Proof of Location; Verifying Physical Space in Virtual Space

Logan Scott,
President, LS Consulting
14 November 2012

Stanford 2012 PNT Challenges and Opportunities Symposium
Ask a Silly Question...

- **Q:** How Can You Be in Two Places at Once When You're Not Anywhere at All
  - *The Firesign Theatre* 1969

- **A:** The Internet
  - *Vinton Cerf et. al. ca. 1974*
Why Location Proofs?
Orthogonal Defense In Depth: Location Is Part of Identity
What Is A Location Proof?

- Antispoof ≠ Proof of Location
  - How Do I Know I’m Where I Think I Am?
    - Antispoof
  - How Do I Prove to You Where I Am?
    - Proof of Location

- Location/Time Signature Elements Can Include:
  - Cryptographic GPS RF Signal Structures
  - Overlapping Systems: GNSS, WiFi, e-Loran, Camera, IEEE P1588 Timing Standard, etc.

- Location Proofs Should Be Ephemeral
  - Need Time Expiry, You Could Have Moved
Proof of Location Can Mitigate Against False Reporting

- What was the Motivation?
  - Prank
  - Smuggling
  - Diversion

- $300,000 per Incident

This Guy Wants to Pull the Trigger. He Needs the 1 Hour Key. Where Is He?

- Stingers for Syrian Rebels?
  - Location Restricted?
  - Time Restricted?

- More Generally, Location Dependant FMS Capability
  - Radar Guidance Modes
  - Sensor Capabilities
Smart Phones & Tablets Present Formidable Security Challenges
How Do You Know GPS Position Is Good?

- Smart Phone/Tablet Security Challenges Apply to Both Civil & Military Users

- Commercial Software & Hardware
  - Counterfeit Parts / Supply Chain Injection
  - Firmware & Software Updates
  - Unsecured Infrastructure & Hardware

- Need to Secure Millions of Users
  - Accidents Will Happen
Location Based Information
Embargo Can Mitigate Compromises

- A Smart Device Can Access/Hold A Great Deal of Information
  - Detailed Base Maps Accessible Only When ON Base
  - Intelligence or Mission Data Accessible Only When Relevant To Current Location
  - Intellectual Property Access with Location/Time Restrictions

- Location Is Part of NSA Security Paradigms
  - “It is an important and valuable capability to track the geo-location of mobile devices ... Such tracking can help locate lost or stolen devices and can be used as part of the authorization decision process (there may be different access rules depending on whether user is inside or outside a given facility or country).”

NSA, Mobility Capability Package, March 26 2012, Secure VoIP Version 1.2
Which Map Is More Useful For Directing Mortar Fire?

Cloud Sourced Servers Might Provide Geofiltered Tactical Updates, Maps, and Imagery
Location Based Information Embargo Can Also Apply to Intellectual Property
Don’t Serve Documents to Unauthorized Locations

- Gen. Keith Alexander (NSA chief) recently described the loss of industrial information and intellectual property through cyber espionage as "the greatest transfer of wealth in history."

- Estimated Value ~$500 billion USD

The Civil Community Has Diverse Needs for Location and Time Proofs

- Where Did that {File, Command, Report, Request, Part} Come From?
  - Need to Geofence Sensitive Data
  - Location Restrict Internet Facing ICS/SCADA Command & Control Using Geofiltering
  - E-Mail anti Spearphishing
  - Verify Aircraft Location Reporting

- Many, Many Other Use Cases
Industrial Control Systems are Protected By an Air Gap, Aren’t They?

- Specialty Search Engines to Find ICS/SCADA Devices
  - http://www.shodanhq.com/
  - http://eripp.com/

ICS-CERT ALERT

ICS-ALERT-12-046-01A—(UPDATE) INCREASING THREAT TO INDUSTRIAL CONTROL SYSTEMS

October 25, 2012

OVERVIEW

ICS-CERT is monitoring and responding to a combination of threat elements that increase the risk of control systems attacks. These elements include Internet accessible industrial control system (ICS) configurations, vulnerability and exploit tool releases for ICS devices, and increased interest and activity by hacktivist groups and others.

On February 14, 2012, several new exploit tools were publicly released that specifically target programmable logic controllers (PLCs), the building blocks of many ICSs. These exploits target PLCs from GE, Rockwell Automation, Schneider Electric, and Koyo. In addition, one of the exploits targets the EtherNet/IP protocol, which is deployed by numerous PLC vendors in addition to those listed here. The payloads purportedly can affect any device that uses the EtherNet/IP protocol and could allow an attacker to crash or restart affected devices.

