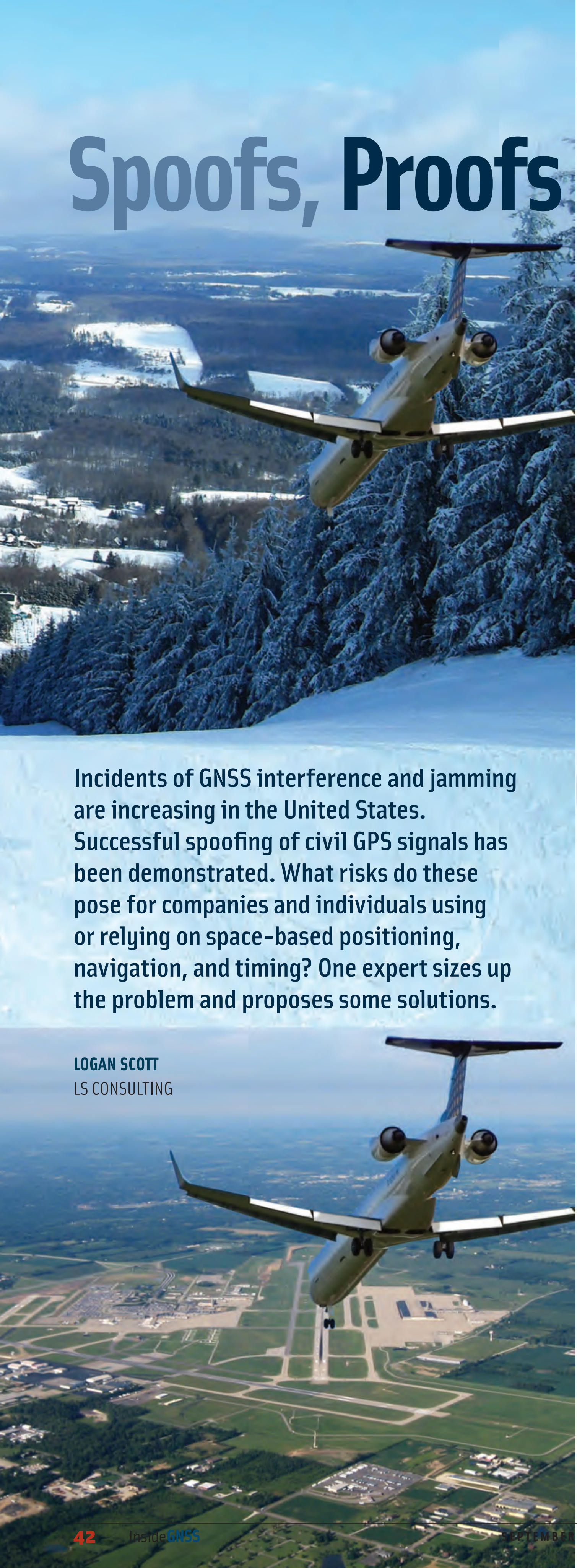


Spoofs, Proofs & Jamming

Towards a Sound National Policy for Civil Location and Time Assurance

Incidents of GNSS interference and jamming are increasing in the United States. Successful spoofing of civil GPS signals has been demonstrated. What risks do these pose for companies and individuals using or relying on space-based positioning, navigation, and timing? One expert sizes up the problem and proposes some solutions.

LOGAN SCOTT
LS CONSULTING

wikipedia Commons photos

"Here is Edward Bear, coming downstairs now, bump, bump, bump, on the back of his head, behind Christopher Robin. It is, as far as he knows, the only way of coming downstairs, but sometimes he feels that there really is another way, if only he could stop bumping for a moment and think of it. And then he feels that perhaps there isn't."
— A.A. Milne, *Winnie-the-Pooh*

Is our faith in the integrity and infallibility of the Global Positioning System misplaced or, perhaps, insufficiently grounded?

Well, consider these recent developments: GPS plays a foundational role in the FAA's Next Generation Air Transportation System (NextGen) Implementation Plan, which explicitly calls for "efforts to facilitate the entry of unmanned aircraft systems (UAS)" into the national air space (NAS). Moreover, Congress has mandated civil UAS introduction into the NAS by late 2015, and the Department of Defense (DoD) is planning to introduce UAS into the national air space by next year (2013).

Yet, in June of this year, Todd Humphreys and his team at the University of Texas at Austin demonstrated the controlled capture of a small, civil drone aircraft at White Sands Missile Range using a well-known RF spoofing attack protocol. The significance of this test is not that it demonstrated ground-breaking technology — it didn't. The significance of the drone exercise resides in the concrete demonstration of how insidious a successful spoofing attack can be.

As a nation, do we have a well-reasoned national posture regarding civil location and time assurance? Do we understand the risks we assume when we rely on GPS? Can we improve our defensive posture? Or are we, like Edward Bear, doomed to doing things the same way we always have?

United States military and civil infrastructure has become critically dependent on GPS for providing timing and location. GPS works so well, and is disrupted so infrequently, that security issues surrounding its use have largely been ignored within the general user community.

Professor David Last, a British a radionavigation expert and consultant, has characterized GNSS as "the stealth utility" — its disruption can show up anywhere, often in unexpected and unpleasant ways. Systems that might appear to

NovAtel
QinetiQ

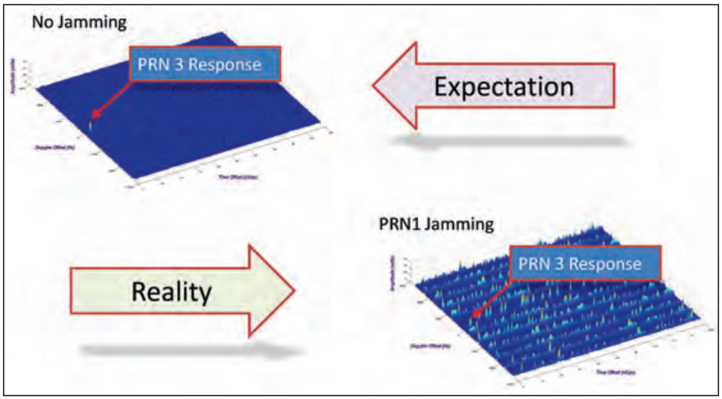


FIGURE 1 The Pole Star Receiver was confused. Simple checks would have kept receiver from reporting false position.

have no connection with GPS have failed during GPS jamming incidents because of unrecognized GPS dependencies. For example, in the well-known 2007 outage in San Diego, errant 500 milliwatt transmissions from a U.S. Navy ship jammed GPS signals and caused medical paging systems, which were frequency-disciplined by GPS, to fail.

GPS is a double-edged sword; on the one hand, an extraordinarily useful utility that is inexpensive to use, but on the other hand, a system technology that introduces major and often times poorly understood vulnerabilities.

The purpose of this article is to look at a wide spectrum of location-assurance security issues and describe possible hardening approaches that could be used to establish a defense in depth against intentional or unintentional intrusions into GPS operations.

Absent a widely understood and accepted consensus on these issues, establishing a coherent and integrated national posture regarding civil location assurance appears unlikely to occur. Instead, we will continue to flail about with stove-piped, spot solutions of varying effectiveness and limited application. Finally, although my focus here will mainly be on civil issues, much of the thinking is applicable to military applications.

What is Location and Time Assurance?

In the past, location assurance was mostly about accuracy, availability, and integrity with respect to one's own position. GPS receiver design tended towards standalone devices that reported position, velocity, and time to a human operator or to a guidance and control algorithm within a navigation system. Location was about navigating the individual.

