PTP Vulnerabilities in Light of MiFID II

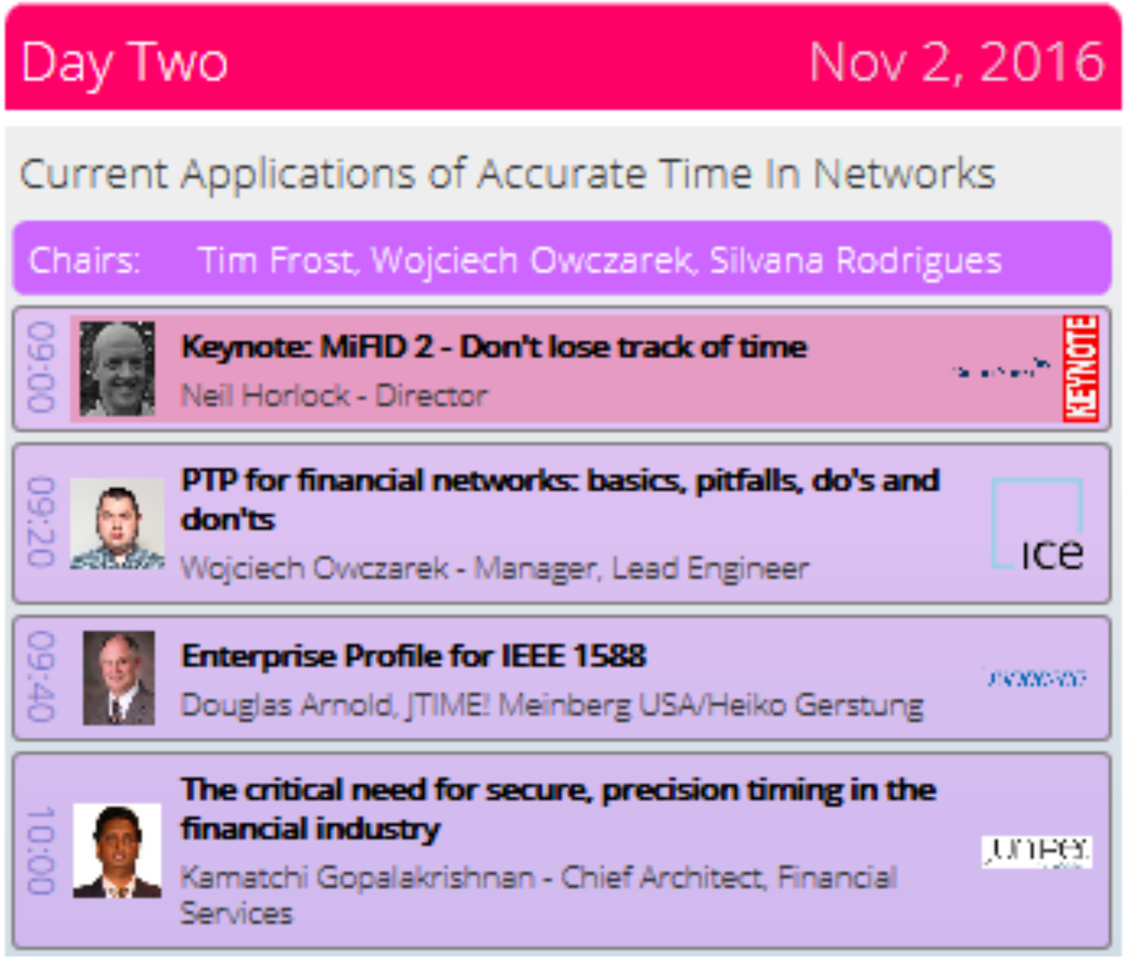
Michael Schukat / Joe Desbonnet

November 2nd 2016

Presentation Outline

- MiFID 2 time sync requirements vs PTP
- Byzantine faults and multi-source time synchronisation solutions
- How about Advanced Persistent Threads (APT)?
- Case study: APT resilience of a multi-source time synchronisation solution
- Alternative solutions to increase APT resilience of time synchronisation networks

MiFID 2 @ ITSF 2016



Day Two Nov 2, 2016

Current Applications of Accurate Time In Networks

Chairs: Tim Frost, Wojciech Owczarek, Silvana Rodrigues

09:00 **Keynote: MiFID 2 - Don't lose track of time**
Neil Horlock - Director
KEYNOTE

09:20 **PTP for financial networks: basics, pitfalls, do's and don'ts**
Wojciech Owczarek - Manager, Lead Engineer
ice

09:40 **Enterprise Profile for IEEE 1588**
Douglas Arnold, JTIME! Meinberg USA/Heiko Gerstung

10:00 **The critical need for secure, precision timing in the financial industry**
Kamatchi Gopalakrishnan - Chief Architect, Financial Services

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

EUROPEAN REGIONAL DEVELOPMENT FUND

ENTERPRISE IRELAND

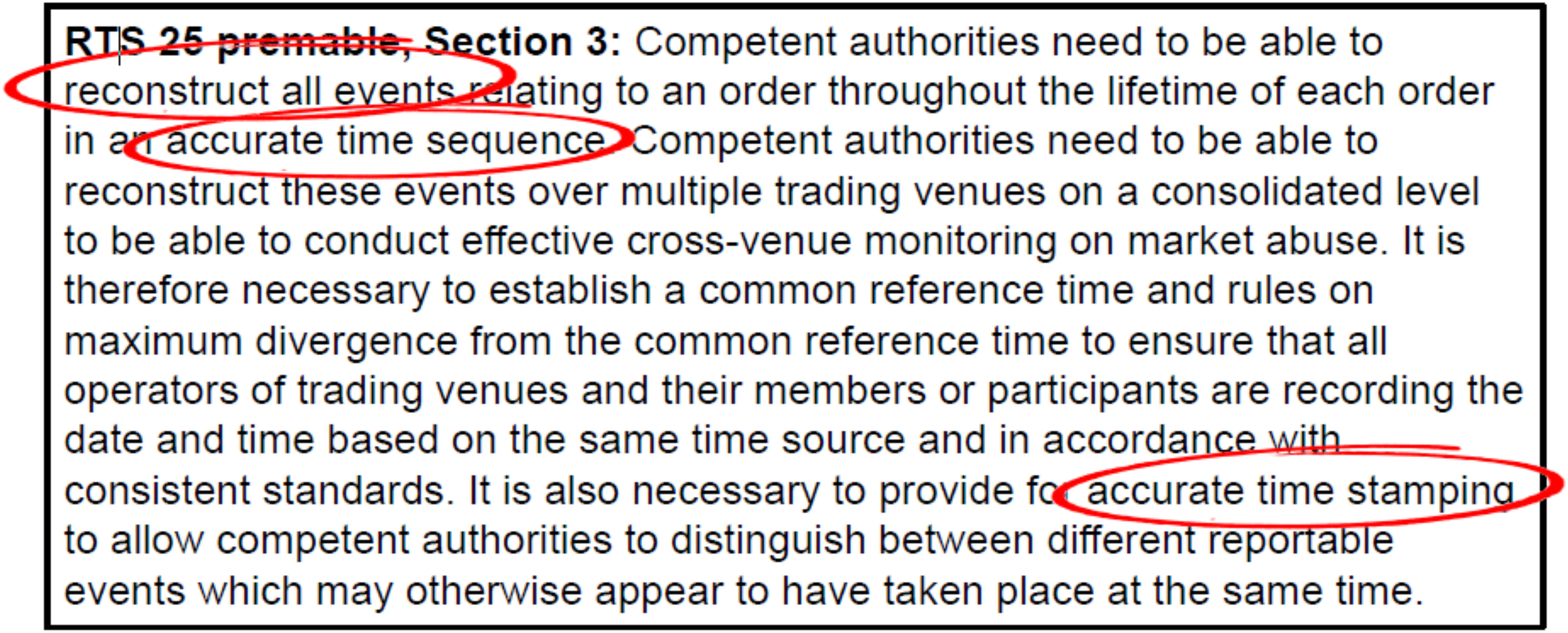
NUI Galway
OÉ Gaillimh

European Securities and Markets Authority (ESMA) Guidelines

- Operators of trading venues and their members or participants shall **establish a system of traceability of their business clocks to UTC. This includes ensuring that their systems operate within the granularity and a maximum tolerated divergence from UTC as per RTS 25.** Operators of trading venues and their members or participants **shall be able to evidence that their systems meet the requirements**. They shall be able to do so by documenting the system design, it's functioning and specifications. Furthermore operators of trading venues and their members or participants shall evidence that the crucial system components used meet the accuracy standard levels on granularity and maximum divergence of UTC as guaranteed and specified by the manufacturer of such system components (component specifications shall meet the required accuracy levels) and that these system components are installed in compliance with the manufacturer's installation guidelines.

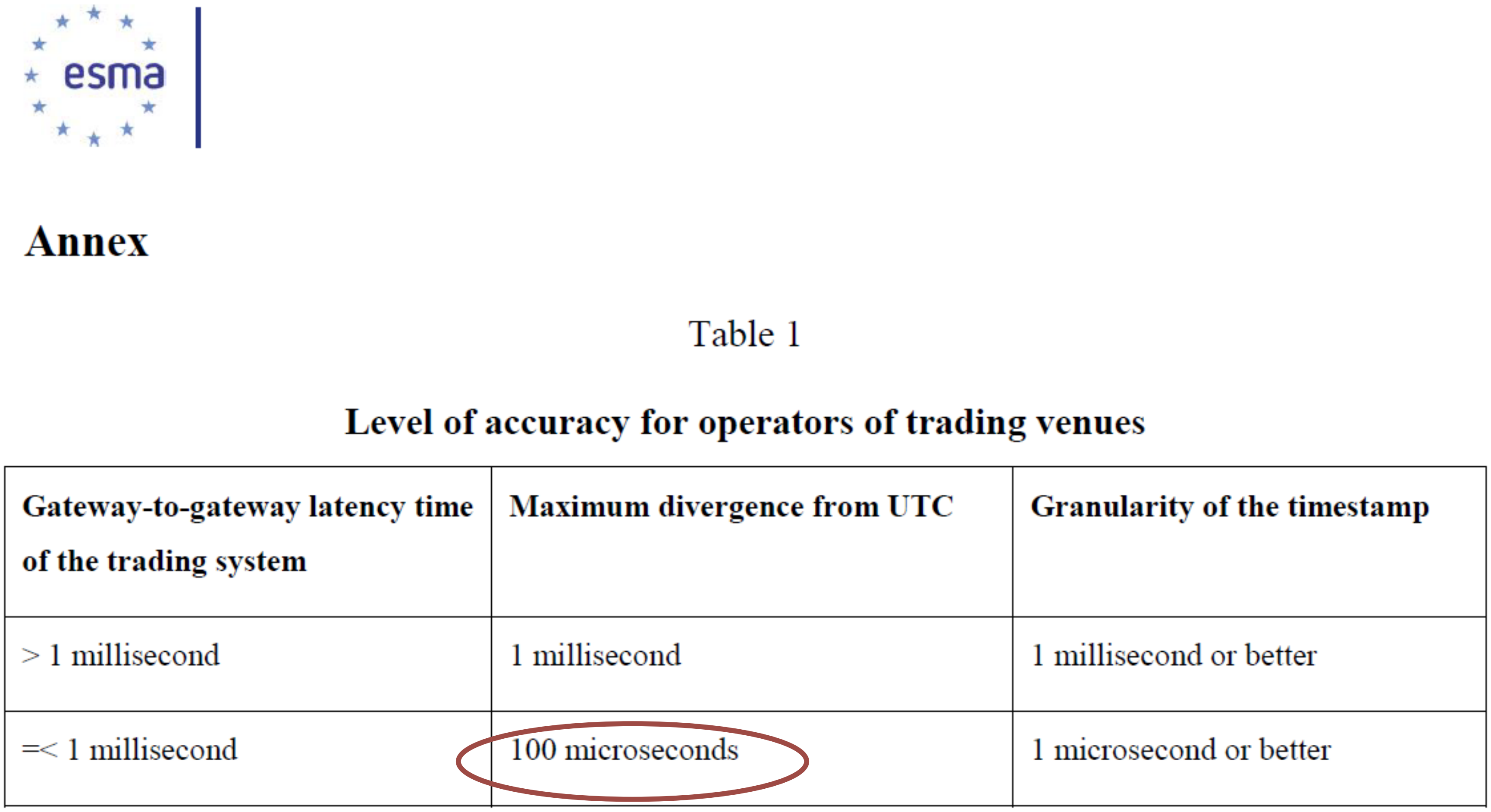
What ESMA cares about

- Accuracy of time stamps!



