LAUR-04-1937

Talk for the Business Contingency Planning Conference, May 23-27, 2004 (Las Vegas, NV)

Think GPS Offers High Security? Think Again!

Roger G. Johnston, Ph.D., CPP

Jon S. Warner, Ph.D.

Vulnerability Assessment Team

Los Alamos National Laboratory

505-667-7414 rogerj@lanl.gov

http://pearl1.lanl.gov/seals.default.htm

Los Alamos
NATIONAL LABORATORY

VAT

Think GPS Offers High Security? Think Again!

Abstract

The Global Positioning System (GPS) is being increasingly used for a variety of important applications. These include public safety services (police, fire, rescue, and ambulance), marine and aircraft navigation, vehicle theft monitoring, cargo tracking, and critical time synchronization for utility, telecommunications, banking, and computer industries. Civilian GPS signals—the only ones available to business and to most of the federal government—are high-tech, but not high-security. They were never meant for critical or security applications. Unlike the military GPS signals, civilian GPS satellite signals are unencrypted and unauthenticated. This makes it easy for even relatively unsophisticated adversaries to jam or counterfeit them. Counterfeiting ("spoofing") of civilian GPS signals is particularly troublesome because it is totally surreptitious, and (as we have demonstrated) surprisingly simple. The U.S. Department of Transportation (DOT) has warned of vulnerabilities and looming problems associated with over-reliance and over-confidence in civilian GPS. Few GPS users appear to be paying attention.

Leon Lopez
Ron Martinez
Adam Pacheco
Jon Warner, Ph.D.

Roger Johnston, Ph.D., CPP
Anthony Garcia
Sonia Trujillo

Los Alamos Vulnerability Assessment Team

http://pearl1.lanl.gov/seals/default.htm

Goal

The goal of this talk is to alert users of civilian GPS to its inherent vulnerabilities.

Don’t become over-reliant or over-confident!

There are no known significant incidents of civilian GPS jamming or spoofing… yet.

We feel this talk is justified because:

- Security users need to understand that there are vulnerabilities associated with GPS.
- DOT has made a great effort to get this vulnerability message out to users, but without much success.
- Discussion of the civilian signal is unclassified.
- We believe that, at this point, we are helping the good guys more than the bad guys.

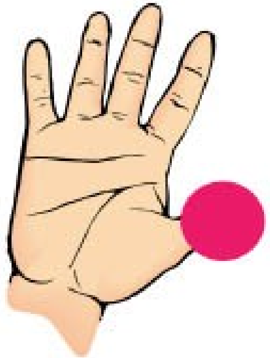
Classification Issues

- Discussion of civilian GPS signals and their vulnerabilities is unclassified.
- Discussion of vulnerabilities in civilian GPS receivers is unclassified.
- Any discussion of military or weapons systems aspects is classified.
- Any discussion of satellite vulnerabilities is classified.

Helping the Good Guys?

- Classic security dilemma: When does discussing security vulnerabilities help the “bad guys” more than the “good guys”?

- Rule of Thumb: If the good guys have a sophisticated understanding of security & vulnerabilities, then limit discussion. If, on the other hand (as with GPS), the good guys have a widespread lack of recognition of serious probl then discuss openly.



GPS Facts

- Officially called the NAVSTAR System (for “Navigation Satellite Timing and Ranging”).
- 21 active satellites (+3 standbys) orbiting at 11,000 miles.
- The satellites are essentially flying atomic clocks that transmit radio signals.
- Fully operational in 1995.
- The civilian (L1) signal is at 1575.42 MHz (UHF band).

GPS Facts

- Signal strength is 1×10^{-16} Watts at the Earth’s surface.

- The GPS receiver knows where each satellite is supposed to be at a given time. The distance to the satellite is then determined by the time of flight of the radio signal.

- Signals from at least 4 satellites are needed to determine an accurate position (latitude, longitude, altitude).

GPS Facts

- (Civilian) position accuracy is 20-40 feet with standard GPS receivers, and 3-16 feet with differential GPS receivers. (The civilian signals are no longer deliberately degraded by DoD as of May 2000.)
- GPS revenues ~$18 billion/year, growing at 30% per year. (30% US, 44% Japan, 23% Europe).
- 16% of all GPS systems are used in the trucking industry.

Some GPS Applications

- art
- watches
- pet collars
- cell phones
- cargo security
- vehicle tracking
- maps & surveying
- outdoor recreation
- time synchronization
- land, sea, & air navigation
- emergency response (fire, ambulance, police)

Cutting Edge GPS Systems

Casio GPS Watch (PAT-2GP)

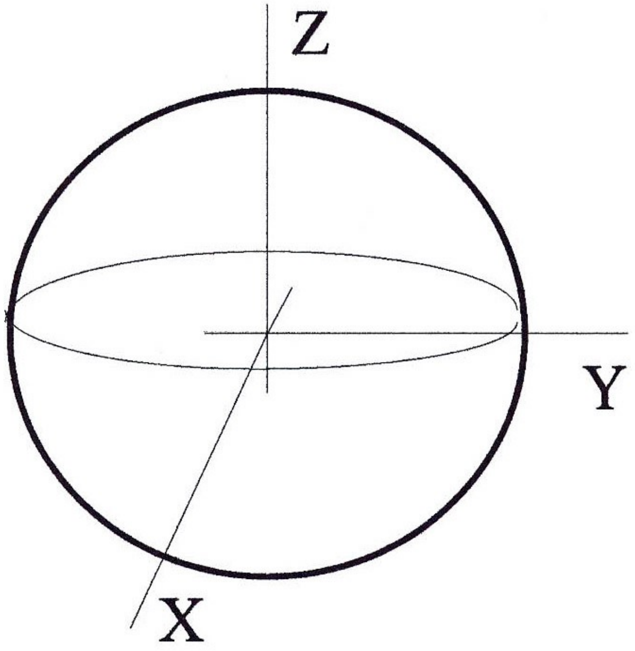
Wherify GPS Personal Locator

Garmin NAVTalk GPS/Cellphone

Motorolla Instant GPS (0.25Óx 0.25Ó)

