Security Aspects of Time Synchronization Solutions

Keynote, WSTS 2022, Denver, CO

Heiko Gerstung
Managing Director, Meinberg

MEINBERG

The Synchronization Experts.

WORKSHOP ON SYNCHRONIZATION AND TIMING SYSTEMS

Introduction

Example of a Timing System

The Chain of Time 

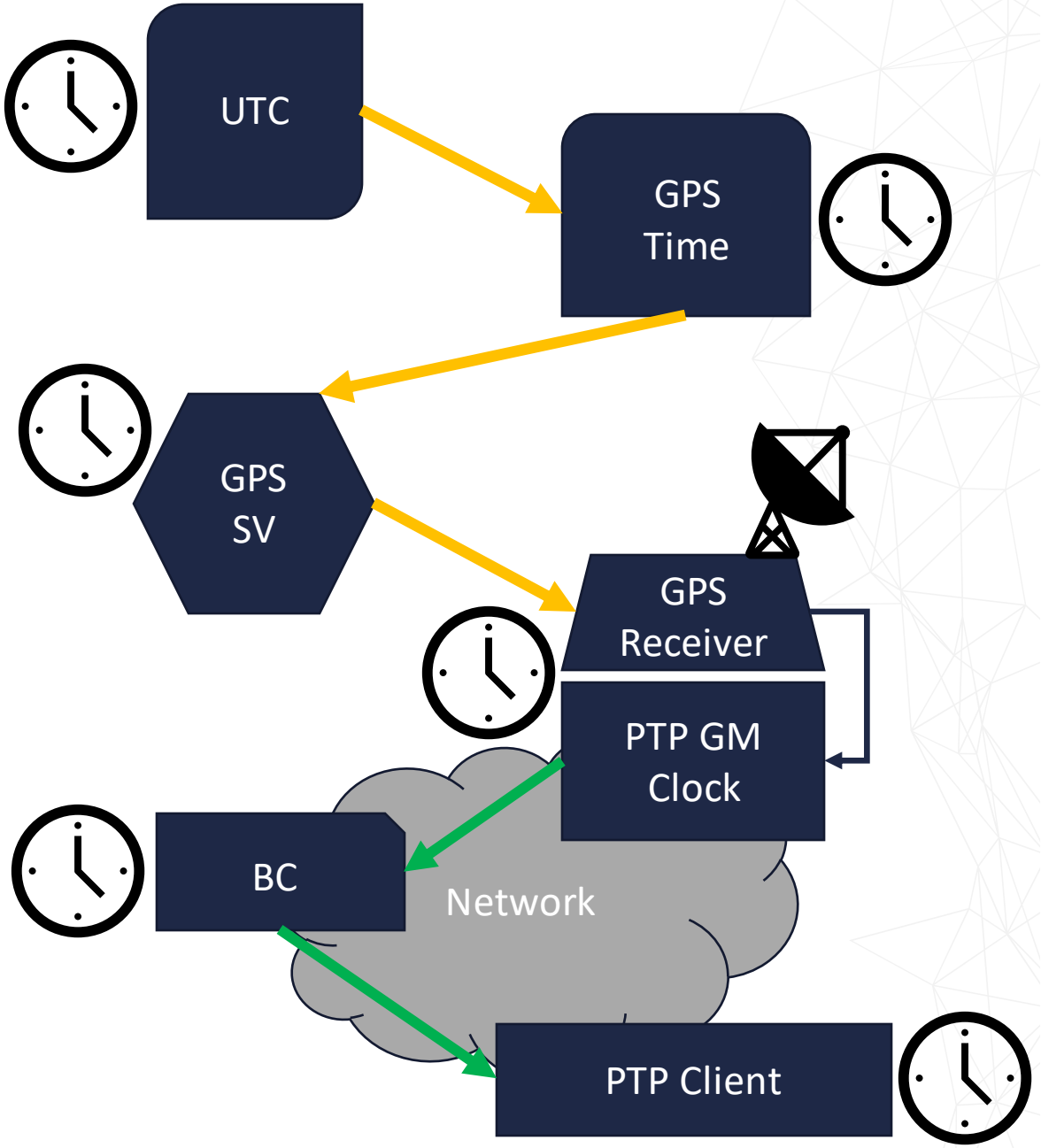
A time synchronization solution typically receives time from one or more external „upstream“ source(s) and distributes it to „downstream“ devices/receivers.

Typically a number of separate clocks is used for this, and there are individual links/connections between those clocks.

