Logan Scott, President, LS Consulting
www.gpsexpert.net

The Role of Civil Signal Authentication in Trustable Systems

Presentation to:
PNT Advisory Board, 6 June 2019
Logan Scott has over 35 years of military and civil GPS systems engineering experience. He is a consultant specializing in radio frequency signal processing and waveform design. At Texas Instruments, he pioneered approaches for building high-performance, jamming-resistant digital receivers.

At Omnipoint (now T-Mobile), he developed spectrum sharing techniques that led to a Pioneer’s preference award from the FCC. He is a cofounder of Lonestar Aerospace, an advanced decision analytics company located in Texas.

Logan has been an active advocate for improved civil GPS location assurance through test based GPS receiver certification, crowdsourced jammer detection and location, and, by adding robust signal authentication features to civil GPS signals. He is currently consulting with AFRL on waveforms for advanced navigation capabilities.

Logan is a Fellow of the Institute of Navigation and a Senior Member of IEEE. In 2018 he received the GPS World Signals award. He holds 43 US patents.
In a Critical Application Which Would You Prefer?

- A GNSS receiver that provides position and time
  - A. in real time **BUT** with limited assurance
  - B. with very high assurance **BUT** with a 6 second delay
    - delay is known to within a few nanoseconds
Real Time, Right?

But What if the GNSS is Only Used to Align the Inertial?
Real Time, Right?

But What if the GNSS is Only Used to Discipline the Clock?
Real Time, Right?

But What if the GNSS is Only Used to Initialize the Worldview?
Real Time, Right?

Would they even notice?
Corrupt GNSS can drive a clock or IMU into an irredeemable error state or prevent TERCOM acquisition.

- **GNSS / Clock**
  - GNSS disciplines the clock’s drift errors

- **GNSS / IMU (inertial measurement unit)**
  - GNSS disciplines the IMU’s error states

- **GNSS / Autonomous**
  - GNSS initializes TERrain COMparison (TERCOM) processes
With a 6 second delay, a GNSS receiver has time to ponder
  - It can look at trends in quality metrics without having to make real-time judgments
  - In a sense, receiver algorithms can look 6 seconds into the “future”

With a 6 second delay, a GNSS receiver can withhold judgment until all the facts are in
  - Did that signal originate from a GPS satellite?
  - Are the watermarks in the right place, at the right power?
IS-AGT-100 Defines an Experimental, Backwards Compatible Security Overlay for the L1C Civil Signal Embodies Most Concepts from my 2003 and 2013 papers

- Message Signing
- Fast & Slow Watermark Channels
  - 6 second epoch
  - 3 minute epoch

Signal Specification and Select Papers are at http://www.gpsexpert.net/chimera-specification
Watermarking Signals with Spread Spectrum Security Codes (SSSC) Can Establish Provenance

- Watermark Generating Key Determines Security Code Values AND Insertion Locations
  - Key Is Changed Once Every 3 minutes

- Key is Published to The User Segment ONLY After Key Has Changed
  - Published By Satellites & via Secure Server
  - Secure Key Storage IS NOT Required in User Equipments

- The Watermark Is Hard To Forge
  - Spoofer/Forger Has to Read SSSC Chips Off The Air
Apriori Receiver Time Uncertainties and Marker Generation Key Time of Publication Determines Which Markers Can Be Used in Authentication

Satellite

Marker Key_{N-1} Used To Generate Markers

Receiver

Markers Potentially Collected By Receiver

- Adversary Could NOT Have Had Marker Generating Key *(OK to Use These for Authentication)*
- Adversary Could Have Had Marker Generating Key

Receiver Knows Time to Be In This Range

Time

6 June 2019 © Logan Scott / LS Consulting
The Transmitted Signal Has 3 Channels

- **Pilot**
- **Data (Signed)**
- **SSSC**

If You Don’t See This Aligned to the Pilot, The Signal Didn’t Come from a GNSS Satellite
Watermarks Provide an Extremely Low False Positives Rate and a High Probability of Detecting Spoofing
Declaring SPOOFING is Like Yelling FIRE in a Crowded Theatre!

Probability of NOT Detecting Watermark
(1.00 sec Segment, WM DF = 5.0%, Pfa = 1.00E-03)

Lower Is Better

99.9% Probability of Detecting Spoofing

Nominal C/No

Probability of a False Positive

\[ P_{fa} = 10^{-3} \]
Fast Key (6 Second) and Slow Key (3 minutes) SSSC Streams Support Diverse User Communities

- **Fast Keys** Change Every 6 Seconds
  - Keys Obtained via Authenticated Out of Band Channel (e.g. Internet)
  - Low Latency Authentication / PoL with Fast Update Rate

- **Slow Keys** Change Every 3 Minutes
  - Keys Transmitted By GNSS Satellite for Standalone Capability
  - Provides Bootstrap into Using Fast Channel if Initial Time Uncertainty is Large

---

**Type 3 Format**

10 msec  Type 3 Format  10 msec

5% Fast Key / 5% Slow Key Duty Factor Time Hopped SSSC

Normal L1C Signal Flow per IS-GPS-800

6 June 2019  © Logan Scott / LS Consulting
CHIMERA Also Signs Data Messages

ECDSA P-224 Signature Is Hashed to Create the Slow Channel Marker Generation Key

From IS-AGT-100
There are a lot of methods for detecting RF spoofing. Many can be manipulated to create false positives DoS.