RTS ~~25 premable,~~ Section 3: Competent authorities need to be able to reconstruct all events relating to an order throughout the lifetime of each order in an accurate time sequence. Competent authorities need to be able to reconstruct these events over multiple trading venues on a consolidated level to be able to conduct effective cross-venue monitoring on market abuse. It is therefore necessary to establish a common reference time and rules on maximum divergence from the common reference time to ensure that all operators of trading venues and their members or participants are recording the date and time based on the same time source and in accordance with consistent standards. It is also necessary to provide for accurate time stamping to allow competent authorities to distinguish between different reportable events which may otherwise appear to have taken place at the same time.

Extract from MiFID II / MiFIR RTS 25



esma

Annex

Table 1

Level of accuracy for operators of trading venues

Gateway-to-gateway latency time of the trading system	**Maximum divergence from UTC**	**Granularity of the timestamp**
> 1 millisecond	1 millisecond	1 millisecond or better
=< 1 millisecond	100 microseconds	1 microsecond or better

100 Microsecond Accuracy!

- No problem with carefully designed and tightly managed NTP / PTP deployments!
- However…

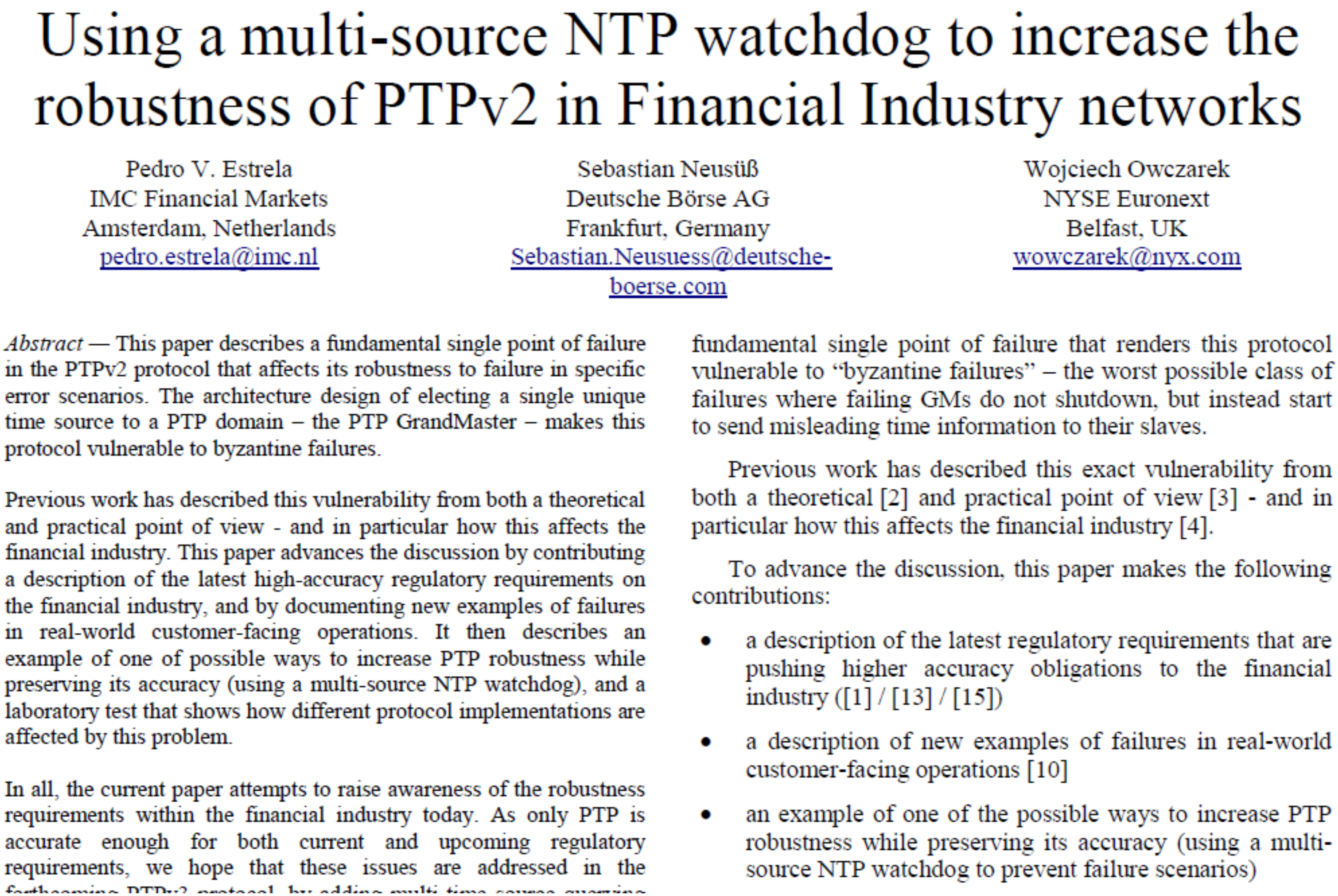
Single source IEEE PTP 1588 cannot meet financial regulatory standards

Victor Yodaiken, 3/30/2016

A 2014 technical paper [IND[i]] written by lead engineers at IMC, NYSE, and Deutsche-Boerse investigates one of the design flaws in IEEE 1588 PTP that makes systems relying on it vulnerable to catastrophic timing errors in ways that would violate financial trading regulatory requirements such as those in MiFID II and CAT[1]. The key point made by the authors is that:

> **the root cause lies in the PTPv2 standard itself: the standard is vulnerable to byzantine failures, so it affects any PTPv2 implementation in which clients trust a single time source**

IND suggests developing solutions that are somewhat similar to the solutions found in TimeKeeper[2], but solutions aside, the paper indicates increasing awareness of "robustness issues" among technically sophisticated financial market firms that had previously relied on the PTP standard.



Using a multi-source NTP watchdog to increase the robustness of PTPv2 in Financial Industry networks

Pedro V. Estrela
IMC Financial Markets
Amsterdam, Netherlands
pedro.estrela@imc.nl

Sebastian Neusüß
Deutsche Börse AG
Frankfurt, Germany
Sebastian.Neusuess@deutsche-boerse.com

Wojciech Owczarek
NYSE Euronext
Belfast, UK
wowczarek@nyx.com

Abstract — This paper describes a fundamental single point of failure in the PTPv2 protocol that affects its robustness to failure in specific error scenarios. The architecture design of electing a single unique time source to a PTP domain – the PTP GrandMaster – makes this protocol vulnerable to byzantine failures.

Previous work has described this vulnerability from both a theoretical and practical point of view - and in particular how this affects the financial industry. This paper advances the discussion by contributing a description of the latest high-accuracy regulatory requirements on the financial industry, and by documenting new examples of failures in real-world customer-facing operations. It then describes an example of one of possible ways to increase PTP robustness while preserving its accuracy (using a multi-source NTP watchdog), and a laboratory test that shows how different protocol implementations are affected by this problem.

In all, the current paper attempts to raise awareness of the robustness requirements within the financial industry today. As only PTP is accurate enough for both current and upcoming regulatory requirements, we hope that these issues are addressed in the forthcoming PTPv3 protocol, by adding multi time source querying

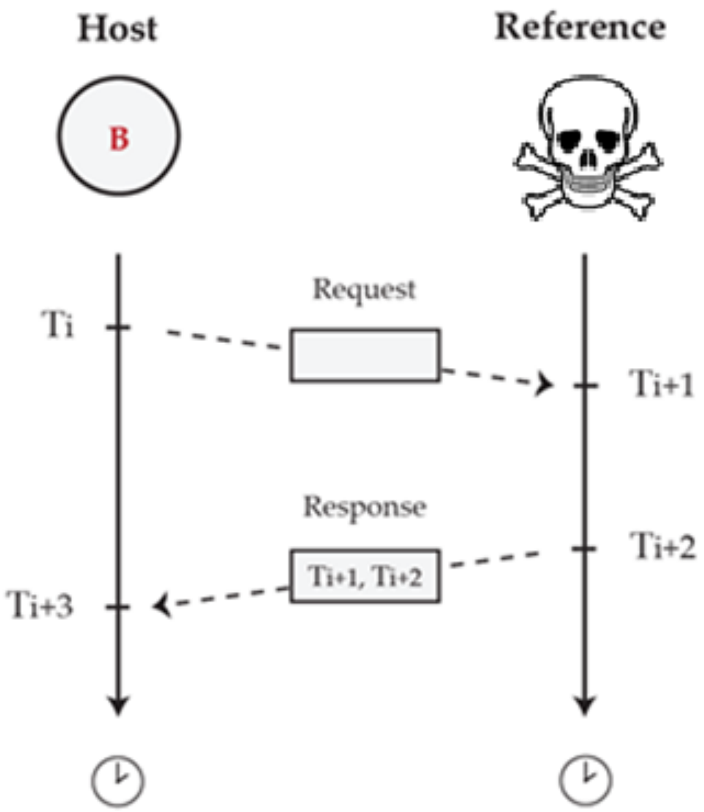
fundamental single point of failure that renders this protocol vulnerable to "byzantine failures" – the worst possible class of failures where failing GMs do not shutdown, but instead start to send misleading time information to their slaves.

Previous work has described this exact vulnerability from both a theoretical [2] and practical point of view [3] - and in particular how this affects the financial industry [4].

To advance the discussion, this paper makes the following contributions:

- a description of the latest regulatory requirements that are pushing higher accuracy obligations to the financial industry ([1] / [13] / [15])
- a description of new examples of failures in real-world customer-facing operations [10]
- an example of one of the possible ways to increase PTP robustness while preserving its accuracy (using a multi-source NTP watchdog to prevent failure scenarios)

Problem: Erroneous Time Reference

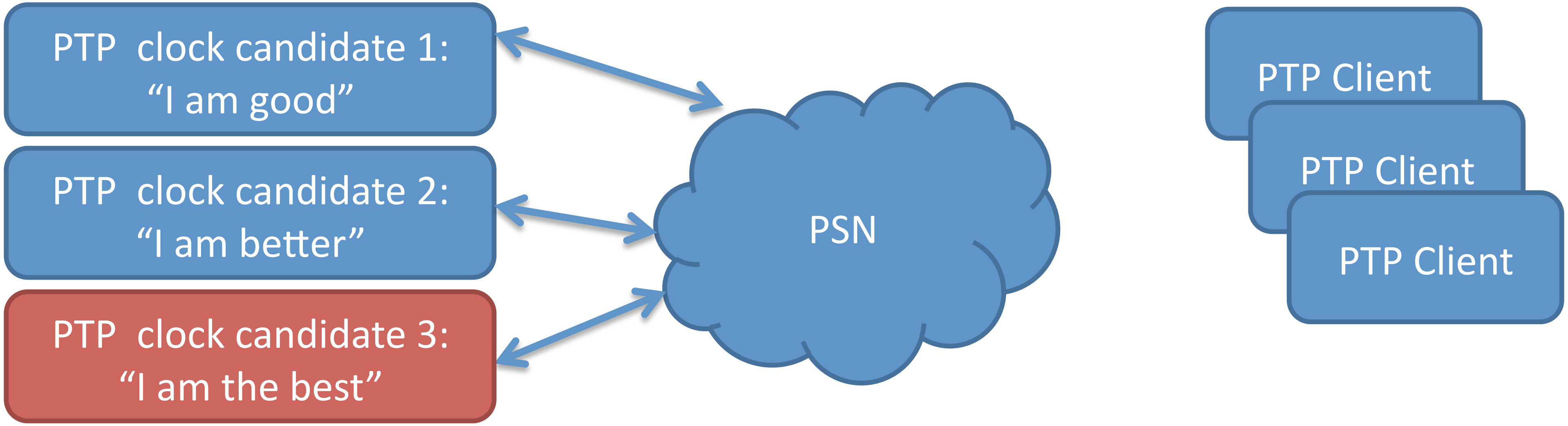


- Time synchronisation is only as good as the time reference!
- A spoofed or manipulated reference will provide incorrect time to all hosts it is connected to
  - E.g. time feeds that are compromised but are advertised as accurate

OSNA OPEN SENSOR NETWORK AUTHENTICATION
EUROPEAN REGIONAL DEVELOPMENT FUND
ENTERPRISE IRELAND
NUI Galway OÉ Gaillimh

Byzantine Fault Scenario I

- Phase 1: BMCA selection process



PTP clock candidate 1: "I am good"

PTP clock candidate 2: "I am better"