The following example illustrates how such a „Chain of Time“ works for a GPS synchronized PTP network.

Chain of Time - Example

- UTC(USNO) -> GPS Time
  GPS Time is synchronized with UTC(USNO)
- GPS Time -> GPS SV Clocks
  Satellite clocks are synchronized with GPS Time
- GPS SV Clocks -> GPS receiver
  GPS receiver receives time from satellites
- GPS receiver -> PTP GM clock
  PTP GM clock is adjusted based on GPS receiver time output, e.g. ToD string + PPS
- PTP GM clock -> PTP BC clock
  The GM clock synchronizes a PTP Boundary clock port
- PTP BC clock -> PTP client clock
  Another BC port synchronizes the PTP client



MEINBERG

Attacks

Attacks

How can we bring it down?

There are typically two types of attacks that can be carried out in regards to timing.

„Disrupt timing“ means stopping the distribution of time entirely by stopping the ability of a system to send or receive timing related messages.

“Manipulate Timing“ refers to changing either the content of timing related messages or manipulating other factors which have a direct or indirect influence on the timing.

Disrupt Timing

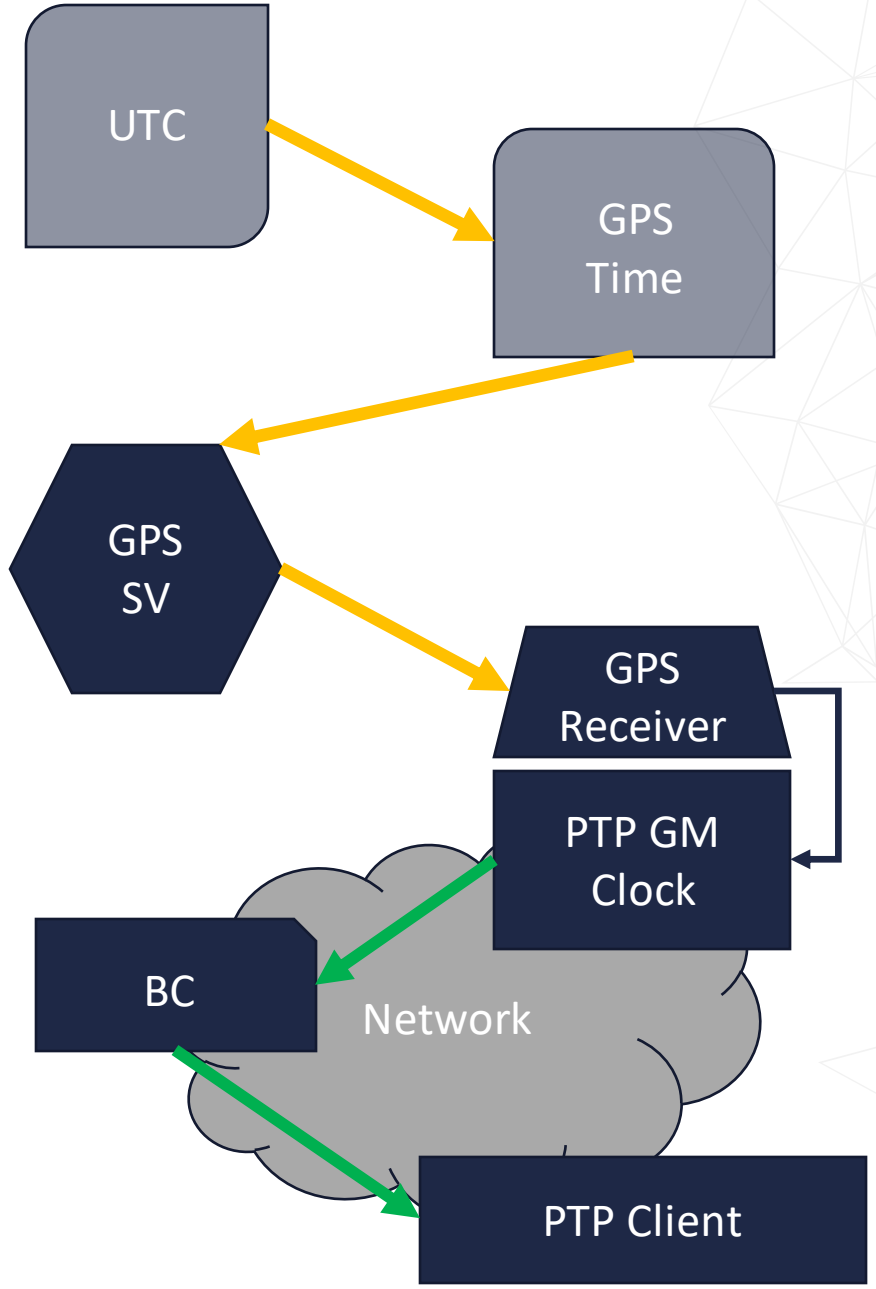
Intercepting or destroying the messages or communication channels used to distribute timing

