THE VULNERABILITY OF GNSS TIMING RECEIVERS TO SPOOFING ATTACKS

Tim Frost and **Guy Buesnel**

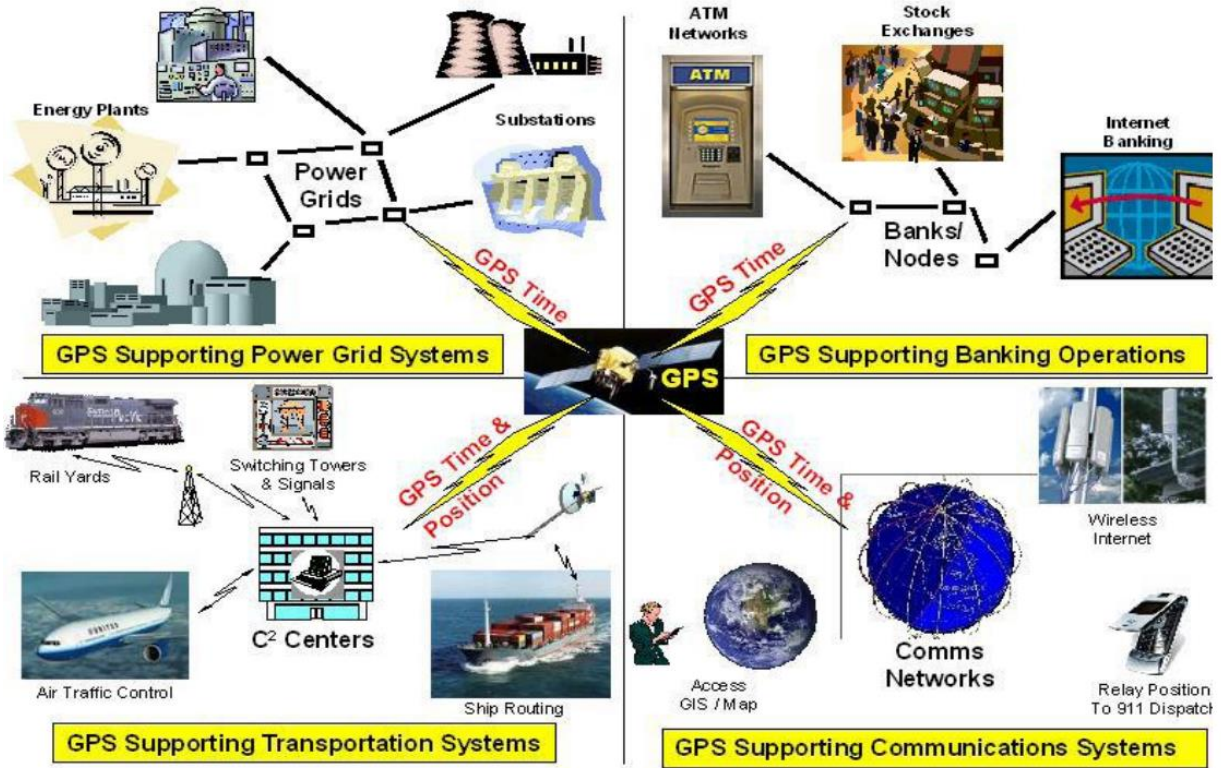
www.calnexsol.com
www.spirent.com

Calnex

Introduction

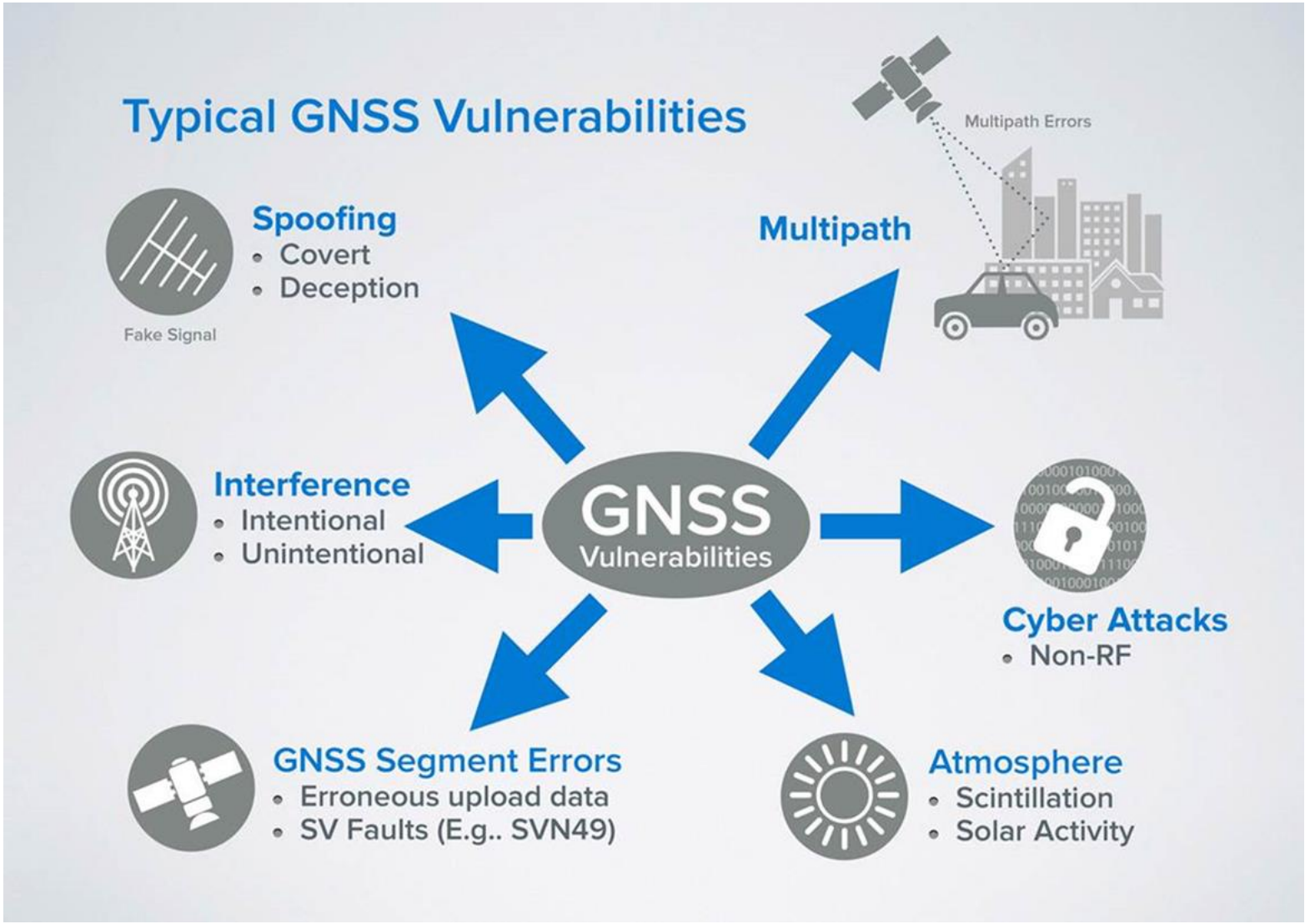
Dependence on GPS timing

- US Department of Homeland Security:
  "15 of the 19 Critical Infrastructure & Key Resources Sectors have some degree of GPS timing usage"