------ Begin Update A Part 1 of 2 ------

A team of researchers recently contacted ICS-CERT with preliminary results from their analytical project to locate Internet facing control system related devices. Using the SHODAN search engine, the researchers compiled a list of more than 500,000 control systems-related devices using supervisory control and data acquisition (SCADA) and other ICS-related search terms. The researchers have brought their findings to the attention of ICS-CERT, citing concerns that an adversary could use the search engine as a shortcut to find vulnerable systems and thereby threaten or attack critical infrastructure. ICS-CERT is working with the researchers and
And Of Course, None of these Workstations Were Connected to ICS Devices Either

- In the eyes of U.S. defense secretary Leon Panetta, it was “probably the most destructive attack that the private sector has seen to date.”
Excerpts from Leon Panetta (Secretary of Defense) speech at the Intrepid Sea, Air and Space Museum in New York, Oct 11 2012

- “An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches,”

- “They could derail passenger trains, or even more dangerous, **derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country.”
Where Did That Part Come From?
Are You an Authorized Printer?
Additive Printing Technology Is Advancing Rapidly

Printed Body with Sharkskin Pattern and Advanced Air Intake Baffles

direct metal laser sintering to additively manufacture fully dense metal parts

14 November 2012 © Logan Scott / LS Consulting
Location Proofs Should Avoid/Limit Trust! He Might Be Lying

The GPS Receiver Is Just One Point of Attack in A Long Chain!

“It worked as promised, but it made my GPS go haywire” One★

NO RF EXPERTISE REQUIRED
Counterfeit Cisco Routers
Some were installed at U.S. Navy Installations

- “In total, ICE and CBP seized more than 94,000 counterfeit Cisco network components and labels” DOJ Press Release

The Smart Phone Is Just One Point of Attack in A Long Chain!

A Good Proof of Location System*
Illuminating the Concept

* But a Not So Good Navigation System
The SatNav System

- Encrypt Spread Spectrum Navigation Signals
  - Encrypt Spreading Sequence, Changing the Key Once Every 5 Minutes
  - Only Control Segment & Space Segment Hold Real-time Keys, NOT THE USER EQUIPMENT

- Release Keys to The Public 5 minutes later
  - This is Not the Same as Current Generation Military Signals Where Keys Are Released Apriori and Have to Be Held in Tamper Resistant, Secure Storage
Why This Is Good For Proof of Location?

- Spread Spectrum Signals Are Hidden Below the Noise and are Hard to Forge Without Keys

- Can Send Raw A/D samples to other Locations Before Keys Are Released ("Time & Location Signature")
  - Communications Links Can’t Forge Location Signature

- Once Keys are Released, Software Entities can Compute Sender’s Location and Time

- Secure Key Storage Is Not Needed In the User Segment
  - It Is Usable In Less Secured Environments
Why This Is A Not So Good Navigation System?

- User Segment Can’t Do Anything with the Signal Except Store It or Send It Elsewhere Until The Keys Are Released
  - Navigation Solutions Have up to a 5 minute Delay
Creating Authenticatable GNSS Signals
Practicable Anti Spoof & Proof of Location
Security Features Can Be Added to Modernized Signal Structure WITHOUT Affecting Tracking
L1C Is My Exemplar

- Modernized Signals Have Two Channels
  - Pilot Channel (Tracking, Unaffected)
  - Modified Data Channel (0.9 dB SNR Loss)
    - Cryptographic Watermarking With Spread Spectrum Security Code (SSSC)
    - 50 bps Data with Cryptographic Data Signing
Time Hopping (TH) SSSC Makes Forging Signals More Difficult
Which Chips are SSSC vs. ICD-GPS-800A?

- SSSC Time Hop Pattern Is Also Determined By Seed Value
- 10% SSSC Substitution for L1C_D Data Channel At 1.023 Mchip/second PN Code Rate
Correlation Responses for Original L1C_D and Type 2, 10% TH BOC(1,1) SSSC

- All Cases
  - 1.5 bit ADC, P2=40%
  - 4.5 MHz Passband
  - 100 msec Blocksize

**Tx:L1C_D** **Rx:L1C_D**

Case 9, L1C Search Correlation Responses C/No_{max} = 43.2988 dB-Hz

**Tx:L1C_D with 10% SSSC** **Rx:L1C_D**

Case 9, L1C Search Correlation Responses C/No_{max} = 42.1051 dB-Hz

Real Time

Down 1 dB

Unmodified Signal

**Tx:L1C_D with 10% SSSC** **Rx:SSSC**

Case 9, L1C Search Correlation Responses C/No_{max} = 33.5199 dB-Hz

Down 10 dB

Need Cipher Seed
Spoof/Forgery Chip Reading Errors
Lower SSSSC Correlation Response

\[ P_{\text{correct}} = 1 \]
(Have the Key)

\[ P_{\text{correct}} = 0.9 \]
(19 dBiC Spoof Gain)

\[ P_{\text{correct}} = 0.8 \]
(16 dBiC Spoof Gain)