Manipulate Timing

Directly changing messages or influence other factors that are relevant for time distribution

Attacks – Disrupt Timing

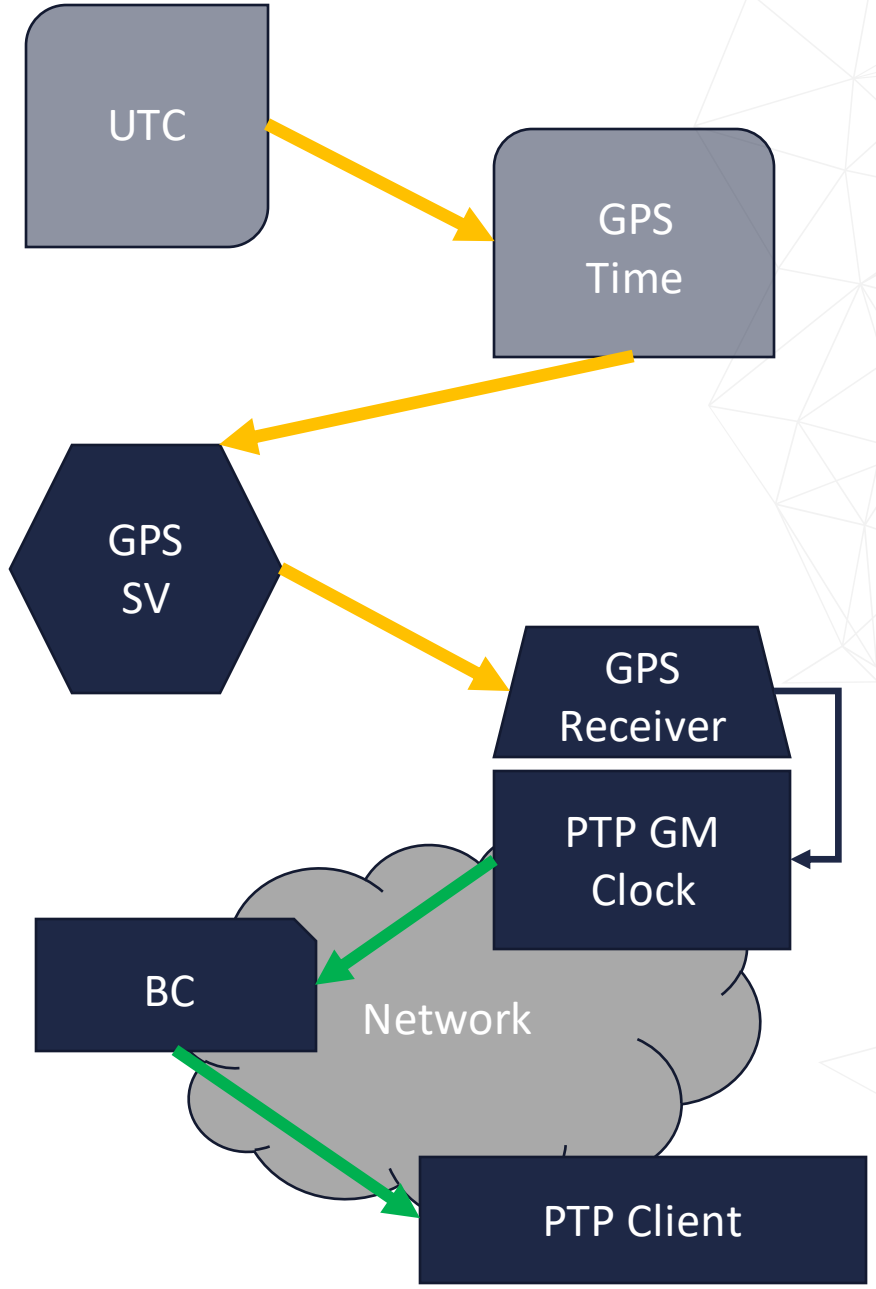
- GPS SV Clocks -> GPS receiver
  - Jam GPS signals
  - Physically block the signal (sauerkraut attack)
  - Damage antenna/antenna cable/receiver
- GPS receiver -> PTP GM clock
  - Hack PTP GM, modify configuration, internal software or bring down the system
- PTP GM clock -> PTP BC clock
  - Intercept/block PTP traffic between GM and BC
  - BMCA attack to force BC to use „unusable“ rogue GM
  - Hack BC, modify configuration, internal software or bring down the BC
- PTP BC clock -> PTP client clock
  - Intercept/block PTP traffic between BC and PTP client
  - Hack PTP client, modify configuration, internal software or bring down the PTP client