Today, GPS receivers automatically report location to diverse applications, and their role has shifted towards providing the basis for relative navigation. As an example, the FAA's NextGen relies on automatically generated GPS position reports from aircraft to coordinate navigation through national airspace. In the future, I expect automobiles and robotic vehicles will be networked devices, cooperatively navigating with respect to each other for improved safety and efficiency. This networking aspect of location holds great promise, but it fundamentally alters the security landscape, introducing new vulnerabilities.

One of the greatest misconceptions surrounding location and time assurance is the presumption that this is solely a GNSS receiver issue. It is not. Assuring the "truthfulness" of this data is also a cybersecurity issue.

An attack on location and timing information may not even use RF spoofing or jamming of GPS itself. Cyber attack offers a more likely avenue of attack against poorly protected network-accessible systems. Such attacks are easier, don't require specialized hardware, and can be conducted from anywhere. The attack can be more anonymous, and, world-class experts — hackers — are available for hire at very reasonable rates.

Routine software and map updates provide opportunities to infect civil GPS receivers with targeted malware. Even if the GPS receiver is working fine, a man-in-the-middle attack may simply inject false positions into the system data stream — in short, lie about position. Cell phone apps for conducting this sort of attack are readily available. To hijack a UAV, an attacker might alter its waypoint database or disrupt its command and control links, while leaving its GPS receiver alone. Just about any component of an integrated system might be suborned, especially if it connects to a network.

Discussion of location assurance security architectures raises the important question of where we place trust in a system. The Stanford Encyclopedia of Philosophy entry on trust begins, "Trust is important, but it is also dangerous." When evaluating system architectures, we have to ask: how do we deal with a potentially corrupted GPS, a corrupted communications link, a corrupted autopilot, and so on and so forth? How can we prove location and time to remotely located second parties?

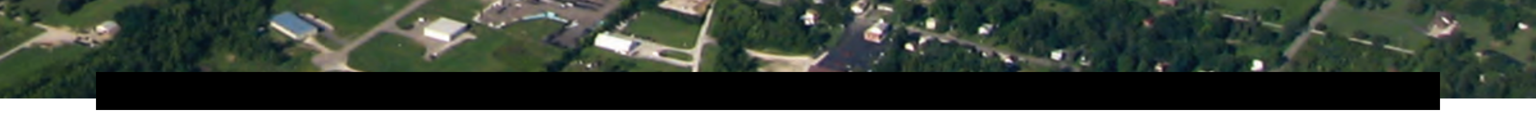
Overview of Defenses

Let's take a look at several broad and overlapping categories of strategies for mitigating vulnerabilities:

- individual situational awareness (ISA): knowing you are under attack and reporting it
- global situational awareness (GSA): understanding the attack and mounting a response
- legislative and electronic countermeasures, crosschecks, and backups
- authenticatable signals for proofs of location to second parties and antispoofing.

Some of these are straightforward to implement. Others require an act of national will. The approaches are applicable in varying degrees to both military and civil GPS receivers. The remainder of the paper will focus on these topics in varying detail followed by a series of recommendations.

Individual Situational Awareness (ISA). The receiver is the first line of defense. By the time the cavalry shows up you may be dead. One of the great weaknesses in many civil GPS receivers is that they implicitly trust everything they see and fail to perform basic sanity checks.



For example, during the Pole Star maritime jamming experiments conducted by British authorities in 2008, shipboard GPS was “spoofed” by a Gold code structure jammer, and the navigation system reported incorrect positions and speeds in excess of 100 knots. See **Figure 1**.

According to the subsequent report on the Pole Star experiment, this affected many dependent systems that rely on GPS, such as the ship’s automatic identification system transponder, the dynamic positioning system, the gyro calibration system, and the digital selective calling system. Simple signals checks could have detected the problem.

Last year’s Department of Homeland Security (DHS) report, “National Risk Estimate: Risks to United States Critical Infrastructure from Global Positioning System Disruptions,” showed strong reliance on GPS in diverse applications within the transportation, emergency services, communications, and energy sectors. Numerous dependencies were found and, it was noted that even basic jamming scenarios could persist undiagnosed for several days.

The DHS study observes that maintenance personnel often lack the training to recognize symptoms of GPS degradation due to interference and that many GPS receivers don’t alert users to the presence of jamming or interference. This results in a lot of ineffective flailing about, checking cables, restarting systems, and so on.

Some basic signals and navigation checks can detect, diagnose, and characterize jamming and spoofing attacks, and these do not require much in the way of hardware. I described some of these in presentations to the ION GNSS 2003 conference and the National Space-Based PNT Executive Committee Advisory Board cited in the Additional Resources section near the end of this article. (L. Scott, 2003 and 2011).

Using simple algorithms, receivers can measure numerous jammer parameters, such as received jammer power (J/N), jammer type, and pulse characteristics. Most of these measurements can be accomplished in less than one millisecond.

The trick is to do the signal checks and then report the results . . . *loudly*. Warn users when hazardously misleading information (HMI) is a possibility. You may not be able to continue operation but at least you have been alerted to the existence of the problem.

Receivers should also protect themselves against cyber attack. When you plug a receiver into the Internet, how do you know what site it is accessing? How do you know it is receiving uncorrupted maps and software?

Classic digital signature algorithms can help ensure authenticity and should be part of every receiver’s repertoire. Receivers should also be capable of signing their outputs and

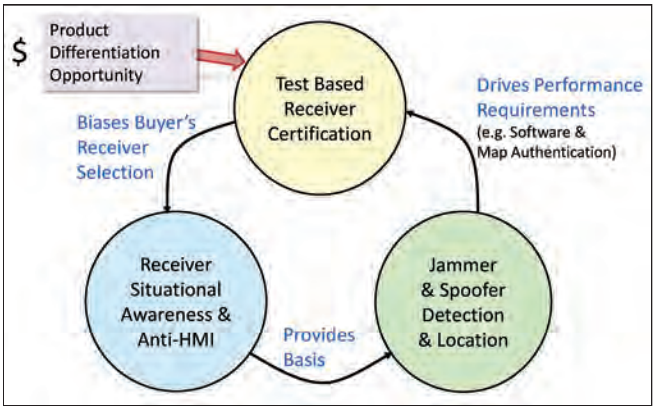

$ Product Differentiation Opportunity
Test Based Receiver Certification
Drives Performance Requirements
(e.g. Software & Map Authentication)
Biases Buyer's Receiver Selection
Receiver Situational Awareness & Anti-HMI
Provides Basis
Jammer & Spoofer Detection & Location

FIGURE 2 Test based receiver certification provides a path towards situational awareness.

proving who they are (attestation). Consider incorporating into the receiver trusted platform module (TPM) capabilities, as recommended by the Trusted Computing Group, a 10-year-old industry organization established to develop, define, and promote open, vendor-neutral industry specifications for trusted computing. TPM is not perfect, but it can go a long ways towards securing a receiver.

Referring to **figure 2**, a test-based receiver certification program would ensure minimum capabilities for situational awareness, and would provide the non-specialist GPS user community with a selection criterion for purchases with critical applications. The cellular telephony industry has been doing formal compliance testing for years and could provide a model for the GPS industry. A white paper referenced in Additional Resources, *GPS for Critical Infrastructure Certification Standard, Level 1,* details a few thoughts on how a receiver certification test might be structured.