Source: http://www.gps.gov/multimedia/presentations/2012/10/USTTI

Overview of GNSS Vulnerabilities

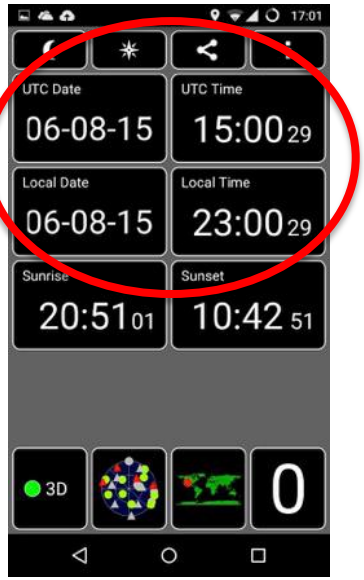


GPS disruptions and Timing…

- Two Chinese Researchers (Huang and Yang) built a low cost SDR spoofer
- Demonstrated how this device could spoof position and date/time
- Here a car parked in an underground car-park is reporting its position as the middle of a lake!
- All the code needed to programme the SDR was freely available on the internet

GPS disruptions and Timing…

- Huang and Yuang also spoofed some well-known smart phones…
- The Cellphone clock was spoofed to display wrong date/time with auto-calibration enabled !!
- One Cellphone ended up displaying a time and date in the future –



First time (known) that non-GPS specialists have spoofed navigation signals successfully

Types of spoofing attack

- For reference and further reading:

- Multi/Single channel (loosely synchronized) with smooth deception signal
  - The attacker creates one or more deception signals starting with an initial offset between 500 to 600 metres and an attenuation of 10 dB.
  - A pseudorange ramp decreases the code delay (you must take into account the bandwidth of the receiver PLL when you determine the pseudorange ramp speed). When the code delay is close to zero, increase the strength of the deception signal to force the receiver correlator to lock on to the new, false, signal.
- Multi/Single channel (loosely synchronized) with fixed Doppler offset
  - This attack is the same as before, but the deception signal does not change its Doppler. The code/carrier delay (with respect to the Line of Sight) changes in steps of 5 to 10 metres, or uses a pseudorange ramp
- Multi/Single channel (tightly synchronized)
  - The deception signal is generated with an initial code delay (with respect to the Line of Sight) of few metres. The strength of the deception signal slowly increases, starting with an initial attenuation of 5 to 10 dB. The deception signal then slowly moves away from the Line of Sight, causing a position shift and avoiding the loss of lock.
- Sinusoidal deception signal
  - The deception signal attempts to attack more than one receiver in a given area by changing the code and signal strength with a sinusoidal pattern.
- Jam rather than spoof
  - To avoid detection of an attacking signal based on signal strength or tracking function and then forcing the receiver to shift to acquisition state, you can perform a jamming attack before the spoofing attack (for example, signal record and replay, signal simulation and loosely synchronized spoofing) resulting in loss of code lock
- Navigation data modification (Available for GPS L1 and Galileo E1 only)
  - The deception signal degrades the position calculated by the receiver by changing the content of the navigation messages used in the position calculation.
- Data replay attack
  - The deception signal is generated by replaying data from space, in order to cheat any detection based on space data authenticity verification.

How to detect spoofing in a receiver

- Power Levels
  - The spoofing signal is likely to have a noticeably higher power level
- Monitor position
  - If a fixed timing receiver starts “moving”, there’s a problem!!
- Bound and Compare range rates
  - Code and Carrier range rate changes will be different for a spoof signal
- Doppler Shift Check
  - Doppler shift is likely to be incorrect with a spoofer in a fixed location
- Verify Received Navigation Data
  - Compare Almanac/Ephemeris to known data
  - Check for ‘missing/default’ Navigation data
- Jump Detection
  - Observable should remain within a tolerable range, check for sudden changes