MEINBERG

Attacks – Manipulate Timing

- GPS SV Clocks -> GPS receiver
  - Spoof GPS signals
- GPS receiver -> PTP GM clock
  - Hack PTP GM, modify configuration or internal software
- PTP GM clock -> PTP BC clock
  - Intercept and change PTP messages between GM and BC
  - Delay attack: Intercept and release PTP msg
  - BMCA attack, forcing BC to use a rogue GM with wrong timing
  - Hack BC, modify configuration or internal software
- PTP BC clock -> PTP client clock
  - Intercept and change PTP traffic between BC and PTP client
  - Delay attack: Intercept and release PTP msg
  - BMCA attack, forcing client to use a rogue GM/BC with wrong timing
  - Hack PTP client, modify configuration or internal software

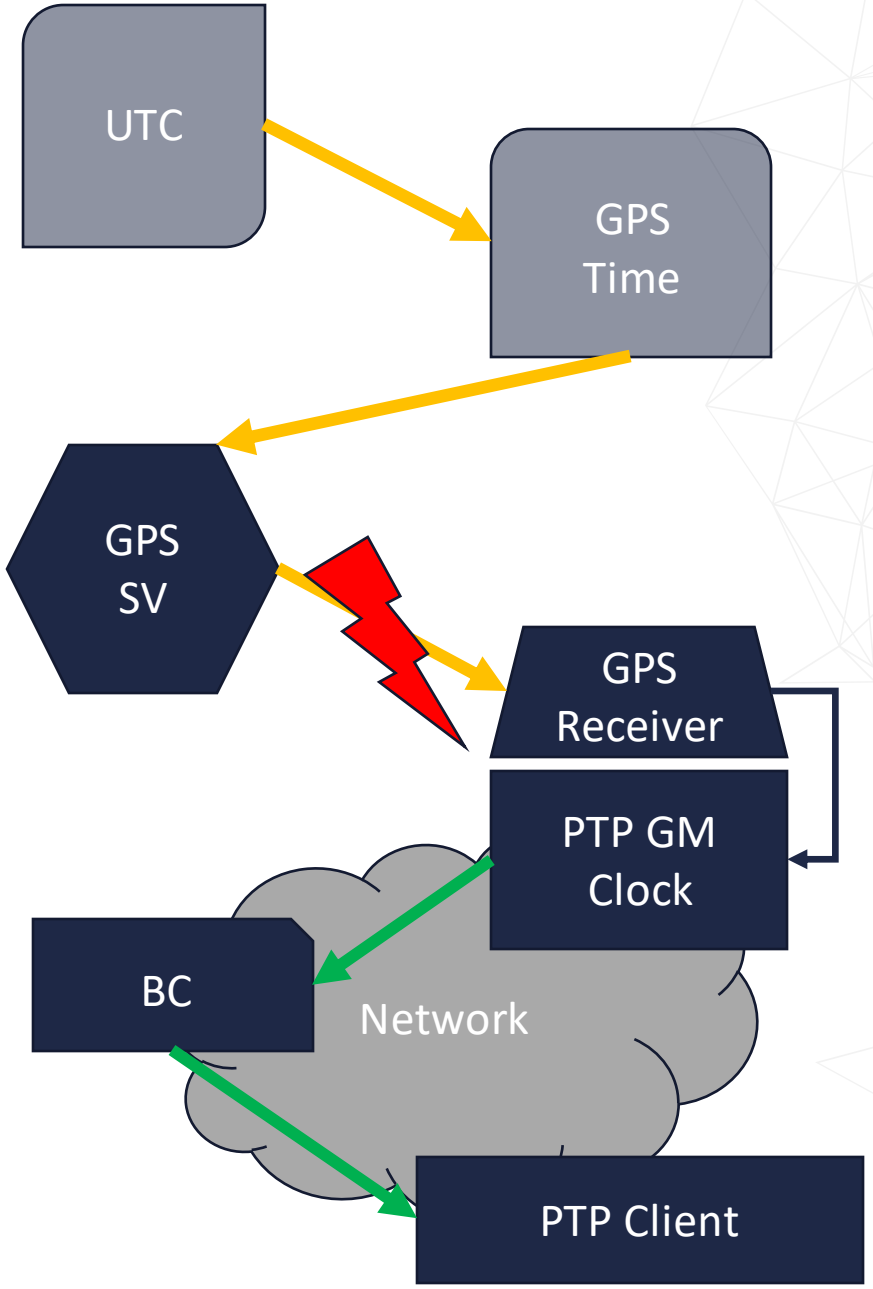


MEINBERG

Monitoring / Detection 

Detect Disruptive Timing Attacks

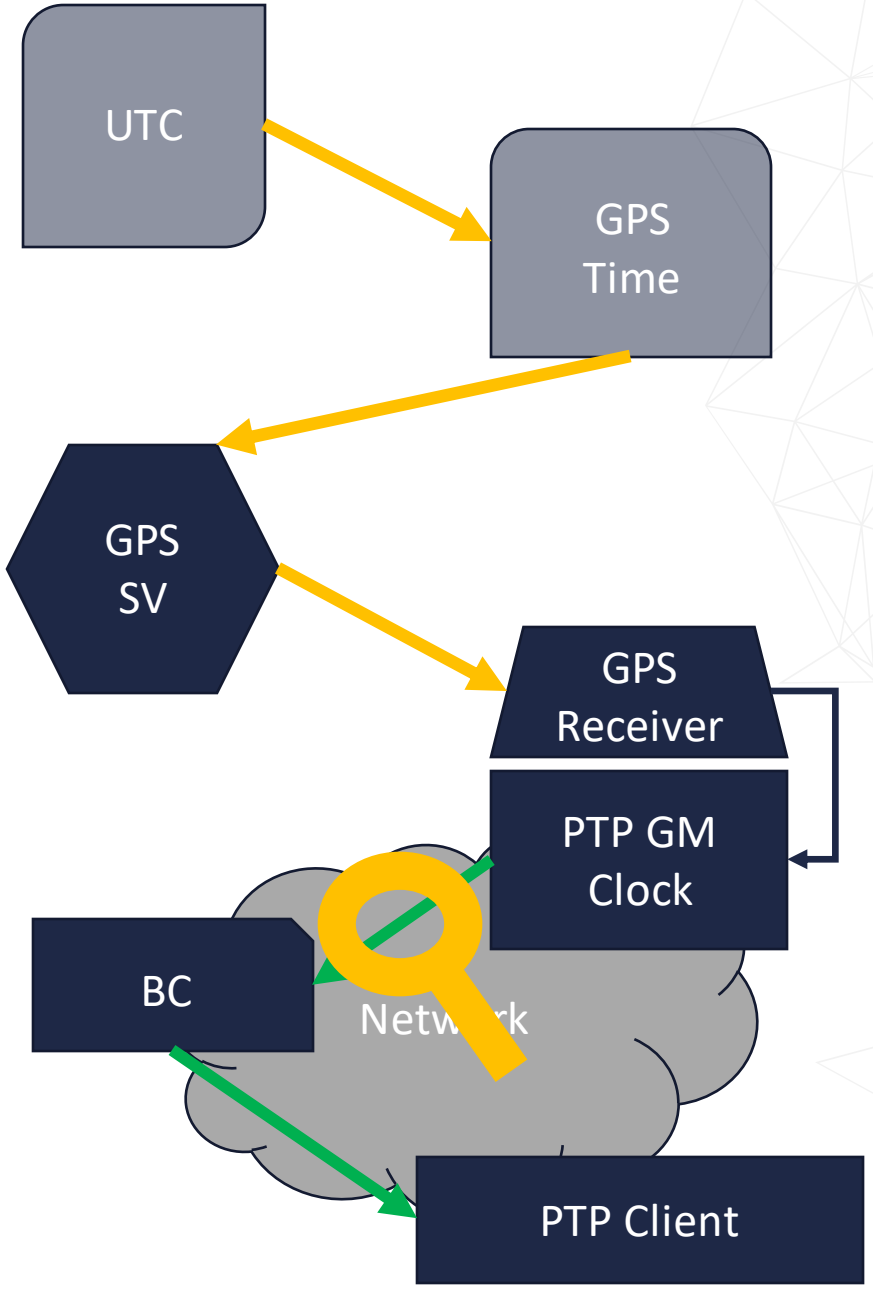
- GPS SV Clocks -> GPS receiver
  - Monitor GPS reception status of receiver
    - Operational: sync status of receiver, GPS reception (SV data)
- GPS receiver -> PTP GM clock
  - Monitor PTP GM state
    - Operational: sync status, clock status
    - Timing: offset to GPS
- PTP GM clock -> PTP BC clock
  - Monitor PTP BC state
    - Operational: system status of BC, PTP port state, sync source (GM)
    - Timing: offset to GM
- PTP BC clock -> PTP client clock
  - Monitor PTP client state
    - Operational: system status of PTP client, port state, sync source (BC)
    - Timing: offset to BC



