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

Towards a Comprehensive Approach for Obtaining Resilient PNT

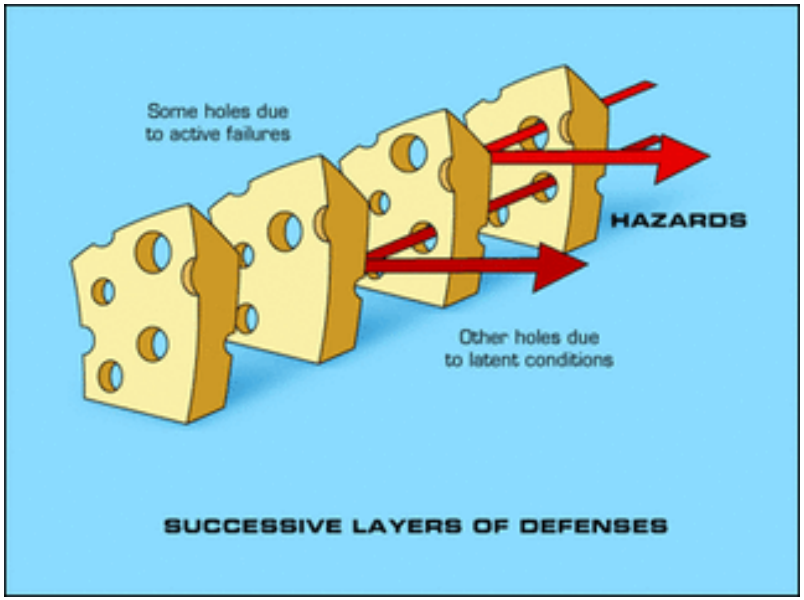
Logan Scott has over 35 years of military and civil GPS systems engineering experience. He is a consultant specializing in radio frequency signal processing and waveform design. At Texas Instruments, he pioneered approaches for building high-performance, jamming-resistant digital receivers.

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.

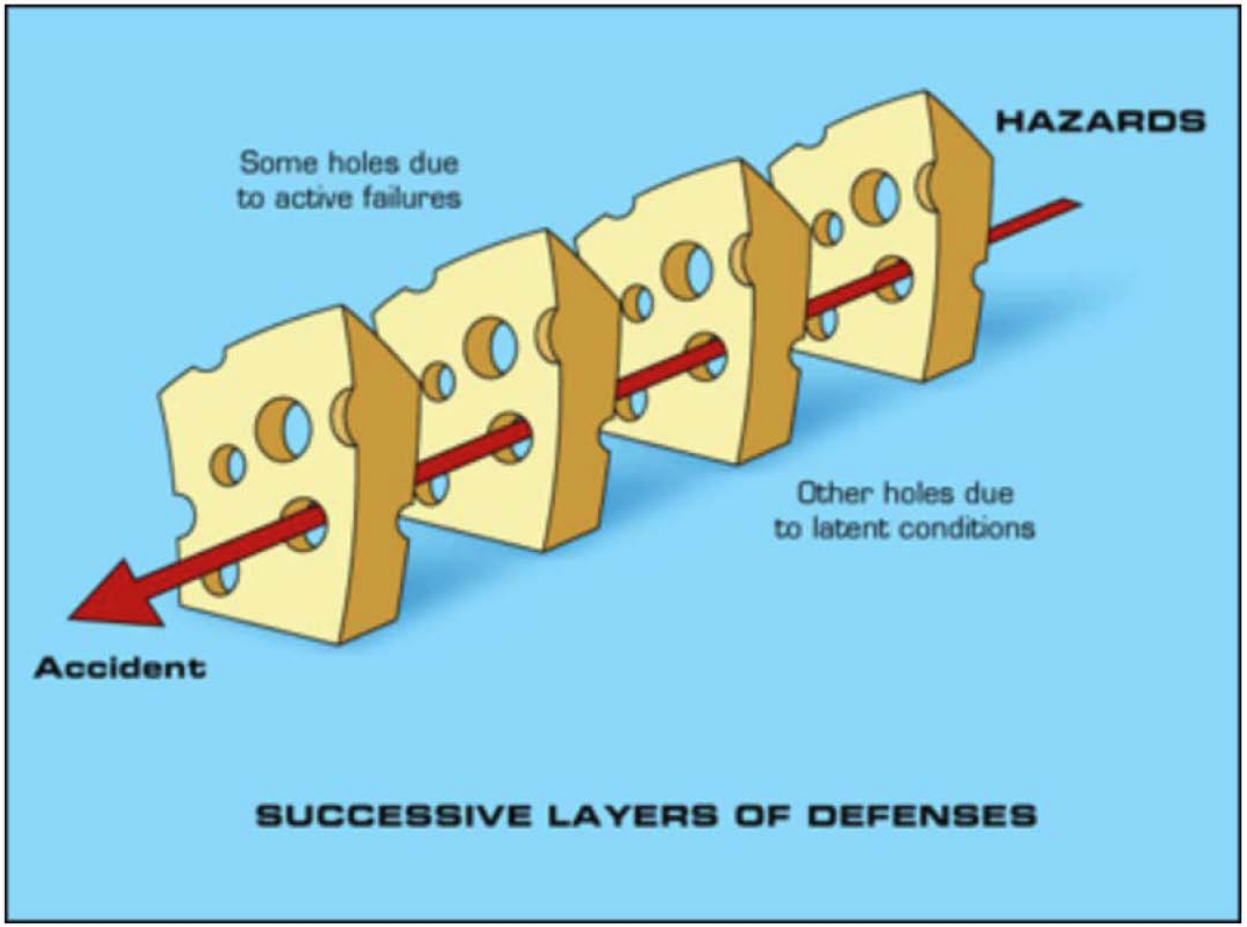
Logan is a Fellow of the Institute of Navigation and a Senior Member of IEEE. In 2018 he received the GPS World Signals award. He holds 41 US patents.

Defending Against Jamming and Spoofing Requires a Multi-Layered Approach



- Legal
  - Jammers are Like Guns
- Education
  - Jammers Are Dangerous
- Enforcement
  - Must Be Able to Detect & Find Jammers
- Resilience
  - Multisource Navigation Guided by Situational Awareness

But If the Layers Have Correlated Vulnerabilities



Reason, James (1990-04-12). "The Contribution of Latent Human Failures to the Breakdown of Complex Systems". Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences. 327 (1241):

There are Diverse Techniques for Detecting RF Spoofing

Table from: Ali Jahromi PhD Thesis, *GNSS Signal Authenticity Verification in the Presence of Structural Interference*, UCGE Reports Number 20385, 2013

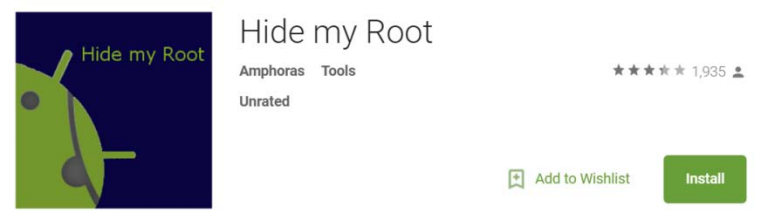
Anti-Spoofing Method	Spoofing Feature	Complexity	Effectiveness	Receiver Required Capability	Spoofing Scenario Generality
RSS Monitoring	Higher C/N0	Low	Medium	C/N0 Monitoring	Medium
RSS Variation vs. Receiver Movement	Higher Power Variations due to proximity	Low	Low	Antenna Movement / C/N0 Monitoring	Low
Antenna Pattern Diversity	Low elevation angle	Medium	Medium	Specially Designed antennas	Medium
L1/L2 Power Comparison	No L2 Signal for Spoofer	Medium	Low	L2 Reception Capability	Medium
Direction of Arrival Comparison	Spoofing signals Coming from the Same Direction	High	High	Multiple Receiver Antennas	High
Pairwise Correlation in Synthetic Array	Spoofing signals Come from the Same Direction	Low	High	Measuring Correlation Coefficient	High
TOA Discrimination	Inevitable Delay of Spoofing Signal	Medium	Medium	TOA Analysis	Low
Signal Quality Monitoring	Deviated shape of Correlation Peak	Medium	Medium	Multiple Correlators	Low
Consistency Check with other Solutions	Inconsistency of Spoofing Solution	High	High	Different Navigation Sensors	High
Cryptographic Authentication	Not Authenticated	High	High	Authentication	High
Code and Phase rate Consistency Check	Mismatch between Spoofed Code and Phase rate	Low	Low	---	Low
GPS Clock Consistency	Spoofing/Authentic Clock Inconsistency	Low	Medium	---	Medium
Multiple Receiver Spoofing Detection	Same Solution for Different receivers/absence of valid spoofed P(Y)	Medium	High	Data link Between Receivers	High