<table>
<thead>
<tr>
<th>Anti-Spoofing Method</th>
<th>Spoofing Feature</th>
<th>Complexity</th>
<th>Effectiveness</th>
<th>Receiver Required Capability</th>
<th>Spoofing Scenario Generality</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSS Monitoring</td>
<td>Higher C/N0</td>
<td>Low</td>
<td>Medium</td>
<td>C/N0 Monitoring</td>
<td>Medium</td>
</tr>
<tr>
<td>RSS Variation vs. Receiver Movement</td>
<td>Higher Power variations due to proximity</td>
<td>Low</td>
<td>Low</td>
<td>Antenna Movement / C/N0 Monitoring</td>
<td>Low</td>
</tr>
<tr>
<td>Antenna Pattern Diversity</td>
<td>Not available due to elevation angle</td>
<td>Medium</td>
<td>Medium</td>
<td>C/N0 Monitoring</td>
<td>Medium</td>
</tr>
<tr>
<td>L1/L2 Power Comparison</td>
<td>No L2 signal for spoofer</td>
<td>Medium</td>
<td>Low</td>
<td>L2 Reception Capability</td>
<td>Medium</td>
</tr>
<tr>
<td>Direction of Arrival Comparison</td>
<td>Spoofing signals coming from the same direction</td>
<td>High</td>
<td>High</td>
<td>Measuring Correlation Coefficient</td>
<td>High</td>
</tr>
<tr>
<td>Pairwise Correlation in Synthetic Array</td>
<td>Spoofing signals come from the same direction</td>
<td>Low</td>
<td>High</td>
<td>Measuring Correlation Coefficient</td>
<td>High</td>
</tr>
<tr>
<td>TOA Discrimination</td>
<td>Inevitable delay of spoofing signal</td>
<td>Medium</td>
<td>Medium</td>
<td>TOA Analysis</td>
<td>Low</td>
</tr>
<tr>
<td>Signal Quality Monitoring</td>
<td>Deviated shape of correlation peak</td>
<td>Medium</td>
<td>Medium</td>
<td>Multiple Correlators</td>
<td>Low</td>
</tr>
<tr>
<td>Consistency Check with other Solutions</td>
<td>Inconsistency of spoofing solution</td>
<td>High</td>
<td>High</td>
<td>Different Navigation Sensors</td>
<td>High</td>
</tr>
<tr>
<td>Cryptographic Authentication</td>
<td>Not authenticated</td>
<td>High</td>
<td>High</td>
<td>Authentication</td>
<td>High</td>
</tr>
<tr>
<td>Code and Phase rate Consistency Check</td>
<td>Mismatch between spoofed and authentic Code and Phase rate</td>
<td>Low</td>
<td>Low</td>
<td>---</td>
<td>Low</td>
</tr>
<tr>
<td>GPS Clock Consistency</td>
<td>Inconsistency of spoofing clock</td>
<td>Low</td>
<td>Medium</td>
<td>---</td>
<td>Medium</td>
</tr>
<tr>
<td>Multiple Receiver Spoofing Detection</td>
<td>Same solution for different receivers/absence of valid spoofed P(Y)</td>
<td>Medium</td>
<td>High</td>
<td>Data link Between Receivers</td>
<td>High</td>
</tr>
</tbody>
</table>

Two Ways to Cheat at Pokémon Go

Hint: Method 1 Costs Less and is More Reliable

**Method 1**

- Hide my Root
  - Android
  - Tools
  - Unrated
  - Install

**Method 2**

- Fake GPS Location Spoof Free
  - Incorporate Apps
  - Entertainment
  - Everyone
  - Install

This is a Man in the Middle Attack
Monetizing Location Spoofing By Becoming a Virtual Ridesharing Driver

Pokémon Go was an early example of a new style of exploit

1. Sign Up to Be a Driver using Stolen ID
2. Install Location Spoofer App
3. Obtain OP Credit Card(s) & Identities and Sign Up as a Rider(s)
4. Accept Rides in Virtual Space and Get Paid for it

Scale Up by Renting a Botnet or Hire some Smurfs
Cyberspoofing Is Oftentimes a More Effective Method
- Can Be Used to Corrupt Databases with Location Dependent and/or Crowdsourced Entries
  - Traffic Estimates
  - The US Census
- Can Bias Conclusions Drawn from the Database
  - Where Traffic Flows
  - Where Money Flows

Watermarking Can Play an Important Role in Detecting Location Spoofing By Providing Location Signatures
Problems of Location Check For Valid Watermarks etc.
Less Trust in the Sender and Intervening Comms

- Location Signature is ~125 Kbyte (Nominal)
- Diverse Trust Models Are Possible

**Authenticated Source**
- Ephemeris / Symbol Stream
- Watermark Generating Keys

**Location Signature Stream** is sent or sequestered before watermark keys are published.

- Location Authentication Object
  - No RF Needed
  - Can Be All S/W
  - Local, Remote, or Cloud Based

*RF Front End & Downconversion* → *A/D* → *Communications Interface* → *Local GPS Receiver (Optional in Some Cases)*
Prospects for Chimera in US Systems

- Almost ANY navigation signal can be watermarked with backwards compatibility

- Implementing CHIMERA is Not That Hard
  - Message Signing Can Be Done in Software
  - Watermarks are a PN Code Generator Modification in the SV
    - Digital / FPGA Change Only
    - NO Analog or Modulator Changes

- NTS-3 Will Broadcast Chimera on an Experimental Basis
  - 2022 Launch

- Secure-WAAS Signal Design Described in 2003 Paper Remains Valid with a couple of tweaks
  - Modulators are on the Ground
A special thanks to USAF Capt. Katie Carroll and the entire team at AFRL for bringing this vision to fruition.