Expecting and Detecting Compromise in Clocks

WSTS 2021

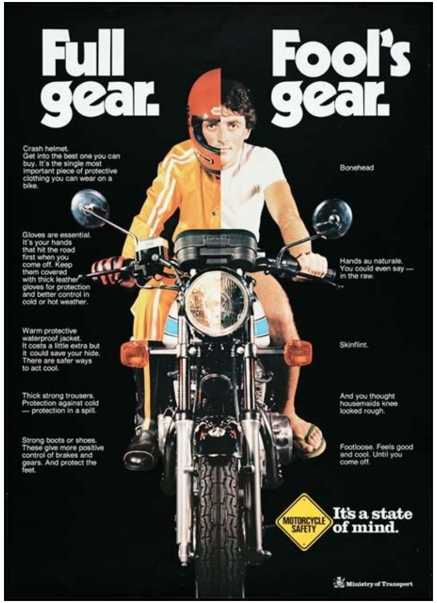
Ken Hann, Sr Director R&D

OSCILLOQUARTZ
An ADVA Company

Background and motivation

1) Critical services ~100% dependent on GNSS for timing
2) GNSS open to denial (jamming) and falsification (spoofing)
3) Spoofing is now so accessible a 12-year-old could do it.
3) Little preparation for terrestrial synchronization distribution

Two kinds of motorcyclists…



Crash helmet. Get into the best one you can buy. It's the single most important piece of protective clothing you can wear on a bike.

Gloves are essential. It's your hands that hit the road first when you come off. Keep them covered with thick leather gloves for protection and better control in cold or hot weather.

Warm protective waterproof jacket. It costs a little extra but it could save your hide. There are safer ways to act cool.

Thick strong trousers. Protection against cold — protection in a spill.

Strong boots or shoes. These give more positive control of brakes and gears. And protect the feet.

Bonehead

Hands au naturale. You could even say — in the raw.

Skinflint.

And you thought housemaids knee looked rough.

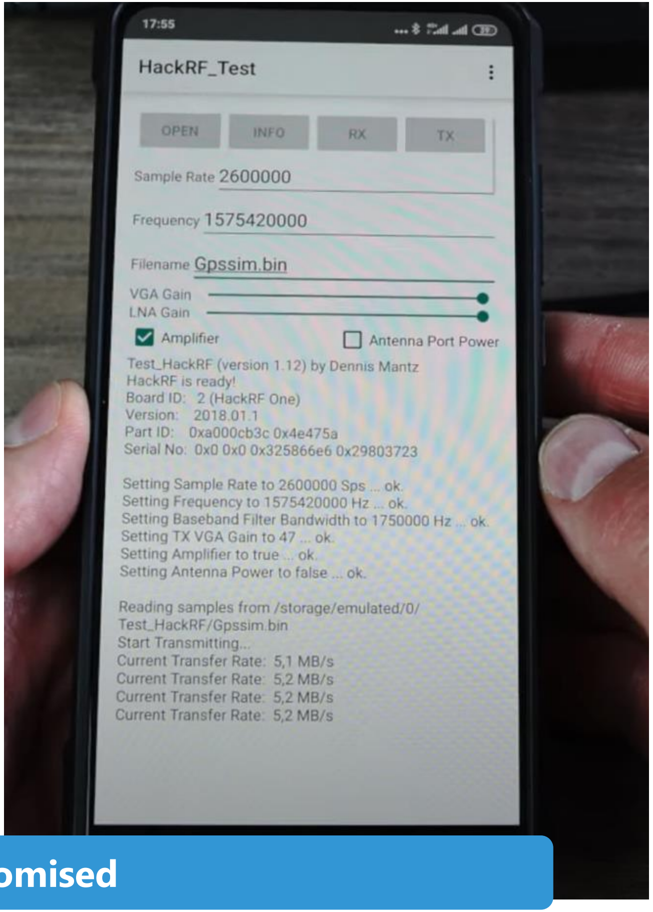
Footloose. Feels good and cool. Until you come off.