Global Situational Awareness (GSA): An individual receiver has limited ability to discern a jammer's location, but reports from multiple receivers can characterize GPS disruptions and help determine the location of jammers/interferers. This is the idea behind DHS's Patriot Watch Interference Detection and Mitigation (IDM) program and the UK's GAARDIAN system developed by a team led by Chronos Technology. Such systems disseminate information on a jamming incident to enforcement agencies and potentially, to other users so they can be on their guard.

One of the key challenges in practically implementing such concepts will be synthesizing an informed assessment based on diverse reports from multiple sites and from diverse receiver types with wildly varying measurement and reporting capabilities. A successful GSA program would aid immensely in this process by drawing on a large body of "expert witnesses" in the form of multiple ISA-capable receivers.

Rather than getting no report, or a report that "My GPS doesn't work," an ISA-certified receiver containing a suite of situational awareness algorithms would report such data as:

- best estimate of observer location (with uncertainties)
- time of event and duration
- apparent C/N_0(s)
- received jam-to-noise ratio (J/N)
- jammer type (Gaussian, CW, Swept FM, Gold, Spoof)
- pulse/sweep characteristics

Ideally, these receivers could digitally sign reports (with attestation) to combat false reporting attacks on an IDM system.

Such information is essential in sorting jammers into track files. As a jammer moves about, multiple receivers may see the same jammer. The RF fingerprint of a jammer helps in associating reports so as to gain a clearer picture of its movement as a function of time. This factor can be critical in finding an offender. For instance, if a particular jammer goes by every day at the same time (e.g., 3 p.m.) but only on school days, there is a pretty good chance someone is using the company car to pick up the kids.

Obtaining wide-area geographic coverage is very problematic for an IDM system. Low-power jammers, such as so-called personal privacy devices (PPDs), may be detectable for only a few hundred feet in a ground mobile environment but can affect aircraft operations out to several miles. Hundreds of thousands of detectors would be needed to cover the United States.

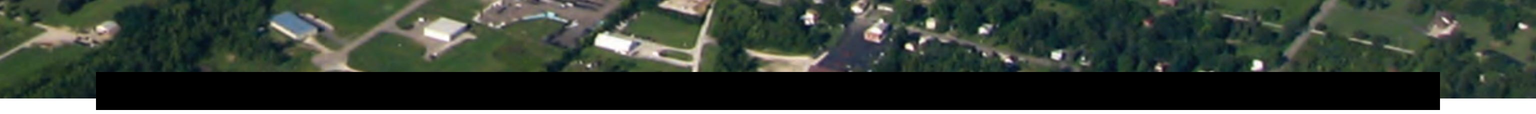
So, opportunistic observation — what we would call "crowd-sourcing" — is needed. Given enough observers, jammer locations can be determined directly based on received jammer strength. **Figure 3**, based on a paper presented at the ION GNSS 2011 conference (L. Scott 2011A), illustrates how the location of a small, 200-milliwatt jammer could be determined to within 40 meters if even a modest number of nearby cell phones were to report on jamming.

To be effective, IDM systems will require not only intelligent receivers, but lots of them, along with a reporting infrastructure that can provide timely alerts for response by public agencies.

Legislative Measures. In a civil society, the rule of law can protect individual and common interests. In the U.S., using, selling, advertising, or importing jammers (even one) is illegal and monetary penalties can exceed $100,000 per violation.

So far, most of the jamming incidents affecting civil operations appear to have been accidental or unintended. For instance, the trucker who accidently jammed FAA systems at Newark's Airport when he deliberately jammed his employer's GPS. Hopefully, strong laws will discourage casual jamming. That said, GPS/cellular jammers are an effective way to prevent police from tracking stolen vehicles, and organized theft rings are importing and using jammers for that purpose.

Electronic Countermeasures, Crosschecks, and Backups. Electronic countermeasures (ECM) are normally the purview of military users where jamming attacks are deliberate and intended. Some leading civil GPS equipment manufacturers, however, have shown that civil equipment can be made more robust against jamming.



For example, most commercially available GPS jammers use a swept FM waveform, for which there is a simple and strong "look-through" countermeasure. Jamming tends to be ground-based and, consequently, fixed installations can reduce jamming susceptibility by using antennas with low horizon gain. The key in all of this is for users and particularly manufacturers to educate themselves about possible threats and their mitigation.

That said, I don't see classic ECM techniques as a solution for the civil community. The most effective point defense ECM techniques (e.g., adaptive array antennas) have inherently large size, weight, power, and price footprints as well as export restrictions (e.g., ITAR – International Traffic in Arms Regulations). Also, most ECM techniques degrade accuracy. In particular, adaptive arrays are often incompatible with centimeter accuracy RTK receivers.

Absent an adaptive array, a determined and skilled adversary is going to win the battle to deny a particular signal. The best defense for civil users is agility: using a multitude of diverse signals and systems to crosscheck location and maintain good situational awareness regarding potential jamming and spoofing. Even if a few satellite signals are denied, continued operation is often possible.

An adversary will find it difficult to jam and/or spoof everything simultaneously, especially in integrated multi-technology systems where component subsystems have uncorrelated vulnerabilities. Loran is very difficult to jam or spoof over a wide area and could provide a formally validated backup to GPS. National policy should reinstate an authenticatable enhanced-Loran (eLoran) system, if not for navigation, then at least for timing crosschecks.

Are receivers with a Selective Availability/Anti-Spoofing Module (SAASM) an answer for non-governmental civilian users?

Probably not. Keyed SAASM receivers rely on encrypted military signals and thus do not have the same set of vulnerabilities as a civil receiver. DoD plans for introducing UAS call for use of keyed SAASM receivers and independent 3D radar surveillance to detect potential air space conflicts.

This is all to the good, but SAASM may prove unwieldy for civil users. Myriad operational and physical security challenges exist to using keyed military receivers in a civil environment, especially if the organization proposing to use these has significant foreign ownership. Just keying receivers is a daunting logistics challenge, and, without the keys, a SAASM receiver will have the same vulnerabilities as a civil receiver.

Returning to the UAS question for a moment, sole-source navigation is clearly vulnerable. In Humphreys' spoofing demonstration mentioned at the outset of this article, he spoofed only L1 C/A-code signals. GLONASS L1 signals, and/or GPS L5, and/or L2C pseudorange measurements could have detected presence of the spoofing. The victim receiver could have detected spoofing by checking for inconsistencies between J/N measurements and apparent C/No. A sudden change in IMU state covariance estimates was also probably seen when spoofing motion was applied. The attack was probably quite detectable and didn't have to lead to a controlled capture.

Establishing which signals are real and which are fake is an important requirement when continued operation is needed during a spoofing attack. The UAS could have continued operation using GLONASS L1 signals. Part of the reason Humphreys' attack succeeded is that civil GPS signals have absolutely no proof-of-origin features; so, spoofing civil GPS receivers is a straightforward proposition.

Securing UAS operations is critical before introducing UAS assets into national air space. Similar arguments apply for other transportation sectors. The problem is solvable, but backups, independent surveillance, signal authentication, and proofs of location are essential components.