PTP clock candidate 3: "I am the best"

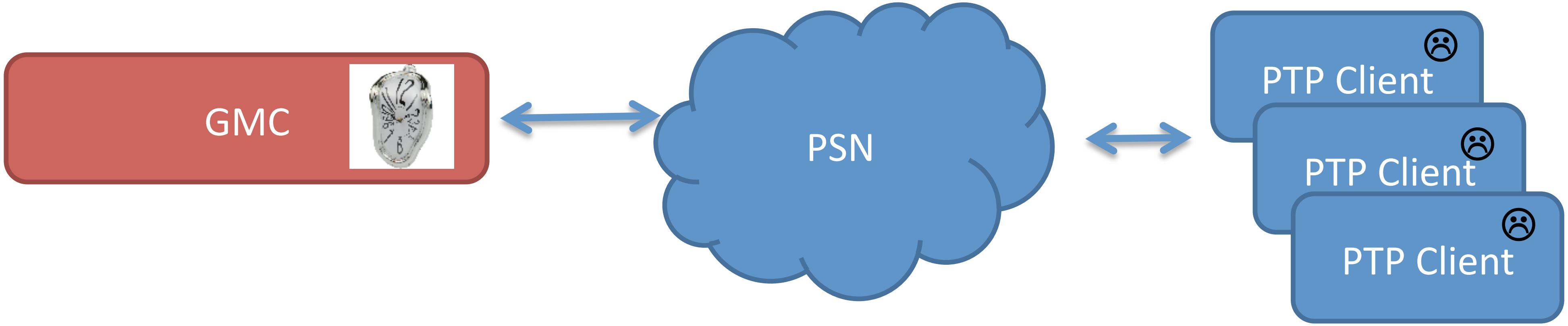
PSN

PTP Client

PTP Client

PTP Client

- Phase 2: Grandmaster clock acts up funny



GMC

PSN

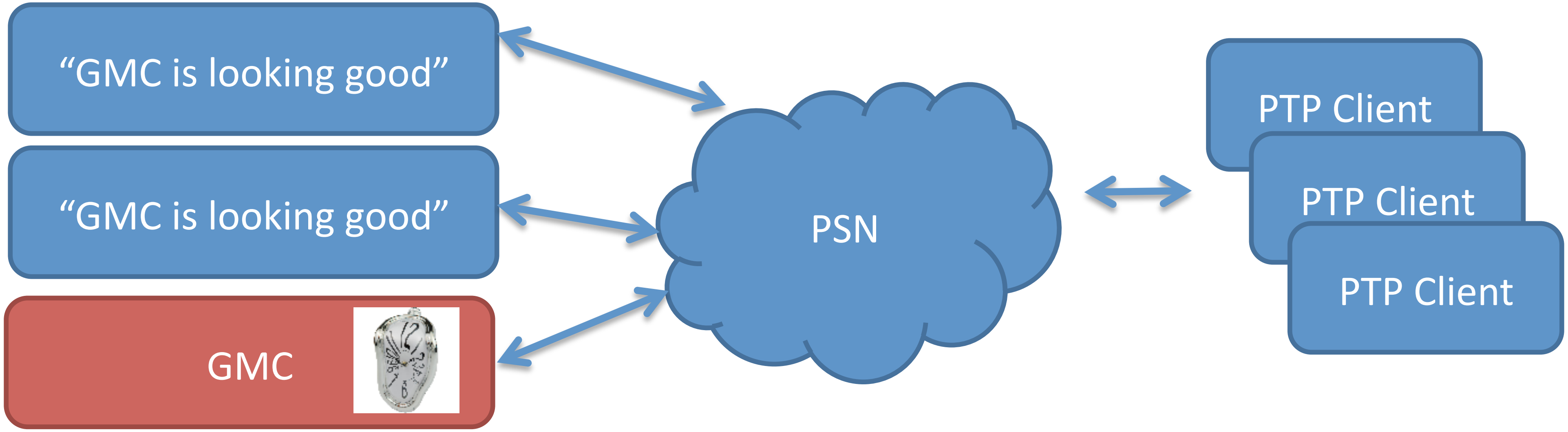
PTP Client ☹

PTP Client ☹

PTP Client ☹

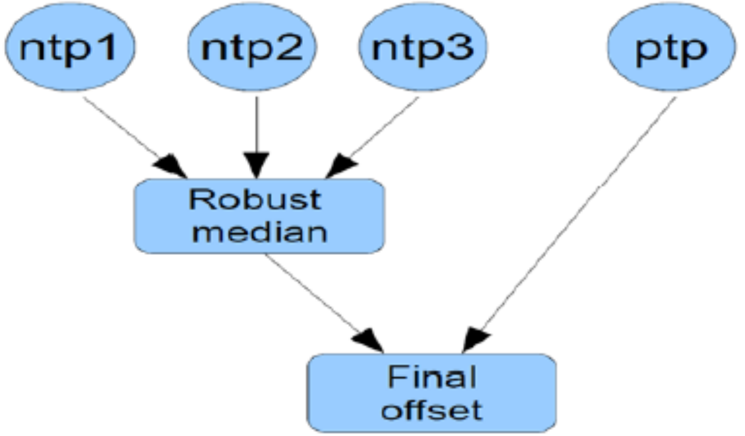
Byzantine Fault Scenario II

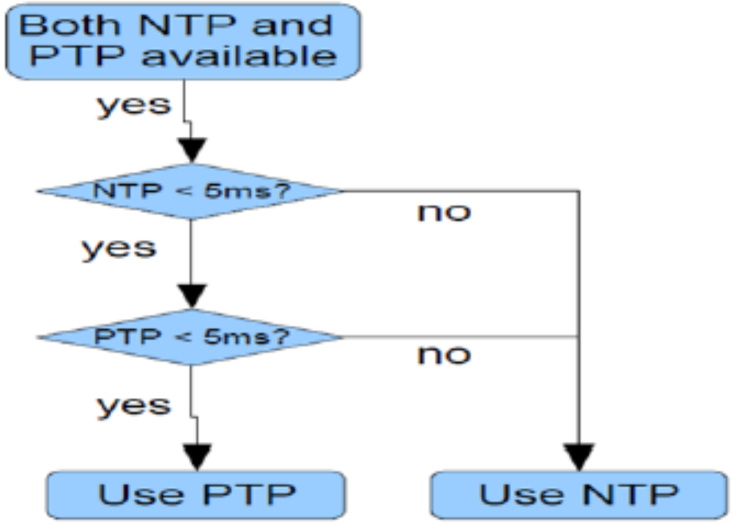
- Also: As the active GMC continued to send “Announce” packets as normal, with the same BMC parameters (in particular priority, clock class and variance), the inactive GMs had no reason to take over!!



Solution: Multi-Source Time Synchronisation I

- Multi-Source Watchdog (Estrela et al, 2014)