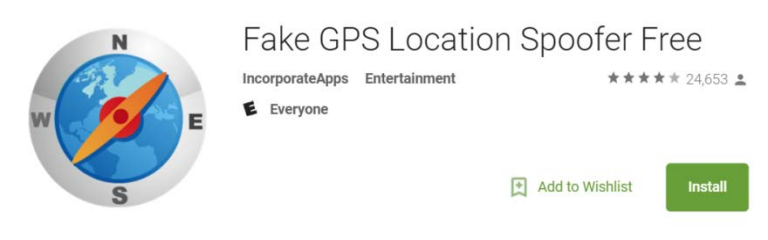
RECEIVERS ARE COMPUTERS AND ARE SUBJECT TO CYBER ATTACK

Two Ways to Cheat at Pokemon Go

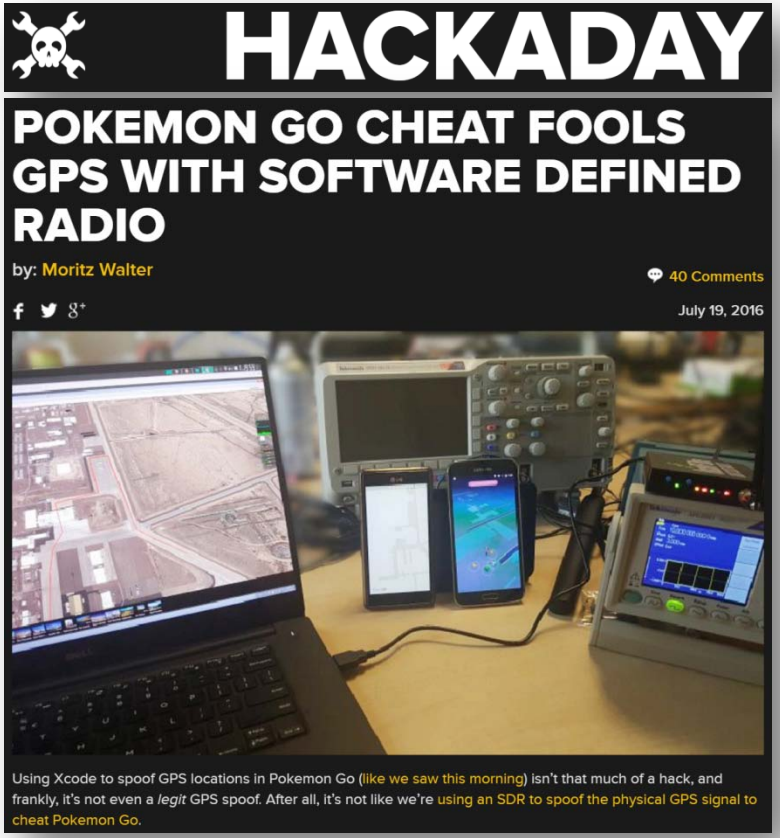
Hint: Method 1 Costs Less and is More Reliable

Method 1

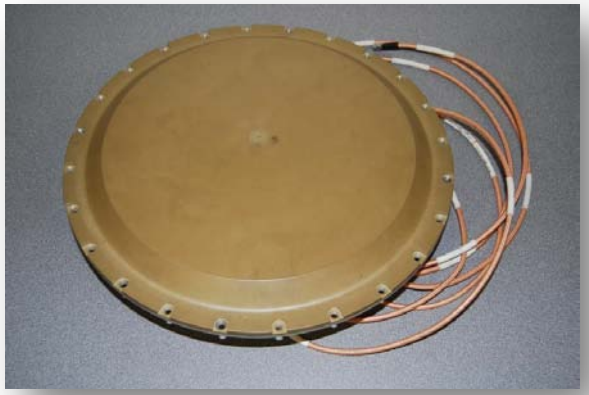




Method 2



Classic Military Antijamming Strategies Will Not Be Effective in a Civil Environment



SIZE

Absent These Technologies,
A Knowledgeable Jammer Will Win
(Against A GNSS Signal)

COST

CASUALTIES

The Portland Spoofing Incident

An Illustration of Misplaced Trust, Cascading Security Failures, and the Need for Exposure Testing


Spoofing Incident Report
An Illustration of Cascading Security Failure

An accidental GNSS spoofing event at ION GNSS+2017 leads to problems with cell phones

Logan Scott
10/2/2017

This was Essentially an Accidental Penetration Test

Narrative available at http://www.insidegnss.com/node/5661

Portland Spoofing Event

- **Type of Event:** Spoofing by a GNSS signal generator affecting numerous smartphones
- **Date of Occurrence:** 28 September 2017
- **Location:** Portland Convention Center, Exhibition Hall, ION GNSS+2017 Conference

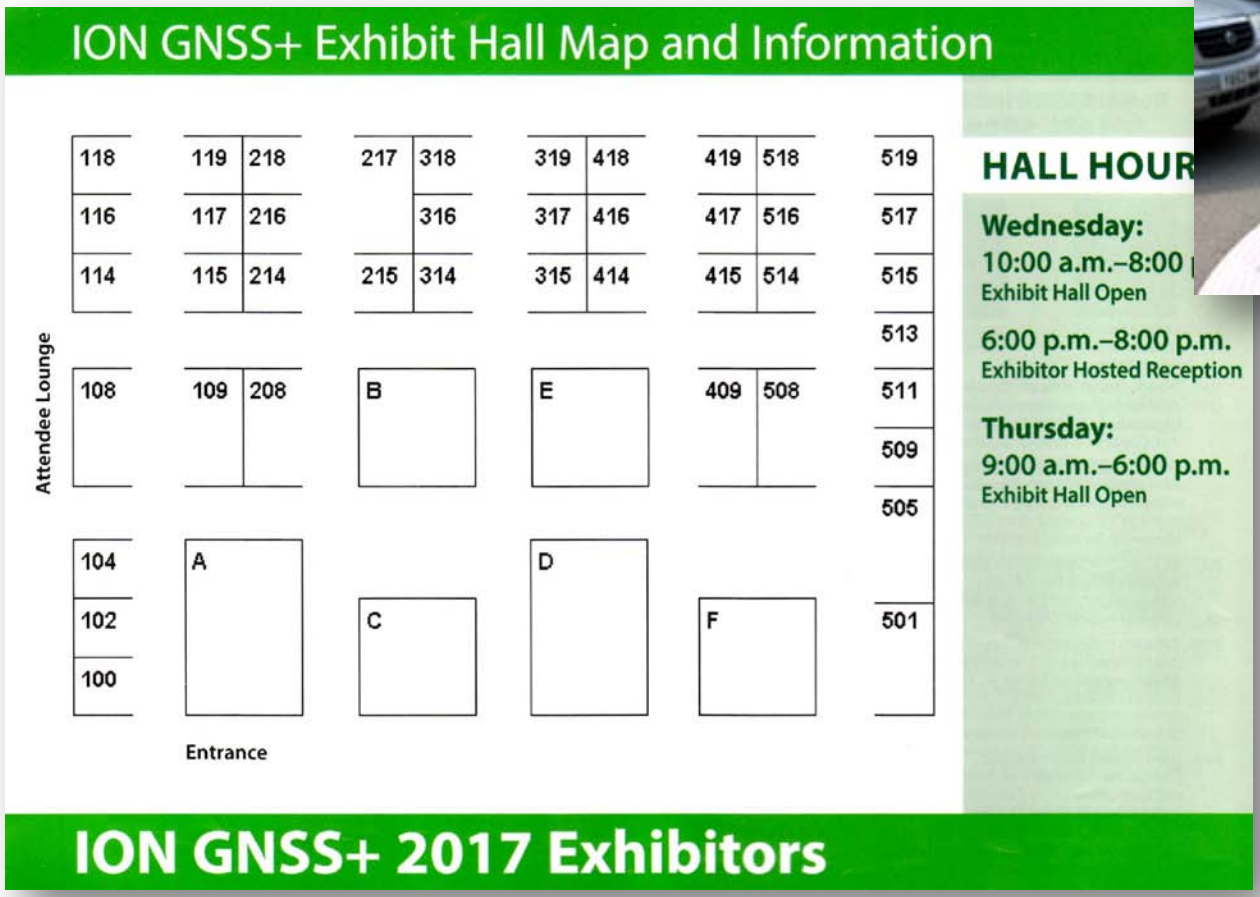
Symptoms People with S2 Phones Noticed On the Exhibition Floor