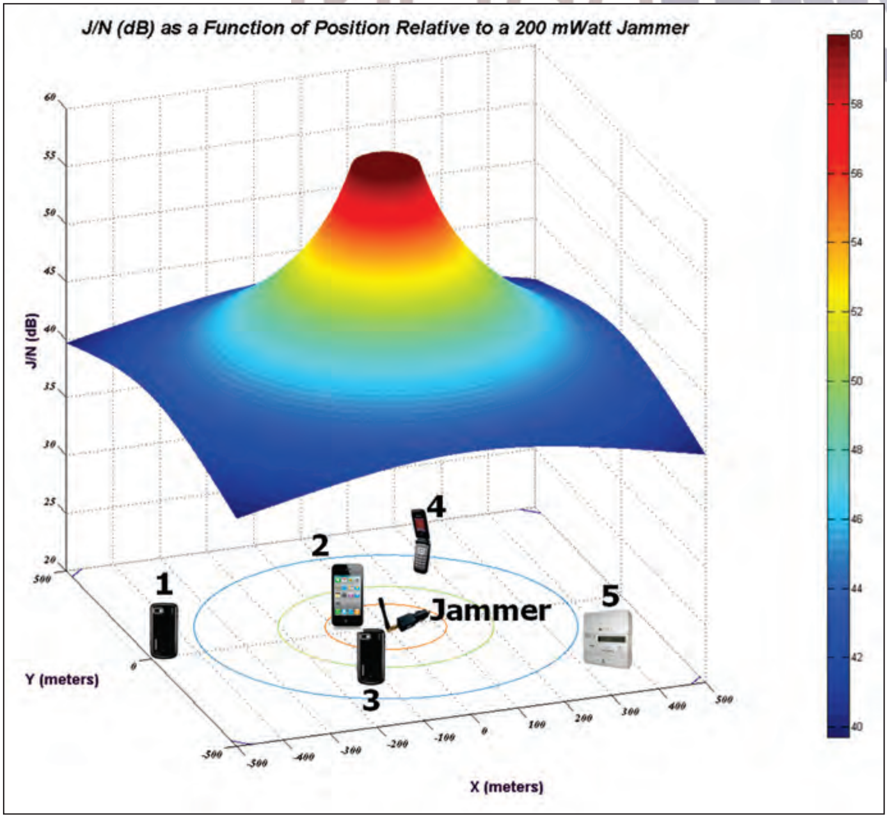
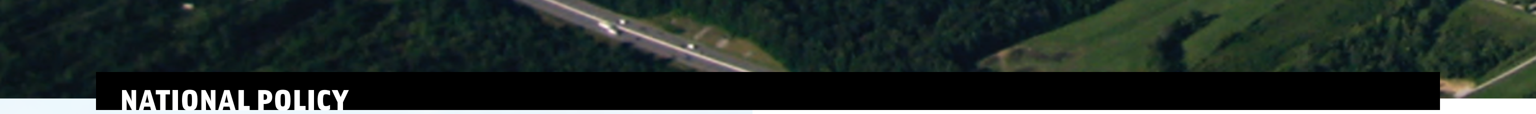


FIGURE 3 Crowdsourcing for jammer detection and location. Devices report jamming parameters and own position to J911, where, using the aggregate of received jamming strength reports, J911 can determine jammer position to ~40 meters. J911 can report interference events to networked users like traffic reports.



Authenticatable Signals for Proof of Location

Hardening systems against spoofing, jamming, and cyberattack is a powerful proposition, but ultimately operators must still place a measure of trust in the receiver and the reporting chain. This is particularly true when receiving position reports from a remote location.

Earlier, I noted the need for proofs of location operable on untrusted receivers and systems — that is, proofs of location that don't require one to trust the reporting party or any intervening parties. With authenticatable signals, hard-to-forge location signatures can be created and, such signals make spoofing much more difficult.

The Internet Security Alliance, a multi-sector trade association promoting public/private solutions to cybersecurity, has pointed out that the Internet is "an inherently global technology. In fact virtually every component of the system is designed, developed, manufactured or assembled off US shores and beyond the reach of US government oversight. *We must develop a way to construct a secure system out of potentially insecure parts.*" (emphasis added)

By some estimates, 15 percent of all spare and replacement integrated circuits purchased by DoD are counterfeit. Supply chain injection is often achieved using Internet purchasing systems with limited traceability.

Even supposedly secure hardware can be compromised. In a paper summarizing a real-world effort to extract the American Encryption Standard (AES) key from a military-grade FPGA marketed as "virtually unbreakable" and "highly secure," British researchers Sergei Skorobogatov and Christopher Woods demonstrated that "it is possible to extract the AES key from the Actel/Microsemi ProASIC3 chip *in a time of 0.01 seconds* using a new side-channel analysis technique called Pipeline Emission Analysis (PEA)." (emphasis added)

The point is this: how can you trust the location and/or time someone sends to you if you don't have independent means of verification? Having a receiver cryptographically sign position reports is a start in that it mitigates against certain attacks, but you are still placing a high level of trust in the receiver and it's ability to secure it's signing keys.

Location proofs seek to reduce requirements for trust in the GPS receiver and any intervening systems, such as cell phones, communications links, routers, switching centers, and so on. Why is this needed? Consider the following use cases:

In May of 2012, the U.S. Coast Guard responded to two bogus mayday calls, possibly linked. These calls were possibly a diversionary ploy in support of smuggling operations. The cost of mounting the searches was about $300,000 per incident. A proof of location on the call origin would have avoided this deception.

Internet-facing industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems control vast swaths of national infrastructure. These are the systems used for opening valves on pipelines, shifting phase on electric power grids, and controlling flows through chemical plants and oil refineries.

In principle, these are air-gapped systems and should not be reachable via Internet. In practice, however, sometimes they can be reached. For example, a paper by E. P. Leverett (cited in Additional Resources) describes how a specialty search engine called Shodan was used to find more than 7,500 control devices directly connected to the Internet. Traversing an enterprise's Internet accessible network often provides another avenue of access to control devices.

ICS systems are under active cyber attack. In 2011 the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) received 198 incident reports, up from 41 the prior year. Remote commands could be restricted to come only from authorized locations but only if strong proofs of location are available.

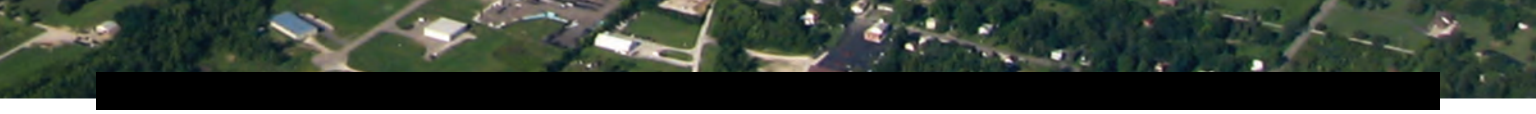
Recently, more than $75 million was siphoned away from ~60 banking institutions using malicious software installed on bank servers, according to a report by Fox News (see Additional Resources). A modern automobile has 70 to 100 embedded processors running 100 million lines of code and, yes, car-owners can receive firmware updates to their on-board applications, including navigation, route guidance, and braking subsystems. To prevent malicious insertion of malware, software updates could be restricted to come only from authorized locations and/or be performed only at authorized locations. But, again, these efforts will succeed only if strong proofs of location are available.

Smart phones and tablets have become the primary computer resource for millions of users, and location-based apps represent one of their most popular features. These devices represent a formidable information-security challenge because they can hold and access vast reservoirs of information, much of it very sensitive. They are mobile and can be lost or stolen.

Recent research sponsored by software security provider Symantec estimated that information represents almost half of a typical organization's value. Gen. Keith Alexander, director of the National Security Agency (NSA) and head of the U.S. Cyber Command, recently described the loss of industrial information and intellectual property through cyber espionage as "the greatest transfer of wealth in history" — estimated loss: about $500 billion.

In a recent Mobility Capability Package description focusing on the architectural components of providing a secure VoIP capability using commercial grade products, the NSA observes, "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)."