Calnex

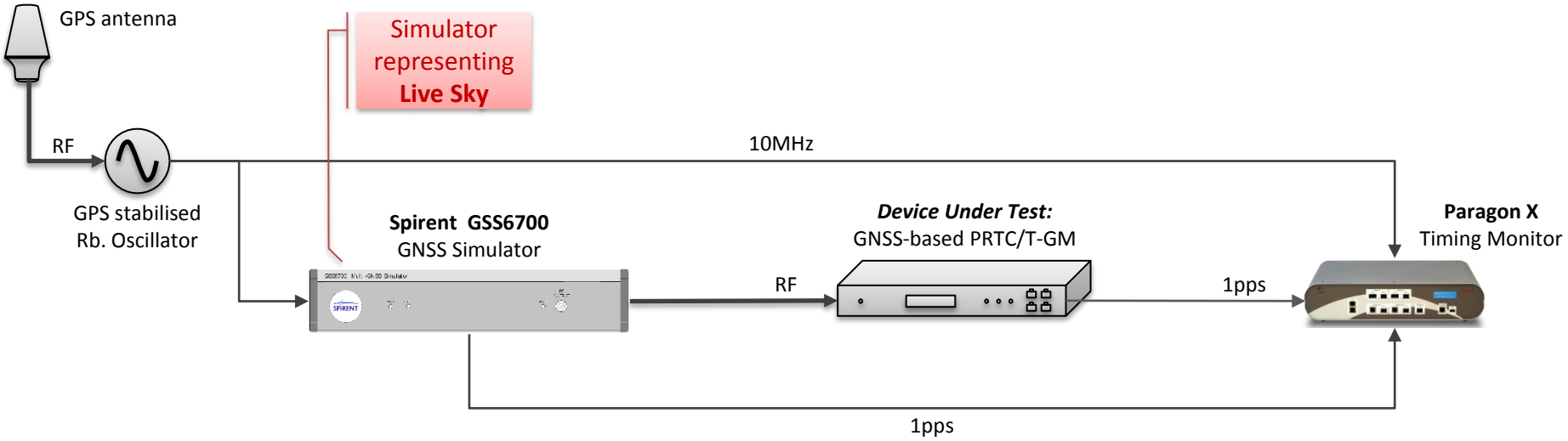
Experimental Results

Test 1: Pseudo-range Ramp

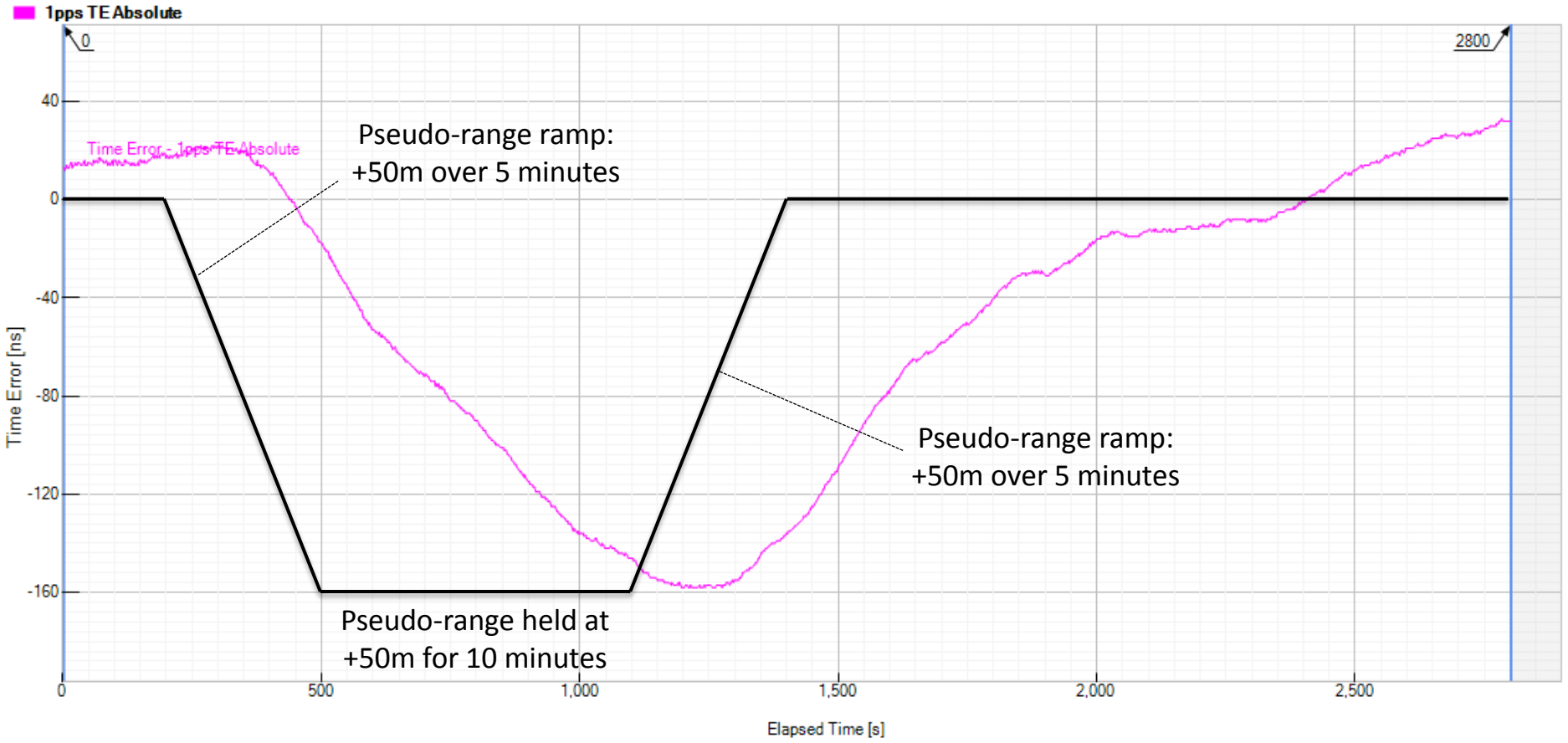
- Pseudo-range allows the receiver to calculate its distance from the satellites
- Changing the pseudo-range on one satellite will affect the receiver's position calculation
  - The satellite will appear to be either closer to or further away from the receiver than it actually is
- Changing the pseudo-range on all satellites keeps position stable, but affects the receiver's time calculation

- **Test applied:** gradually change the pseudo-range on all satellites and monitor effect on the receiver

Experimental Setup 1: Pseudo-range Ramp



Device A: Response to Pseudo-Range Ramp



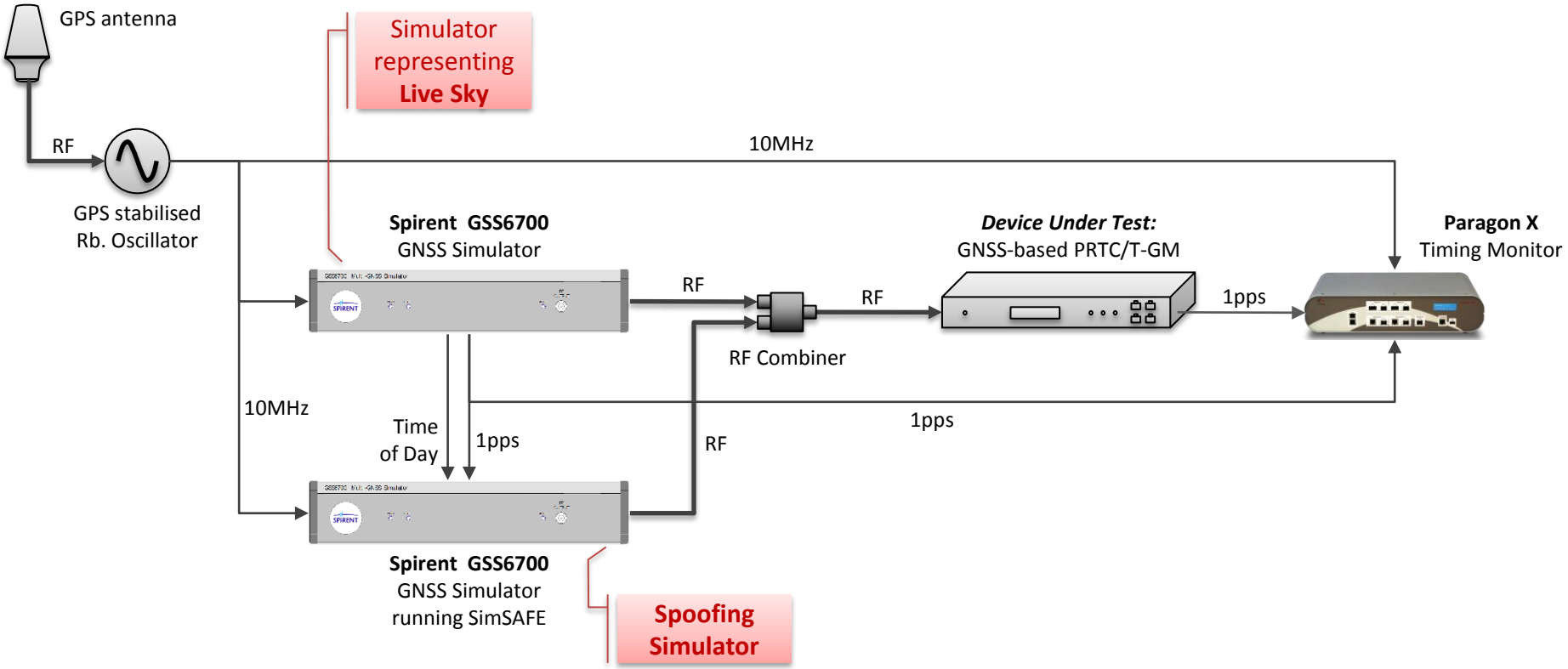
- Devices B and C showed similar responses