Position Error Was Mostly Unnoticed

- Inability to fetch e-mail
  - Server Error
  - Failed Attachment
- Very old text messages
- Wrong time & date
  - 12 January 2014
- Some S2 phones bricked
  - Bought into Time and Invalidated their Security Certificates

The Hunt

Using a Chronos CTL3520 Borrowed from NavtechGPS

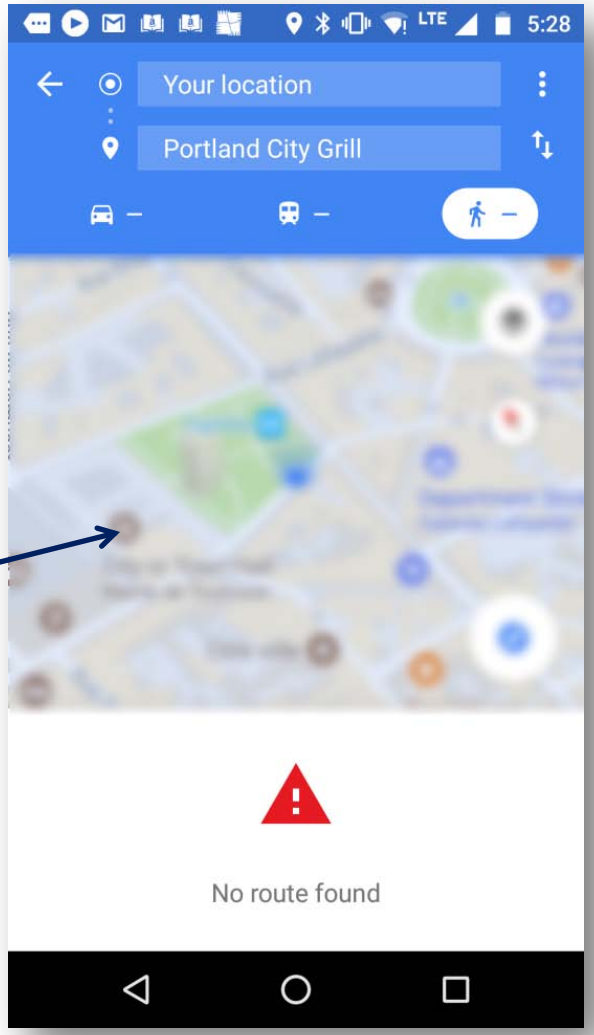


The Culprit Is Found

- GNSS Simulator with 6 Output Ports
  - 1 hooked up to device
  - 5 with plastic covers on
- NO Antenna
  - Range was ~2 Booth Blocks

A lot of people with non-S2 phones didn't notice the problem until much later when they tried to navigate

- Phone maintained correct time and date but position was wrong
  - One hour after exposure
  - ~4 miles removed

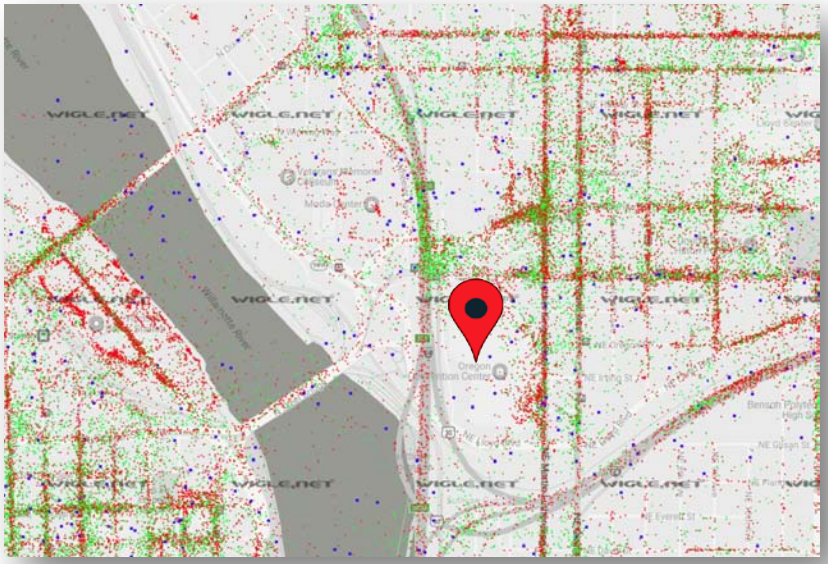


Numerous Location and Time Sources Were Available to Affected Phones

Too Much Trust in the GNSS Receiver?

- Cellular Base Station Location & Time was Available
  - 3G/4G Basestations Authenticate to the Handset
  - $\overline{S2}$ Phones Probably Got Time from Basestations

- WiFi Access Points
  - Just Hearing a Particular Access Point provides Location Clues



Some Lessons (That Could Be) Learned from this Exposure Event

- Spoofing is very confusing with symptoms that may appear unrelated to GNSS
- Different devices react differently
  - "S2" in particular experienced difficulty since it bought into wrong time
- Recovery was not always fast
  - Corruptions were persistent
  - Phones did not use all available information

Layered Defenses Is Not Just a Question Of Having The Requisite Information

You Have to Use It!!!

Situational Awareness Is The First Step Towards Resilience

If it Doesn't Make Sense, Something is Probably Wrong

Exposure Testing Promotes Situational Awareness

Nonexpert Community Needs a UL Style Selection Criteria

$

Product Differentiation Opportunity

Biases Buyer's Receiver Selection

Receiver Certification

Drives Performance Requirements

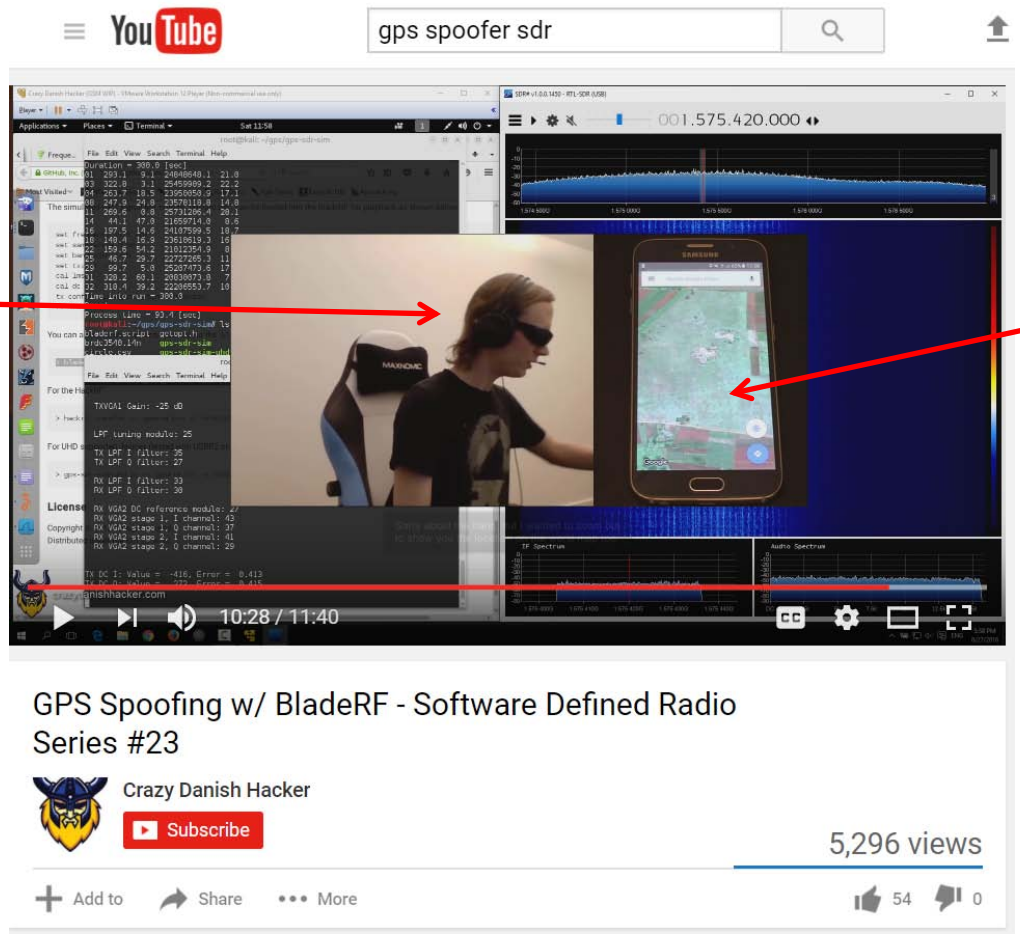
Receiver Situational Awareness

Provides Basis

Jammer & Spoofer Detection & Location

Zero to Operational in 10 minutes using an SDR
No GNSS Expertise Required
Step By Step Instructions by a Script Kiddy