OPEN SENSOR NETWORK AUTHENTICATION

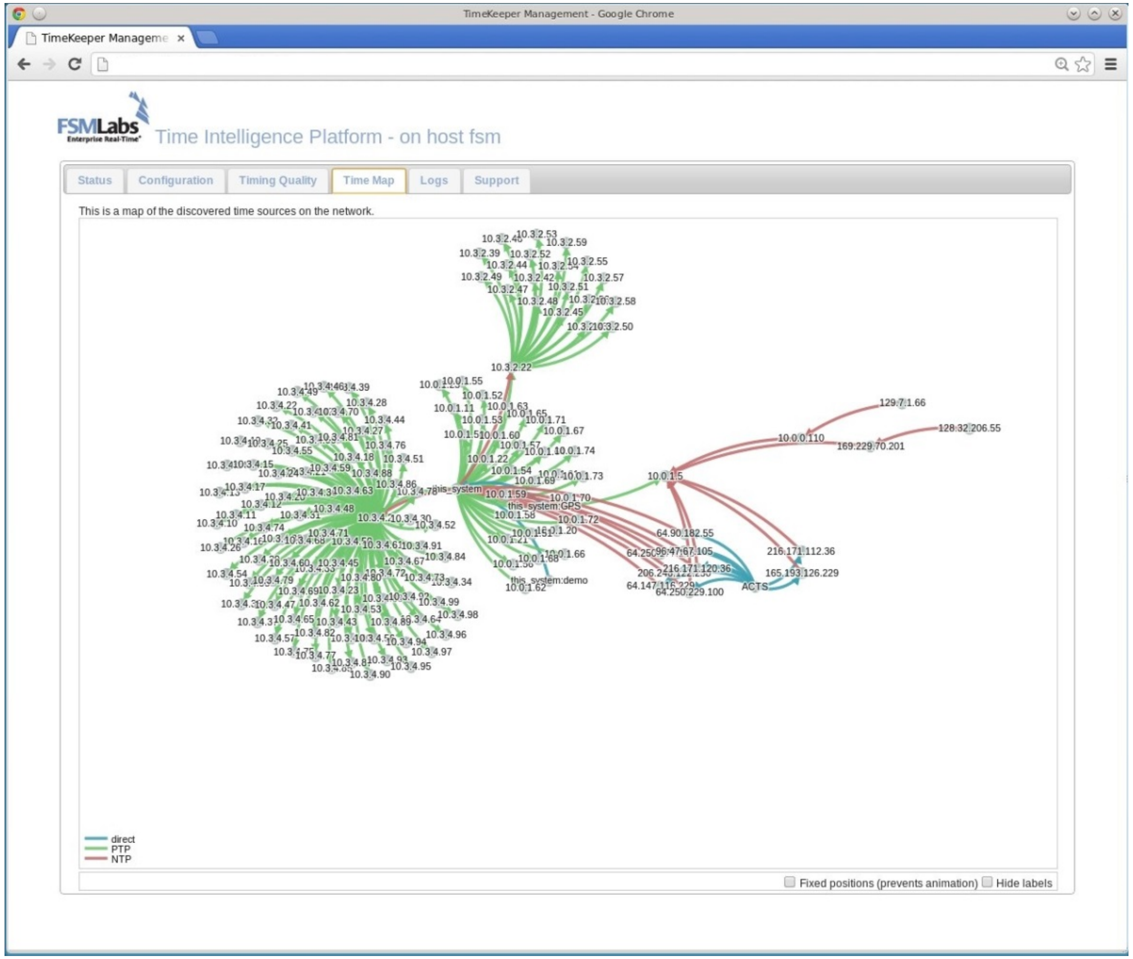
EUROPEAN REGIONAL DEVELOPMENT FUND

ENTERPRISE IRELAND

NUI Galway OÉ Gaillimh

Solution: Multi-Source Time Synchronisation II

- FSMLabs TimeKeeper



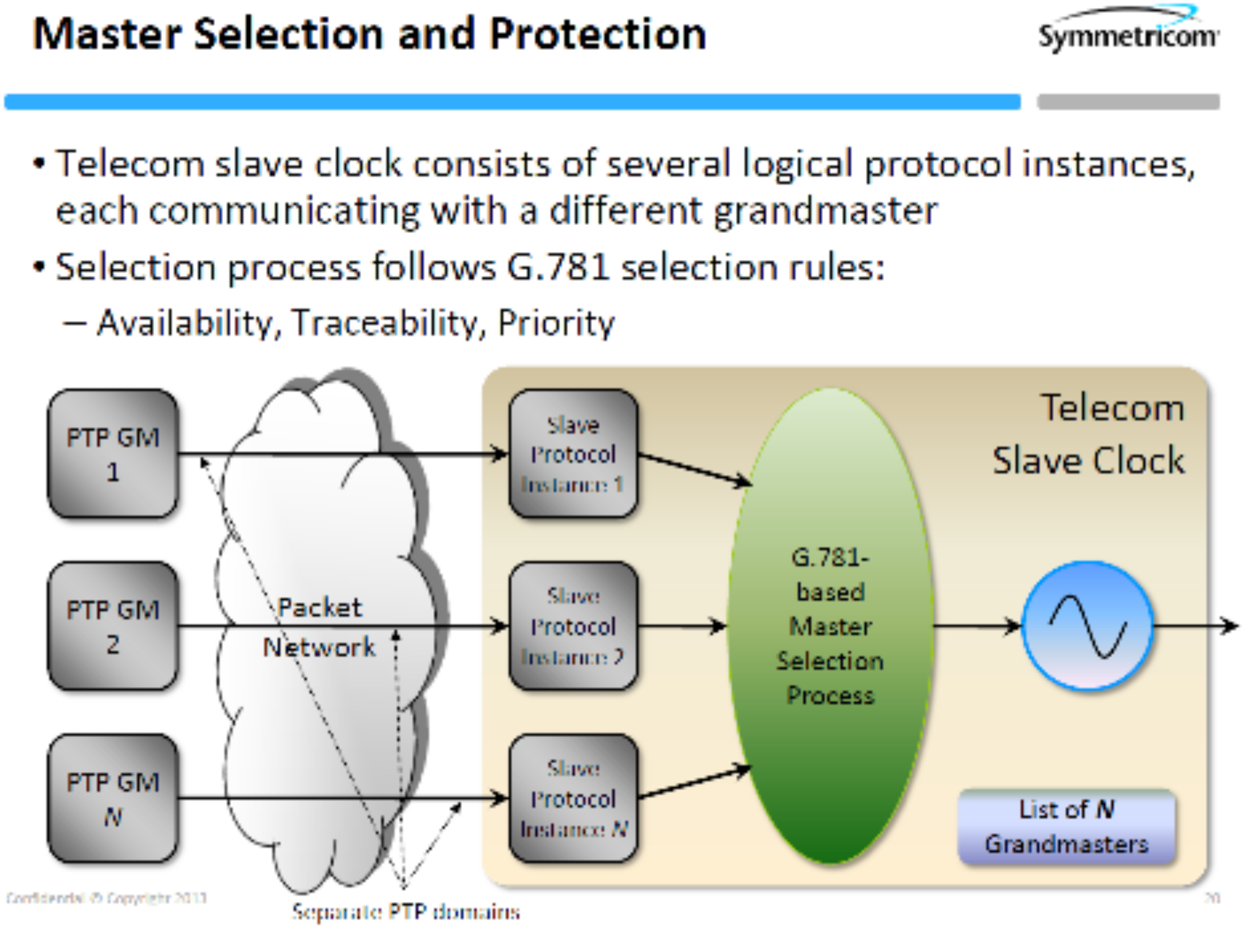
TimeKeeper Management - Google Chrome

Time Intelligence Platform - on host fsm

This is a map of the discovered time sources on the network.

Solution: Multi-Source Time Synchronisation III

- The PTP Telecom Profile for Frequency (G.8265.1)



Master Selection and Protection

- Telecom slave clock consists of several logical protocol instances, each communicating with a different grandmaster
- Selection process follows G.781 selection rules:
  - Availability, Traceability, Priority

Symmetricom
PTP GM 1
PTP GM 2
PTP GM N
Packet Network
Separate PTP domains
Slave Protocol Instance 1
Slave Protocol Instance 2
Slave Protocol Instance N
G.781-based Master Selection Process
Telecom Slave Clock
List of N Grandmasters
Confidential © Copyright 2011
20

Image courtesy of Symmetricom

European Securities and Markets Authority (ESMA) Guidelines

- Operators of trading venues and their members or participants shall establish a system of traceability of their business clocks to UTC. **This includes <u>ensuring</u> that their systems operate within the granularity and a maximum tolerated divergence from UTC as per RTS 25.** Operators of trading venues and their members or participants shall be able to evidence that their systems meet the requirements. They shall be able to do so by documenting the system design, it's functioning and specifications. Furthermore operators of trading venues and their members or participants shall evidence that the crucial system components used meet the accuracy standard levels on granularity and maximum divergence of UTC as guaranteed and specified by the manufacturer of such system components (component specifications shall meet the required accuracy levels) and that these system components are installed in compliance with the manufacturer's installation guidelines.

European Securities and Markets Authority (ESMA) Guidelines

- Operators of trading venues and their members or participants shall establish a system of traceability of their business clocks to UTC.
  This includes ensuring th its their te within the
  granularity from UTC as per
  RTS 25. O s or
  partic s meet the
  requ ng the
  syste ermore
  opera ticipants shall
  evide ed meet the
  accuracy sta aximum divergence of
  UTC as guaranteed and sp the manufacturer of such
  system components (component specifications shall meet the required accuracy levels) and that these system components are installed in compliance with the manufacturer's installation guidelines.

Problem solved???

How about APT that target Timing Infrastructure of Trading Venues?

- An **advanced persistent threat** (APT) is a set of stealthy and continuous computer hacking processes targeting a specific entity
- An APT usually targets organizations and/or nations for business or political motives

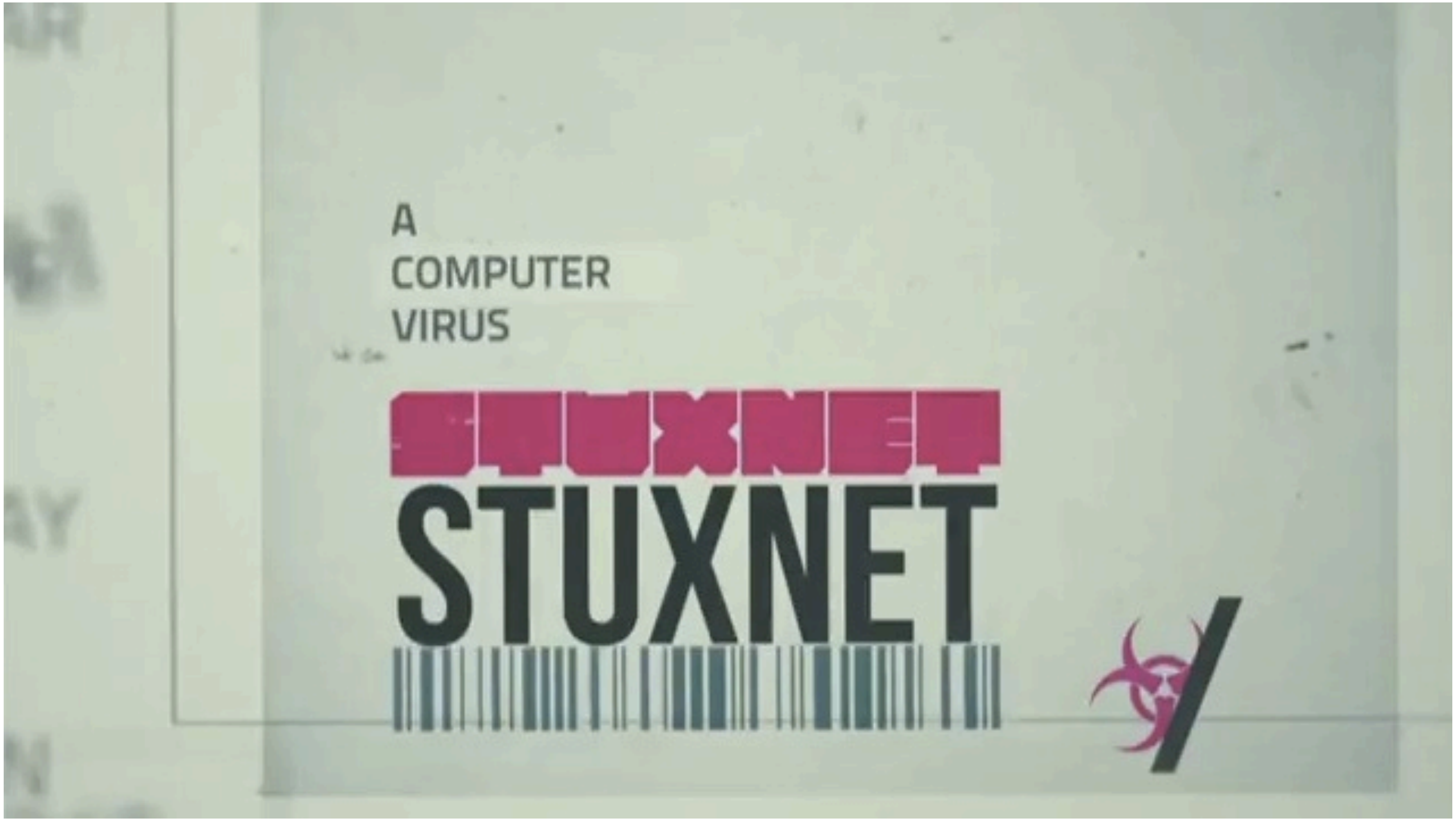
APT Definition

- The “**Advanced**” process signifies sophisticated techniques (i.e. malware and / or known vulnerabilities) to exploit some internal (sub)systems.
- The “**Persistent**” process suggests a high degree of covertness over a long period of time
- The “**Threat**” process indicates human involvement in orchestrating the attack

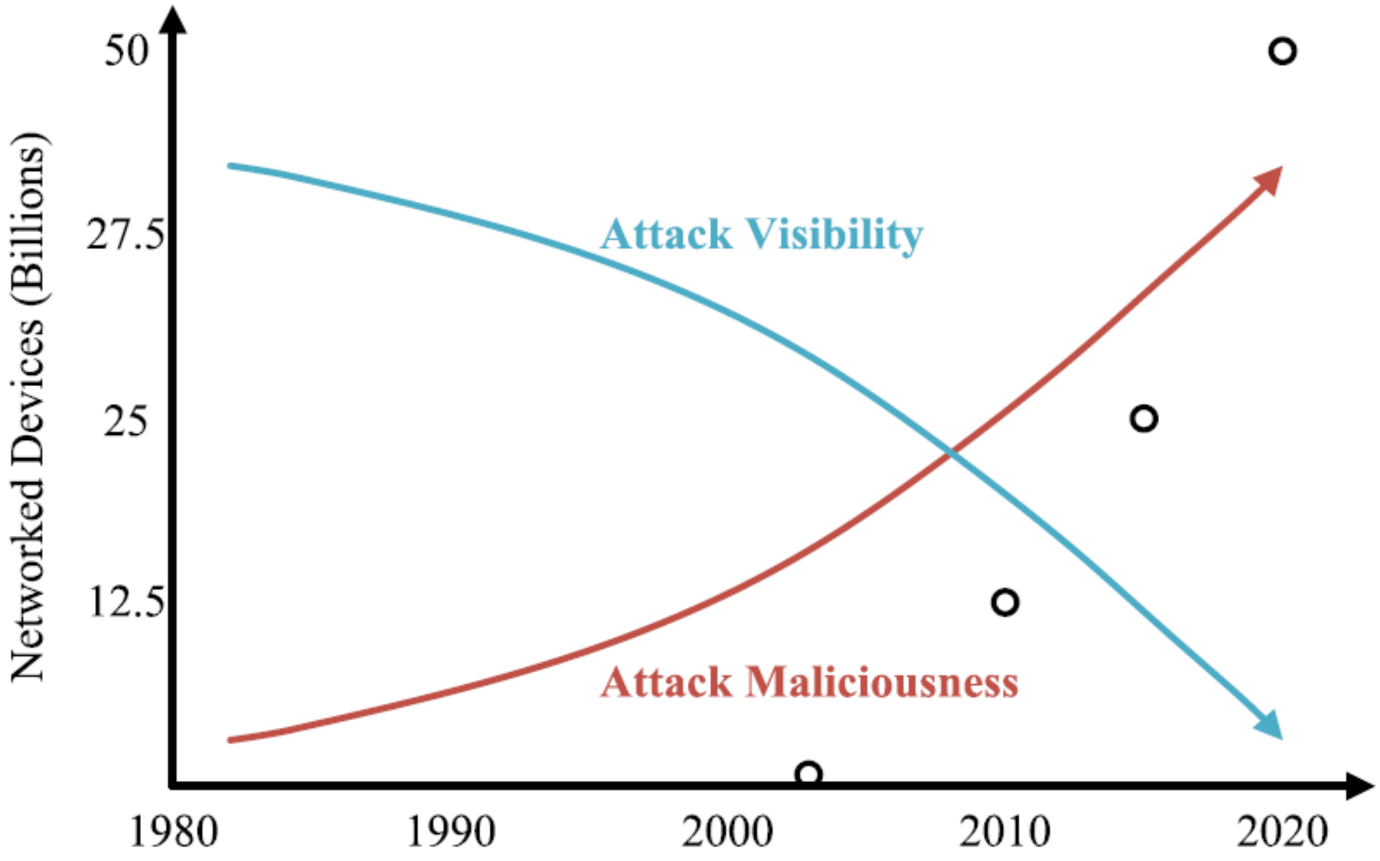
APT Characteristics

- **Customized attacks** — APTs often use highly customized tools and intrusion techniques, developed specifically for a campaign
- **Low and slow**—APT attacks occur over long periods of time during which the attackers move slowly and quietly to avoid detection
- **Higher aspirations**—No “fast-money schemes”, but APTs are designed to satisfy the requirements of international espionage and/or sabotage
- **Specific targets** — APTs are aimed at a very confined range of targets

A realistic Scenario?