How GPS Works

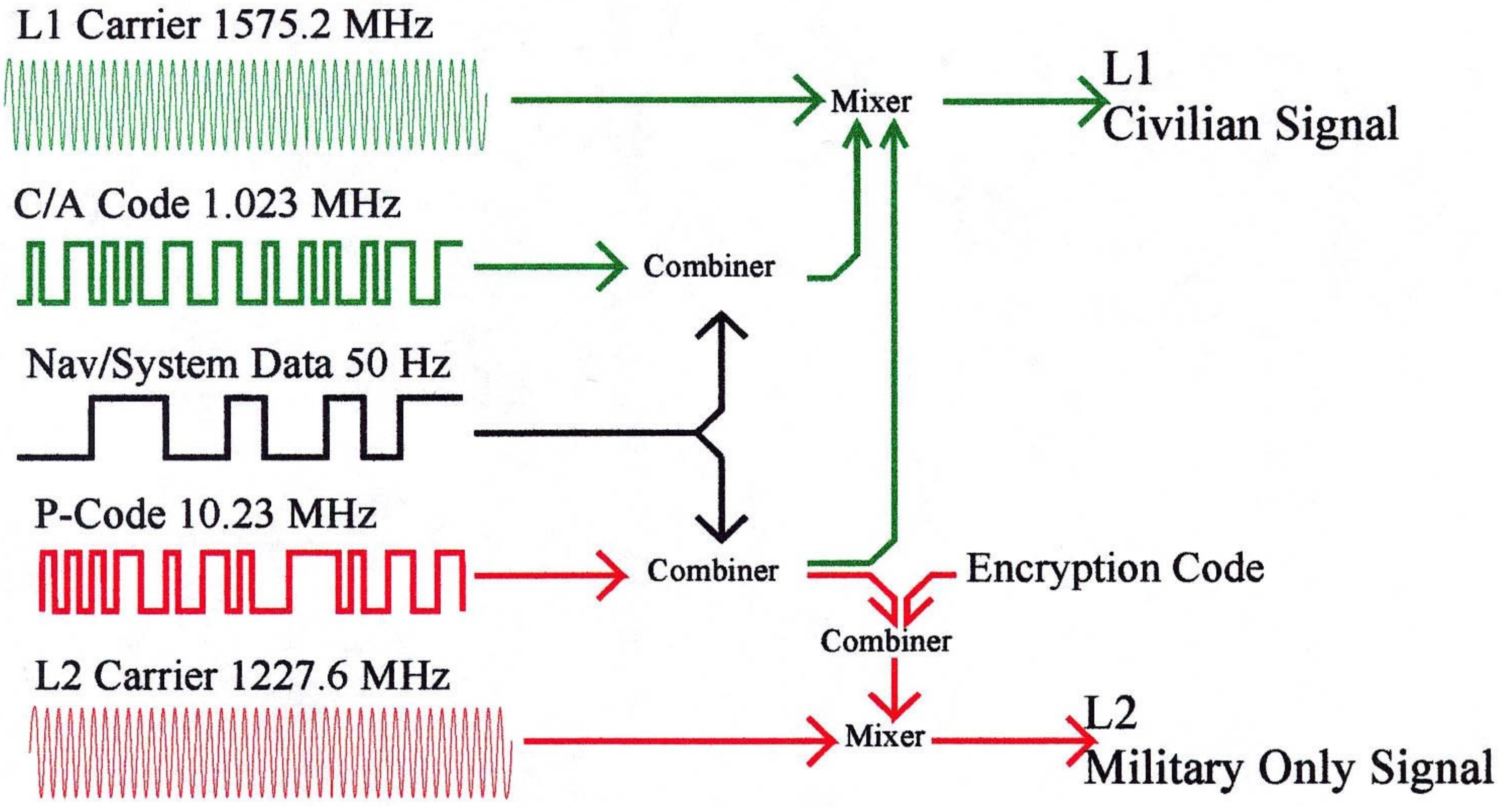
GPS Coordinate System



Earth Centered Earth Fixed
WGS 84

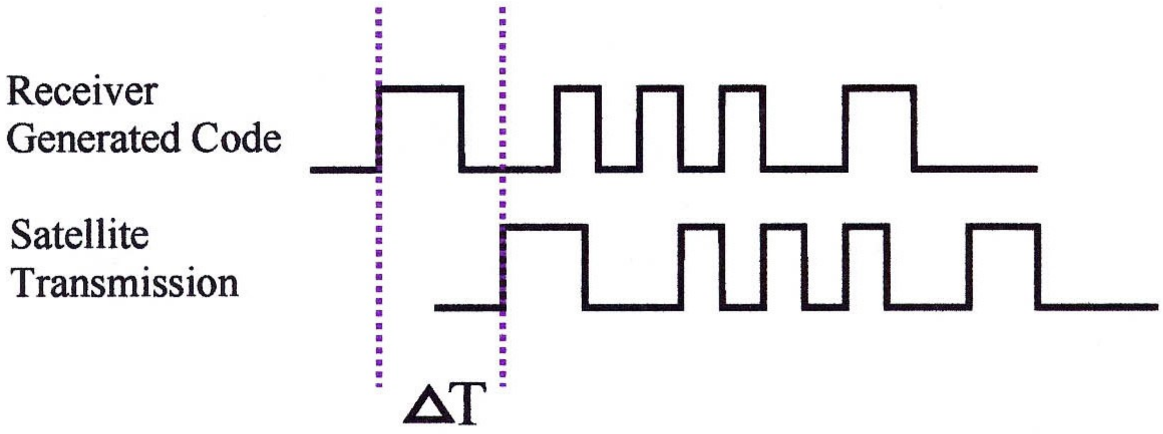
- Transmissions are controlled by atomic clock.
- Satellite position is known precisely at all times.
- Each satellite sends a unique ID number.
- Signal strength at Earth surface = -160dBW (10^{-16} W).