MEINBERG

Detect Manipulative Timing Attacks

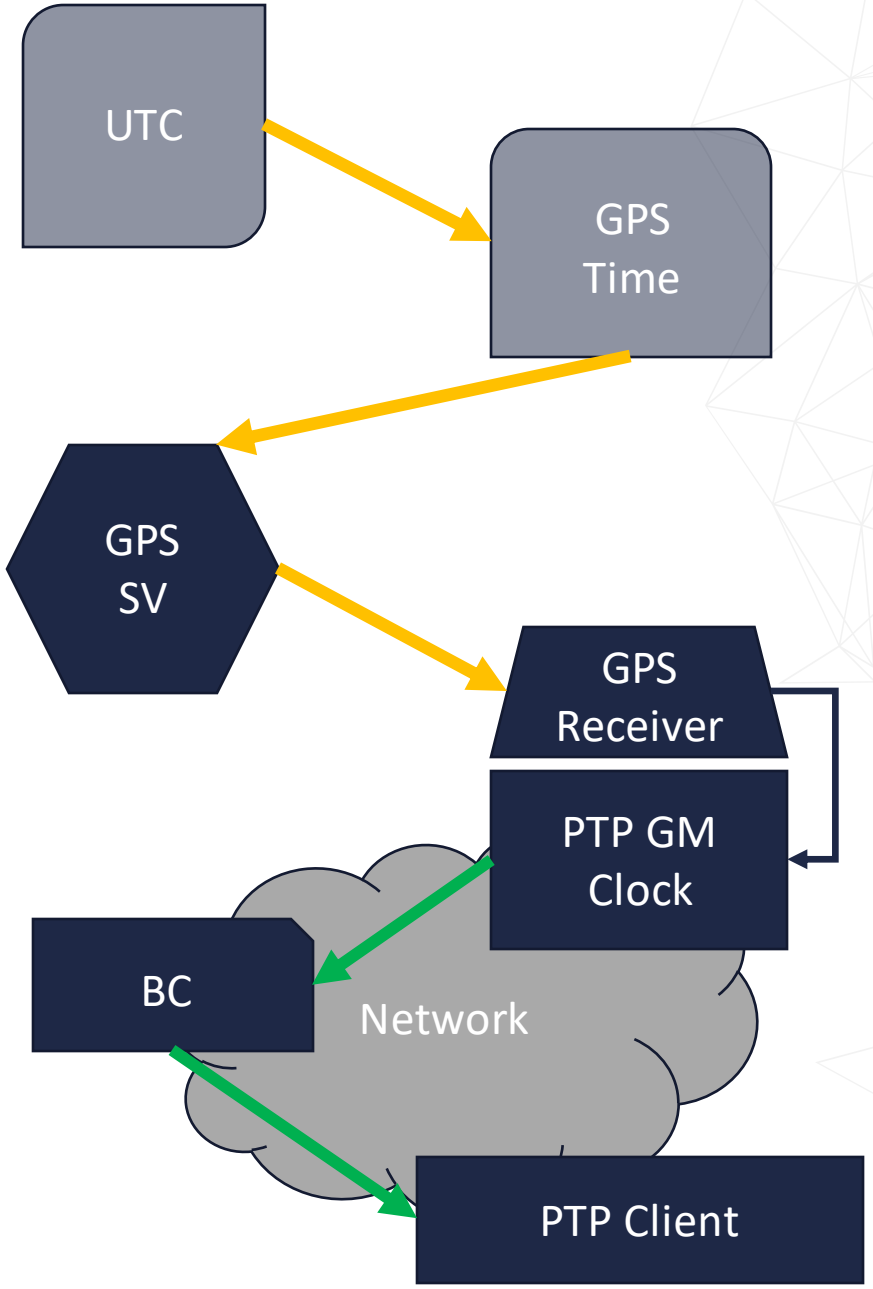
- GPS SV Clocks -> GPS receiver
  - Internal GPS receiver integrity checks/spoofing detection
  - Compare against other receivers/clocks
- GPS receiver -> PTP GM clock
  - Monitor PTP GM state (offset to GPS, clock servo parameters)
  - Compare against other clocks
- PTP GM clock -> PTP BC clock
  - Monitor PTP BC state (sync source=my GM?, port state?)
  - Monitor network traffic (rogue announce msg?)
  - Monitor/measure PTP timing on BC
- PTP BC clock -> PTP client clock
  - Monitor network traffic (rogue announce + delay msg?)
  - Monitor/measure PTP timing on client
- No defense against Delay Attacks -> Monitor delays