In short, security policy could circumscribe a device's capabilities based on its location. Expanding on this, before a cloud server gives access to sensitive information (such items



as base maps, tactical updates, intelligence data, design plans, source code, and computational resources), it could require location verification to ensure access is granted only to an authorized user at a secured facility.

Location is a core component of identity. However, having a device say, "I'm at Lat/Long 21.458181N, 157.752342W," is not sufficient. Proof is needed. **Figure 4** illustrates how this might apply in a military context.

As Avi Rubin, professor of computer science and director of Health and Medical Security Lab at Johns Hopkins University, noted in a recent presentation to the TED (Technology, Entertainment, Design) organization, heart pacemakers, automotive braking systems, voting machines, and many other devices have been hacked. The list is long and growing. Location-aware security paradigms and proofs of location should be part of a defense in depth for critical applications.

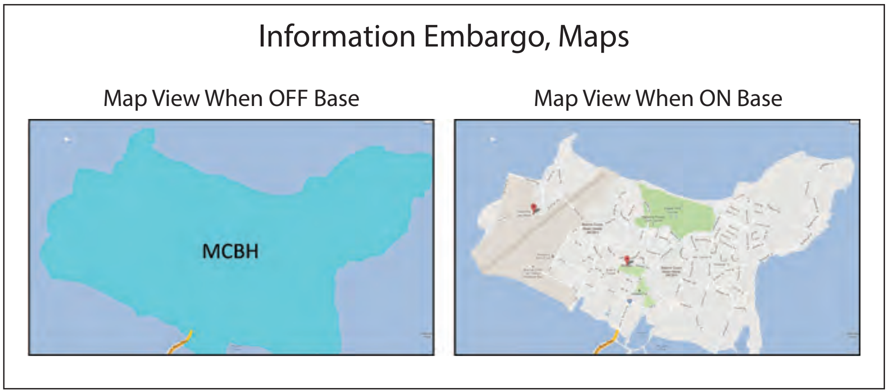


FIGURE 4 Which map is more useful for directing mortar fire? Provable location can georestrict maps, documents, software, and 3D printouts (parts).

So how can location be proved?

Pretty Good Proof of Location (But Not-So-Good Navigation)

For illustrative purposes, imagine a GNSS system in which spreading codes are encrypted and keys needed to generate the secure spreading codes are published by the control segment five minutes after the fact. Access to real-time spreading keys is restricted to the control segment and the space segment (satellites) — both trusted entities. The only thing user segment receivers can do with signals in real time is record raw A/D samples or stream them to other location(s) for storage and sequestration there. Once the spreading keys are published (digitally signed of course), user segment entities can process the raw A/D sample recordings of the signals to obtain the position and time — when the data was recorded — using either conventional processing or snapshot methods, as first described in the paper by Ben Peterson (Additional Resources).

Obviously, this method would not be a great way to build a real-time navigation system, but it would be very useful as a way to prove one's position in the recent past. Because the signal's spreading codes are encrypted, such signals could not be generated directly by a spoofer or forger. In principle, they could be read "off the air." However, the encrypted spread spectrum signals would be buried below the thermal noise floor and, as a result, would prove hard to read directly without a multiple beam, high gain antenna with one beam for each satellite visible.

Encrypted signals would make it hard for a receiver or spoofer to forge a false location signature without telltale signs. Consider this scenario: If a first-party receiver ("Harry") sends a 100 millisecond burst of raw A/D signal samples to a second party ("Thomas") *before the keys are released,* then Thomas can compute Harry's true position when the keys are released, confident that Harry would find it difficult to forge a false location signature in advance of the key's release.

Because the keys needed to generate such encrypted spread spectrum codes would only be published with a delay, secure key storage would not be needed. One would have to be careful that the signature key(s) are not from a forger, but because these key(s) can be published widely, their provenance can be authenticated in a variety of ways. This can be done, for example, by checking to see if they are cryptographically signed by the control segment with a key-signing key. Also, key blobs can be posted widely on the Internet with multiple servers; so, a user can compare results from different servers, which should be identical.

The fact that secure key storage is not needed in user equipment is highly advantageous as this is a very difficult and costly proposition, particularly in widely disseminated civil systems. All of the keys the user segment needs are publishable to anyone, subject to the five-minute delay to obtain secure keys for generating the spreading code.

The approach described here also has another important aspect: proofs of location are short lived and, they have embedded within them a time stamp (GPS time). A location signature (raw A/D samples) must be conveyed to Thomas before the keys are published. Harry can't use an old location, or forge a location signature based on previously published keys.

Extending the concept, portions of the signal might be generated using two-second delay keys whilst other portions are generated with five-minute delay keys. This would provide for a low-latency location proof channel but with a requirement for low-delay A/D sample sequestration.

Pretty Good Proof of Location (and a Good Navigation System)

The principle described in the previous section can be incorporated into any of the second-generation, modernized GNSS navigation signals (e.g., L2C, L5, L1C, and M-code for GPS) without compromising legacy receiver performance.

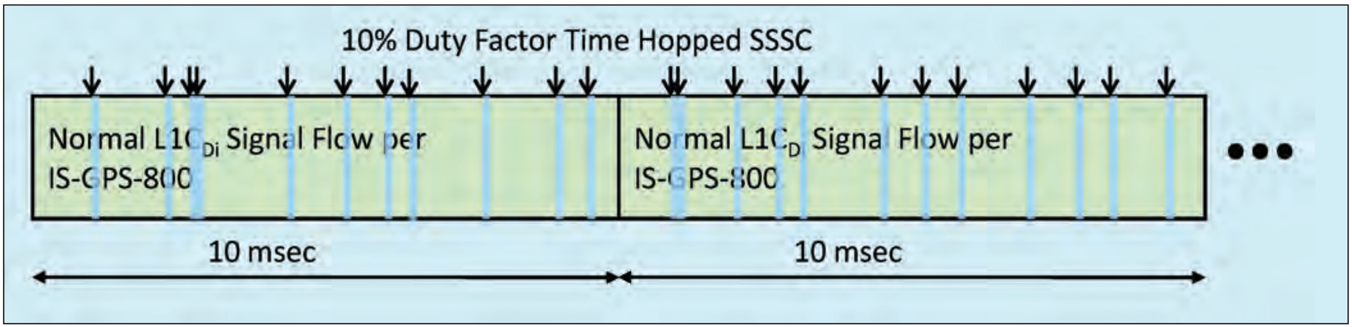

10% Duty Factor Time Hopped SSSC
Normal L1C$_{Di}$ Signal Flow per IS-GPS-800
Normal L1C$_D$ Signal Flow per IS-GPS-800
10 msec
10 msec

FIGURE 5 Watermarking signals with spread spectrum security codes (SSSC) can establish provenance, essential for proof of location using SATNAV. The watermark generating key is changed once every 5 minutes and published to the user segment with a 5-minute delay. The user segment does not have to have secure key storage. The watermark is hard to forge since a spoofer/forger has to read SSSC chips off the air.

Signal	Minimum Spoofer Antenna Gain*	Associated Antenna Diameter	Associated 2-sided 3dB Beamwidth
L1CD	21 diC	26″	18 degrees
L2CM	21 dBiC	34″	18 degrees
L5I	26 dBiC	63″	10 degrees
L1 WAAS	26 dBiC	47″	10 degrees

TABLE 1. Spoofer antenna requirements for various hardened GPS signal types

What follows is a thumbnail sketch of how this might be done. [The interested reader can find more detailed descriptions and supporting technical analysis in the following references in Additional Resources: L. Scott (2003), (2006), (2011B), (2011C), and (2012). The article L. Scott (2003) in particular is important because it establishes an early priority date and, very deliberately, no patents were applied for.]