GPS Signal Structure



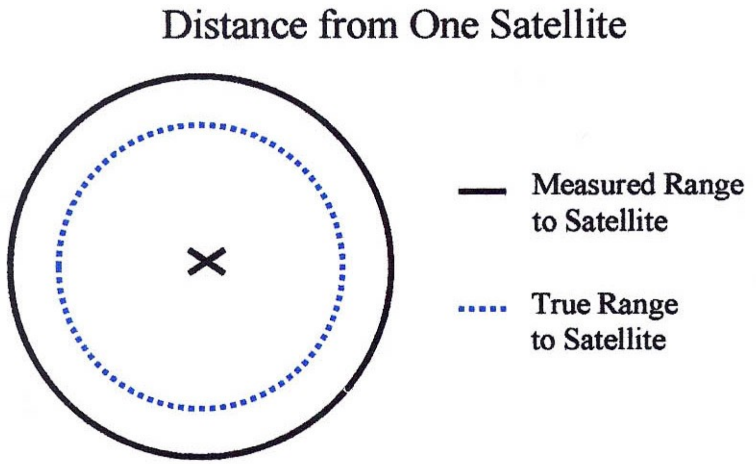
Determining Distance

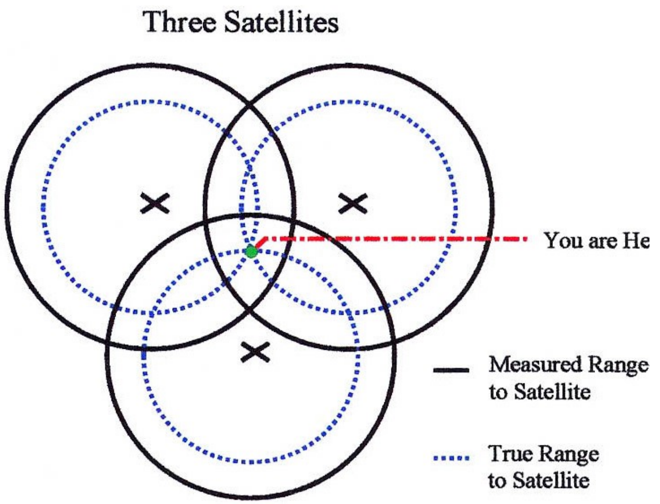
- Satellite repeats unique C/A code every 1 ms.
- Receiver generates satellite code, compares time delay from satellite signal.
- Distance to satellite = ΔT * Speed of Light.



Determining Position

- One satellite is not very helpful.
- Three satellites will give a position.
- Four satellites will give position and altitude.





DOT GPS Warning

“As GPS further penetrates into the civil infrastructure it becomes a tempting target that could be exploited by [hostile] individuals, groups or countries... The potential for jamming exists. The potential for inducing a GPS receiver to produce misleading information exists.”

Attacking GPS Receivers

Blocking: break off the antenna, or shield it with metal; not surreptitious.

Jamming: easy to build a noisy rf transmitter (complete information is on the Internet); not surreptitious.

Spoofing: generate fake satellite signals; surreptitious & surprisingly easy for even unsophisticated adversaries.

Physical attacks: appear to be easy, too.

Jamming

- Low-level jamming can block detection, or induce position errors.

- A 10 Watt battery-powered jammer…

  * can cover hundreds of square miles

  * cost: ~$50 in parts

  * weight: ~1 lb

  * volume: < 50 in^3 in volume

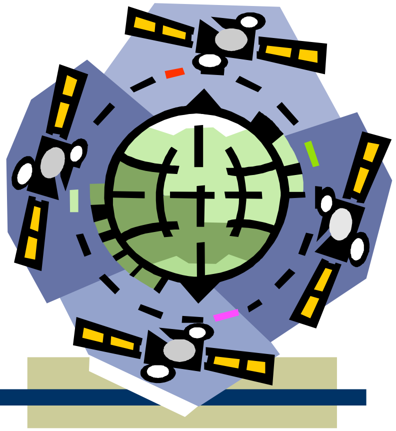
Jamming

"Jammers can be built by people with basic technical competence from readily available commercial components and publicly available information."

Spoofing GPS Receivers

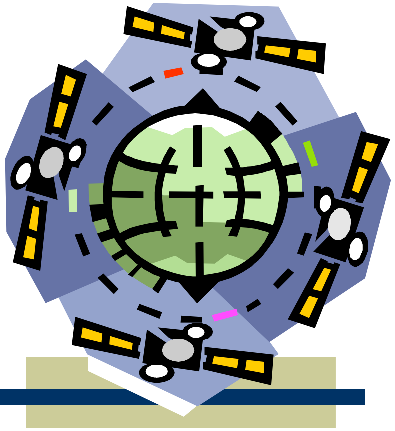
- Easy to do with widely available GPS satellite simulators.
- These can be purchased, rented, or stolen.
- Not export controlled.
- Many are surprisingly user friendly. Little expertise is needed in electronics, computers, or GPS to use them.

GPS Vulnerabilities



- The private sector and 90+% of the federal government must use the civilian GPS satellite signals.
- These are unencrypted and unauthenticated.
- They were never meant for critical or security applications, yet GPS is being used that way!