Test 2: Spoofing from Simulator

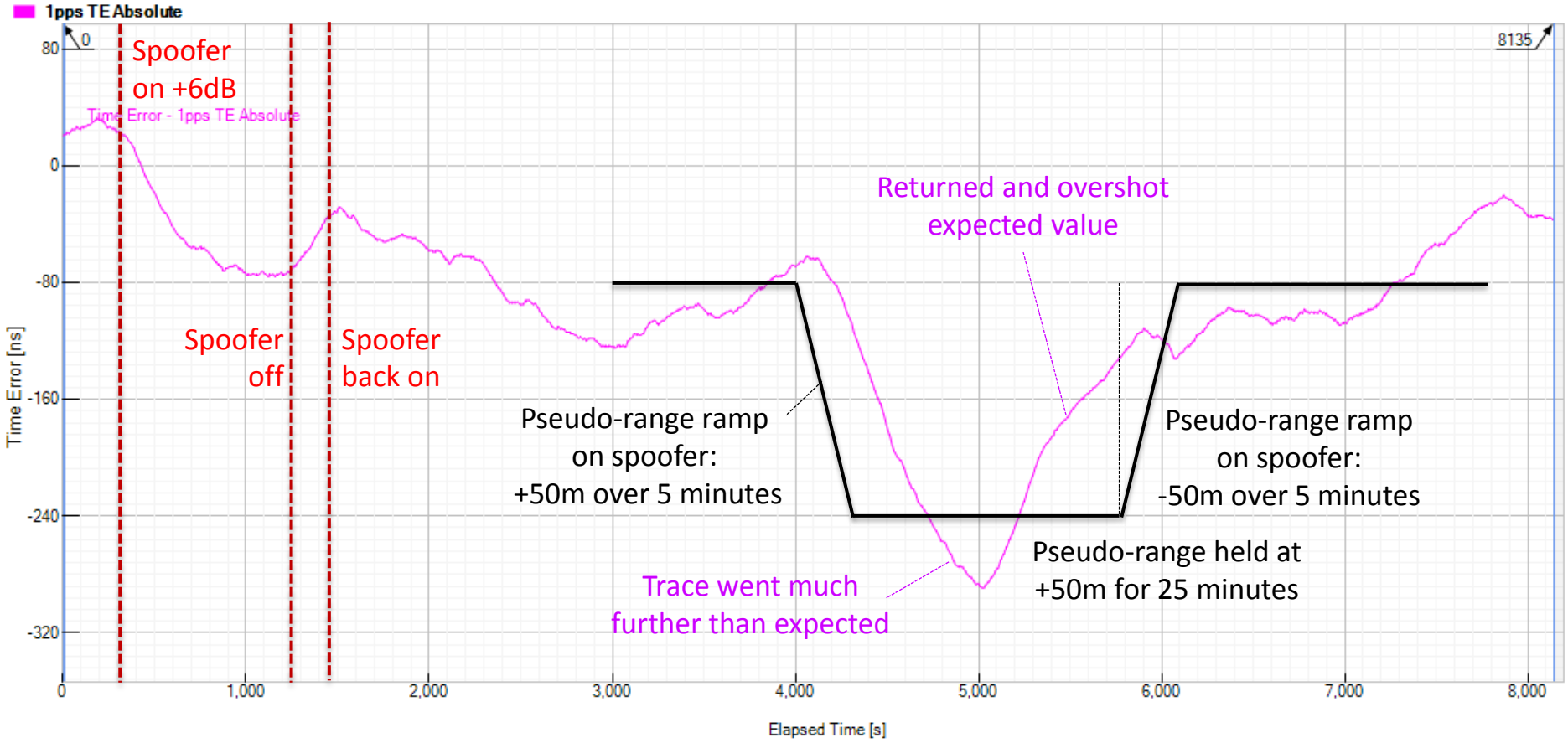
Calnex

- Test 1 didn't involve spoofing at all – it was just a test to see if the time could be manipulated
- Test 2 involves turning on a second simulator
  - Simulator 2 will be at slightly higher power (+6dB)
  - Simulators are synchronised together in position and time, so should be providing the same information
  - Objective is to see if the second simulator "takes over" the receiver
- Next step is to apply a pseudo-range ramp on the second simulator to see if it drags away the time of the receiver