Mitigation / Defense

Defense against Disruptive Timing Attacks

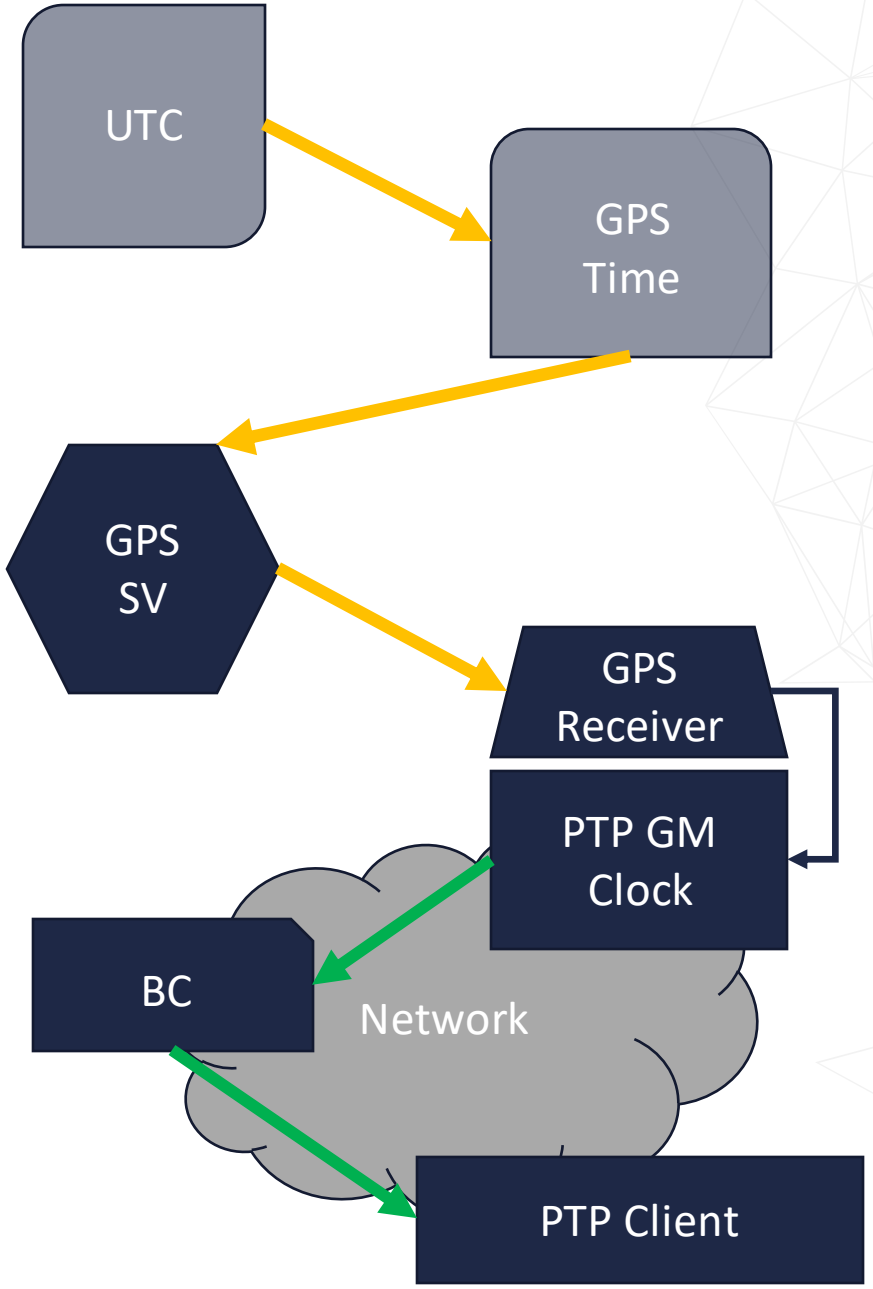
- GPS SV Clocks -> GPS receiver
  - Redundant GPS receivers in different geographic locations
  - Protection against interference/jamming
- GPS receiver -> PTP GM clock
  - Holdover
  - cybersecurity measures to harden the PTP GM clock
- PTP GM clock -> PTP BC clock
  - Holdover
  - Protect (physical) integrity of network (e.g. IEEE 802.1X)
  - Cybersecurity measures to harden the PTP BC
- PTP BC clock -> PTP client clock
  - Holdover
  - Protect (physical) integrity of network (e.g. IEEE 802.1X)
  - Cybersecurity measures to harden the PTP client