GPS Vulnerabilities



- Signal strength will increase, but there will be no encryption or authentication of the civilian GPS signal until at least 2018, if then.

- Civilian GPS signals are used to provide the critical synchronization time standard for national telecommunications, computer, utility, and financial networks.

GPS Vulnerabilities

- Many national networks are somewhat prepared for jamming but not for spoofing, which is easy and would crash the networks.

- The alternate time standard (NIST atomic clock) is also not secure.

- We know of simple, inexpensive counter-measures, but these are not being implemented.

NIST Time Standard

NIST-F1 Cesium Fountain Atomic Clock

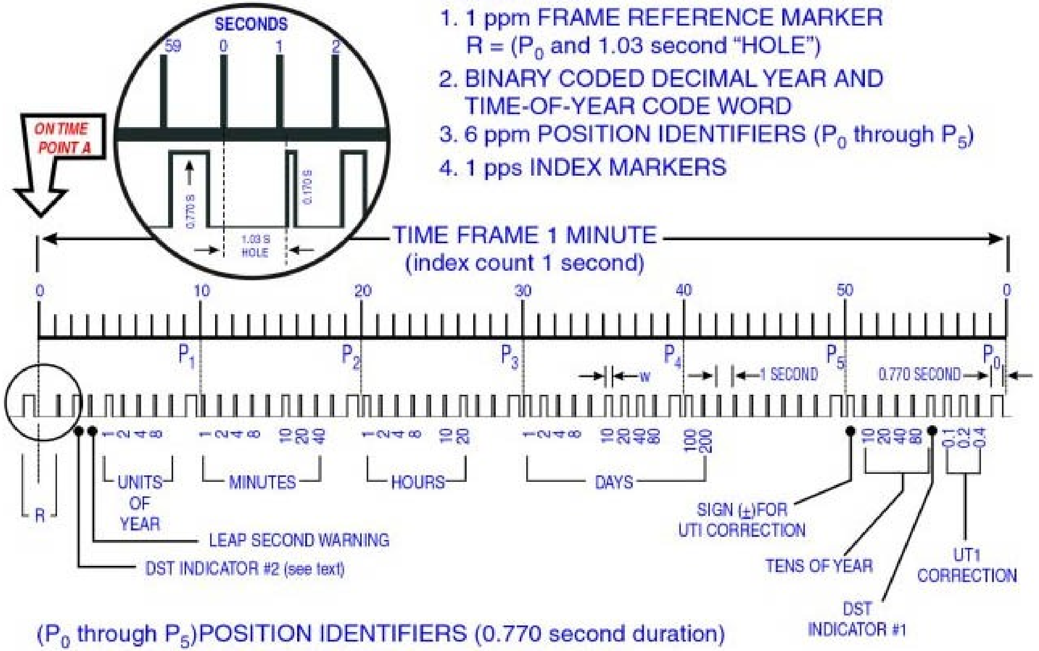
The Primary Time and Frequency Standard for the United States

NIST Time Standard

WWV and WWVH TIME CODE FORMAT

MODIFIED IRIG H FORMAT IS COMPOSED OF THE FOLLOWING:

1. 1 ppm FRAME REFERENCE MARKER R = (P_0 and 1.03 second "HOLE")
2. BINARY CODED DECIMAL YEAR AND TIME-OF-YEAR CODE WORD
3. 6 ppm POSITION IDENTIFIERS (P_0 through P_5)
4. 1 pps INDEX MARKERS



(P_0 through P_5)POSITION IDENTIFIERS (0.770 second duration)

W WEIGHTED CODE DIGIT (0.470 second duration)

DURATION OF INDEX MARKERS, UNWEIGHTED CODE, AND UNWEIGHTED CONTROL ELEMENTS = 0.170 SECONDS

NOTE: BEGINNING OF PULSE IS REPRESENTED BY POSITIVE-GOING EDGE.
UTC AT POINT A = 2001, 173 DAYS, 21 HOURS, 10 MINUTES
UT1 AT POINT A = 2001, 173 DAYS, 21 HOURS, 10 MINUTES, 0.3 SECONDS

NIST Time Standard

- Also not encrypted or authenticated.

- The information needed to counterfeit the NIST time signal is available on the Internet.

- NIST acknowledges the problem but appears to be doing little about it.

Greatest GPS Concerns
(Spoofing & Jamming)

1. Crashing of telecommunications, power, and computer networks (time)
2. Truck hijacking & cargo security (time & position)
3. Vehicle theft (position)
4. Attacks on security & industrial systems (time)
5. Financial transactions (time)
6. Other attacks on computers (time)
7. Tampering with aviation & maritime (time & position)
8. General nuisance jamming

How to Acquire a Civilian Simulator

1. **Build One**
   - Parts readily available.
   - Technical details are on the Internet.
   - Civilian signal characteristics are unclassified & public information.

2. **Rent or Buy One**
   - No questions asked.
   - Not export controlled.
   - Used simulators can be found on the Internet.
   - At least 12 companies sell new simulators.