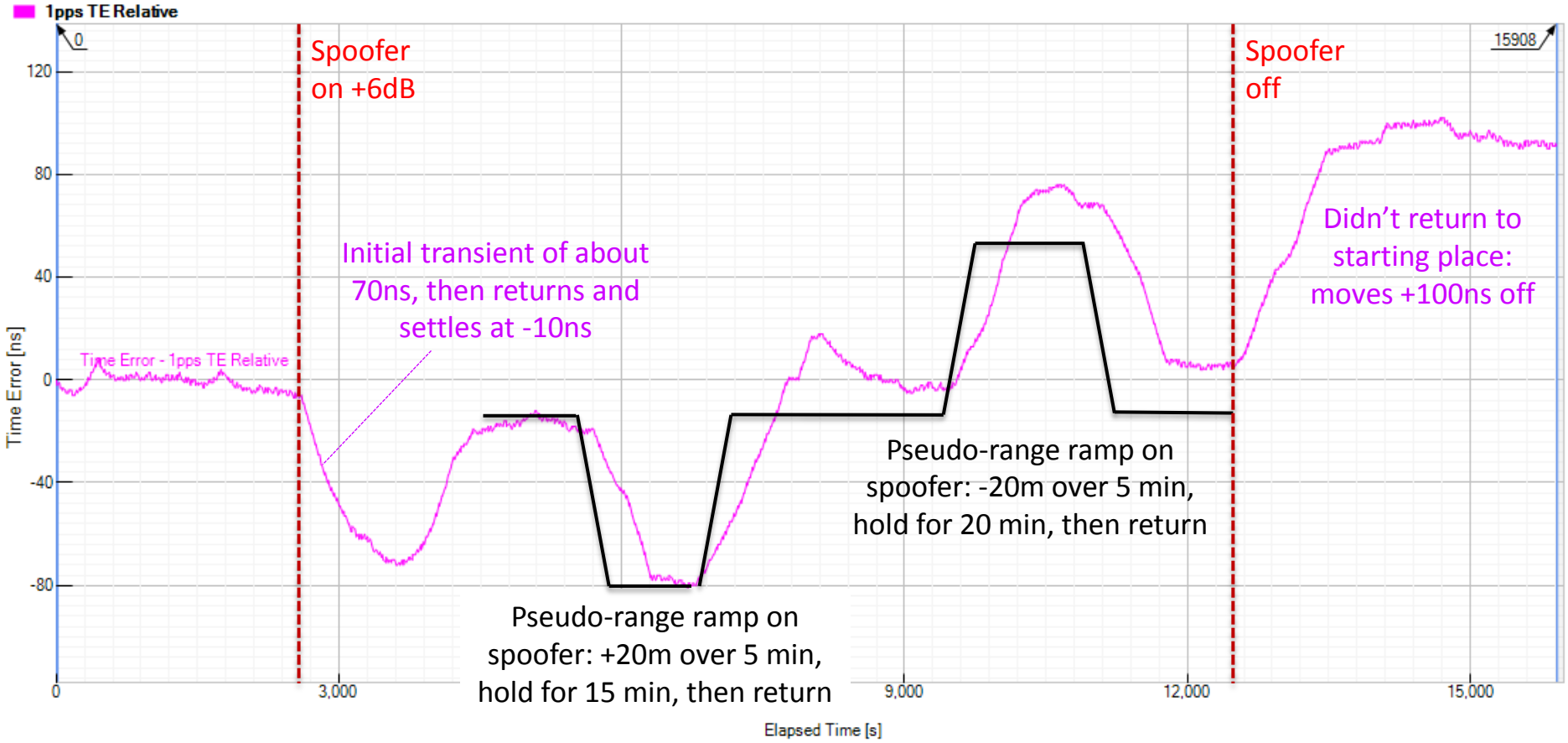
Experimental Setup 2: Spoofing from simulator