GNSS is vulnerable…
So are GNSS timing receivers

Two kinds of GNSS based clocks…

1) Those that have been compromised
2) Those thay have not yet been compromised

Dozens of "How-to" videos for GNSS spoofing a timing receiver…



17:55

HackRF_Test

Sample Rate 2600000

Frequency 1575420000

Filename Gpssim.bin

VGA Gain

LNA Gain

☑ Amplifier □ Antenna Port Power

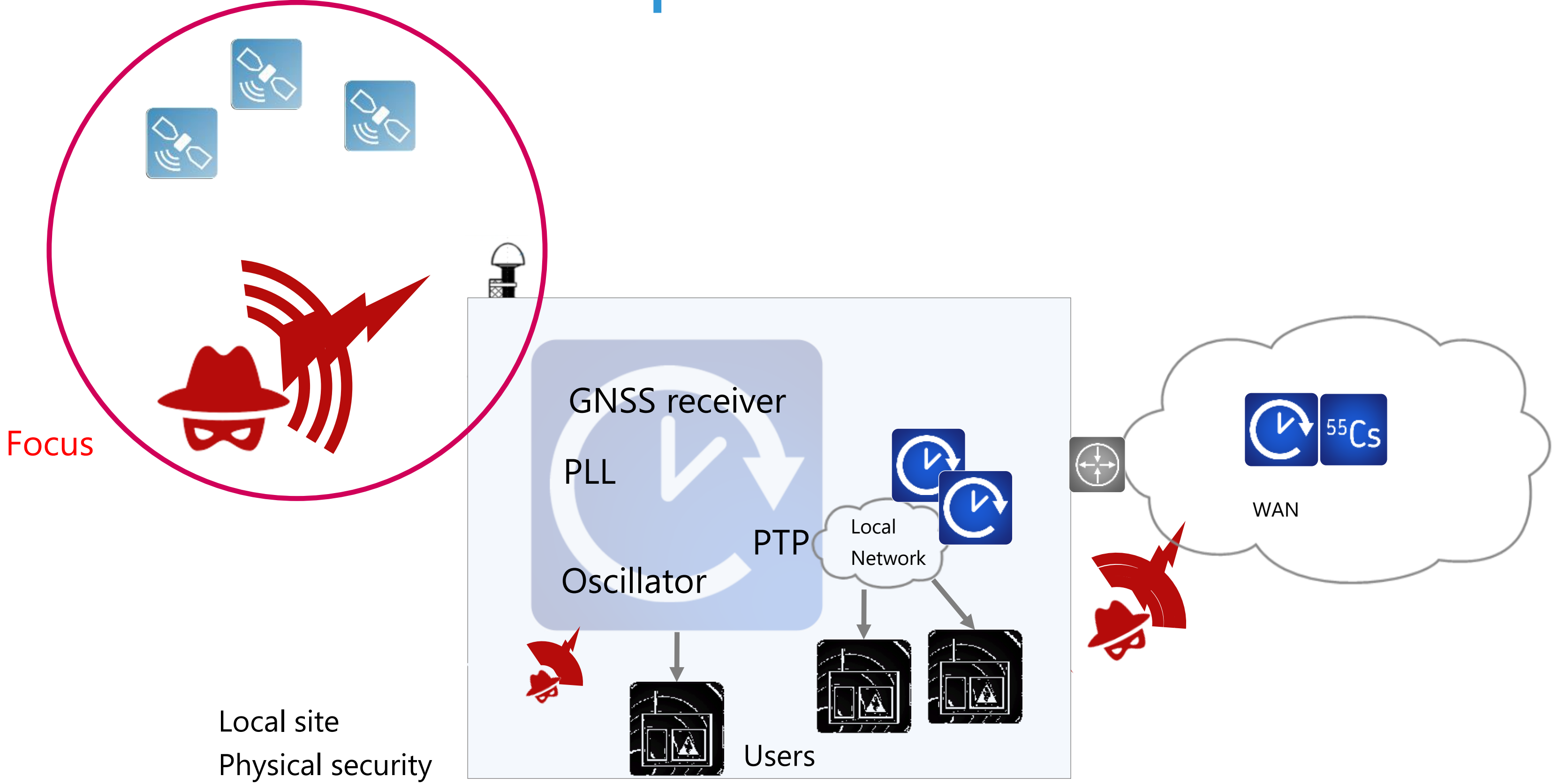
```
Test_HackRF (version 1.12) by Dennis Mantz
HackRF is ready!
Board ID:   2 (HackRF One)
Version:    2018.01.1
Part ID:    0xa000cb3c 0x4e4e475a
Serial No:  0x0 0x0 0x325866e6 0x29803723

Setting Sample Rate to 2600000 Sps ... ok.
Setting Frequency to 1575420000 Hz ... ok.
Setting Baseband Filter Bandwidth to 1750000 Hz ... ok.
Setting TX VGA Gain to 47 ... ok.
Setting Amplifier to true ... ok.
Setting Antenna Power to false ... ok.

Reading samples from /storage/emulated/0/
Test_HackRF/Gpssim.bin
Start Transmitting...
Current Transfer Rate:  5,1 MB/s
Current Transfer Rate:  5,2 MB/s
Current Transfer Rate:  5,2 MB/s
Current Transfer Rate:  5,2 MB/s
```