How to Acquire a Civilian Simulator (con’t)

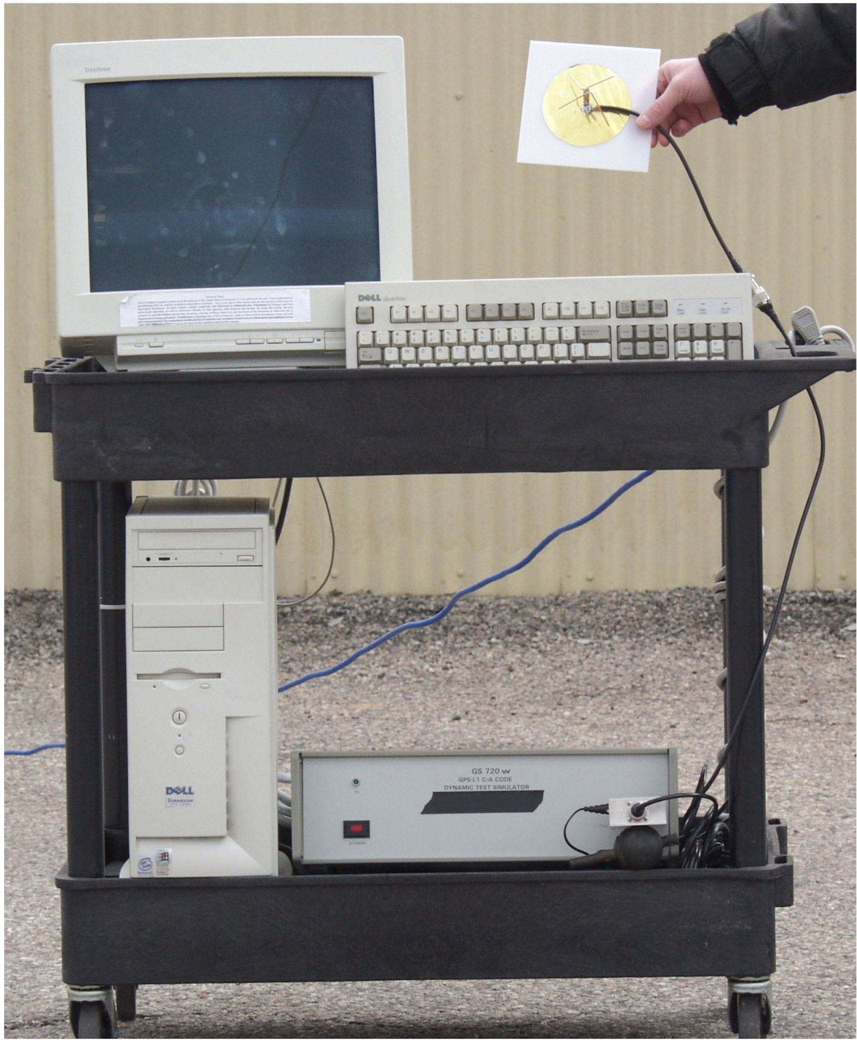
3. **Steal One (outsider or insider theft)**
    - Any company or organization dealing with GPS R&D has at least one.

Some Portable GPS Simulators

CAST 1000

IFR GPS-100

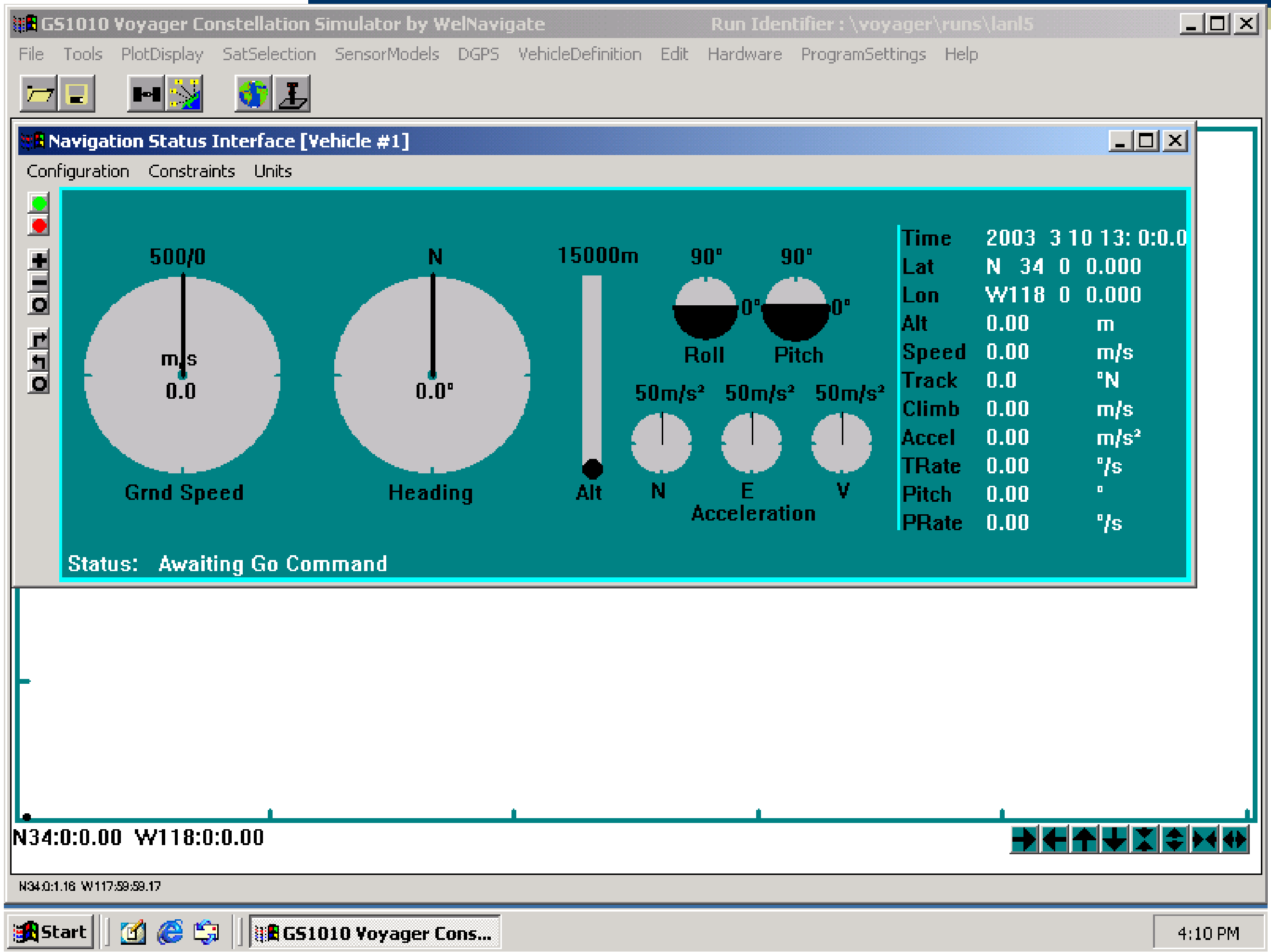
Our GPS Simulator



This Simulator Can:

- Jam
- Meacon
- Simulate the WAAS signal used for aviation
- Broadcast from 10 satellites at once
- Completely counterfeit the GPS signal

The GPS Simulator Is Easy To Use


GS1010 Voyager Constellation Simulator by WelNavigate
Run Identifier : \voyager\runs\lanl5
File Tools PlotDisplay SatSelection SensorModels DGPS VehicleDefinition Edit Hardware ProgramSettings Help
Navigation Status Interface [Vehicle #1]
Configuration Constraints Units
500/0
m/s
0.0
Grnd Speed
N
0.0°
Heading
15000m
Alt
90°
0°
Roll
90°
0°
Pitch
50m/s²
50m/s²
50m/s²
N
E
V
Acceleration
Start
GS1010 Voyager Cons...
4:10 PM

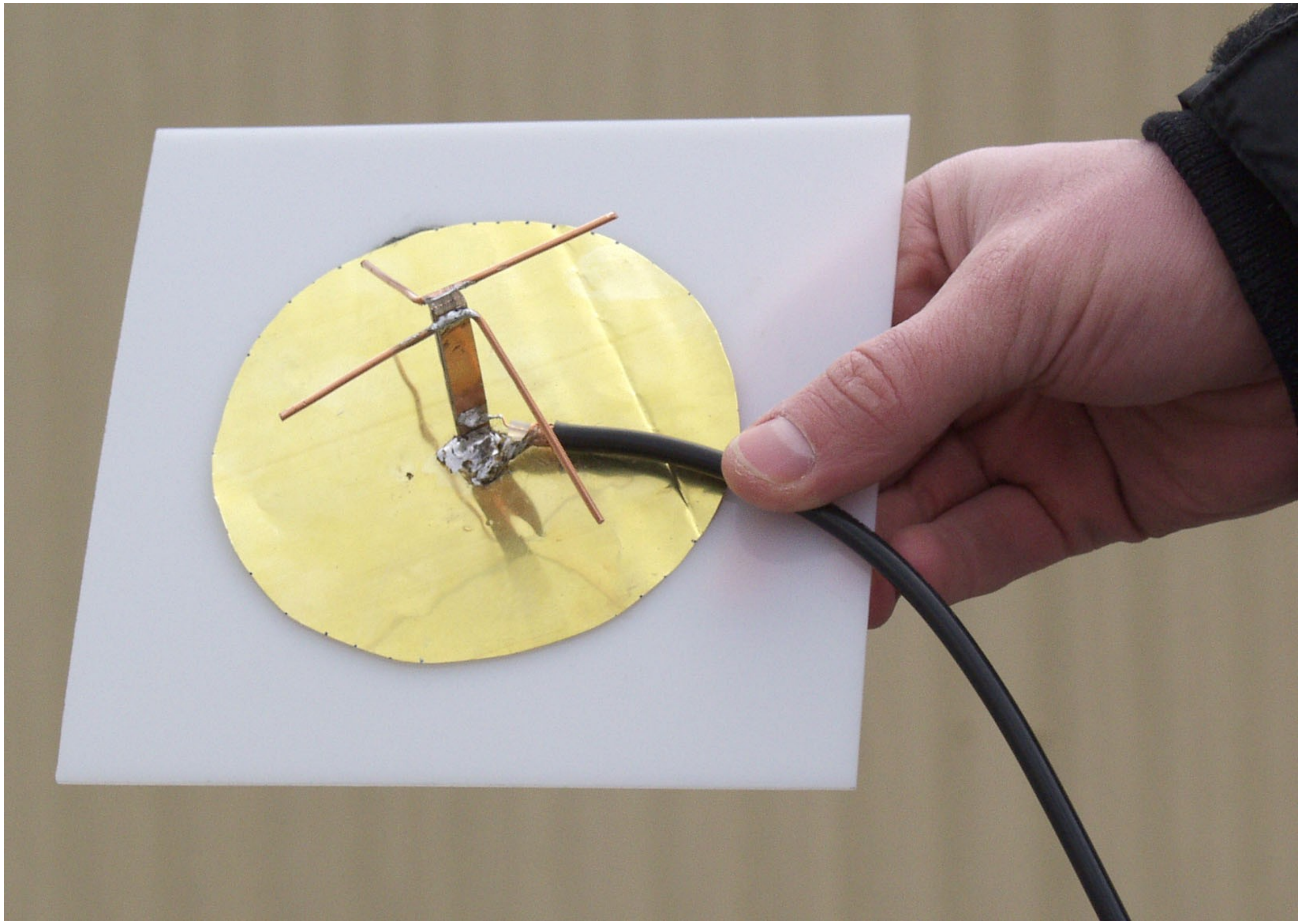
Time 2003 3 10 13: 0:0.0
Lat N 34 0 0.000
Lon W118 0 0.000
Alt 0.00 m
Speed 0.00 m/s
Track 0.0 °N
Climb 0.00 m/s
Accel 0.00 m/s²
TRate 0.00 °/s
Pitch 0.00 °
PRate 0.00 °/s