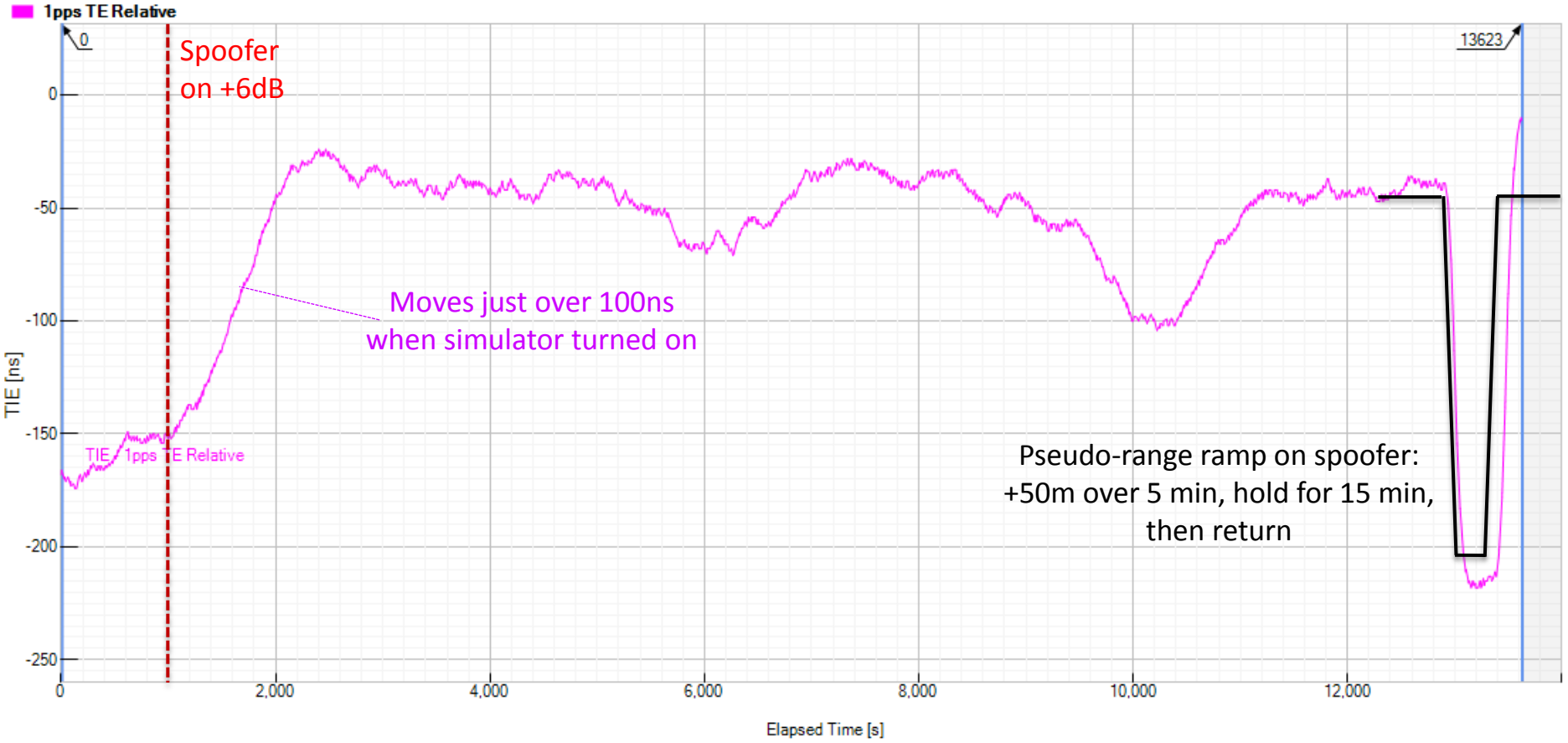
Device A: Spoofing from Simulator



Device B: Spoofing from Simulator



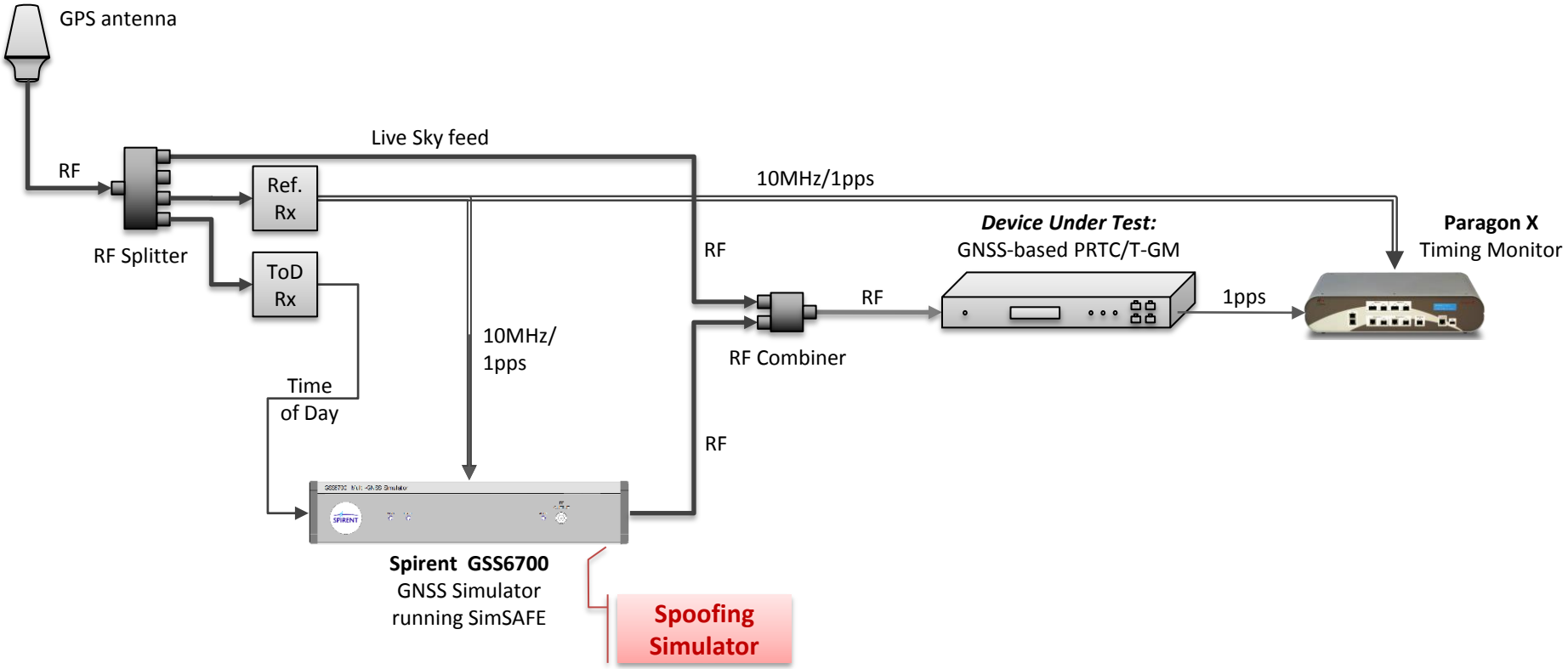
Device C: Spoofing from Simulator



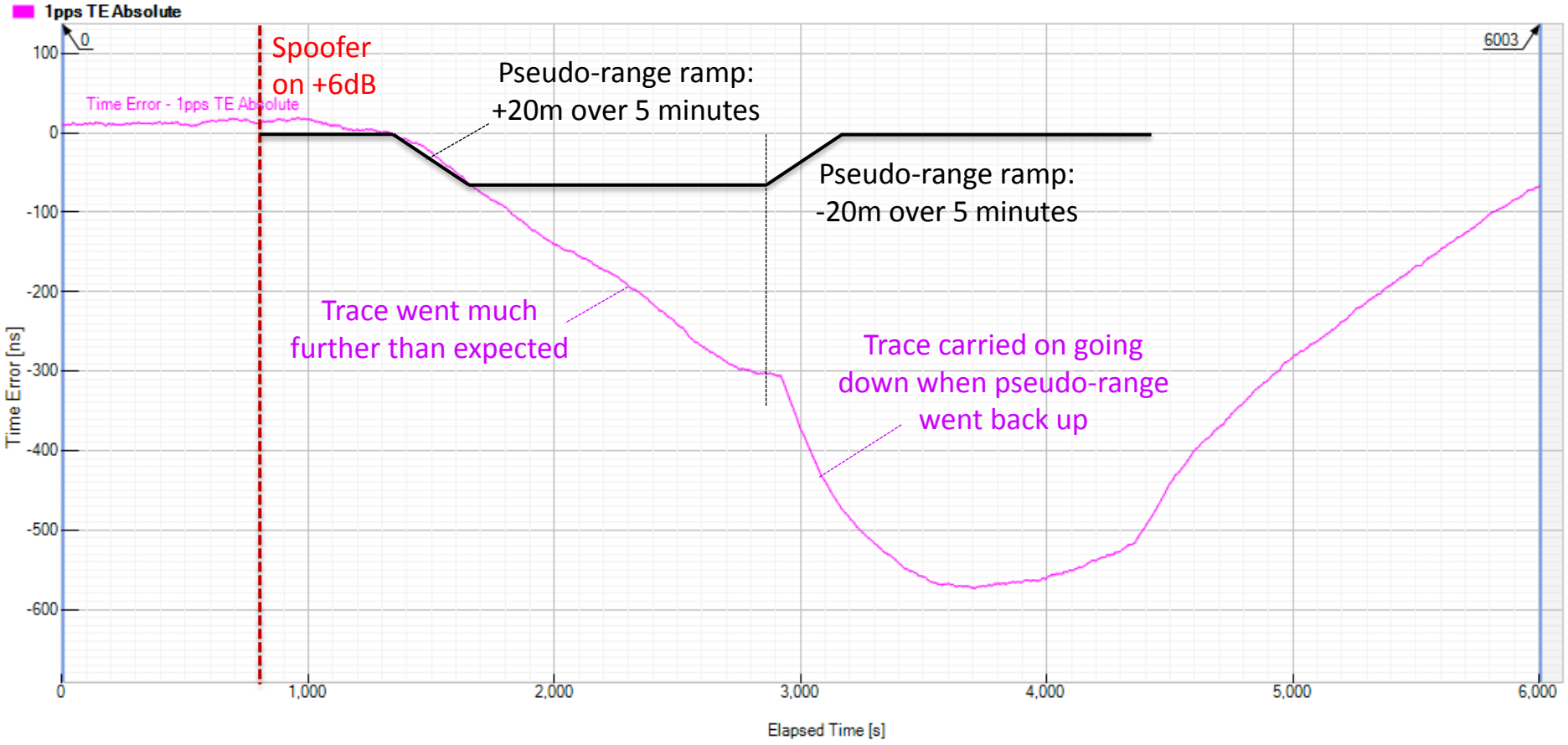
Test 3: Spoofing from Live Sky

- Test 2 was spoofing one simulator with another
- “Live sky” is more challenging, since the conditions are much less controlled
- Test 3 involves trying to spoof a live signal, and move the time of the receiver away from current time