Expect that GNSS will be compromised

How is the clock compromised?



Expecting compromise… Preparing for attack

1) Adopt GNSS monitoring (simple and fast management overlay)

Refer to the talk by Nir laufer

Advanced Monitoring and Troubleshooting of Large Scale GNSS Antennas Installation

2) Spoof and Jam your own clocks (controlled experiment, collect data)

Were the events detected? How? Did the clock recover, or did it require reset?

3) Evaluate impact

Only Local service impacted or also Neigherboring services?

4) Plan for Improved resiliency (step-by-step)

Detecting Compromise... (know what to look for)

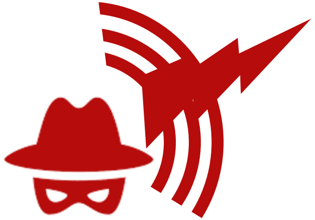
Clocks contain a GNSS modules/chips.
API for management and monitoring, but...

Typically GNSS modules:

1) Do not reliably report spoofing and jamming attacks (limited resources).
2) May not autorecover from the attack. Worst case - require reboot.

External GNSS monitoring gives visability of attacks

Possible outcomes of attack



Remain Locked to Valid GNSS (not impacted of spoofing attempt)

Clock in Holdover (or backup) waiting for attack to subside

Spoofed = clock Locked to Fake GNSS

Spooked = panic and unnecesssary Holdover

Jammed = necessary Holdover (no valid signals)

Spoofing and jamming as part of a wider attack

Huge number of options…

Jamming + Spoofing

- Jamming reduces valid signals “forcing” receiver to accept spoofing signals
- Spoof one constellation, then jam the other constellations
- Jam L2 signals, then spoof L1 signals
- Spoofing signal active at reboot. Could be accepted without question as a valid.

…

- Coordinated attacks e.g. national level 100’s of spoofers. ($300 per device)

Improving GNSS resiliency is essential, but insufficient

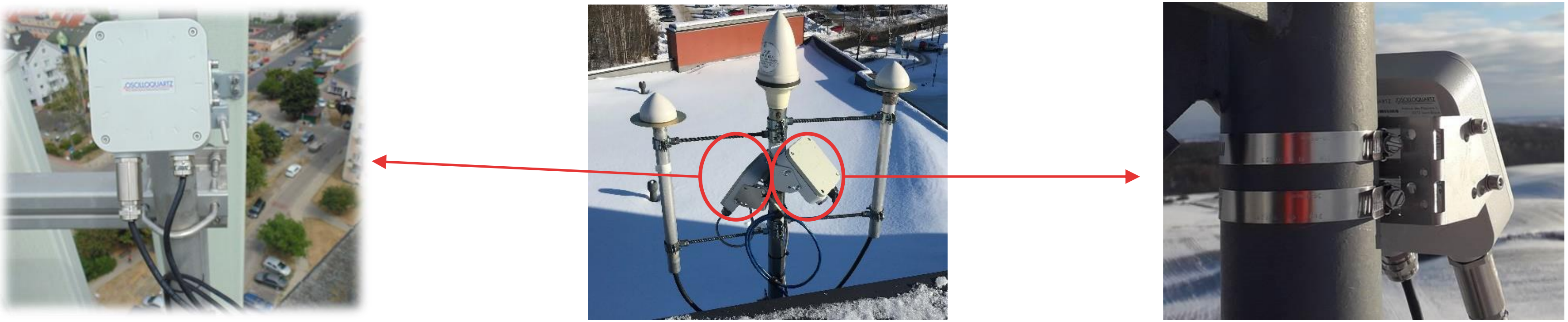
Preventing compromise – Improving resiliency

1) Physical diversity (LAN)
2) Multiband Receivers
3) Terestrial time distribution (WAN)
4) National initiatives?