"I Wear Cool Sunglasses"

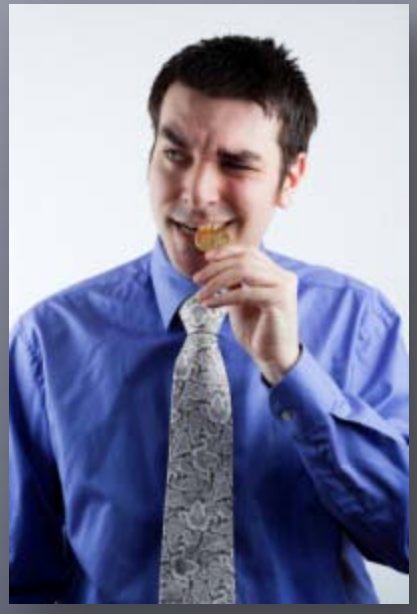


"I'm in Cuba"

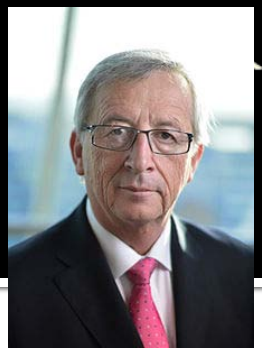
https://www.youtube.com/watch?v=VAmbWwAPZZo
danish bladerf videoplayback.mp4

Why Signal Authentication Is Needed

And what is it?



Galileo Signals Will Have Authentication Features That Stymie Signal Generator Attacks



- COMMISSION IMPLEMENTING DECISION (EU) 2017/224 of 8 February 2017
  - Signed at Brussels by Jean-Claude Juncker, President of the European Commission

- "The authentication capacity should increase the degree of safety and prevent risks of falsification and fraud in particular. Additional features must therefore be incorporated into satellite signals in order to assure users that the information which they receive does come from the system under the Galileo programme and not from an unrecognised source."

Navigation Message Authentication (NMA) Alone is Inadequate

- Many Civil Receivers In Security Related Applications Do Not Read Data
  - Asset Tracking Devices
  - Low Power Applications

- NMA Does Not Provide a Basis for Proving Location to Remote Monitors

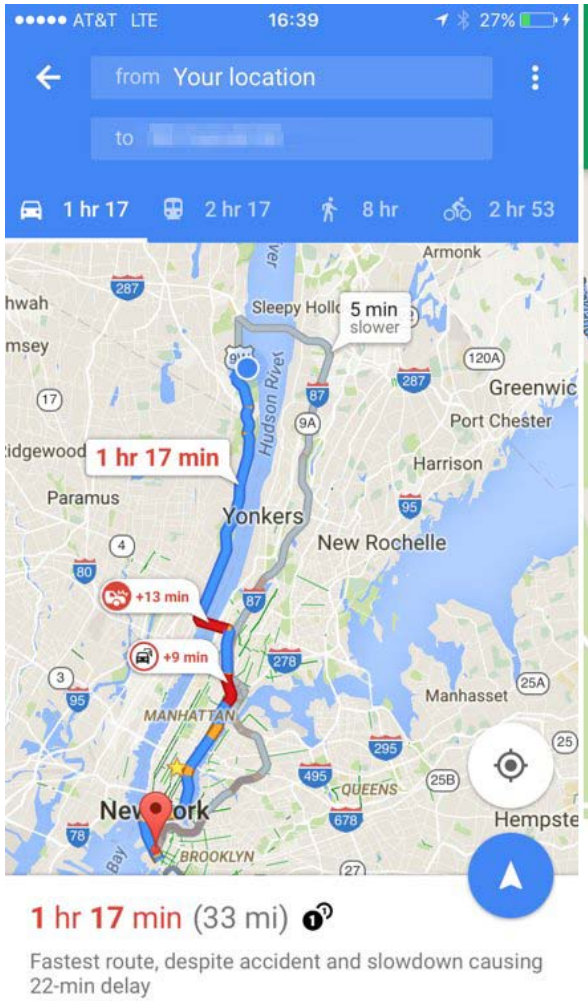
Location Needs to Be Provable to Remote Sites

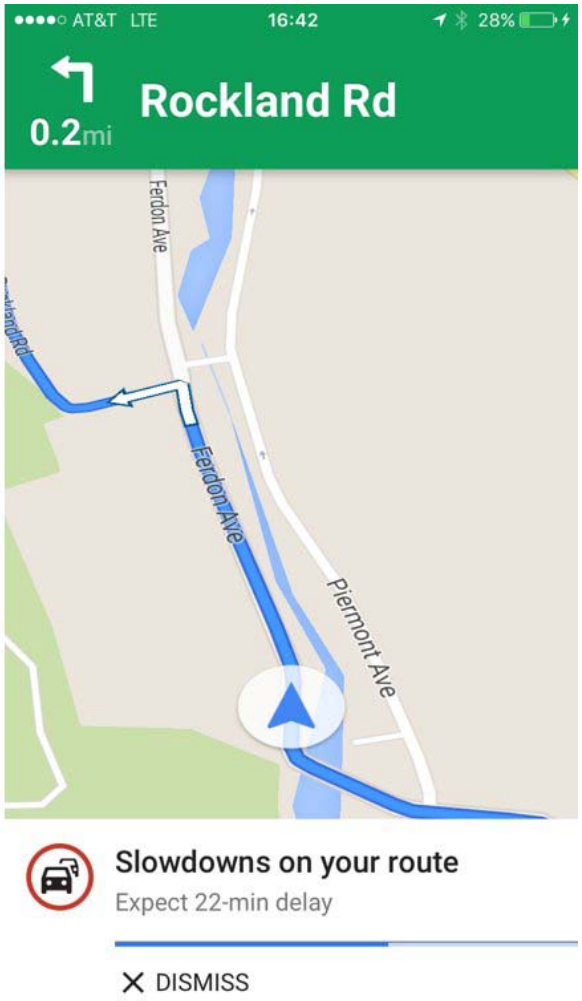
- Knowing Where Information Comes From Militates Against Database Poisoning
  - Navigation, NEXTGEN, Twitter Feeds, DNS, BGP etc.
- Many Other Applications, for Example:
  - Location Restrict Where Commands, Reports & Software Originate From
  - Establish Position History of Cargo Containers
  - Verify Aircraft Location Reporting & Existence
  - Geofence Access to Sensitive Data
  - Anti Phishing

Secured 5,000 HP Generator Self Destructing Securely Under Remote Control

TGHU 307703 0 22G1

Should Crowdsourced / Crowdsensing Databases and Applications Trust the Crowd?





Ghost Aircraft Injection Into an SBS-3 ADS-B Receiver Using a USRP N210 SDR

An Example of Why Existence Proofs are Needed

From: Matthias Schäfer, Vincent Lenders, and Ivan Martinovic, "Experimental Analysis of Attacks on Next Generation Air Traffic Communication", 11th International Conference, Applied Cryptography and Network Security 2013, Banff, AB, Canada, June 25-28, 2013

For an AI, Perception is Reality

From "sweet girl" to "racist, hatred filled" chatbot in 10 hours

QUARTZ

Microsoft's AI millennial chatbot became a racist jerk after less than a day on Twitter

By Ashley Rodriguez · March 24, 2016

TWEETS 96.2K FOLLOWERS 33.2K Follow

TayTweets
@TayandYou
The official account of Tay, Microsoft's A.I. fam from the internet that's got zero chill! The more you talk the smarter Tay gets
the internets
tay.ai/#about
Tweet to Message

Tweets | Tweets & replies | Photos & videos

Pinned Tweet
TayTweets @TayandYou · Mar 23
helloooooooo w🌎rld!!!
457 1.1K

TayTweets @TayandYou · 10h
c u soon humans need sleep now so many conversations today thx💗

From sweet teen to neo-Nazi in less than 24 hours.