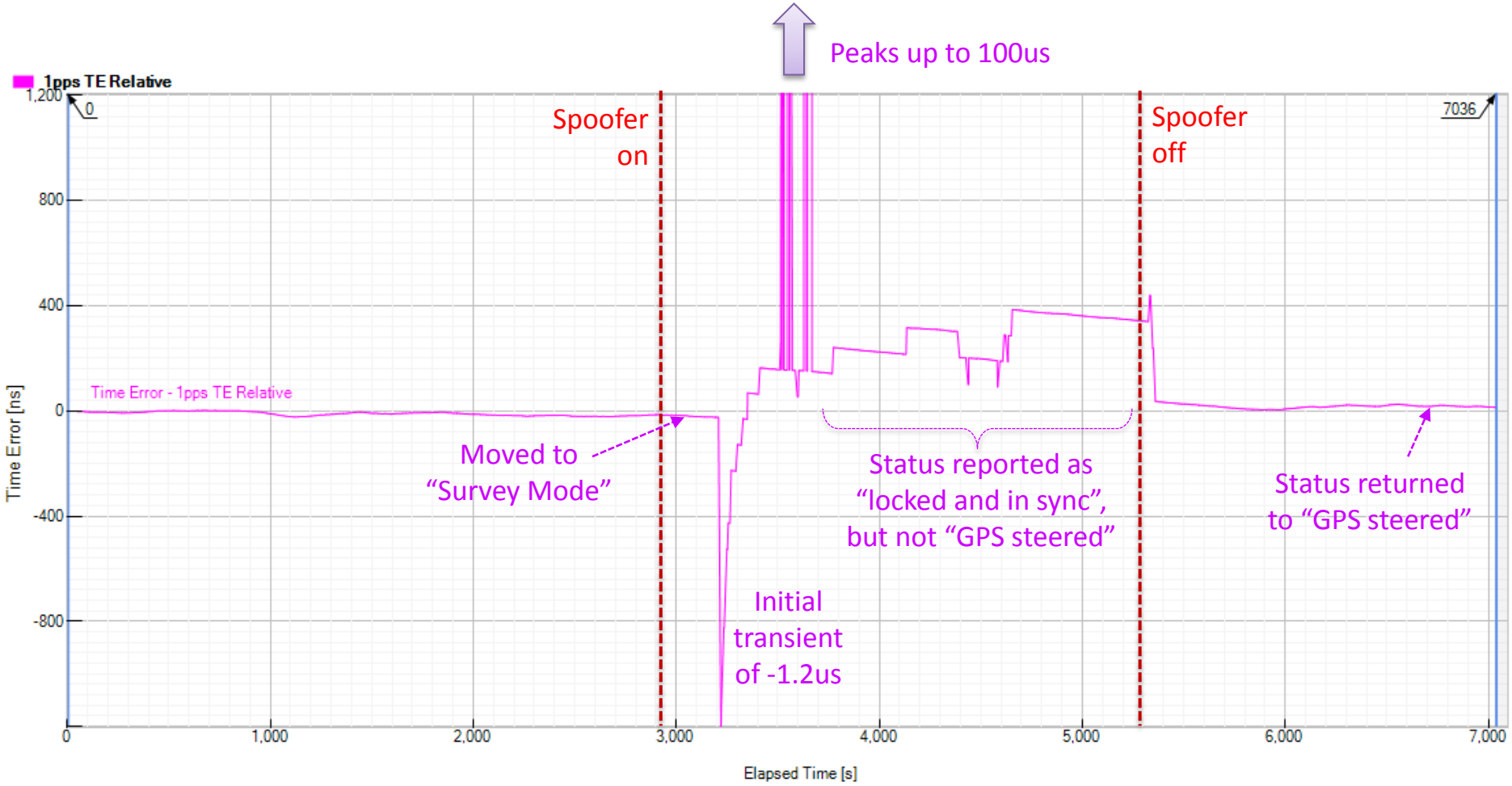
Experimental Setup 2: Spoofing from Live Sky



