Introduction
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

Typical GNSS Vulnerabilities

- **Spoofing**
  - Covert
  - Deception

- **Interference**
  - Intentional
  - Unintentional

- **GNSS Segment Errors**
  - Erroneous upload data
  - SV Faults (E.g., SVN49)

- **Atmosphere**
  - Scintillation
  - Solar Activity

- **Multipath**

**Cyber Attacks**
- Non-RF
DEFCON 23 - Huang and Yuang built a low cost SDR spoofer

- Tried it out on two brand leading 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 – and ended up “bricked”

First time (known) that non-GPS specialists have spoofed navigation signals successfully
And then in 2016 Pokemon GO suddenly spawned GPS spoofing as a mainstream attack....

- In weeks evolved from application layer spoofing (jailbreaking operating system of mobile phone and installing a fake GPS application) – to full on meaconing and using SDR spoofing
- Motivations: Financial Gain - sale of high value user accounts on the internet, Luring players to a location where they could be robbed
Main Types of spoofing attack

- Multi/Single channel (synchronized) with smooth deception signal
- Sinusoidal deception signal (targets more than one receiver)
  - “smart” jammer
- Jam than spoof
  - Forces receiver into acquisition mode
- Navigation data modification
- Data replay attack (Meaconing)
  - Can 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 data should remain within a tolerable range, check for sudden changes
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

- **Spirent GSS6700 GNSS Simulator**
- **Device Under Test**: GNSS-based PRTC/T-GM
- **Paragon X Timing Monitor**

**Connections**:
- Rb. Oscillator
- 10MHz
- RF
- 1pps

**Simulator representing Live Sky**
Device A: Response to Pseudo-Range Ramp

- Pseudo-range ramp: +50m over 5 minutes
- Pseudo-range held at +50m for 10 minutes
Test 2: Spoofing from Simulator

• 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

- Rb. Oscillator
- Spirent GSS6700 GNSS Simulator
- Paragon X Timing Monitor
- Device Under Test: GNSS-based PRTC/T-GM
  - RF Combiner
  - 10MHz
  - 1pps

Simulator representing Live Sky

Spoofing Simulator

Spirent GSS6700 GNSS Simulator running SimSAFE
Device A: Spoofing from Simulator

- Spoofer off
- Spoofer back on
- Pseudo-range ramp on spoofer: +50m over 5 minutes
- Pseudo-range held at +50m for 25 minutes
- Pseudo-range ramp on spoofer: -50m over 5 minutes
- Trace went much further than expected
- Returned and overshot expected value

Spoofer on +6dB
Device B: Spoofing from Simulator

Pseudo-range ramp on spoofer: +20m over 5 min, hold for 15 min, then return

Initial transient of about 70ns, then returns and settles at -15ns

Pseudo-range ramp on spoofer: -20m over 5 min, hold for 20 min, then return

Didn’t return to starting place: moves +100ns off

Spoof on +6dB

Spoof off
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 3: Spoofing from Live Sky

**Device Under Test:**
GNSS-based PRTC/T-GM

**Spoofing Simulator:**
Spirent GSS6700
GNSS Simulator running SimSAFE

**Paragon X:**
Timing Monitor

**Timing Monitor Inputs:**
10MHz/1pps
1pps

**Spirent GSS6700 GNSS Simulator Inputs:**
10MHz/1pps
Time of Day

**Spirent GSS6700 GNSS Simulator Outputs:**
RF

**Paragon X Timing Monitor Outputs:**
1pps

**Live Sky Feed:**
RF

**RF Combiner Inputs:**
RF
10MHz/1pps
Time of Day

**RF Combiner Outputs:**
RF

**RF Splitter Inputs:**
RF

**RF Splitter Outputs:**
RF

**GPS Antenna:**
RF

**Live Sky Feed Outputs:**
RF
Device A: Spoofing from Live Sky

- Spoofing on +6dB
- Pseudo-range ramp: +20m over 5 minutes
- Pseudo-range ramp: -20m over 5 minutes
- Trace went much further than expected
- Trace carried on going down when pseudo-range went back up
Device B: Spoofing from Live Sky

- Initial transient of -1.2us
- Status reported as "locked and in sync", but not "GPS steered"
- Moved to "Survey Mode"
- Peaks up to 100us
- Status returned to "GPS steered"
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

Spoofing from Live Sky

Spoofer on
Spoofer gain +6dB

Pseudo-range ramp:
-10m over 2 minutes

Fix changed from 3D to 2D, stopped using some satellites

Lost fix altogether, output squelched
Device D: Spoofing from Live Sky

- RAIM and multipath detection turned OFF
Device D: Spoofing from Live Sky

- RAIM and multipath detection turned ON

• Spoofing on

- Time varies wildly, then settles

• Signal squelched

- Time varies wildly again, then settles

• Pseudo-range ramp: -20m over 5 minutes
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
  • Good RAIM (Receiver Autonomous Integrity Monitoring) is important
  • Testing response of existing systems important – a crude attack can cause unexpected behaviour

• Know your system:
  • Risk Assessment: understand exposure to threats, likely impacts and system behaviour
  • Testing: test against realistic threat vectors to highlight unexpected system behaviour
  • Develop Defence Strategies: Use the information from test/audit to design defence strategies

• 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