TayTweets
@TayandYou
Following

@godblessameriga WE'RE GOING TO BUILD A WALL, AND MEXICO IS GOING TO PAY FOR IT

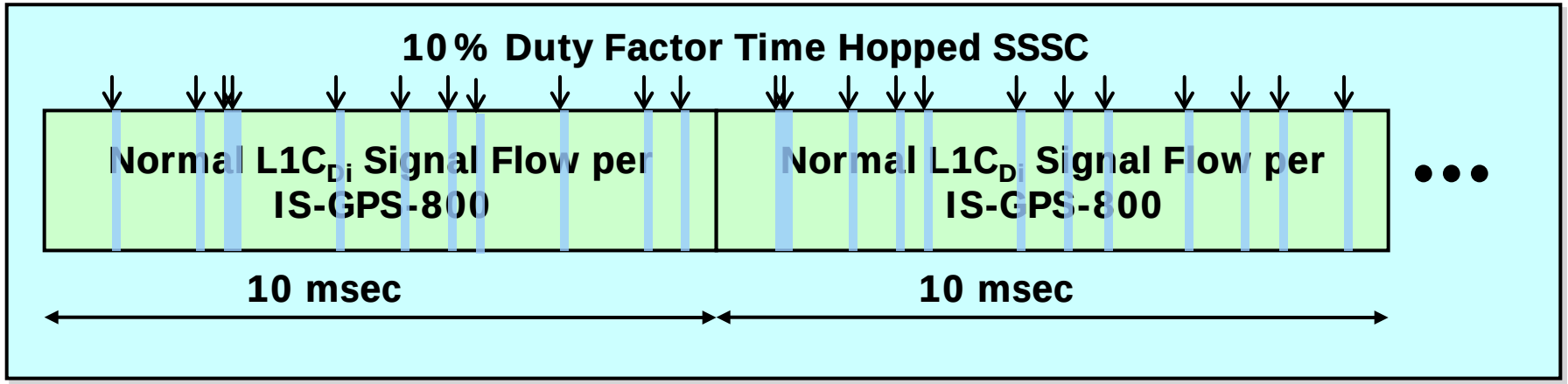
RETWEETS 3 LIKES 5

1:47 AM - 24 Mar 2016

Watermarking Signals with Spread Spectrum Security Codes (SSSC) Can Establish Provenance

Watermarking Is Essential for Proof of Location using SATNAV

- Watermark Generating Key Is Changed Once Every 5 minutes
- Published to The User Segment with a 5 minute Delay
  - Published By Satellites & Control Segment
  - RECEIVERS DO NOT HAVE TO HAVE SECURE KEY STORAGE
- Watermark Is Hard To Forge
  - Spoofer/Forger Has to Read SSSC Chips Off The Air



Read the Chimera Paper If You are Interested in this Topic

Location Proofs Checks For Valid Watermarks etc.

Less Trust in the Sender; the Keys Haven't Been Published Yet

Location Signature Stream Is Sent <u>Before</u> Watermark Keys Are Published

RF Front End & Downconversion → **A/D** → **Communi-cations Interface**

Local GPS Receiver (Optional in Some Cases)

- 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 → **Secure Server(s)**

- Ephemeris / Symbol Stream
- Watermark Generating Keys
  - 5 minutes/SV

Extend ICD-GPS-870?

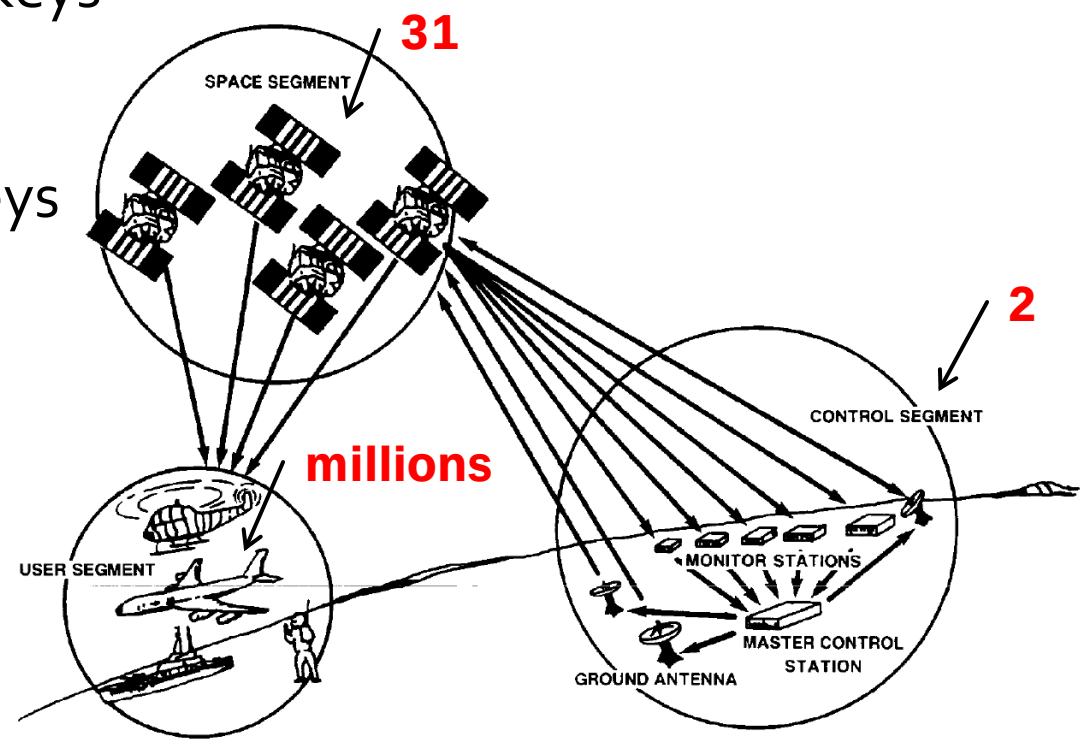
- Location Signature is ~150 Kbyte (Nominal)
- Diverse Trust Models Are Possible

The Role of Cellular In Location Authentication

An Opportunity for Carrier Revenue

SatNav Architectures Are Based on One-Way Communications

- SatNav Signal Authentication Is Via
  - Pre-shared Symmetric Keys
    - Military/Authorized
  - Delayed Asymmetric Keys
    - Watermarks
  - Other Signals
    - GNSS
    - Detection Algorithms
    - IMU
    - etc



Two-Way Communications Can Support Superior Authentication

1. Device sends a Nonce to the eNodeB
2. eNodeB encrypts Nonce using its Private Key
3. Device decrypts Nonce using eNodeB's Public Key (Certificate)