Peak SNR = 0 dB wrt Expected Value

Peak SNR = -2 dB wrt Expected Value

Peak SNR = -6 dB wrt Expected Value

- All Cases
  - 1.5 bit ADC, P2=40%
  - 4.5 MHz Passband
  - 100 msec Blocksize
Location Proof Checks For Valid Watermarks etc.
Less Trust in the Sender; the Keys Haven’t Been Published Yet

Authenticatable GPS Signals

Location Signature Stream Is Sent Before Watermark Keys Are Published

- RF Front End & Downconversion
- A/D
- Communications Interface
- Local GPS Receiver (Optional in Some Cases)

Secure Server(s)
- Ephemeris / Symbol Stream
- Watermark Generating Keys
- 5 minutes/SV

Extend ICD-GPS-870?

- Location Signature is ~150 Kbyte (Nominal)
- Diverse Trust Models Are Possible

Location Authentication Object
- No RF Needed
- Can Be All S/W
- 4 or 5 SV solution
- Local, Remote, or Cloud Based

GPS Receiver Or Control Segment

Or

Control Segment
To Authenticate A Signal, Make Sure the Watermark Is Present at the Correct Level
In Addition to Other Spoof Detections

1. Collect Precorrelation A/D Samples
   - For Location Proof, Must Send to 2\textsuperscript{nd} Party Before Generating Key Is Released

2. Watermark Generating Key Becomes Available (up to 5 minutes later)


4. If Don’t Detect Security Spreading Code at Correct Power Level & Code Phase, Don’t Validate Signal

5. If See Cross Talk Terms, Don’t Validate Signal
SV Sends Watermarking Key Once Every 5 Minutes & Data Stream is Authenticated Using A Public Key Digital Signature Algorithm (~6% of Subframe 3, ICD-GPS-800)
Spoofer/Forger Antenna Requirements for Various Hardened GPS Signal Types

<table>
<thead>
<tr>
<th>Signal</th>
<th>Minimum Spoofer Antenna Gain†</th>
<th>Associated Antenna Diameter</th>
<th>Associated 2-sided 3dB Beamwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_1C_D$</td>
<td>21 dBiC</td>
<td>26”</td>
<td>18 degrees</td>
</tr>
<tr>
<td>$L_2CM$</td>
<td>21 dBiC</td>
<td>34”</td>
<td>18 degrees</td>
</tr>
<tr>
<td>$L_5I$</td>
<td>26 dBiC</td>
<td>63”</td>
<td>10 degrees</td>
</tr>
<tr>
<td>$L_1$ SWAAS</td>
<td>26 dBiC</td>
<td>47”</td>
<td>10 degrees</td>
</tr>
</tbody>
</table>

† Gain Required for Spoofer to Read True SSSC and Generate False SSSC Bursts With Correlation within 1 dB of True SSSC Bursts

$L_1C_D$ Analysis is in Backup Charts
Bent Pipe Delay Establishes Minimum Time Jump When Spoofer Uses Off the Air Signals
If Trusted Time Stamp Sequestration Delay Is Less, Can’t Forge

- Minimum Spoofer Delay
  - Determined By SV with Maximum Bent Pipe Path Length vs. Direct Path Length
  - Geometry Dependant

<table>
<thead>
<tr>
<th>Forger Distance from Victim (km)</th>
<th>Maximum Bent-Pipe Delay (msec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.5</td>
<td>0.01</td>
</tr>
<tr>
<td>15</td>
<td>0.1</td>
</tr>
<tr>
<td>150</td>
<td>1</td>
</tr>
<tr>
<td>1500</td>
<td>10</td>
</tr>
</tbody>
</table>

Proximity Is Important!
Stronger Location Security with Civil Devices
In Addition, Can Send Location Signatures to Remote Authentication Objects

- Local Location Authentication Object
  - Tamper Resistance
  - TPM Capability
  - Time Keeping & Time Stamping
  - Computing Engine

+ : Even Better

- Remote Location Authentication Object
Fast Key (2 Second) and Slow Key (5 minutes) SSSC Streams Support Distinct User Communities