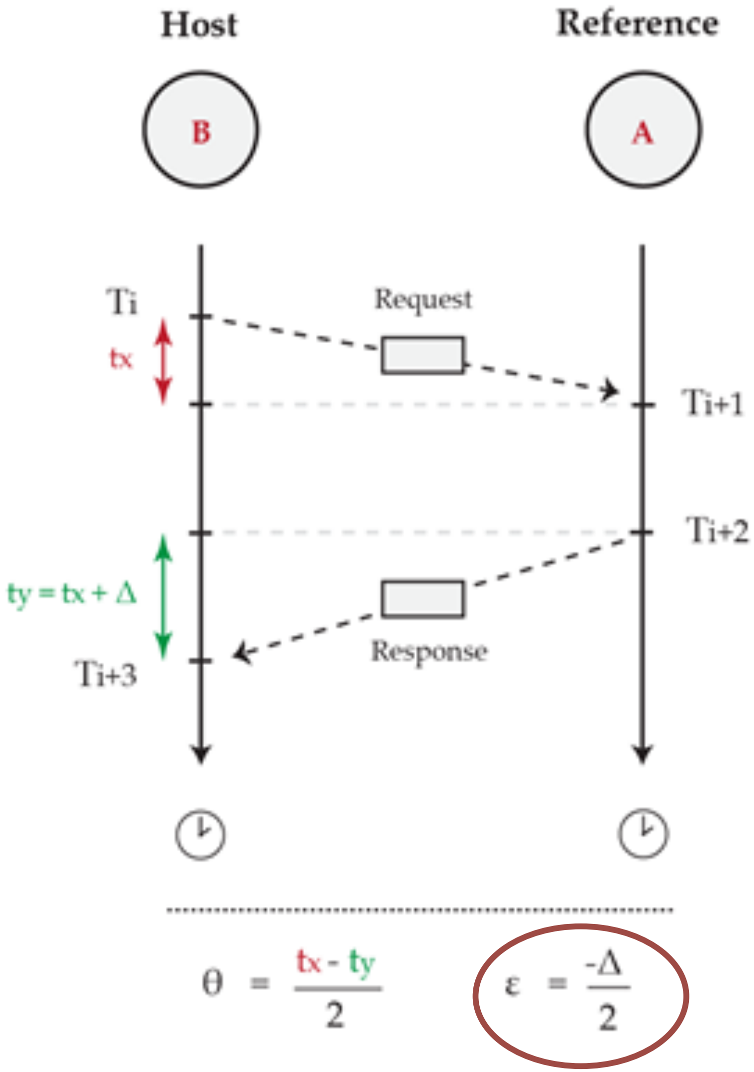
Attack Visibility versus Attack Maliciousness



Questions re APT that aim Timing Infrastructure [of Trading Venues]

- What principal **forms of manipulations** would be implemented?
- What are the **specific targets (e.g. subsystems)** mentioned before?
- Potential **impact** on timing infrastructure
- How **bullet-proofed** are existing concepts of multi-source time synchronisation
- ~~What is the anatomy / timeline of such an APT?~~

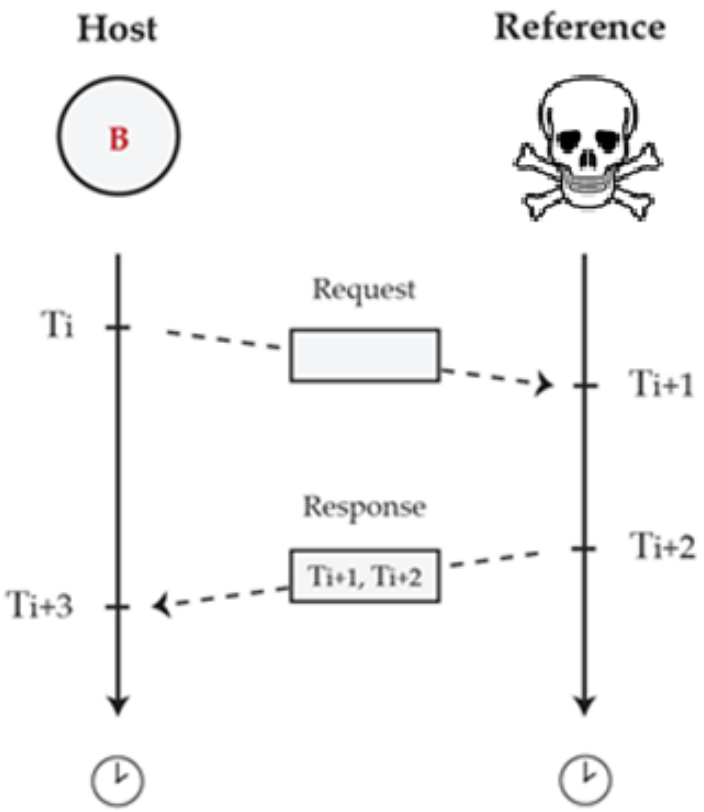
Forms of Manipulations 1: Asymmetric Delays



- Asymmetric delays caused by uplink / downlink differences, for example
  - different ingress/egress router queues
  - different routing paths

  cause time sync errors between host and reference

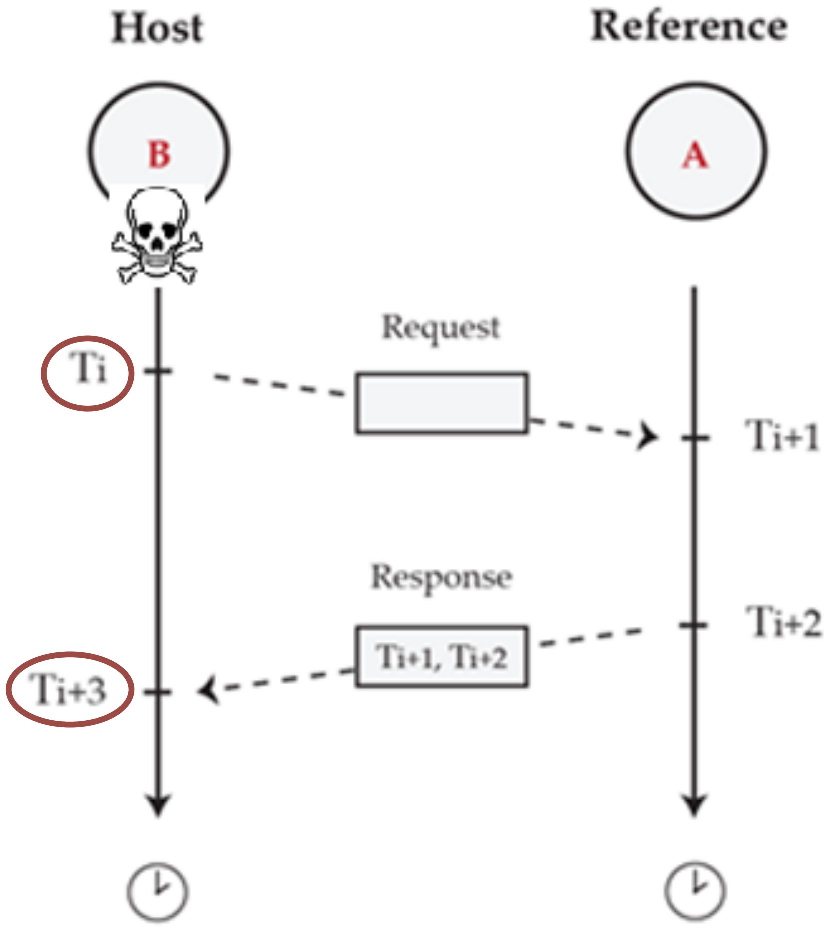
Forms of Manipulations 2: Erroneous Time Reference



- I.e. Byzantine Fault
- A spoofed or manipulated reference will provide incorrect time to all hosts it is connected to
  - Example GPS spoofing / jamming

OSNA OPEN SENSOR NETWORK AUTHENTICATION
EUROPEAN REGIONAL DEVELOPMENT FUND
ENTERPRISE IRELAND
NUI Galway OÉ Gaillimh

Forms of Manipulations 3: Erroneous Time Sync on Host

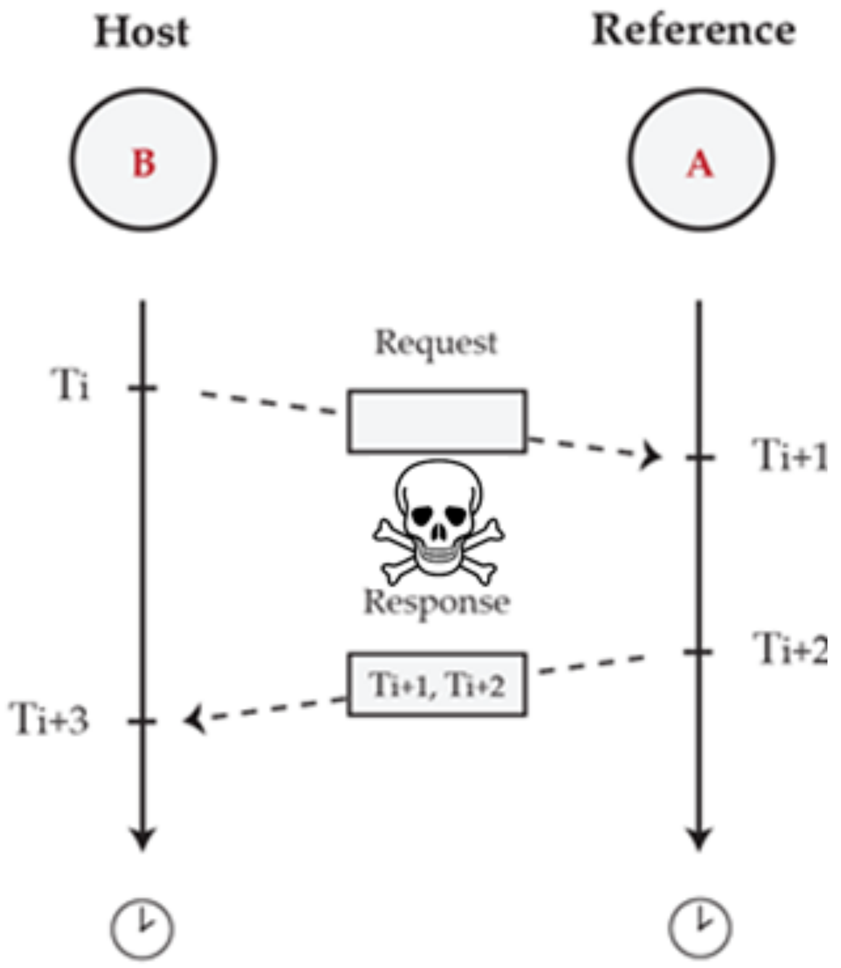


- Likewise manipulated or faulty time-sync software / routines on host will cause local time sync errors