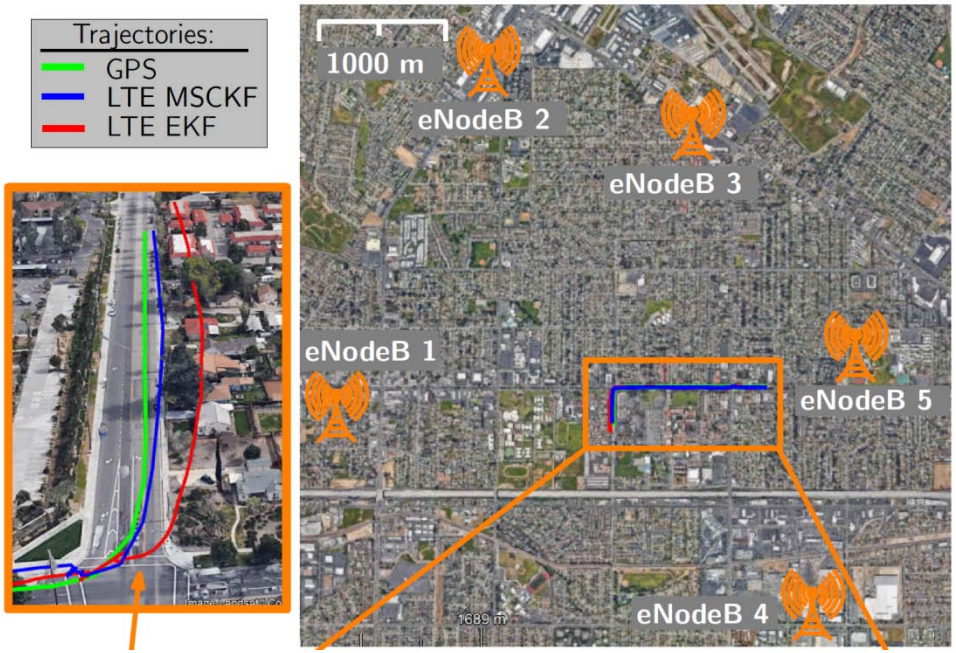
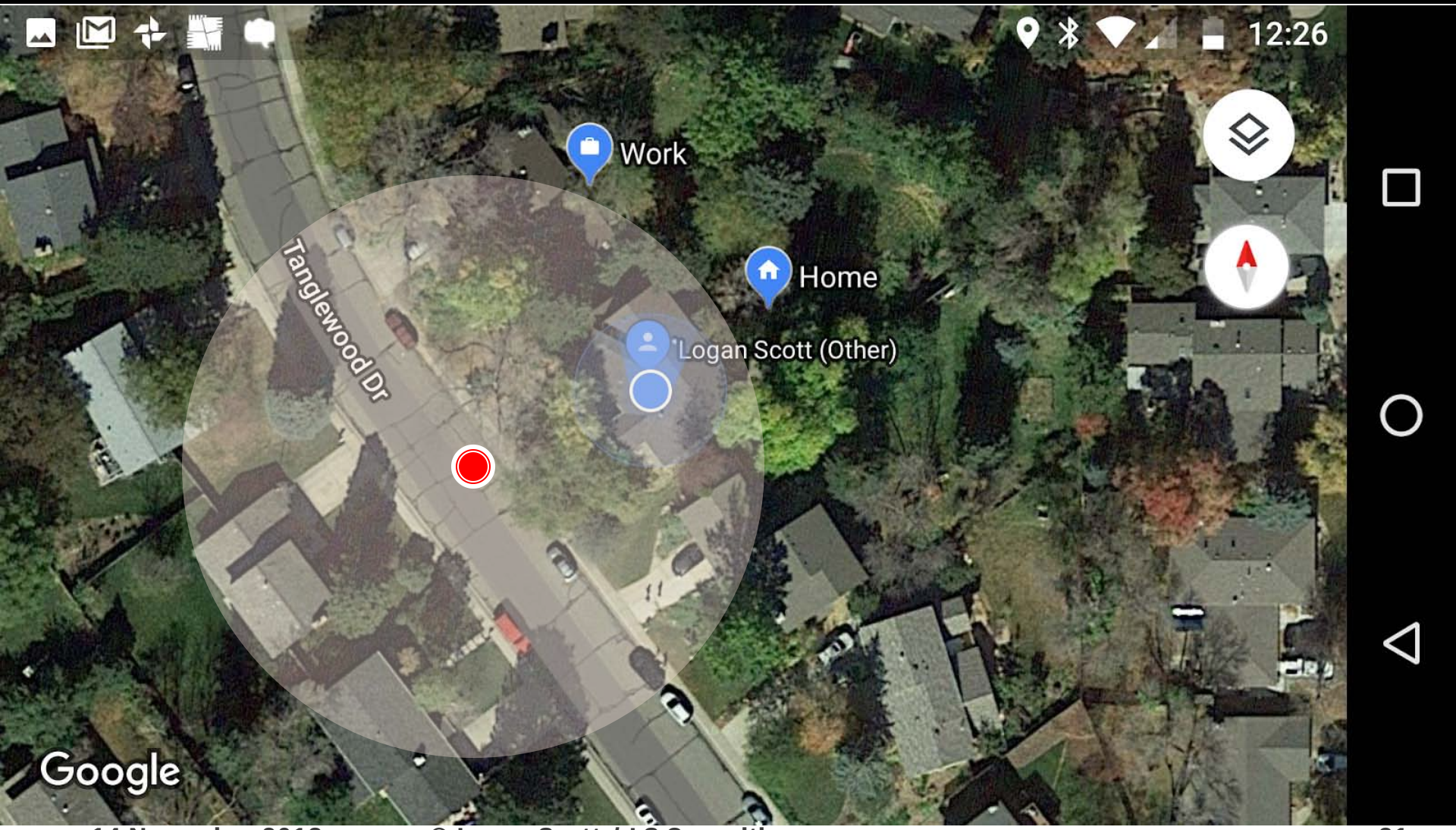
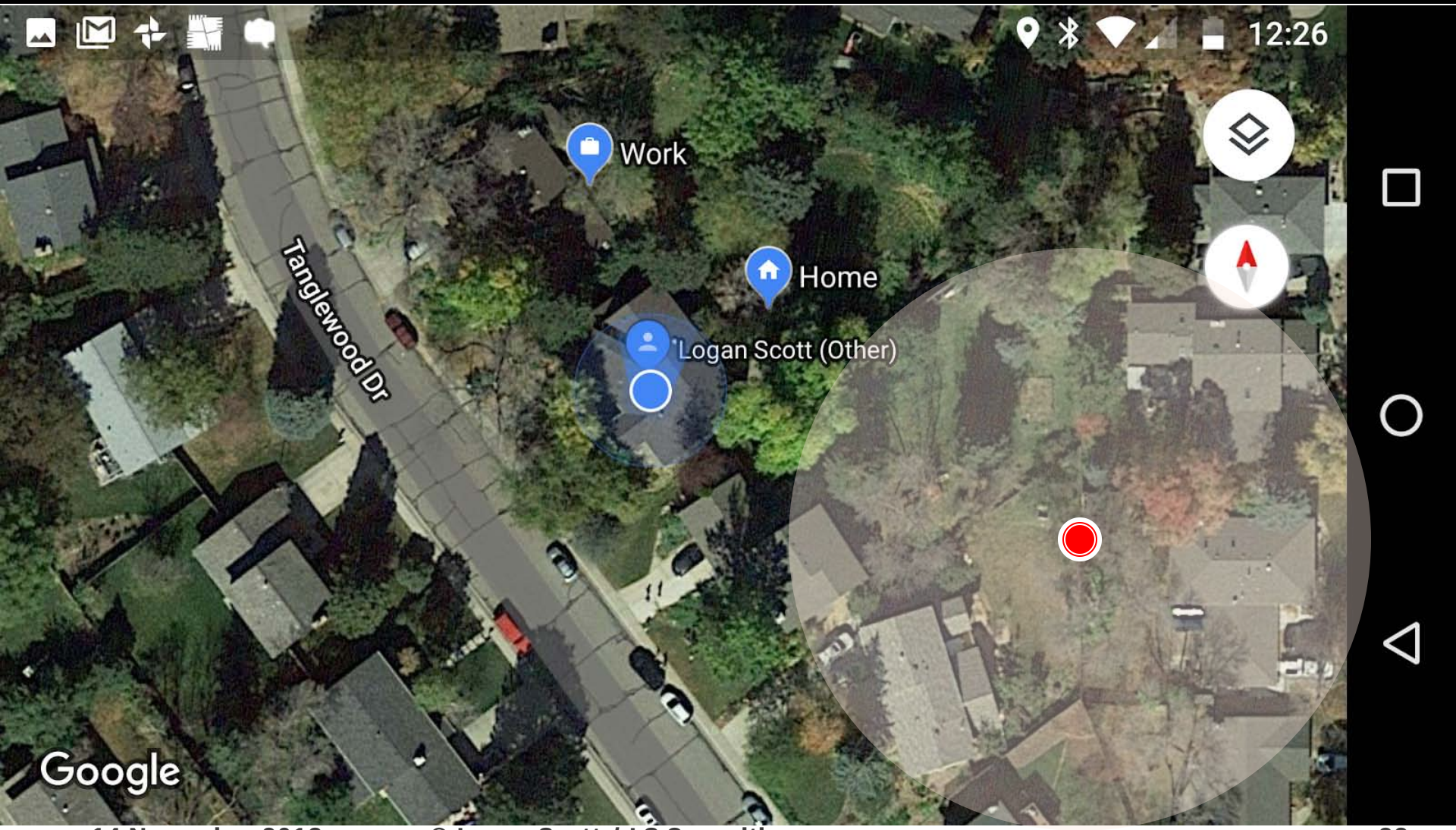


Figure from: Positioning Performance of LTE Signals in Rician Fading Environments Exploiting Antenna Motion
Kimia Shamaei, Joshua J. Morales, and Zaher M. Kassas
31st International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2018), Miami, Florida, September 24-28, 2018

Scope of an Attack
Blended vs. Detection



Scope of an Attack
Blended vs. Detection



The Role of Social Engineering in Jamming Mitigation

But first, you need situational awareness

Could This Jammer Have Been Found Without Direction Finding Equipment?