Status: Awaiting Go Command

N34:0:0.00 W118:0:0.00

N34:0:1.16 W117:59:59.17

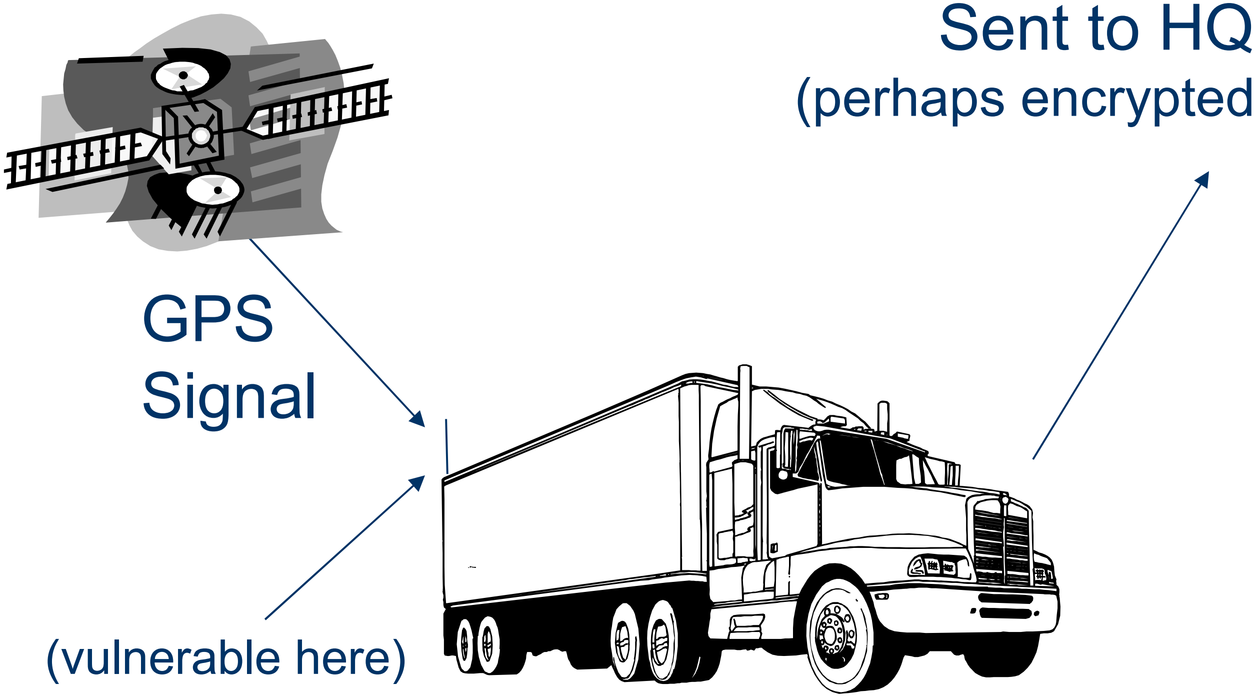
Our Homemade GPS Antenna



GPS Cargo Tracking

GPS Satellite

Tracking Information
Sent to HQ
(perhaps encrypted/authenticated)



GPS
Signal

(vulnerable here)

GPS is great for navigation, but it does not provide high security.

Truck Hijacking & Cargo Theft

Scenario #1: The truck driver is participating in the heist.

1. No need to rf broadcast the fake GPS signals.
2. The bad guys hardwire the GPS satellite simulator to the GPS receiver or its antenna.
3. Headquarters will be misinformed about the truck's location. (Deniable culpability for the driver)

Truck Hijacking & Cargo Theft

Scenario #2: The truck driver is not one of the bad guys, and he cannot get off a panic alarm.

1. The bad guys take out the driver.

2. No need to rf broadcast the fake GPS signals.

3. They hardwire the GPS satellite simulator to the GPS receiver or its antenna.

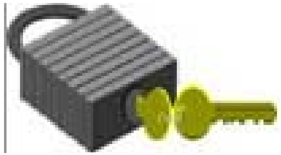
4. Headquarters (HQ) will be misinformed about the truck's location, and will not know where/when the truck was hijacked.

Truck Hijacking & Cargo Theft

Scenario #3: The truck driver is not one of the bad guys, and might be able to get off a panic alarm.

1. The bad guys break the GPS signal lock by:
   - using a GPS jammer or
   - briefly blocking the GPS receiver antenna or
   - waiting for the real GPS satellite signals to be blocked by a bridge, highway interchange, tunnel, tree canopy, or hills

2. The bad guys broadcast counterfeit GPS satellite signals (much stronger than the true signals).



Truck Hijacking & Cargo Theft

Scenario #3 (con't)

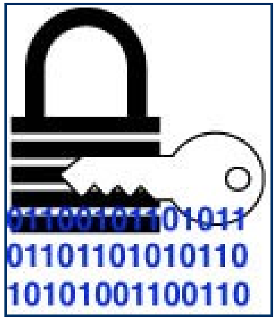
3. The fake GPS satellite signals make the truck appear to be located along its planned route, but much farther ahead or behind than the reality.

4. The truck driver is taken out. If he does manage to get off a panic alarm, security or law enforcement authorities descend on the wrong location. In any event, HQ is clueless.

Spoofing Countermeasures

- Without authentication or encryption, it will always be difficult to detect sophisticated GPS spoofing attacks.

- Our immediate goal, however, should be to detect amateur spoofing attacks based on using GPS satellite simulators, or pre-recording and then playing back real GPS signals ("meaconing").