OPEN SENSOR NETWORK AUTHENTICATION

EUROPEAN REGIONAL DEVELOPMENT FUND

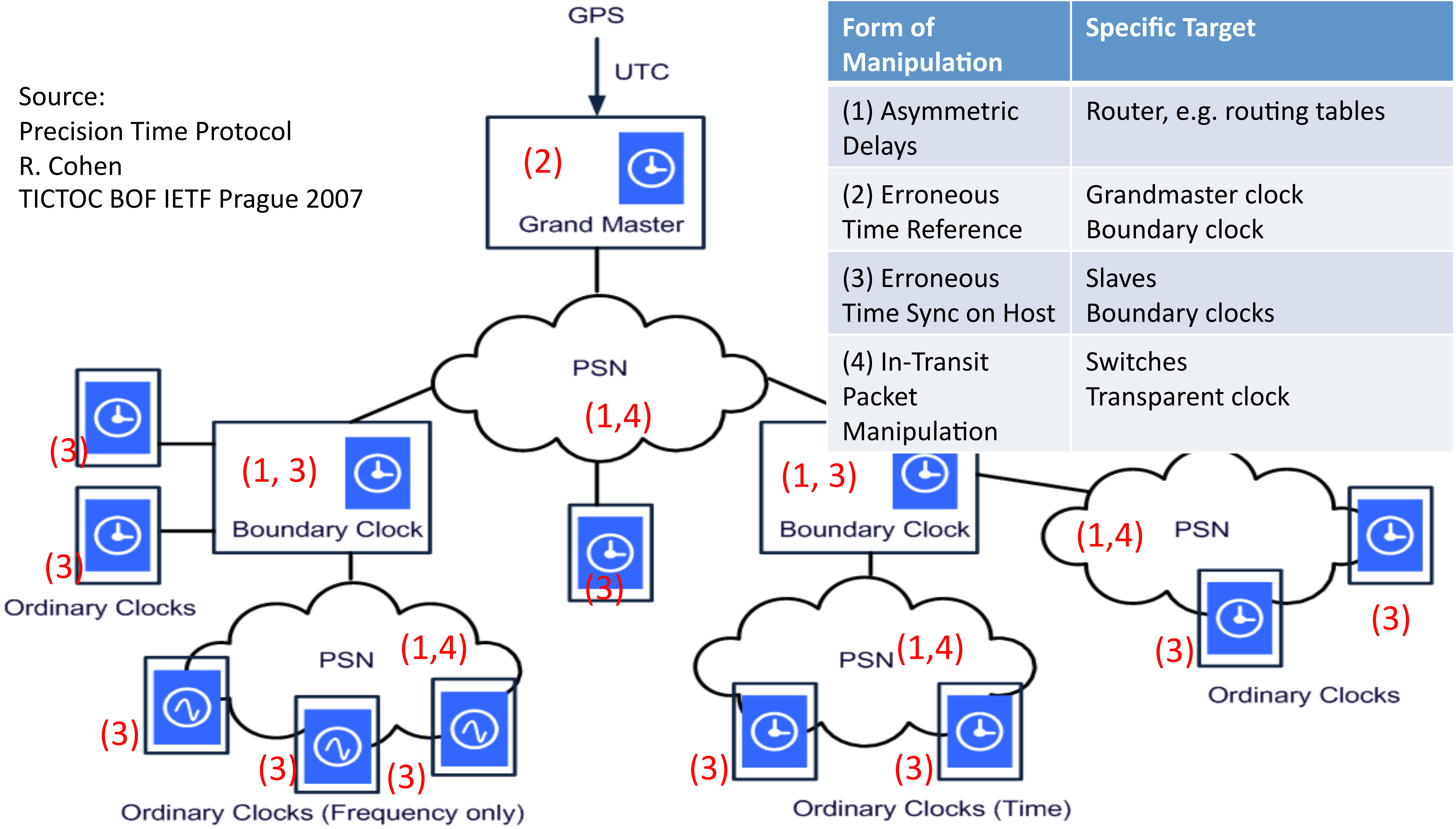
Forms of Manipulations 4: In-Transit Packet Manipulation



Time stamps in request / response packets can be deliberately manipulated in transit, for example by a network switch, causing time sync errors between host and reference

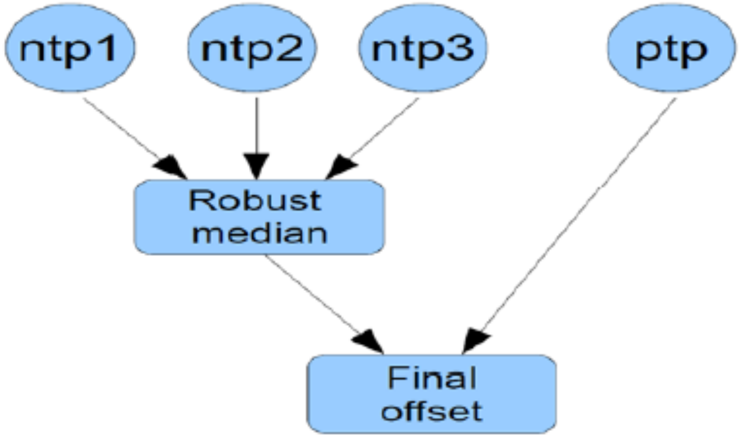
ATPs and PTP: FoM, ST and Impact

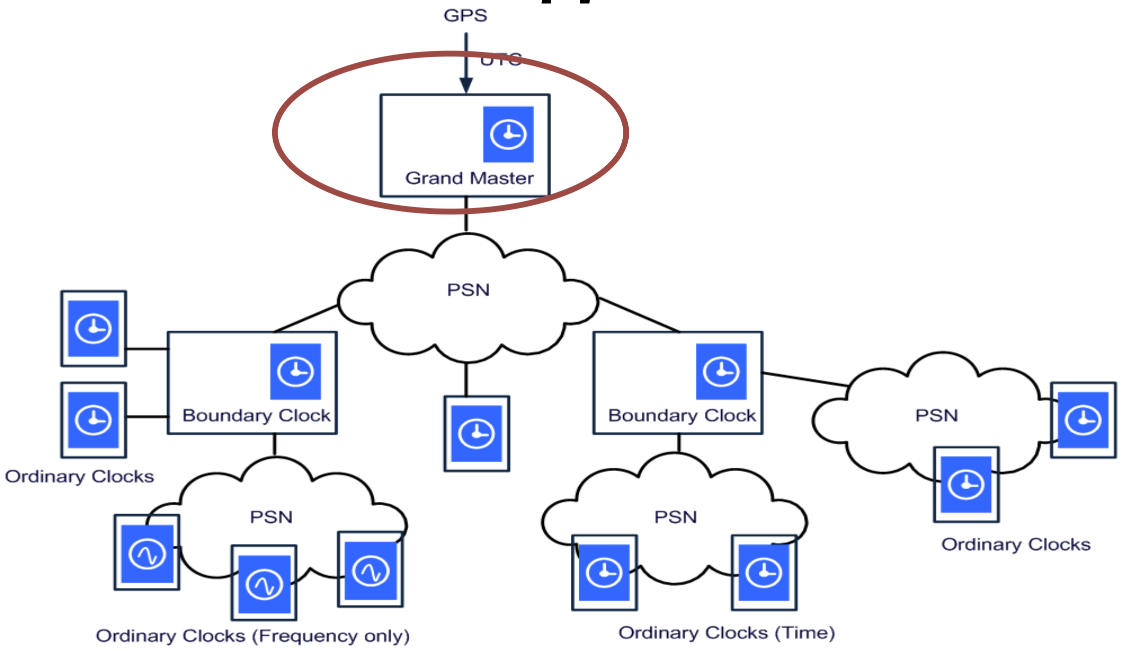
Source:
Precision Time Protocol
R. Cohen
TICTOC BOF IETF Prague 2007



Form of Manipulation	Specific Target
(1) Asymmetric Delays	Router, e.g. routing tables
(2) Erroneous Time Reference	Grandmaster clock Boundary clock
(3) Erroneous Time Sync on Host	Slaves Boundary clocks
(4) In-Transit Packet Manipulation	Switches Transparent clock

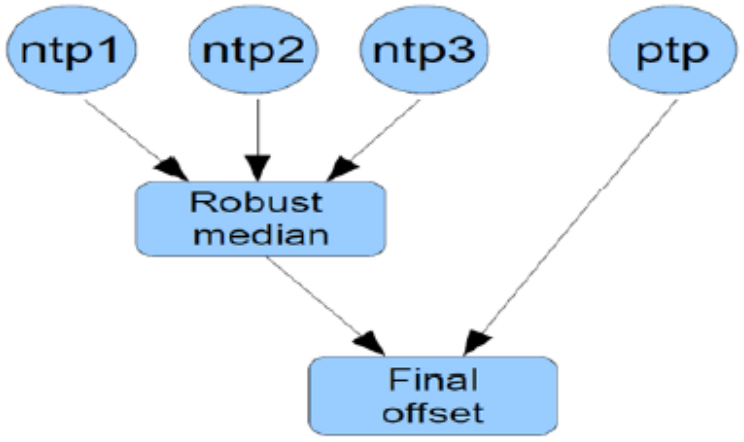
Case Study: Vulnerability of Multi-Source Watchdog I

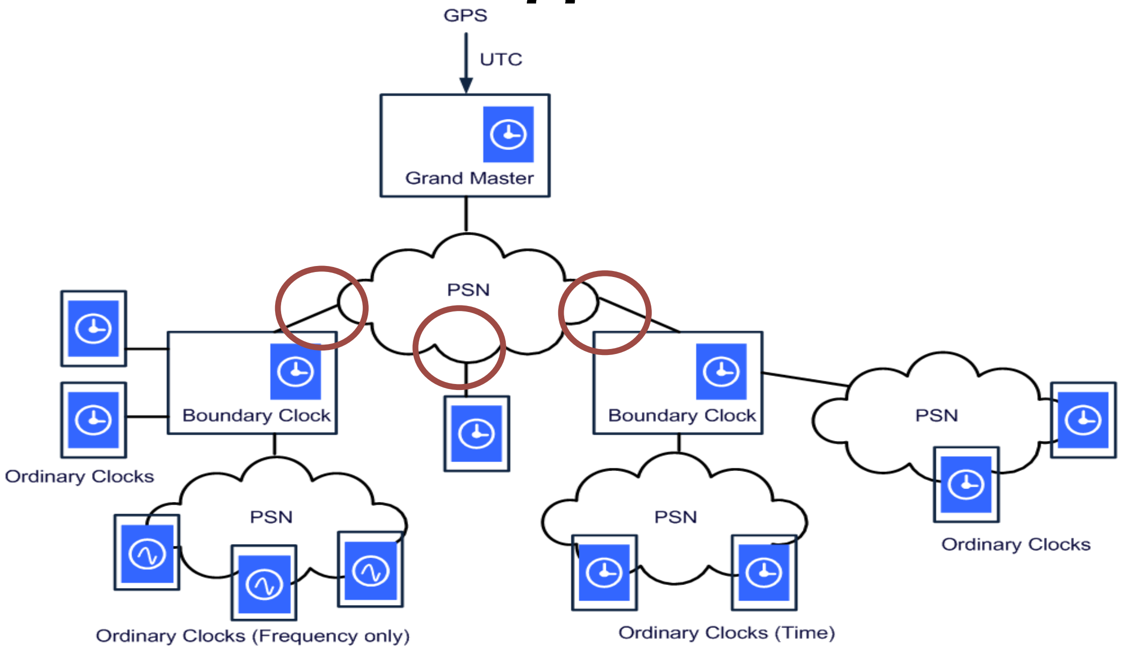




- Manipulation #2: Multiple NTP and PTP time sources need to manipulated in a coordinated fashion
  → Difficult to achieve
  → huge impact

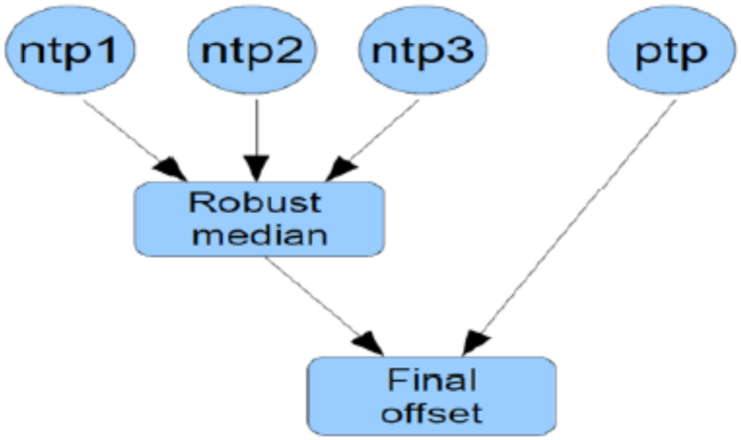
Case Study: Vulnerability of Multi-Source Watchdog II