Device A: Spoofing from Live Sky



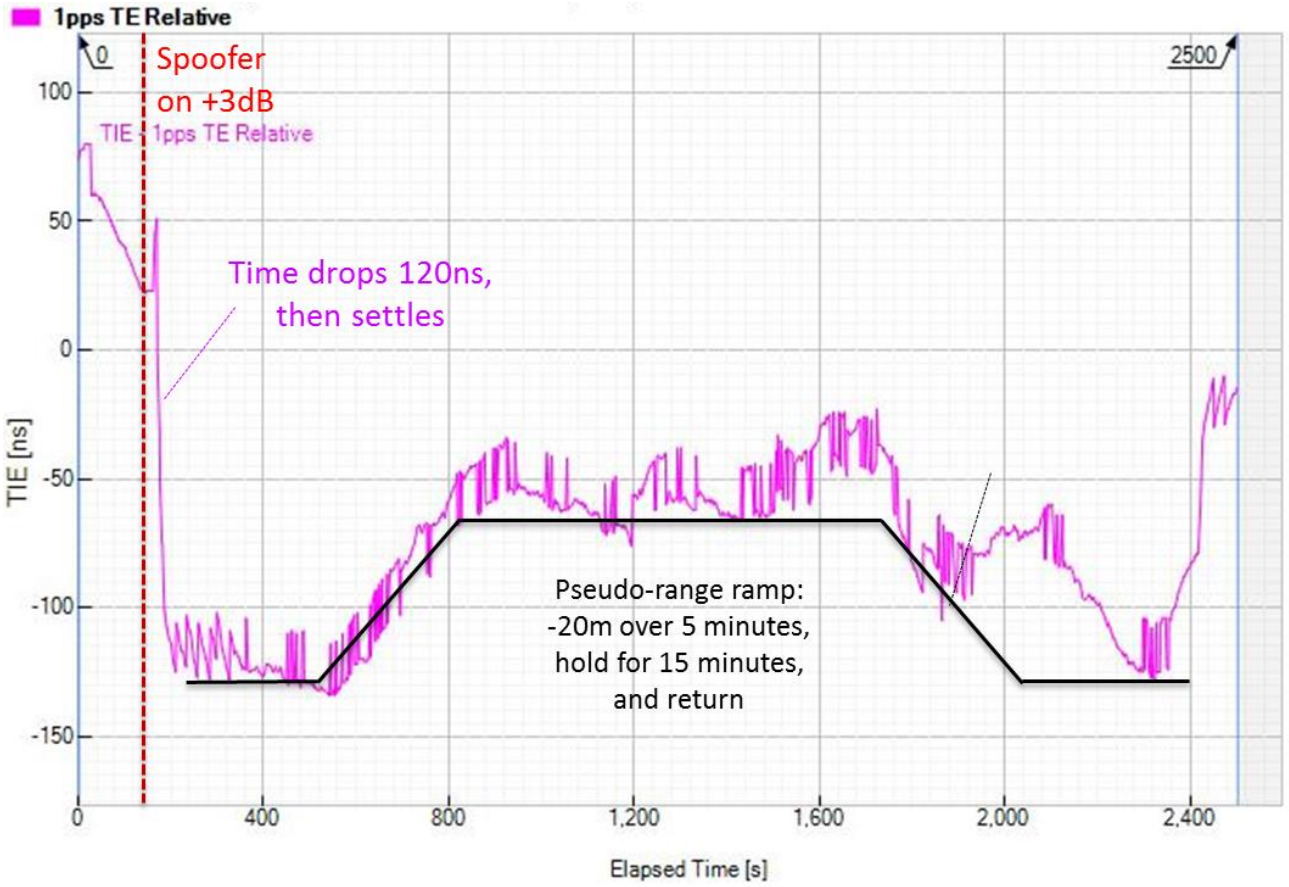
Device B: Spoofing from Live Sky



Device C: Spoofing from Live Sky

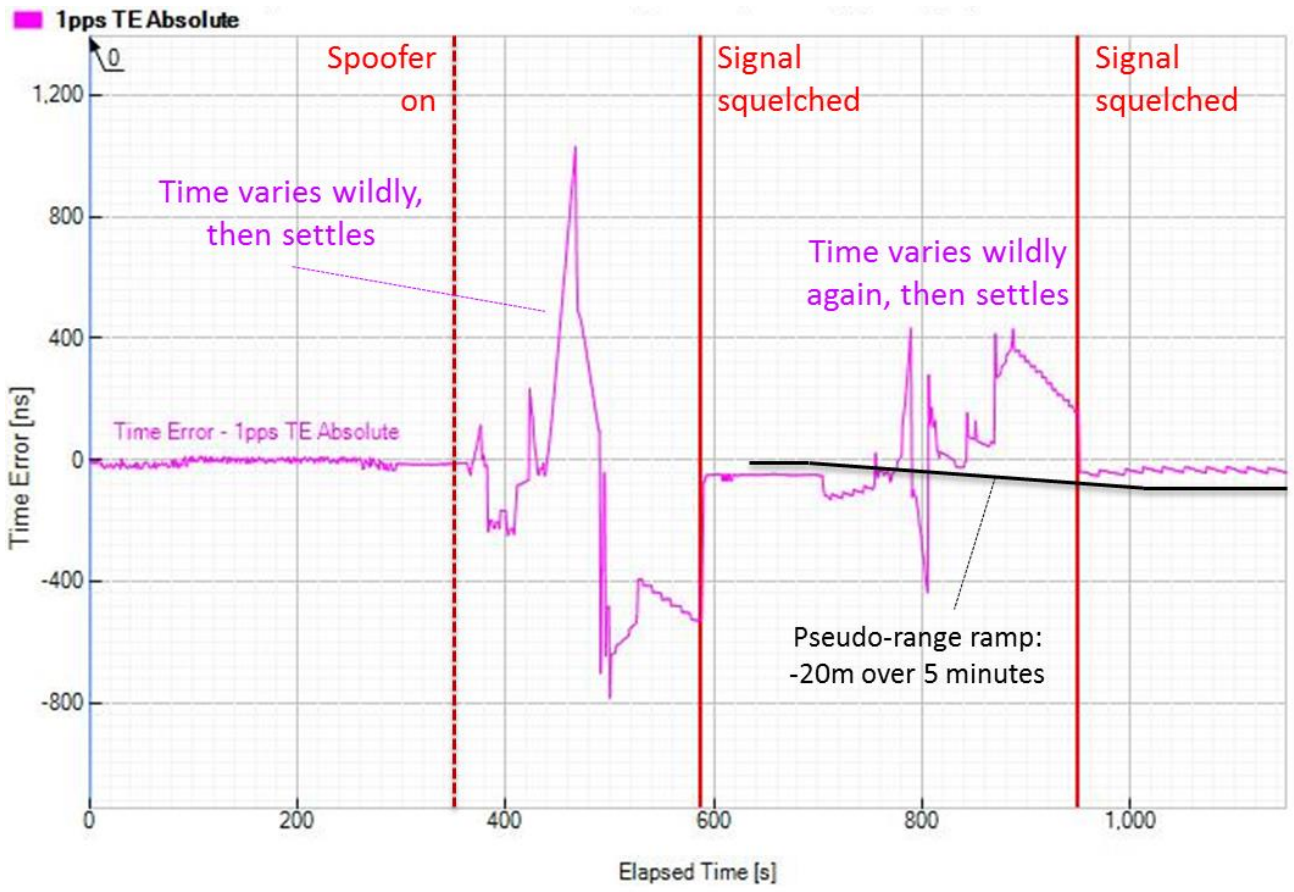
- Used rooftop antenna for better live signal, captured full orbital file overnight to align spoofer more accurately to live signal

Device D: Spoofing from Live Sky



- RAIM and multipath detection turned OFF

Device D: Spoofing from Live Sky



- RAIM and multipath detection turned ON

Conclusions

- Spoofing from live-sky proved more difficult than the simulation initially
  - Once power levels (live sky and simulated) were aligned it was straightforward to tweak the simulated power level in order to take over the target receiver
- There are warning signs in the receiver that a spoofing attack is in progress
  - Testing response of existing systems important – especially as a crude attack can cause unexpected behaviour
- **Know your system:**
  - ***Risk Assessment***: understand exposure to threats, likely impacts and system behavior
  - ***Testing***: test against realistic threat vectors to highlight unexpected system behavior
  - ***Develop Defence Strategies***: Use the information from test/audit to design the most applicable defence strategies and to set alarm/alert thresholds
- Use of complementary or back-up systems is important
  - Use of holdover when uncertain over authenticity of signal
  - Redundancy (e.g., e-LORAN as a complementary system, PTP as a non-wireless based approach)

Thank you for listening!

Tim Frost, Calnex Solutions,
tim.frost@calnexsol.com

Guy Buesnel, Spirent,
guy.buesnel@spirent.com

The following people all helped to make this experiment possible:

- Fabio Simon-Gabaldon – Spirent
- Richard Boyles – Spirent
- Charles Curry – Chronos
- Richard Elsmore – Chronos
- Duncan Davidson – Calnex

Wednesday Night Magic

Live at the Gala Dinner – don’t miss it!