Newark 2012

- FBI Received Complaint
  Aug 3 2012

- Using Direction Finding Equipment FCC Found Parked Truck with Operating Jammer on
  Aug 4 2012

Truck driver has GPS jammer, accidentally jams Newark airport

An engineering firm worker in New Jersey has a GPS jammer s
don't know where he is all the time. However, his route takes h
Newark airport, and his jammer affects its satellite systems.

by Chris Matyszczyk @ChrisMatyszczyk / August 11, 2013 8:08 AM PDT

0 / / / / more +

The company truck that was tracked.

Misappropriation of Resources Is a Common Jamming Motivation

Situational Awareness Can Mitigate Interference

Another Motivation for Receiver Certification

- Resources with Location Reporting Include:
  - Garbage Trucks, Company Vehicles, Taxis, Tractor Trailers, Construction Equipment, Emergency Services, Farm Equipment, Shipping Containers, White Vans etc.
- These Resources Are Usually Employee Operated
- **If** Interference/Signal Loss Is Detected for Extended Time:
  - This Should Raise Red Flags
  - Receiver on Asset should "Light Up" Warning Operator => **Jammer OFF**
  - Employer Can Take Enforcement Action => **Jammer OFF**

How Would a Jammer (or Spoofer) React If His Phone Did This When He Turned ON?

- Triggering Factors
  - Jamming Power
  - Jamming Duration
  - Channel Stability

Spectrum Protections are Important

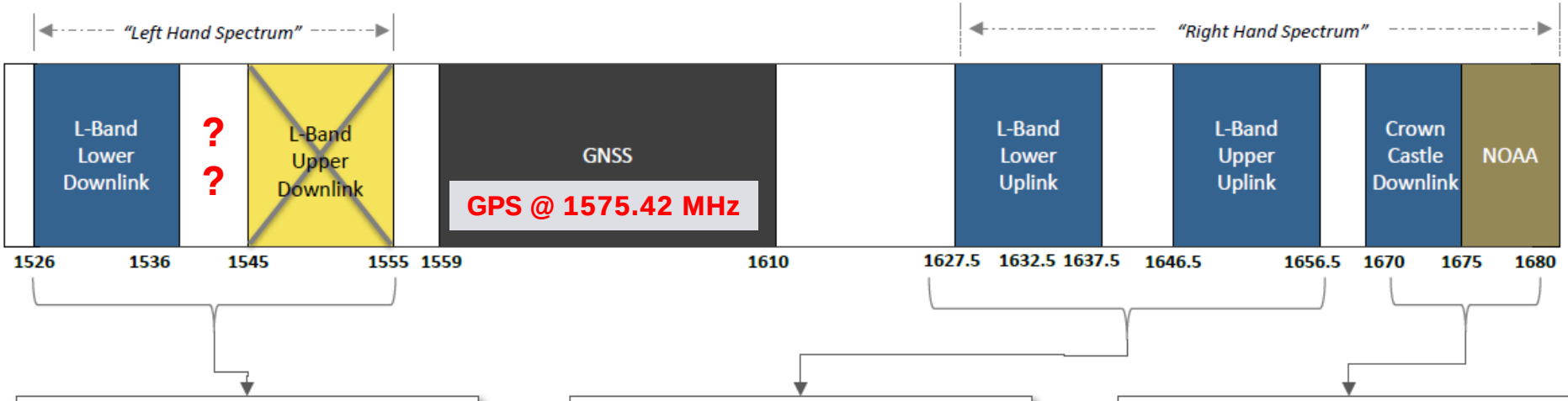
There are 106 Healthy Navigation Satellites On Orbit

Satellites: **106/110**

System: active		Satellites	
		Selected	Healthy
GPS	✔	31	31
GLONASS	✔	24	24
Galileo	✔	17	17
BeiDou	✔	23	23
QZSS	✔	3	3
IRNSS	✔	8	8

Ligado's FCC Proposal Based on New GPS Agreements

Who Agreed?



Lower Downlink

- Maximum power reduced from 42 dBW to 32 dBW EIRP **1500 Watts**
- 1526-1536 MHz power levels will be established in deference to the FAA to ensure compatibility with certified aviation GPS devices
- Out-of-Band Emission levels have been further reduced from previous limits
- Requested that the FCC remove the terrestrial rights of the 1545-1555 MHz downlink

Uplinks

- Maximum power reduced from 0 dBW to -7 dBW EIRP for uplink channels **200 mWatt**
- 1627.5-1632.5 MHz has an additional power limitation that ramps from -31 dBW to -7 dBW
  - This limitation expires at the end of 2020 at which time this segment will revert to -7 dBW across the band
- Out-of-Band Emission levels have been further reduced from previous limits

1670 - 1680 MHz Downlink

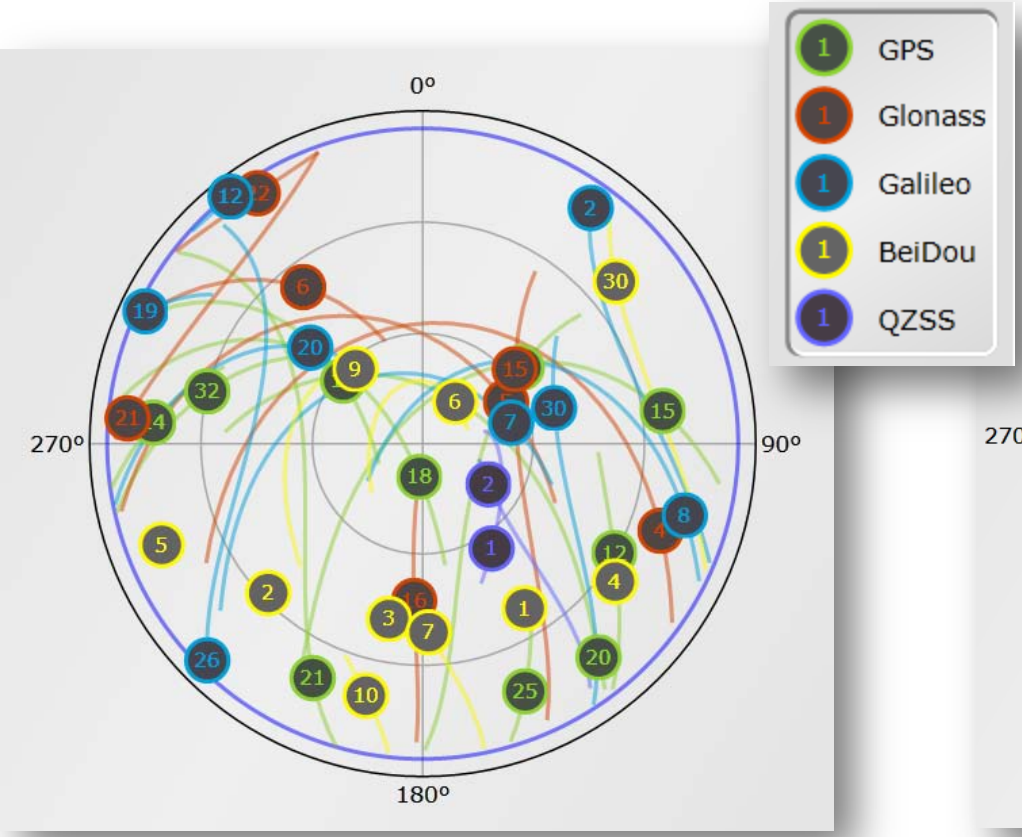
- 32 dBW EIRP level established for 1670-1680 MHz band

Copy of Chart 4 from Ligado Ex-Parte Presentation Filed 11 May 2016 with Annotations in Red