Spoofing Countermeasures

Look (in hardware or software) for artificial characteristics of GPS satellite simulator signals (or pre-recorded real GPS signals):

- wrong time
- suspiciously low noise
- excessive signal strength
- artificial spacing of signals
- no time variation in signal strength
- all satellites have the same signal strength
- do a sanity check (e.g., no 10g accelerations)

Spoofing Countermeasures

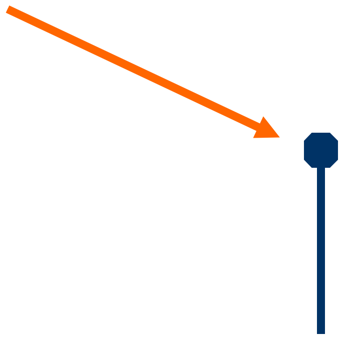
<u>Cost for Retrofitting</u>

$15 per GPS receiver in quantity?

(The cost is low because most GPS receivers already have access to far more information than they use, and this can be used to spot spoofing attacks.)

Physical Spoofing Countermeasures

- Polarization discrimination
- Angle-of-Arrival discrimination



Broader Issues

There are two general lessons here:

1. We must be careful not to confuse **inventory** functions with **security** functions.

2. High-tech does not guarantee high security.

Inventory

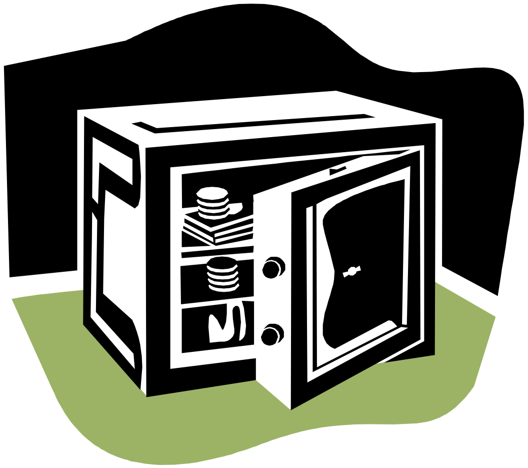
- Counting and locating our stuff.

- No nefarious adversary.

- Will detect innocent errors by insiders, but not surreptitious attacks by insiders or outsiders.

Security

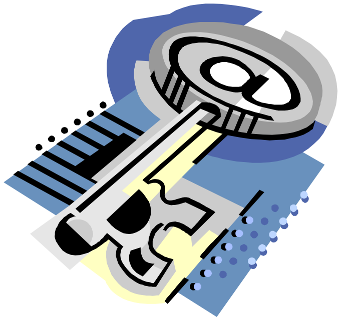
Meant to counter nefarious adversaries, typically both insiders & outsiders.



Inventory & Security

A single device or system will usually not do a good job of both inventory and security.

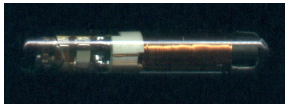
At best, it will be a compromise: neither the best for inventory nor the best for security.



Other examples of inventory or high-tech technologies that frequently fail to provide good security:

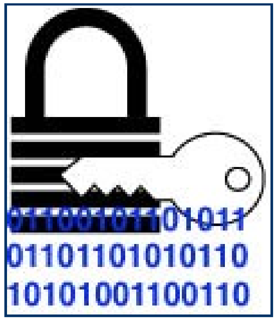
- bar codes

- rf transponders (RFIDs)



- contact memory buttons

- data encryption/authentication



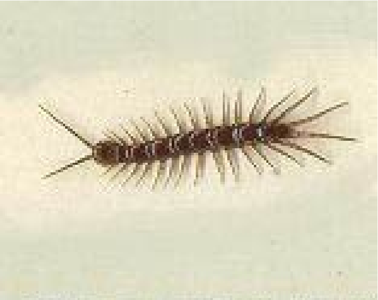
Why High-Tech Security Devices Are Usually Vulnerable To Simple Attacks

Still must be physically coupled to the real world

Still depend on the loyalty & effectiveness of user's personnel

The increased standoff distance decreases the user's attention to detail

Many more legs to attack



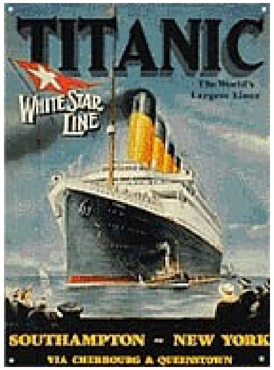
Why High-Tech Security Devices Are Usually Vulnerable To Simple Attacks (con't)

The high-tech features often fail to address the critical vulnerability issues

Users don't understand the device

Developers & users have the wrong expertise and focus on the wrong issues

The "Titanic Effect": high-tech arrogance



For More Information:

GPS

Garmin, “GPS Guide for Beginners”, http://www.garmin.com/aboutGPS/manual.html

John A. Volpe National Transportation Systems Center, Final Report for the US Department of Transportation, 29 August 2001, http://www.navcen.uscg.gov/archive/2001/Oct/FinalReport-v4.6.pdf

US Coat Guard Navigation Center, “GPS Reference Information”, http://www.navcen.uscg.gov/gps/geninfo/default.htm

JS Warner and RG Johnston, “A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing”, The Journal of Security Administration 25, 19 (2002)

JS Warner and RG Johnston, “GPS Spoofing Countermeasures”, http://www.homelandsecurity.org/bulletin/Dual%20Benefit/warner_gps_spoofing.html

Satellite Navigation and Positioning Group, http://www.gmat.unsw.edu.au/snap/gps/gps_survey/principles_gps.htm

For More Information:

NIST Time Standard

NIST Time Standard, http://www.boulder.nist.gov/timefreq/stations/iform.html

NIST Time Standard Authentication and Certification, http://www.boulder.nist.gov/timefreq /time/authentication.htm

Michael A. Lombardi, “NIST Time and Frequency Services”, NIST Special Publication 432 (2002)

A new scholarly, non-profit, peer review journal:

The Journal of Physical Security

http://jps.lanl.gov