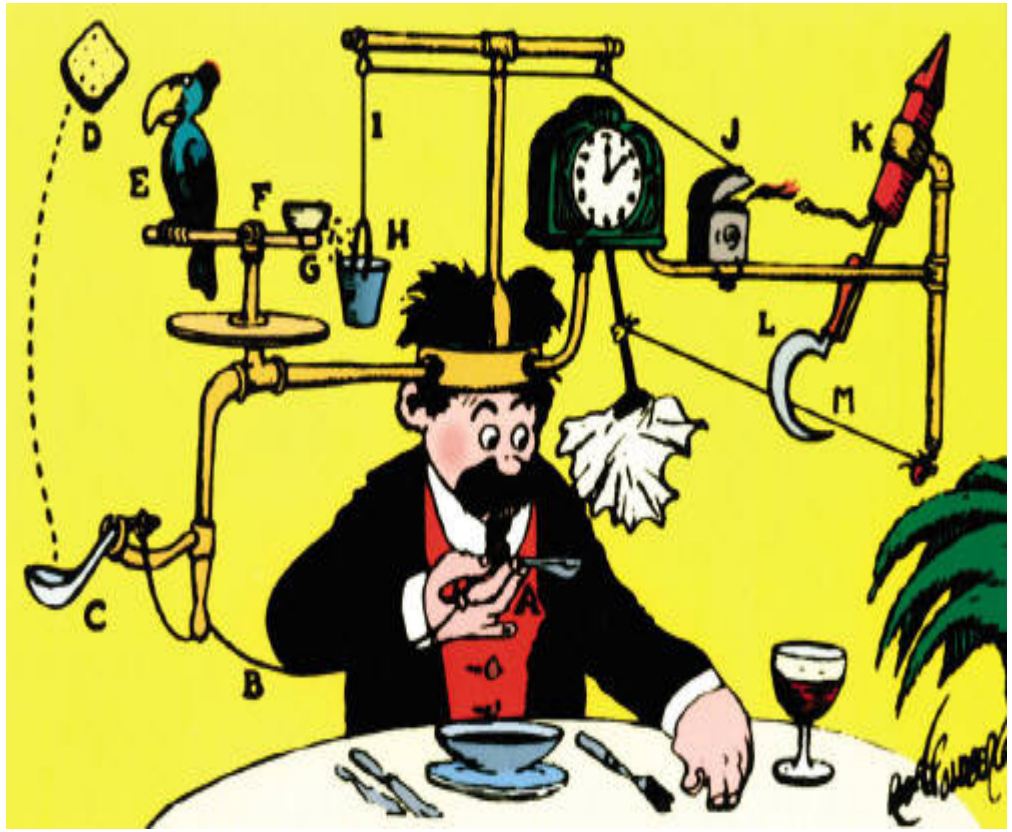
FSMLabs Inc.

TimeKeeper.

www.fsmlabs.com

Number of techniques in practice and proposals for secure clock distribution

- Existing NTP “authentication” standards
- IETF RFC 7384 Time Protocol Security Requirements October 2014
- Annex K of IEEE 1588
- Multiple new standards proposals for encryption of IEEE 1588
- Even time over TLS or IPSec!



Security is easy to get wrong.

Without a threat assessment, it is easy to construct "security" mechanisms that do not offer any actual protection.

Encrypting time protocol packets does what?

- Is time secret? (it could be)
- Is encrypted time safer? (Simply delaying PTP/NTP messages is a compromise)
- Do encrypted time packets introduce failures? (For examples if it takes multiple packets to encode a time update, losing any one breaks the update)
- Does encryption introduce too much compute overhead? (depends)
- Does encryption break anything? (e.g. transparent clocks)