Second-generation GNSS signals generally comprise two channels: a pilot channel and a data channel. The pilot channel is spread spectrum–modulated but does not have low rate (e.g., 50 bits per second) data modulated onto it. This allows for continued successful operation at lower signal-to-noise ratios, either due to attenuation or jamming. The data channel is also spread spectrum-modulated, but with a different spreading code and with a low rate data component to convey satellite orbital (ephemeris) and other data.

These two channels are transmitted synchronously and at the same frequency, either in phase quadrature or time division-multiplexed. Together, they constitute a modernized signal. For civil GPS, the data channel is used only for data conveyance and in some cases, initial acquisition. The pilot channel provides the primary inputs for navigation: pseudorange and pseudorange rate.

The data channel could be modified to include cryptographic signing and watermarking features that would allow for improved antispoofing and proof of location. Using the L1C signal as an exemplar, elements of the 50 bps data stream can be signed cryptographically, by each satellite using a unique signing key. This does not encrypt the 50 bps data stream; it just appends a digital signature to the data stream, which could be transmitted once every five minutes (representing a six percent duty factor on Subframe 3 of the CNAV navigation message).

Legacy receivers should ignore this message while "security-conscious" receivers would verify that the data stream originated from a GPS satellite, is correct, and is not fictitious. This forces potential spoofers to use off-the-air, collected data streams — a difficult proposition against receivers that read data and check for excess signal delay.

Cryptographic data signing is an important antispoofing step but is still inadequate for two reasons:

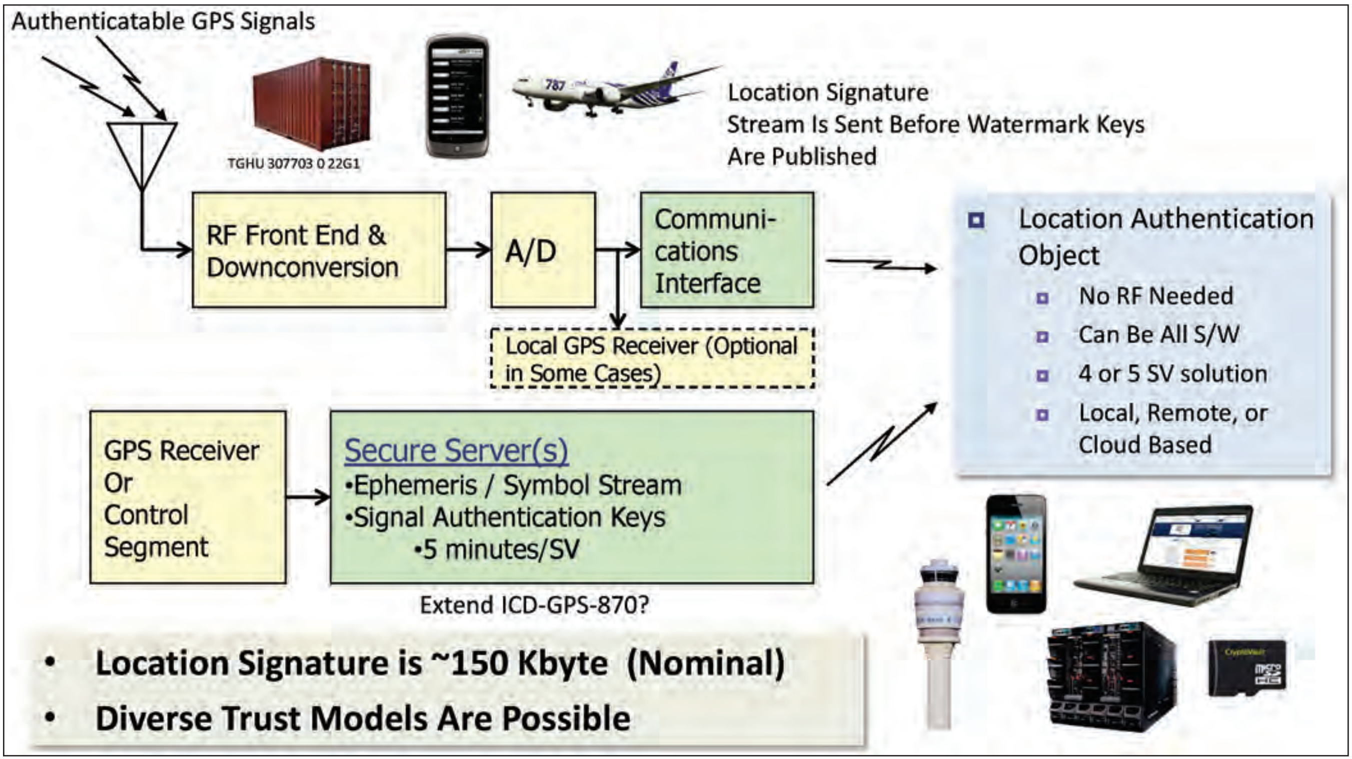
1. Most battery-operated GPS receivers don't read 50 bps data. They turn on for only a few milliseconds to measure pseudoranges and pseudorange rates to available satellites, and then they turn off. Satellite ephemeris is obtained via a network connection.
2. Data signing does not provide a mechanism for proving location to a remotely located second party (Thomas).

Figure 5 shows a signal construct that could overcome these limitations. Here, 90 percent of the data channel's timeline is devoted to transmitting normal L1CD (ICD-GPS-800B) signal while the remaining 10 percent of the timeline is repurposed to transmitting an encrypted, spread spectrum watermark based on the aforementioned 50-bps data stream signature. The watermark features both an encrypted, spread spectrum security code (SSSC) and a cryptographically controlled, time-hopping insertion pattern. This latter feature combats certain power-modulation attacks by making it difficult for a forger to be certain which chips are SSSC versus normal ICD-GPS-800B.

Implementing this watermarking protocol would reduce the signal-to-noise ratio (SNR) for data reading by 0.9 decibel, but navigation performance would be unaffected because this is the purview of the pilot channel, which remains unaltered. Also note that the satellite must know the digital signature before it is transmitted; so, data message updates would need to be restricted to the signing interval.

Figure 6 outlines how such a signal might be used in a proof of location. A GPS front-end downconverts the signal to intermediate frequency, A/D converts the ensemble of all L1C GPS signals in view, and forwards them to an *authentication object* where they are sequestered. The nominal duration of the location-signature burst would be about 100 milliseconds and would be about 150 kilobytes in size.

Once a satellite publishes the key needed to generate the



Authenticatable GPS Signals

Location Signature Stream Is Sent Before 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
•Signal Authentication Keys
•5 minutes/SV

Extend ICD-GPS-870?