MEINBERG

Defense against Manipulative Timing Attacks

- GPS SV Clocks -> GPS receiver
  - Use multiple GPS receivers at different geographic locations
  - Use protected signals (GPS SAASM, Galileo PRS, OS-NMA)
- GPS receiver -> PTP GM clock
  - cybersecurity measures to harden the PTP GM clock
  - Use additional time sources
- PTP GM clock -> PTP BC clock
  - Protect (physical) integrity of network (e.g. IEEE 802.1X)
  - Utilize PTP security
  - Define a list of valid GMs
  - Cybersecurity measures to harden the PTP BC
- PTP BC clock -> PTP client clock
  - Protect (physical) integrity of network (e.g. IEEE 802.1X)
  - Utilize PTP security
  - Define a list of valid BCs
  - Cybersecurity measures to harden the PTP client

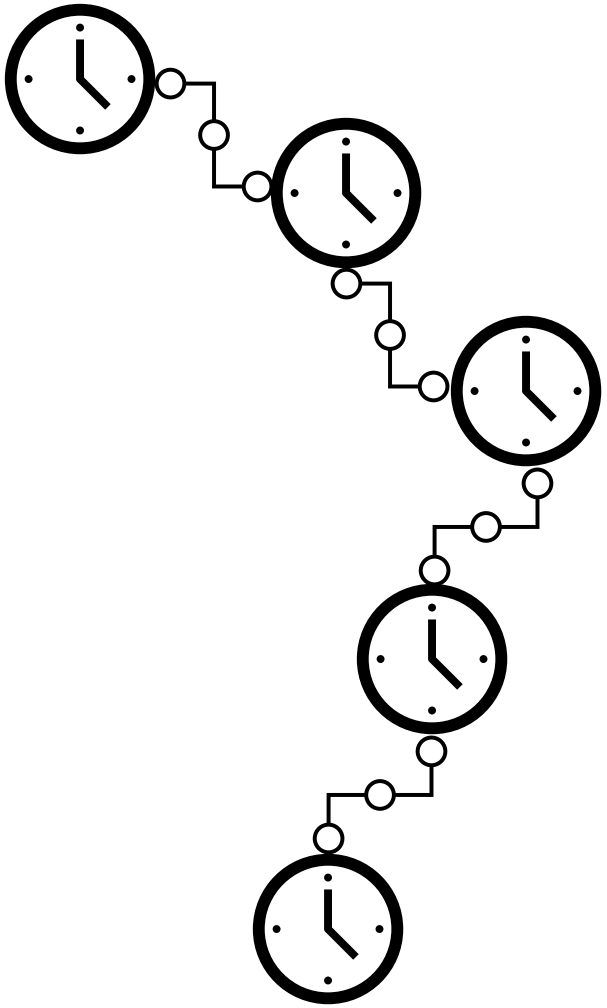


MEINBERG

Conclusions!

Conclusion

Security for Timing means Security for the Chain of Time – (almost) all parts of the chain can be attacked



- Find out your Chain of Time
- Determine potential attacks, detection methods and defense measures for each link of the chain

MEINBERG

Thank you!

Heiko Gerstung
heiko.gerstung@meinberg.de
twitter.com/hgerstung - linkedin.com/in/heikogerstung

MEINBERG
The Synchronization Experts.

WORKSHOP
ON
SYNCHRONIZATION
AND
TIMING SYSTEMS