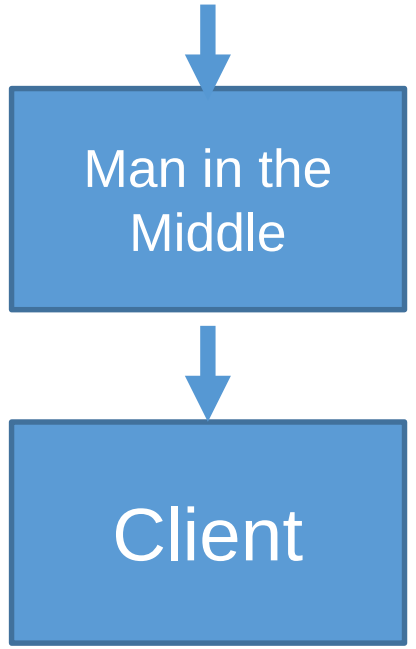
Distinction between “internal” and “external”

- In enterprise computing, core networking is within a “secure network”.
- External networking goes out e.g. over the internet.

Two very different threat models.

Man in the middle

- Man in the middle attackers can always compromise time by delaying packets
- A successful man-in-the-middle attack on an internal network is a major compromise that may make secure time delivery irrelevant.
- Time over an external network cannot be protected from man-in-the-middle attacks.



Authentication – if done efficiently makes fake time sources and denial of service harder

- This is specified in NTP authentication standards
- PTP currently has no efficient standard and PTP multicast and transparent clock are problems.

Complex features of clock sync software have already **caused** security problems.