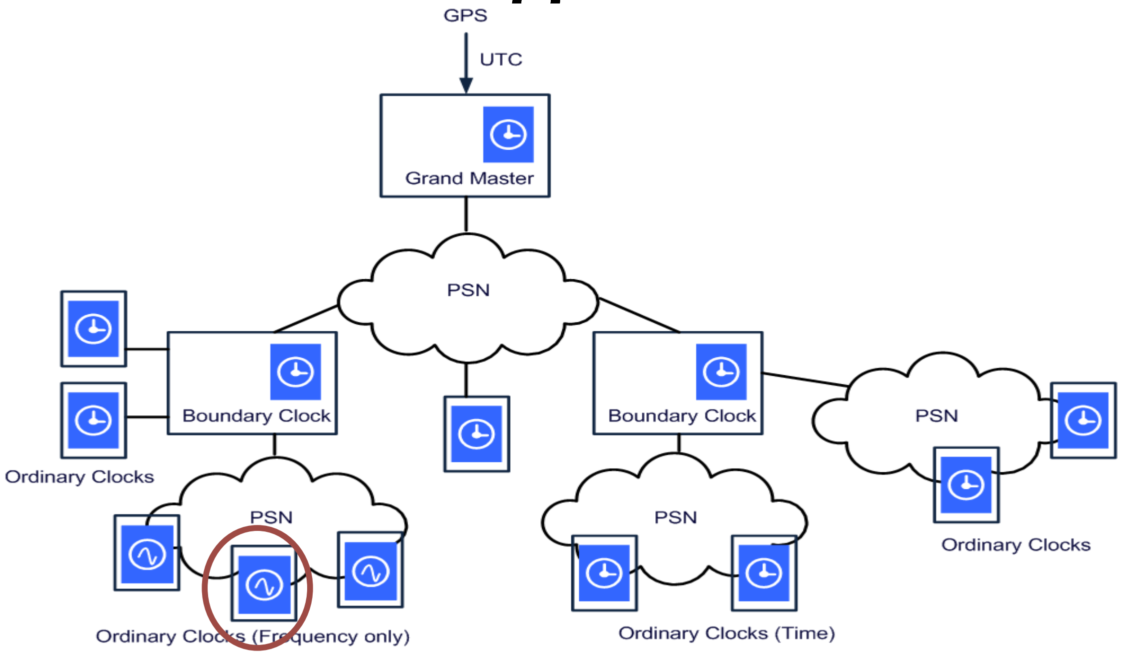




- Manipulation #1: PSN gateway switch(es) systematically manipulate time sync NTP and PTP packets
  → straight forward to achieve only if single entry point
  → significant impact on underlying timing infrastructure

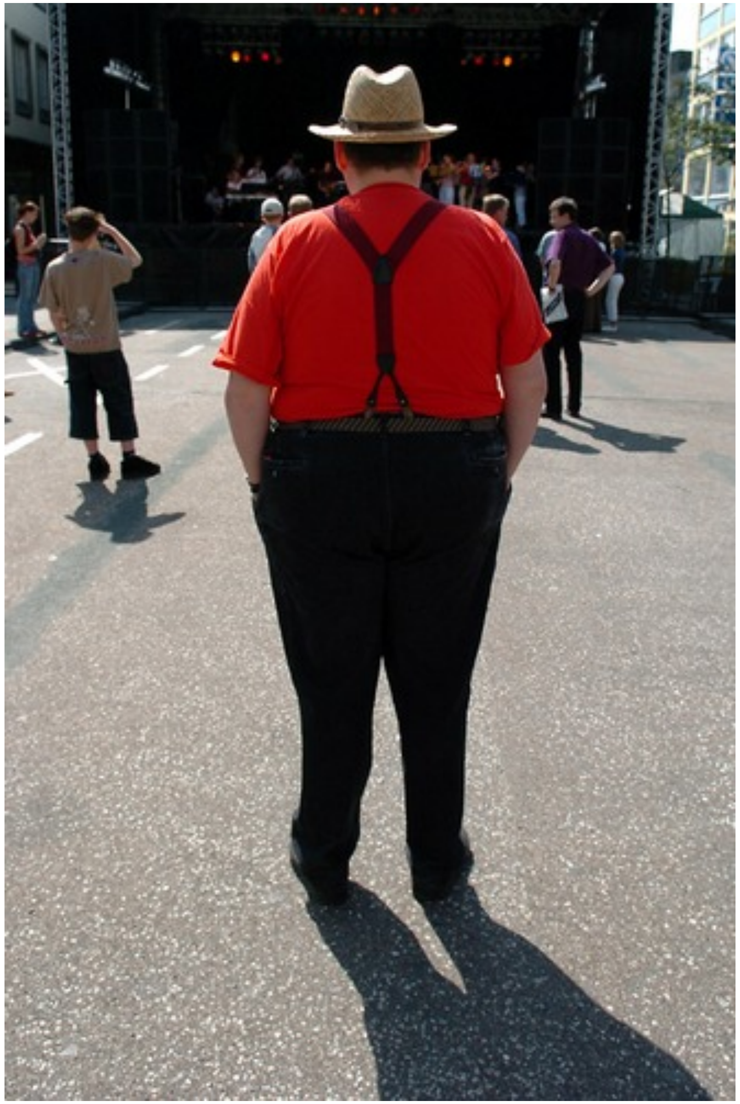
Case Study: Vulnerability of Multi-Source Watchdog III





- Manipulation #3: End point software manipulation
  → simple
  → low impact

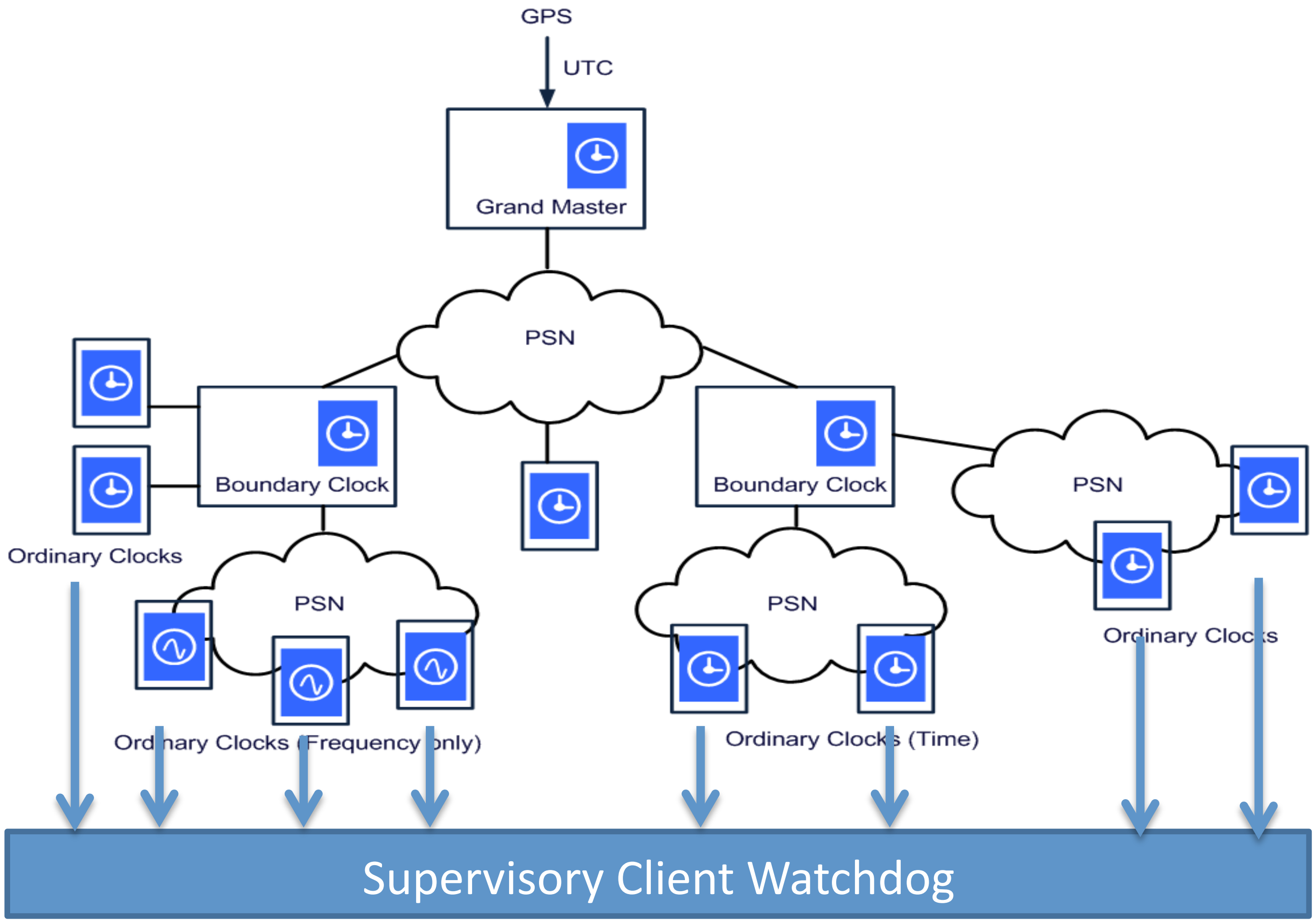
Supervisory Client Watchdog



- Complementary to multi-source time synchronisation
- Another line of defense against APT
  - M-STS is not 100% bullet proof
  - "Belt and suspender" approach
- Independent of underlying time synchronisation protocol

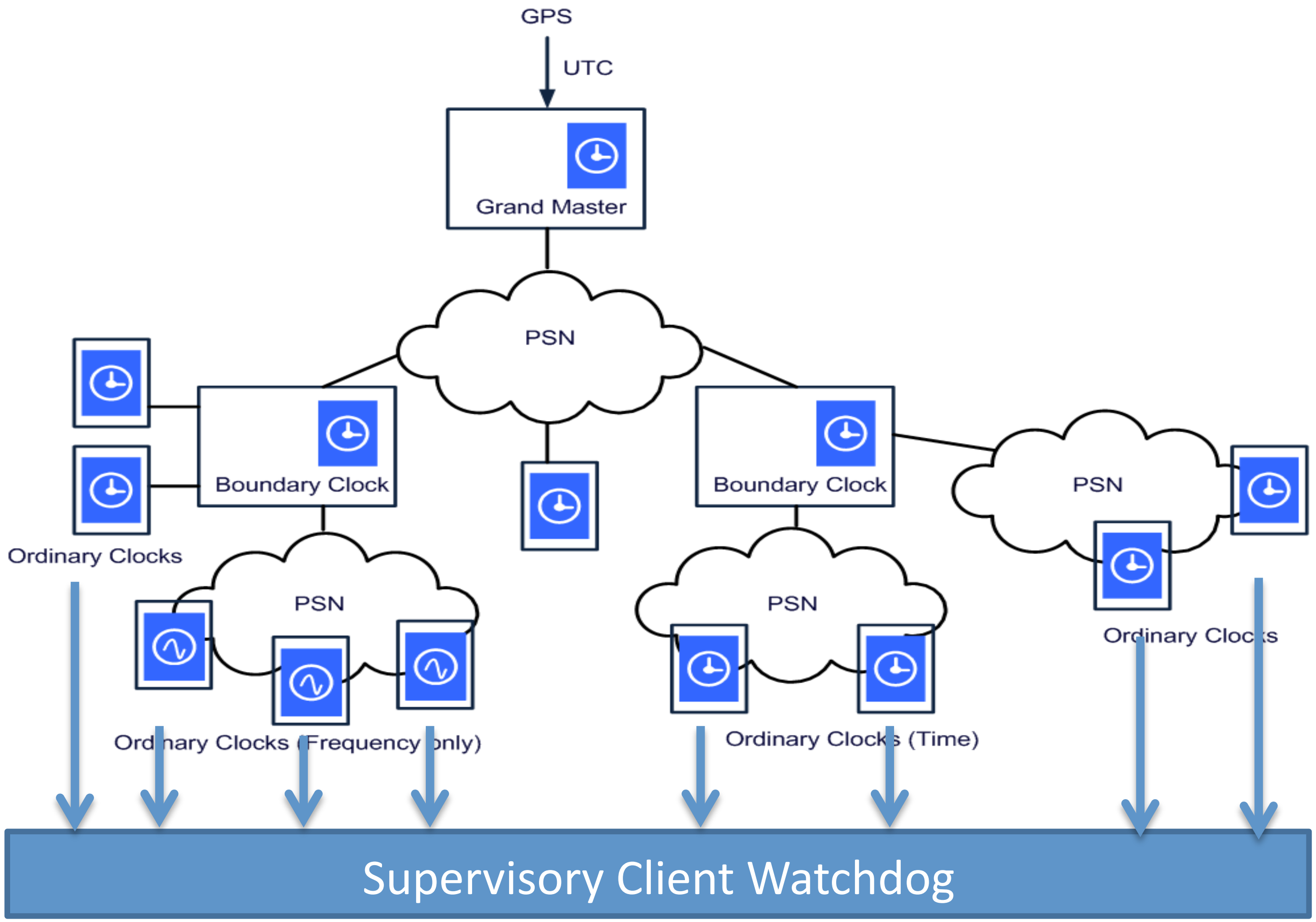
Supervisory Client Watchdog I

Idea:
End points / hosts / slaves continuously report their individual host clock error, e.g. phase offsets, to central watchdog