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

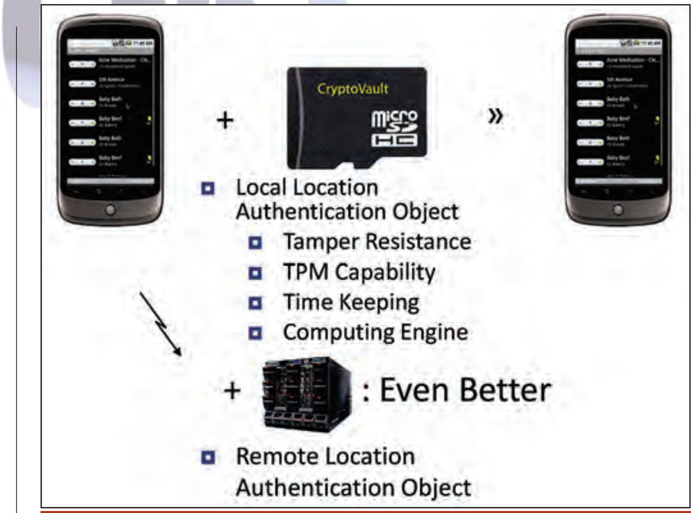
FIGURE 6 When keys are published, location authentication object(s) checks previously sent location signature for valid watermarks etc and computes sender's location and time.

watermark (the 50 bps data digital signature), an authentication object can validate that signal by checking to see that its watermark signal has the same C/N0 as the regular ICD-GPS-800 signal. A spoofer will find it difficult to generate a valid watermark as it would need to read individual spread spectrum chips off the air with a low probability of error. Table 1 gives some sense of how large an antenna the spoofer would need in order to forge a signature.

Returning to Figure 6, it is extremely important to note that the authentication object does not expressly require any RF reception capabilities. The first-party (still Harry's) GPS front-end has done all of the required GPS signal reception. Authentication objects can be 100 percent software entities using well-known software defined radio (SDR) techniques to process samples.

They also don't have to operate in real time. An authentication object can run in a general-purpose computing environment, a graphics processing unit, another cell phone, or on specialized hardware. In short, authentication objects can physically be anywhere — local, remote, or cloud-based. In order for the authentication object to determine Harry's location, in addition to the location signature (raw A/D samples), it needs the authentication keys and satellite ephemeris data. This data might be made available in several ways:

1. The control segment could publish keys (with appropriate delays) and ephemeris to the Internet and/or SIPRNet.
2. Secured server(s) with attached GPS receivers could collect required information and publish it as the data becomes available.



+ »

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

+ : Even Better

- Remote Location Authentication Object

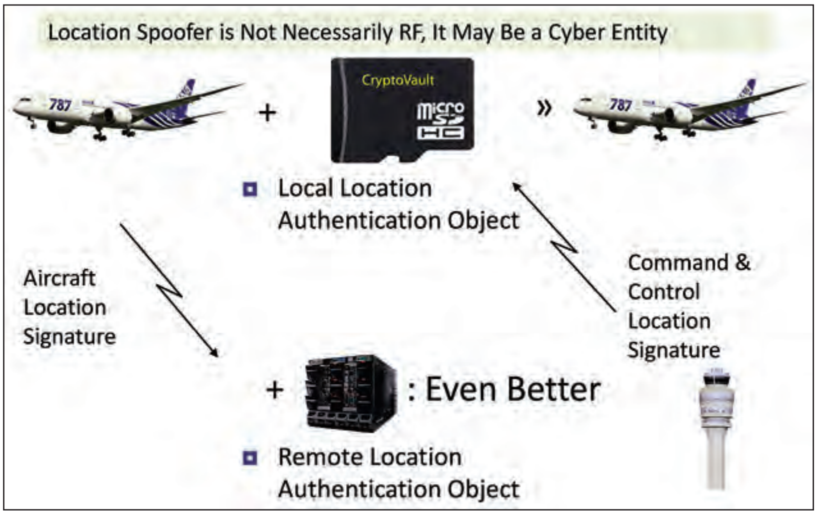
FIGURE 7 Stronger location assurance with civil devices.

3. Harry might provide the information from off-the-air received satellite signals.

This last approach is quite interesting as it raises the possibility of independent location verification within a standalone device. Figure 7 illustrates how a smart phone's location might be secured using authenticatable signals. A local authentication object in the form factor of a microSD (secure digital) card slips into the phone.

Ideally, the device would be tamper-resistant and have TPM capabilities in addition to timekeeping and a position-computing engine. The GPS receiver integral to the phone would feed location signatures to the microSD for sequestration. Once authentication keys are published either via satellite or via Internet, it could compute location and sign the results. In effect, the microSD card provides independent verification to the phone's internal GPS.

Expanding on the concept, occasionally location signatures could be sent from the phone to external, authentication objects at remote locations for additional independent verification. This might be required only when accessing particularly sensitive or remote data, or it might be done to check the local microSD device ("watching the watchers"). Other data, such as inertial measurement unit and compass outputs, celltower IDs, or signals from other GNSS systems, might also be sent to location authentication objects as additional location-signature elements for crosscheck analysis.



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

787
+
CryptoVault
micro SD HC
»
787
▪ Local Location Authentication Object
Aircraft Location Signature
Command & Control Location Signature
+
: Even Better
▪ Remote Location Authentication Object

FIGURE 8 Civil aircraft can prove their location. Autonomous aircraft raises the bar for location security performance.

Figure 8 repeats the secured smart phone scenario except that now the device to be secured is an aircraft, possibly of foreign registry. Typically, automatic dependent surveillance–broadcast (ADS-B) transponders don't support data rates high enough for frequent location signatures, but other onboard communications systems (e.g WiFi support systems) could be used on occasion to validate the onboard GPS receiver and local location authenticator.

Finally, I should acknowledge that other techniques for proving location have been proposed — such as those in the articles by M. Psiaki *et alia* and S. Lo *et alia*. However, these solutions suffer from a variety of drawbacks. Most importantly, they can't operate in a standalone configuration but rather require network connectivity to convey location signatures. A further disadvantage is that they presume military codes are secure, and, so, they place trust not only in the control segment and space segment, but also in the hundreds of thousands of keyed military user equipments.

Why is a National Posture Needed?

> *"Leadership is the art of getting someone else to do something you want done because he wants to do it."*
> — Dwight D. Eisenhower

One very astute observer has noted that location assurance suffers from the "tragedy of the commons": many see the need for it but no one wants to pay for it. Or else, they have responsibility but only in a restricted domain, for instance, civil airspace.

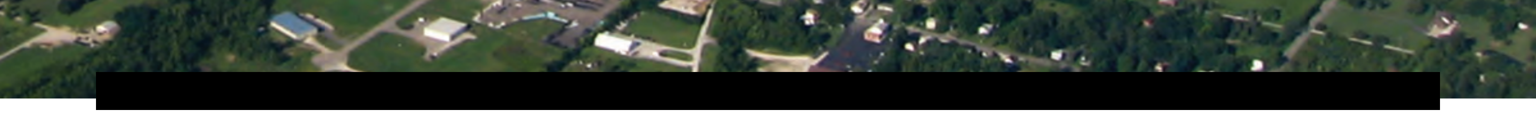
Leadership is needed to encourage industry to be more security-aware and to develop location assurance approaches with wide applicability across several domains. Stovepipes are not the answer.

Indeed, the realm of location assurance could be where GPS loses its "Gold standard" status. Galileo, and perhaps Compass, will include civil signal authentication features. To promote higher use of their systems, civil receivers used in their respective countries may be required to use authenticatable signals, and the authentication keys could be sold as a source of revenue.

If these systems also include "proof of location" capabilities unsupported by GPS, GPS competitiveness as a worldwide civil system will diminish. In the United States, we could even find ourselves reliant on these foreign GNSS systems in critical security applications.