NTP : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

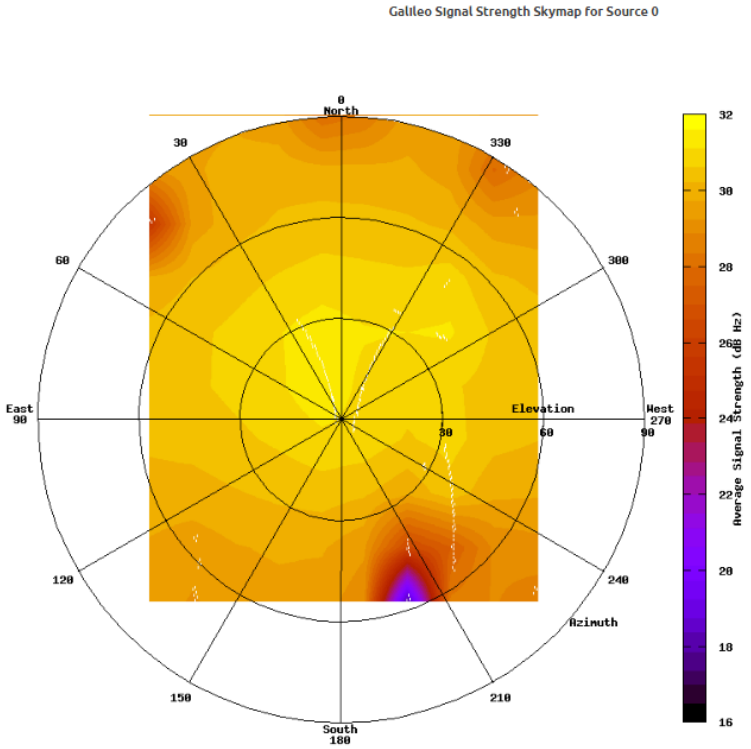
Copy Results Download Results

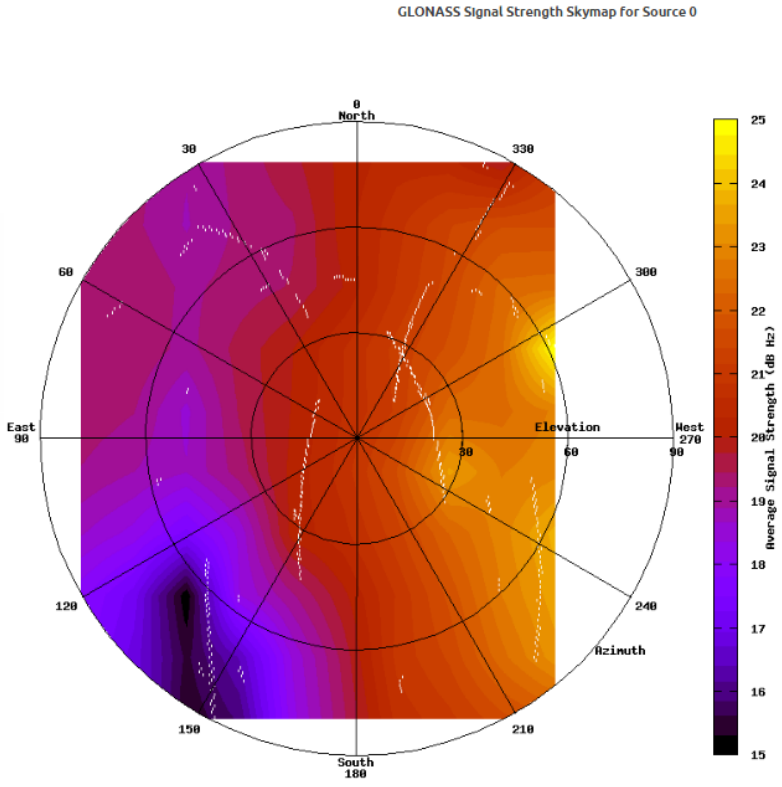
#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2016-9312	399		DoS	2017-01-13	2017-02-10	5.0	None	Remote	Low	Not required	None	None	Partial
ntpd in NTP before 4.2.8p9, when running on Windows, allows remote attackers to cause a denial of service via a large UDP packet.														
2	CVE-2016-9311	476		DoS	2017-01-13	2017-02-10	7.1	None	Remote	Medium	Not required	None	None	Complete
ntpd in NTP before 4.2.8p9, when the trap service is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted packet.														
3	CVE-2016-9310	400			2017-01-13	2017-02-10	6.4	None	Remote	Low	Not required	Partial	None	Partial
The control mode (mode 6) functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to set or unset traps via a crafted control mode packet.														
4	CVE-2016-7434	20		DoS	2017-01-13	2017-02-10	5.0	None	Remote	Low	Not required	None	None	Partial
The read_mru_list function in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (crash) via a crafted mrulist query.														
5	CVE-2016-7433	682			2017-01-13	2017-02-10	5.0	None	Remote	Low	Not required	None	None	Partial
NTP before 4.2.8p9 does not properly perform the initial sync calculations, which allows remote attackers to unspecified impact via unknown vectors, related to a "root distance that did not include the peer dispersion."														
6	CVE-2016-7431	20		Bypass	2017-01-13	2017-02-10	5.0	None	Remote	Low	Not required	None	Partial	None
NTP before 4.2.8p9 allows remote attackers to bypass the origin timestamp protection mechanism via an origin timestamp of zero. NOTE: this vulnerability exists because of a CVE-2015-8138 regression.														

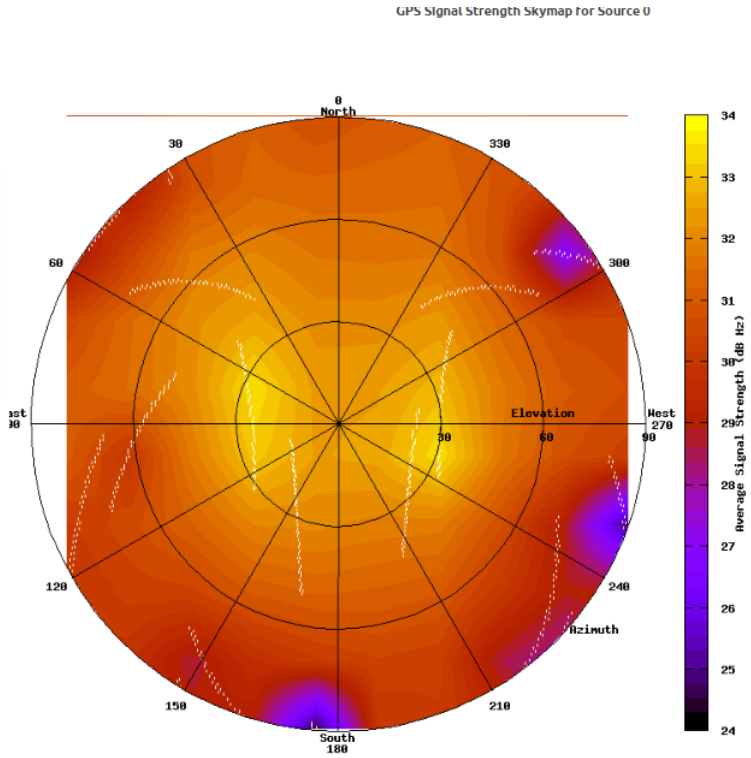
More practical solutions involve using nature of time distribution to cross check