Refer to the talk by Nino De Falcis

GPS/GNSS Jamming & Spoofing Mitigation Best Practices & Strategies

Most GNSS disturbances are localized - Diversity across Building or campus increases resiliency



- Timing network provides timing resiliency
- Networks can be small scope or wide (LAN/WAN…)
- Smart antennas with fiber can reach many kilometers

Smart antennas provide easy diversity

Multiband provides some additional resiliency

Main feature of Multiband is high accuracy
PRTC-B (40ns) accuracy

Multiband receivers have improved resilency:

1) Newer sw with some degree of spoofing detection
2) Additional bands which may provide improved resiliency

Multiband alone does not prevent Jamming and Spoofing

Cesium provides extended holdover (ePRTC)
(for Core Time base sites)

ePRTC with Cesium backups

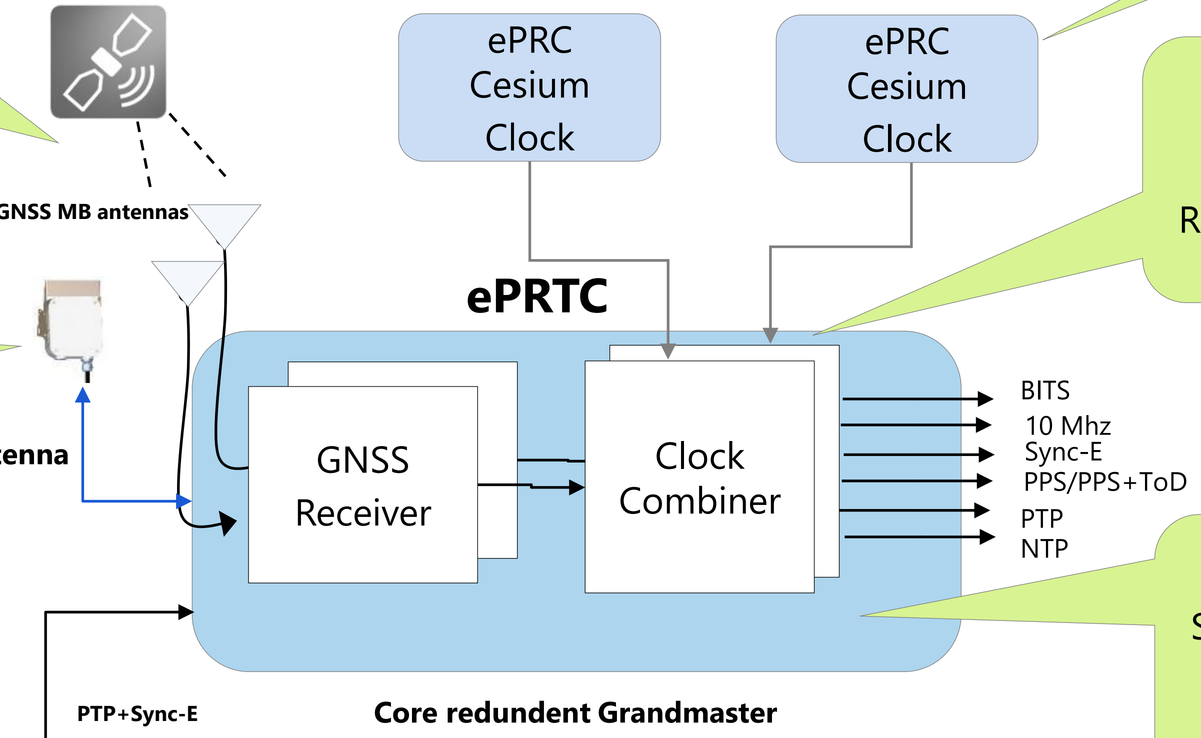
Multi band , multi constellation GNSS

Advanced jamming and spoofing detection

Backup from peer site

carrier grade fully Redundant HW

Sync and GNSS assurance



OSCILLOQUARTZ An ADVA Company

Typical network timing hierarchy

Core time base network

Single-digit number of locations for large operator

ePRTC enabled, TE ≤ ±**30ns**

Aggregation network

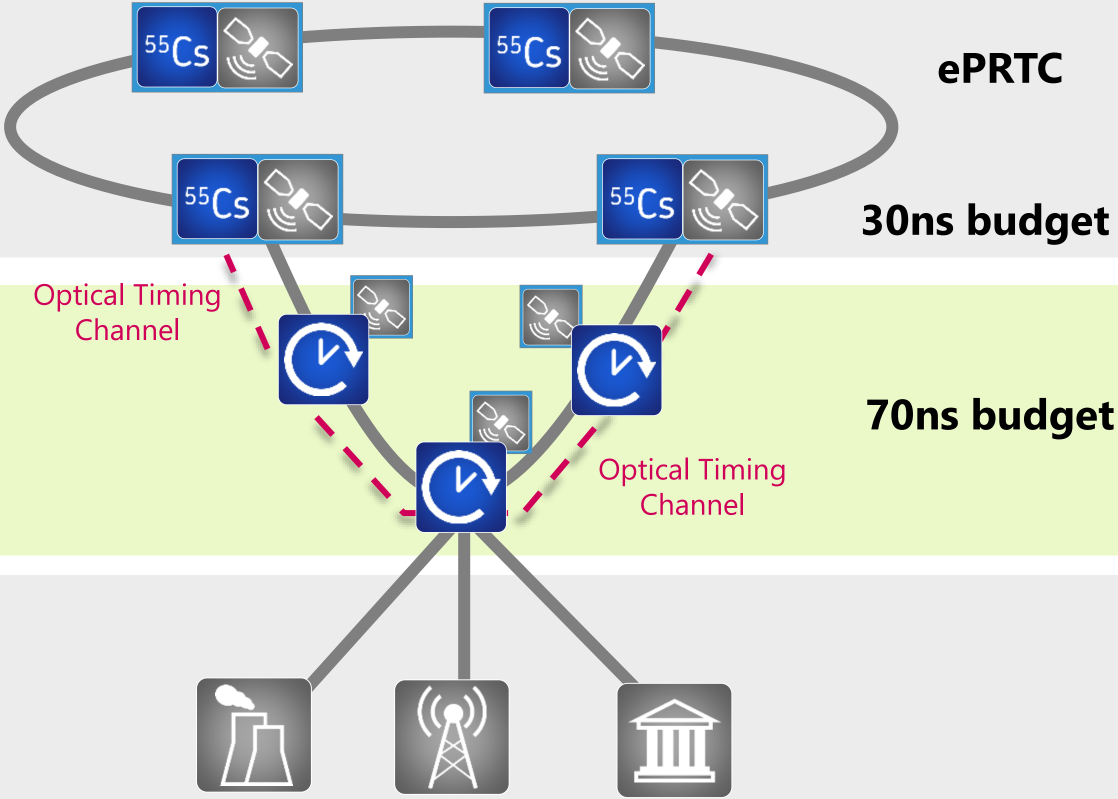
Hundreds of locations for large operator

PRTC enabled, TE ≤ ±**100ns**

Feeders to end application

Thousands of locations for large operator

TE ≤ ±**1100ns**



OSCILLOQUARTZ An ADVA Company

Summary – GNSS is too big to fail !!!

1) Wake up, and Evaluate the threats on existing networks!

2) Use network level GNSS monitoring

   -> Gives visability on GNSS receiver behavour

   -> Use real ”jamming/spoofing” experiments (cf. military exercises)

3) Improve timing resiliency with hierarchical timing networks

Selecting the right wave improves packet clock performance

Thank You

OSCILLOQUARTZ
An ADVA Company

Thank you

Khann@adva.com

IMPORTANT NOTICE

The content of this presentation is strictly confidential. ADVA is the exclusive owner or licensee of the content, material, and information in this presentation. Any reproduction, publication or reprint, in whole or in part, is strictly prohibited.
The information in this presentation may not be accurate, complete or up to date, and is provided without warranties or representations of any kind, either express or implied. ADVA shall not be responsible for and disclaims any liability for any loss or damages, including without limitation, direct, indirect, incidental, consequential and special damages, alleged to have been caused by or in connection with using and/or relying on the information contained in this presentation.