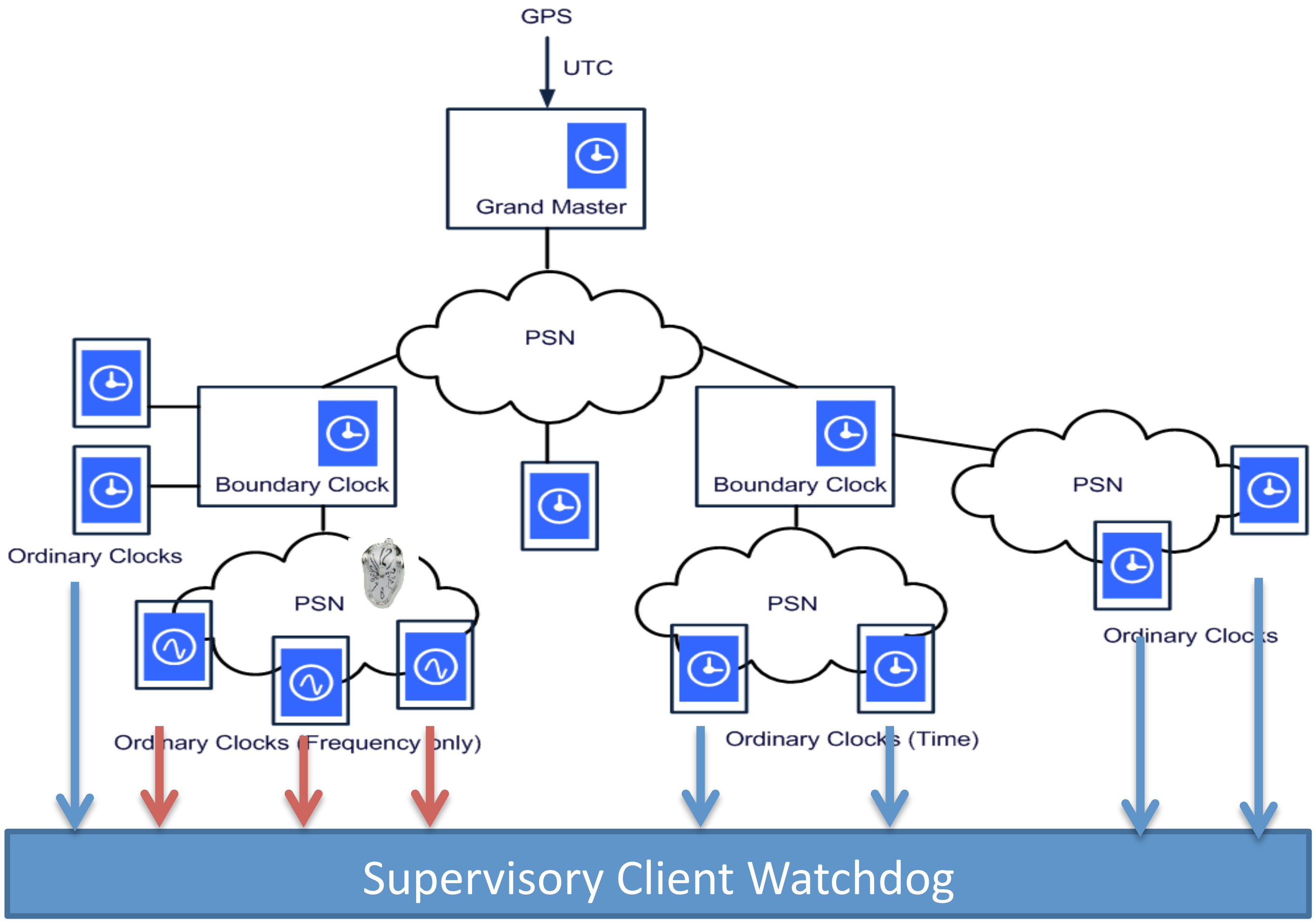
Supervisory Client Watchdog II

Idea (cont.): SCW dynamically builds models of individual and collective clock errors



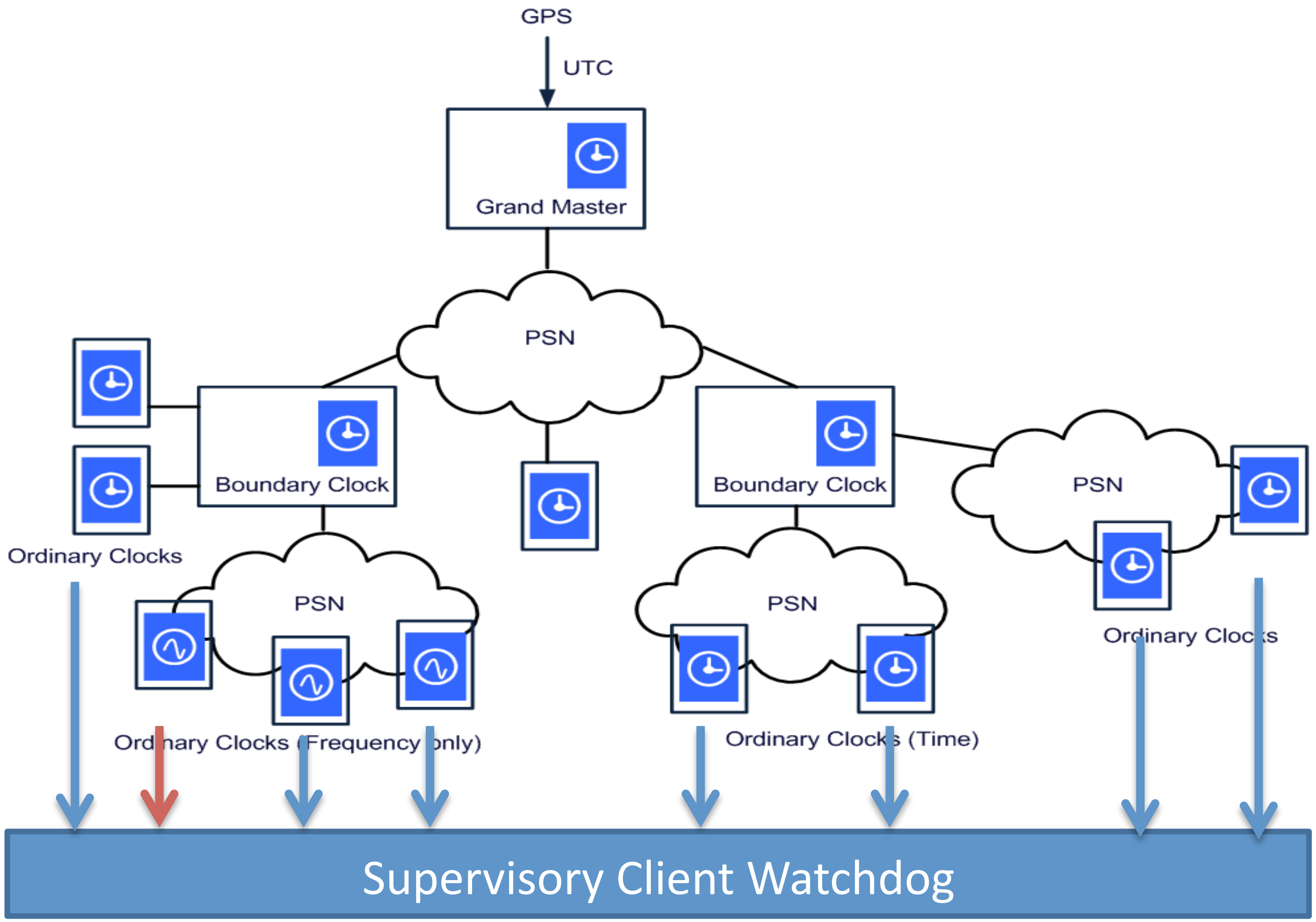
Supervisory Client Watchdog III

Idea (cont.): A Byzantine Fault will cause a deviation of estimated / modelled errors of a group of end points



Supervisory Client Watchdog IV

Idea (cont.): However, SCW are robust to identify false positives, e.g. sudden changes of individual clock errors due to other factors

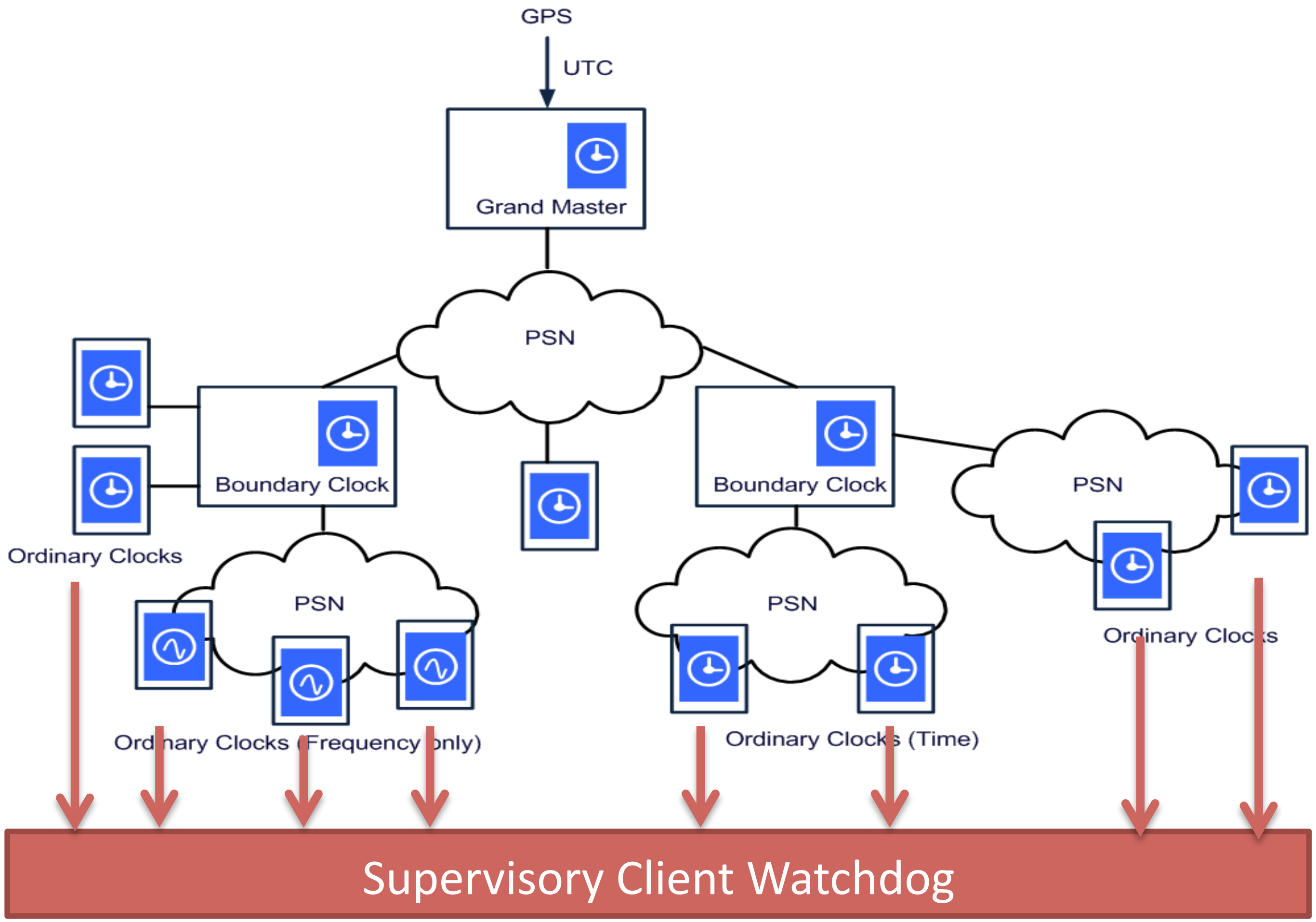


Supervisory Client Watchdog V

Issues to be addressed:

- SCW is single point of failure
  - TPM
- In transit manipulation of clock error messages
  - Digitally signatures
  - Public key encryption
  - PKI / Digital certificates

- **Work in progress!**



Summary

- APTs will eventually target time synchronisation networks
  - Financial networks are high-profile targets
- Multi-Source Time Synchronisation concepts alleviate the problem, but are not fully bullet-proof
- We suggest a Supervisory Client Watchdog as another line of defense

OSNA
OPEN SENSOR NETWORK AUTHENTICATION

EUROPEAN REGIONAL DEVELOPMENT FUND

ENTERPRISE IRELAND

NUI Galway
OÉ Gaillimh

I · T · S · F

OSNA

OPEN SENSOR NETWORK AUTHENTICATION

Thank you - go raibh maith agat – Danke

EUROPEAN REGIONAL DEVELOPMENT FUND

ENTERPRISE IRELAND

NUI Galway
OÉ Gaillimh

39