- **Fast Keys Released With 2 Second Renewal Rate**
  - Obtained via Internet ONLY (ICD-GPS-870? and Others)
  - Provides Low Latency, Short Duration Proofs of Location with Fast Update Rate
    - Aircraft, UAVs, Timing
- **Slow Keys Released With 5 Minute Renewal Rate**
  - Keys Transmitted By Satellite
  - Supports Autonomous Checking without Separate Communications Channel

![Diagram showing Type 3 Format with 10 msec intervals and 5% Fast Key / 5% Slow Key Duty Factor Time Hopped SSSC]
Civil Aircraft Can Prove Their Location
Autonomous Aircraft Raises the Bar for Location Security Performance

Location Spoofer is Not Necessarily RF, It May Be a Cyber Entity

Aircraft Location Signature

Local Location Authentication Object

CryptoVault

Command & Control Location Signature

Remote Location Authentication Object

+ : Even Better
## Civil Authentication Capabilities for Planned & Existing Systems

Possible Revenue Stream / Expect Required Use in Sponsoring Countries

<table>
<thead>
<tr>
<th>System</th>
<th>Civil Authentication Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>e-Loran</td>
<td>Demonstrated Capability (TESLA Protocol), Watermarked PPM may be possible for Proof of Location</td>
</tr>
<tr>
<td>Galileo (EU)</td>
<td>Commercial Services (E6) &amp; Safety of Life (E5b) will Have Signal Authentication &amp; Possibly Proof of Location</td>
</tr>
<tr>
<td>Compass (PRC)</td>
<td>Yes, ???</td>
</tr>
<tr>
<td>Glonass (Russian)</td>
<td>Unknown, Not Part of Current Capability Set but CDMA versions would present modernization opportunity</td>
</tr>
<tr>
<td>GPS (US)</td>
<td>Currently Not Part of Planned Capability Set, Possible for “Nibbles” Satellites</td>
</tr>
</tbody>
</table>
Code Generators Are, Probably, One of the More Readily Modified GNSS Satellite Components
This is Not an SVN 49 Scale Modification!

- They Are a Digital Components (FPGA?)
  - Code Generation Itself Is Not All that Time Critical
  - The Output Latch Is What Is Time Critical
  - Can Switch OFF Watermark Insertion

Chip needs to be ready “sometime” before latch clock

Code Generator

Output Latch

To Transmitter Modulation

Code Clock
Signal in Space Authentication Features Are Needed For Proof of Location & AntiSpoofing
GPS Can Help Secure Critical Infrastructure

- **It Is Important**
  - PVT Is a Critical & Often Hidden Element of Civil Infrastructure
  - Threat Surface Is Expanding & User Community is Largely Unawares
  - “Proof of Location & Time” Capability Is An Unmet Need
  - GPS may be Locked out of International Markets

- **It Is Doable**
  - PKI Approach Does NOT Require User Equipment to Hold Secrets
  - Minor Impact On Receivers that Want to Authenticate
  - No Impact on Receivers That Do Not Want to Authenticate
  - Strong Signal In Space Authentication Is Possible for L5I, L2CM, L1CD and L1 WAAS

- **Benefit Is Immediate**
  - Do Not Need Full Constellation, Even One SV Can Provide Significant Location Assurance Gain
  - Possible Revenue Stream for GPS
Related Papers by Logan Scott

- **Policy Recommendations**
  1. Towards a Sound National Policy for Civil Location and Time Assurance; Putting the Pieces Together, InsideGNSS Magazine, September/October 2012

- **Cryptographic Signal Authentication**
  2. L1C Should Incorporate Cryptographic Authentication Features, May 2006 Comments on ICD-GPS-800
  4. Location Signatures: Proving Location to Second Parties without Requiring Trust 12 June 2012, JNC 2012

- **Jammer Location “J911”**

- **Receiver Certification**
  2. Level 1 Draft Specification posted at: http://logan.scott.home.comcast.net/~logan.scott/
Backup
Location is a Fundamental Identity Attribute
Proof of Location Has A Role In Securing Cyberspace

- Gen. (ret) Michael V. Hayden, Principal, The Chertoff Group†

  “Part of our cyber policy problem is its newness and our familiar experience in physical space does not easily transfer to cyberspace. Casually applying well-known concepts from physical space like deterrence, where attribution is assumed, to cyberspace where attribution is frequently the problem, is a recipe for failure.”