- Security for time distribution does not (usually) involve keeping time secret
- Security should be focused on detecting and reacting to compromise of time sources
- There is always an overlap between security and fault-tolerance – but this is especially marked in time delivery.
- Goal should be to secure time delivery and to leave general security issues to standard techniques.
- Time is (sort of) physical so we can use “measurement” to secure.

Multi-constellation cross check for GNSS



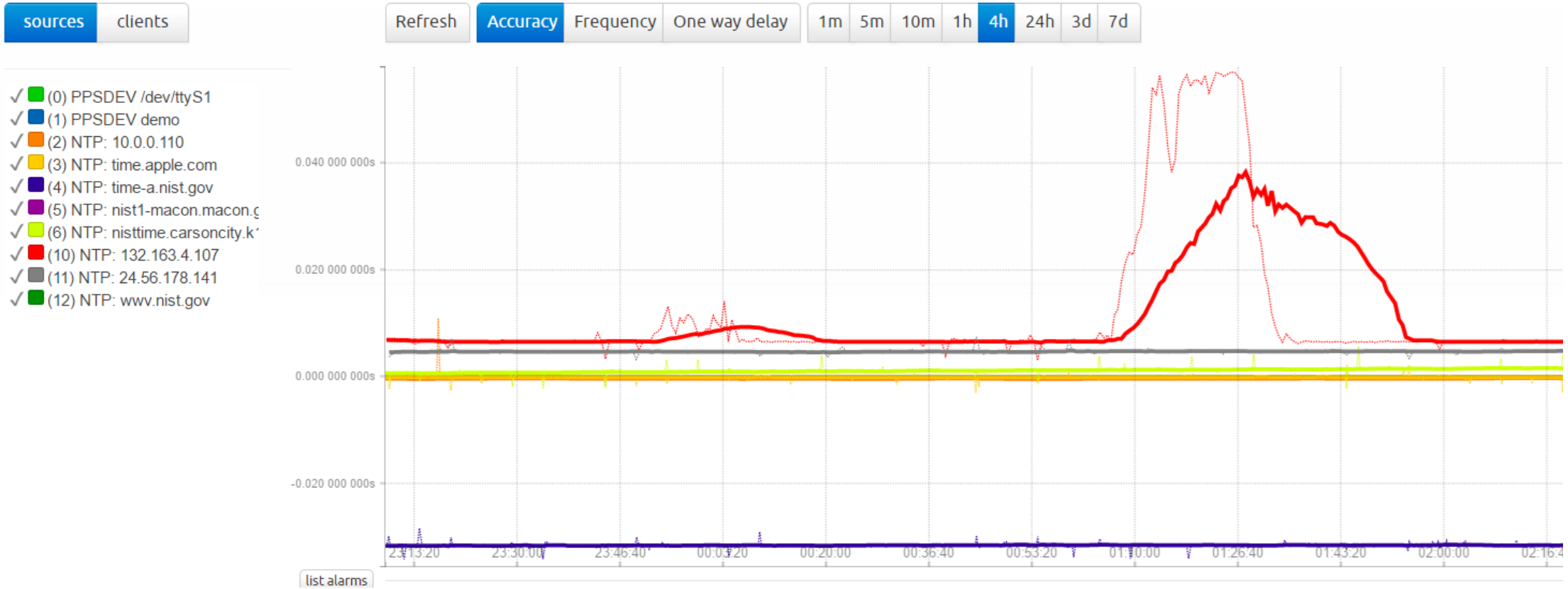




Spoofing one GNSS source is much easier than spoofing two or three

Multiple constellations are already accessible from commercial low cost GPS receivers. Combining multiple constellations with multiple sources produces a robust time channel.