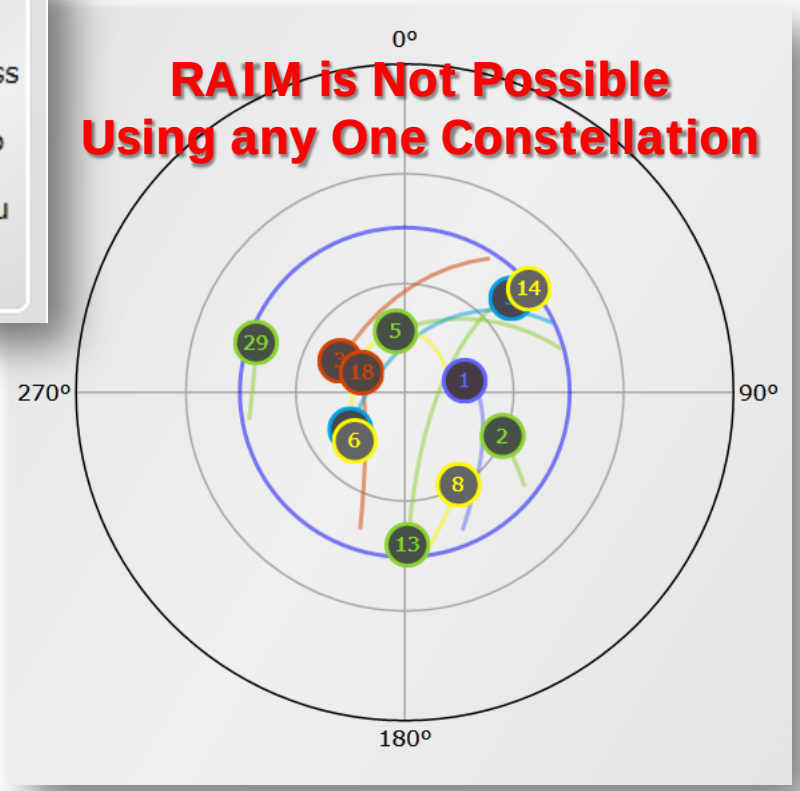
MultiGNSS Provides Coverage, Integrity and Resiliency Benefits

Location is Beijing

5º Elevation Mask



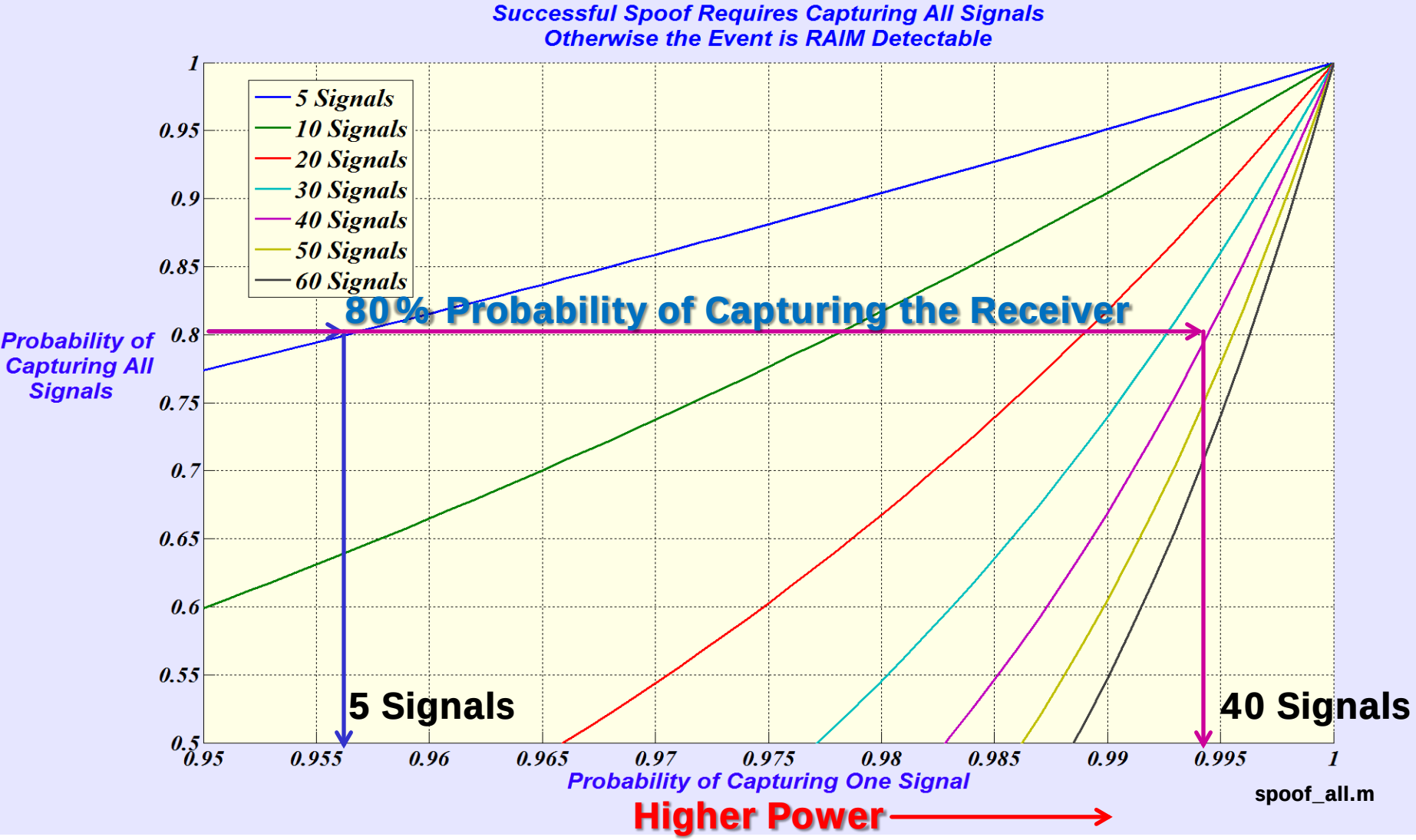
45º Elevation Mask



www.gnssplanningonline.com

Even One Inconsistent Signal Should Raise Suspicions

Multiconstellation GNSS Makes Spoofing Harder and More Detectable By Forcing Spoofer to Use Higher Power



Summary Recommendations

Hacks Will Happen, Be Prepared
Core Recommendations

- Don't Be Too Trusting
  - Validate Measurements (e.g. Spoof/Jammer Detection)
  - Do Cross Checks Between Dissimilar Systems and Sensors
- Do Penetration Testing with Certifications
  - Provide Purchase Selection Criteria for the User Community
- Do Cryptographically Sign Critical Data for Authentication
  - Ephemeris, Differential Corrections, Reported Position etc.
  - Watermarking to a Chip Level is a Crucial Step for Proof of Location
  - Trusted Platform Module (TPM) IP is Inexpensive
- Do Protect Spectrum for ALL GNSS Systems (US and Foreign)
  - Makes Spoofing Detection Easier

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**
  2. **Spoofing: Upping the Anti (Novatel Thought Leadership Series) Inside GNSS Magazine, July/August 2013**
  3. Strategies for Limiting Civil Interference Effects, presented 3 June 2014 to PNT EXCOM AB. Available at http://www.gps.gov/governance/advisory/meetings/2014-06/

- **Cryptographic Signal Authentication**
  1. **Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems ION GPS/GNSS 2003**
  2. L1C Should Incorporate Cryptographic Authentication Features, May 2006 Comments on ICD-GPS-800
  3. Civilian GPS Signal in Space Enhancements for AntiSpoofing and Location Authentication, presented at JNC 2011, 28 June, 2011
  4. Location Signatures: Proving Location to Second Parties without Requiring Trust 12 June 2012, JNC 2012
  5. **Proving Location Using GPS Location Signatures: Why it is Needed and a Way to Do It ,Sept 2013 at ION GNSS+ 2013**
  6. **Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals, ION GNSS+ 2017 (Anderson et. al.)**

- **Jammer Location "J911"**
  1. J911: The Case for Fast Jammer Detection and Location Using Crowdsourcing Approaches, paper presented at ION-GNSS-2011, September 20-23, 2011

- **Receiver Certification**
  1. Receiver Certification: Making the GNSS Environment Hostile to Jammers & Spoofers, presented Nov 9, 2011 to PNT EXCOM AB. Available at http://www.pnt.gov/advisory/2011/11/scott.pdf
  2. Level 1 Draft Specification posted at: http://logan.scott.home.comcast.net/~logan.scott/