Among the priority activities needed to begin to achieve location assurance at a national level:

- **Raise awareness about civil threats.** Educate industry about civil threats and detection methods. The DHS's National Risk Estimate is a great start, but it needs wider dissemination. Fund university research on location assurance.
- **Encourage Individual Situational Awareness in receivers through test-based receiver certification.** This is the GPS equivalent of penetration testing used throughout the security industry. It is the low hanging fruit. It doesn't have to be expensive and the potential gains are immense. The trick will be to keep it simple so it is sees wide adoption. In the May/June issue of *Inside GNSS,* Jules McNeff observes that we've been talking about receiver certification for 20 years. The time to act is now.
- **Establish mechanisms for substantive and meaningful input to the GPS program from the civil sector.** Military and civil priorities are not the same and, too often, civil needs take a back seat, especially now that the civil budget has been cut once again.
- **Develop systems for collecting and disseminating information about jamming and spoofing incidents.** Civil reporting has to be a two-way street; otherwise, why bother to report. Connected receivers should be able to access disruption reports in much the same way as they access traffic conditions.
- **Provide indigenous backup capability, particularly for time, and promote its use.** Yes, I'm talking about eLoran.
- **Phase in authenticatable L1C, L2C, L5, and Wide Area Augmentation System (WAAS) GPS civil signals.** This is obviously a



long lead item, but it is essential to the maintain leadership status for the Global Positioning System.

One of the great lessons from our recent fires here in Colorado is that fire mitigation is best done in advance. We learned this lesson in 2002, and again in 2012. Renovating a house while it is on fire is very difficult, especially if the house was built without any regard for fire safety.

Additional Resources

[1] American Enterprise Institute, event July 9, 2012, "Cybersecurity and American Power," video at <http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power>

[2] Bellows, C., "GPS Operations Center." 47th meeting of the Civil GPS Service Interface Committee (CGSIG), Fort Worth, Texas, USA, September 24, 2007

[3] Charette, R., "This Car Runs on Code", *IEEE Spectrum,* February 2009

[4] CNN News, <http://edition.cnn.com/2012/06/20/travel/yacht-sos-hoax>, accessed 7 July 2012

[5] Department of Defense, Small Business Innovation Research (SBIR) topic MDA12-026, "Marking of Components for Avoidance of Counterfeit Parts" <http://www.dodsbir.net/sitis/archives_display_topic.asp?Bookmark=42686> accessed August 26, 2012

[6] Department of Homeland Security, "National Risk Estimate: Risks to United States Critical Infrastructure from Global Positioning System Disruptions," briefed by Brandon Wales, Director, DHS Homeland Infrastructure Threat & Risk Analysis Center, at November 9, 2011, PNT ExCom Advisory board. <http://www.gps.gov/governance/advisory/meetings/2011-11/wales.pdf> (accessed August 24, 2012)

[7] Federal Aviation Administration, *NextGen Implementation Plan,* March 2012

[8] Federal Communications Commission, Enforcement Advisory No. 2012-02, March 6, 2012

[9] Fox News, <http://www.foxnews.com/tech/2012/06/25/drones-vulnerable-to-terrorist-hijacking-researchers-say>

[10] Fox News, <http://www.foxnews.com/tech/2012/06/26/cyber-bank-robbers-attempt-billion-dollar-heist-targeting-your-money>

[11] Grant, A., and P. Williams, N. Ward, and S. Basker, "GPS Jamming and the Impact on Maritime Navigation," The Journal of Navigation, 62, 173–187. The Royal Institute of Navigation, 2009

[12] Internet Security Alliance, "The Cyber Security Social Contract for the Obama Administration and the 111th Congress" at <http://www.whitehouse.gov/files/documents/cyber/ISA%20-%20The%20Cyber%20Security%20Social%20Contract.pdf Accessed 3 July 2012>

[13] Leverett, E. P., *Quantitatively Assessing and Visualising Industrial System Attack Surfaces,* University of Cambridge, Computer Laboratory, Darwin College, June 2011 MPhil Dissertation

[14] Lo, S., and D. de Lorenzo, P. Engel, D. Akos, and P. Bradley, "Signal Authentication, A Secure Civil GNSS for Today," *Inside GNSS,* Sept/Oct 2009

[15] McNeff, J., "GPS Receiver Specifications Compliance and Certification," *Inside GNSS,* May/June 2012

[16] Mitch, R., and R. C. Dougherty, M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon,. "Signal Characteristics of Civil GPS Jammers," ION GNSS 2011, Portland, Oregon, USA, September 22, 2011

[17] National Security Agency, "Mobility Capability Package," Secure VoIP Version 1.2, March 26 2012. Also NSA BAA-002-12

[18] Peterson, B., and R. Hartnett and G. Ottman, "GPS Receiver Structures for the Urban Canyon", The 8th International Technical Meeting of The Satellite Division of the Institute of Navigation, September 12-15, 1995, especially the section titled "Obtaining Fixes without Time from Satellites, starting on page 1329

[19] Psiaki, M., and B. W. O´Hanlon, J. A. Bhatti, and T. E. Humphreys, "Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals", ION GNSS 2011

[20] Qiu, D., and S. Lo, P. Enge, D. Boneh, and B. Peterson, "Geoencryption using Loran," The 2007 Institute of Navigation International Technical Meeting, San Diego, California, USA, January 22, 2007

[21] Rubin, A.,"All Your Devices Can be Hacked," <http://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked.html>, October 2011

[22] Scott, L., GPS for Critical Infrastructure Certification Standard, Level 1. Available at <http://logan.scott.home.comcast.net/~logan.scott/Critical%20Infrastructure%20GPS%20Certification.pdf>

[23] Scott, L. (2003), "Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems" ION GNSS 2003

[24] Scott, L. (2006), "L1C Should Incorporate Cryptographic Authentication Features," May 2006 Comments on ICD-GPS-800

[25] Scott, L. (2011), Receiver Certification: Making the GNSS Environment Hostile to Jammers & Spoofers, presented Nov 9, 2011, to Space-Based PNT EcCom Advisory Board. Available at <http://www.pnt.gov/advisory/2011/11/scott.pdf>

[26] Scott, L. (2011A), "J911: The Case for Fast Jammer Detection and Location Using Crowd-sourcing Approaches," ION GNSS 2011, Portland, Oregon, USA, September 22, 2012

[27] Scott (2011B), "Civilian GPS Signal in Space Enhancements for Anti-Spoofing and Location Authentication", presented at JNC 2011, June 28, 2011

[28] Scott, L. (2011C), "Civilian GPS Signal in Space Enhancements for Location Authentication & AntiSpoofing" presented to Independent Review Team, December 7, 2011

[29] Scott, L. (2012), "Location Signatures: Proving Location to Second Parties without Requiring Trust," JNC 2012, June 12, 2012

[30] Skorobogatov, S., and C. Woods, "In the blink of an eye: There goes your AES key (DRAFT of May 28, 2012)"

[31] Symantec, "State of Information Global Results 2012," <http://www.symantec.com/content/en/us/about/media/pdfs/2012-state-of-information-global.en-us.pdf>

[32] Trusted Computing Group, "Trusted Platform Module," <http://www.trustedcomputinggroup.org/developers/trusted_platform_module>, accessed July 7, 2012

[33] U.S. Senate Committee on Armed Services report, "Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain," May 21, 2012

Author

Logan Scott, principal in LS Consulting, of Fort Collins, Colorado, specializes in radio frequency signal processing and waveform design for communications, navigation, radar, and emitter location. He has more than 30 years of military and civil GPS systems engineering experience. As a member of the senior technical staff at Texas Instruments, he pioneered approaches for building high-performance, jamming-resistant digital receivers. He is currently active in precision indoor navigation, a jammer location system, nuclear materials detection, and, location based encryption and authentication. Logan holds 34 U.S. patents. He holds a BSEE degree from Columbia University, New York. IG