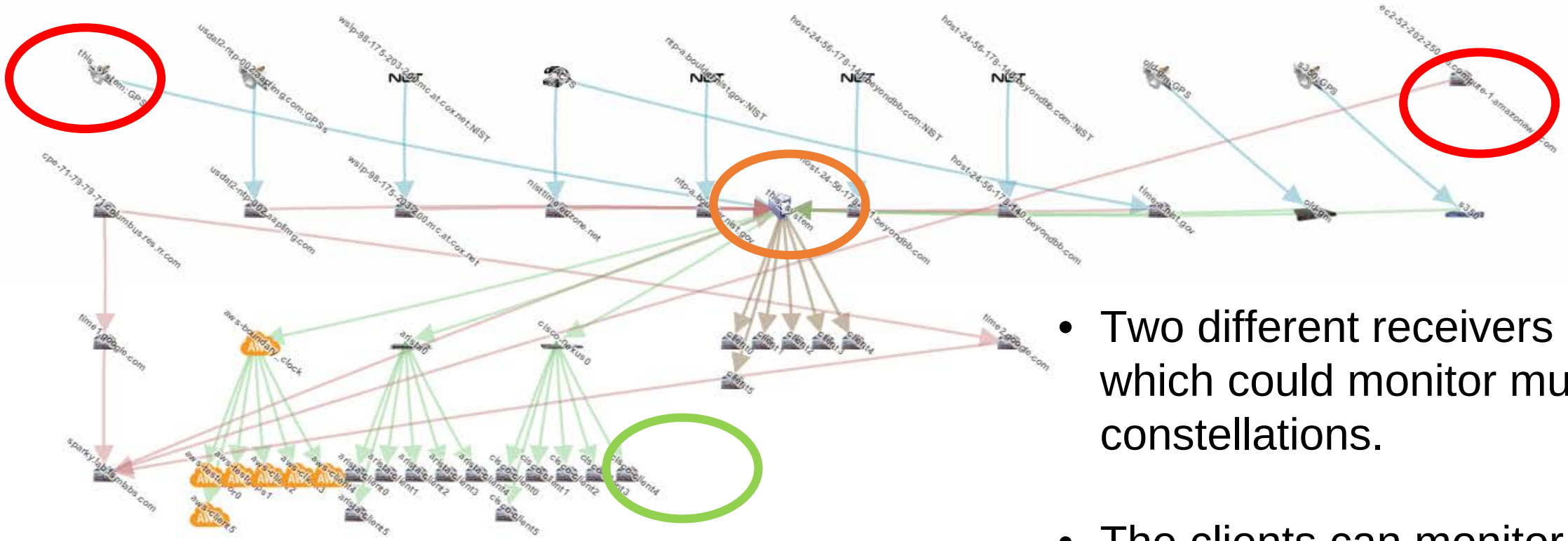
Security from multiple sources available over network.



Same techniques introduced to provide fault-tolerance and fail-over increase security

- Mix of multiple network reference clock sources
  - NTP
  - PTP IEEE 1588 multicast
  - PTP IEEE 1588 unicast (telco)
- Live cross check for sanity allows detection of compromise

Defense in depth



- Two different receivers each of which could monitor multiple constellations.
- The clients can monitor multiple GMs

IEEE 1588 Best Master Clock is a security problem

- The standard requires client (slave) devices to accept the accuracy advertised by a GM as accurate
- One rogue (or faulty) GM can take down a time network

- Solution is to use multiple domains and additional non PTP reference time sources.

Conclusion

- Securing time delivery is not a traditional security problem
  - Encryption may not address the key issues
  - Data does not necessarily need to be kept secret over the wire
  - Real-time is key (slowing down time delivery packets is an attack interface)
- Defense in depth is best practice in security and time delivery is well suited to this approach.
- Don’t reinvent standard security methods (like TLS)
- Don’t introduce security holes with complex methods

Contact info

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

Telephone: 1-512-263-5530