† Testimony before House Permanent Select Committee on Intelligence, Chairman Mike Rogers (R-Mich), Cyber Threats and Ongoing Efforts to Protect the Nation Oct 4, 2011.
Although we do not believe significant market data delays were the primary factor in causing the events of May 6, our analyses of that day reveal the extent to which the actions of market participants can be influenced by uncertainty about, or delays in, market data. SEC, Findings Regarding the Market Events of May 6, 2010
“I Better Sell That Stock” said the Robot after reading the news

UAL Flash Crash Sept 2008

- News story was actually 6 years old, from 2002, but was time stamped as current
- UAL dropped 76% from $12.30 to $3 in a matter of ~3 minutes

Stock Chart from: Berger et al., Rumors in Financial Markets 1 December 2010
Congressional Concerns About Two of the World’s Four Largest Telecoms-Equipment Makers

October 2012

For Immediate Release
October 8, 2012

Susan Phalen (Rogers)
Susan.Phalen@mail.house.gov
Heather Moeder Molino (Ruppersberger)
Heather.Molino@mail.house.gov

Chairman Rogers and Ranking Member Ruppersberger Warn American Companies Doing Business with Huawei and ZTE to “use another vendor”

WASHINGTON, D.C. – The Chairman and Ranking Member of the House Intelligence Committee, Mike Rogers (R-MI) and C.A. Dutch Ruppersberger (D-MD), today released a report recommending to U.S. companies considering doing business with Chinese telecommunications companies Huawei and ZTE to find another vendor. The report encourages U.S. companies to take into account the long-term security risks associated with either company providing equipment or services to our telecommunications infrastructure. Additionally, the report recommends that U.S. government systems, particularly sensitive systems, exclude Huawei or ZTE equipment or component parts.

Graphic from: Economist, 4 August 2012
Authenticatable Signals Can Become a GPS Revenue Source
“Proof of Location” Has Value

- EU expected to require signal authentication in transportation sectors.
  - Galileo Commercial Services (CS) Signal Has Authentication Features
  - Authentication Keys Will be “For Fee”
  - De facto requirement to use Galileo

- Sell Authentication Keys on Amazon, iTunes etc.
  - Commercial Retailers have Distribution Channels in Place
  - Issue is one of Compliance, not Security
    - If 10% of user’s cheat; that means 90% paid

- There Is Also Another Control Segment Business In Low Latency Location Authentication
Secure Signal Generation at the Satellite

- 10% of Data Channel Signal Stream Is Cipher Stream

- Cipher Stream Seed
  - Cipher Stream Generator
  - L1CΔ Code Generator
    - PN Code Clock
  - Time Hop Selection
  - Select
    - IS-GPS-800 Stream
    - 100 sps Data Symbols
    - BPSK -> BOC Squarewave
  - The SSSC Code

- SSSC Can Also Have Crypto Controlled Phase Component
- Can Time Multiplex Type 1 / Type 2 Bursting
Cooperating Location Authenticators At Geographically Dispersed Sites Can Makes The Forger’s Job More Difficult

A. Can Select Path with Minimum Sequestration Delay

B. Can Bound Target Receiver’s Location Based on Relative Sequestration Delays
   - e.g. 3 delays can compute 3D location

14 November 2012 © Logan Scott / LS Consulting
Spoofers’ Probability of Reading an L1C\textsubscript{Di} SSSC Chip in Error as a Function of Receive Antenna Gain

High Gain Antenna Is Needed to Read L1C\textsubscript{Di} SSC Directly

Probability of Reading A Chip In Error

\begin{align*}
S = -163.0 \text{ dBW} / NF = 2.0 \text{ dB} / \text{Loss} = 1.0 \text{ dB}, 1.02 \text{ Mch/sec}
\end{align*}
Spoofing Is Detectable By Low $L_1C_{Di}$ SSSC Correlation Power

**SSSC Median Power (dB)**

$$SSSC	ext{ Median Power (dB)} = 20 \log_{10} (P_c - P_e) = 20 \log_{10} (1 - 2P_e)$$

- $S = -163.0$ dBW / NF = 2.0 dB / Loss = 1.0 dB, 1.02 Mch/sec

Spoofing Is Detectable By Looking at SSC Correlation Power
High Gain Antennas Are Big and Impractical for Spoofers

L1 Antenna Characteristics (80% Aperture Efficiency)

- Two Sided 3 dB Beamwidth (Degrees)
- Aperture Width (inches)

Two Sided 3 dB Beamwidth (degrees)

Circular Aperture Diameter (inches)

Peak Gain (dBiC)
SSSC C/No Estimation Accuracy with Coherent Processing Using 0.2 Second Data Record at 10% SSSC Duty Factor Requires Phase Lock

Coherent Receiver: 1 msec SSSC Burst every 0.010 sec (DF=10.0%) , 0.20 sec Collection Interval

Nominal L1C_D C/No with 0dBiC Gain Towards SV is ~ 40 dB-Hz

CN0 Estimation Accuracy.xlsx