LA-UR- 04-1692

Approved for public release;
distribution is unlimited.

Title: Think GPS Offers High Security?
Think Again.

Author(s): Roger G. Johnston
Jon S. Warner

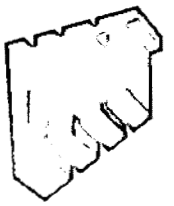
Submitted to: Business Contingency Planning Conference
Las Vegas, NV
May 23-27, 2004

ABSTRACT
IS ON
PAGE 3.

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

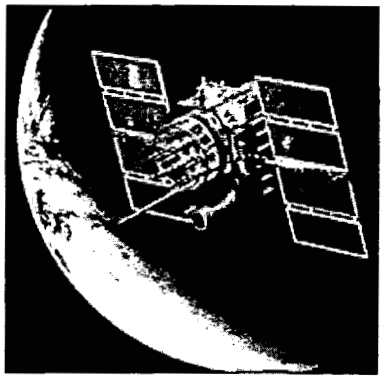


Think GPS Offers High Security? Think Again.

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.

GPS Facts

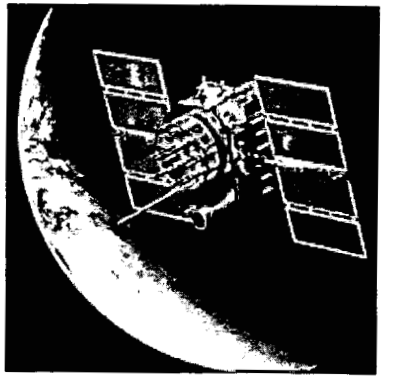


- Officially called the NAVSTAR System (for "Navigation Satellite Timing and Ranging").
- Fully operational in 1995.
- 21 active satellites (+3 standbys) orbiting at 12,000 miles.
- The satellites are essentially flying atomic clocks that transmit radio signals.
- The civilian (L1) signal is at 1575.42 MHz (UHF band).
- Signal strength is $1x10^{-16}$ 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).
- (Civilian) position accuracy is 20-40 feet with standard GPS receivers, and 3-16 feet with differential GPS receivers.

Some GPS Applications

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

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."

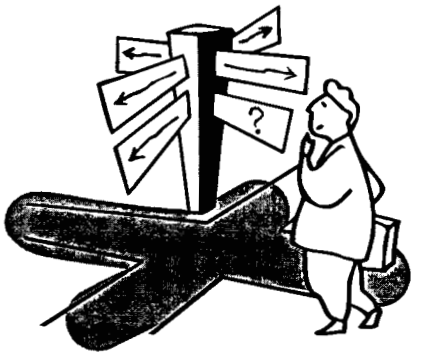
Attacking GPS Receivers

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

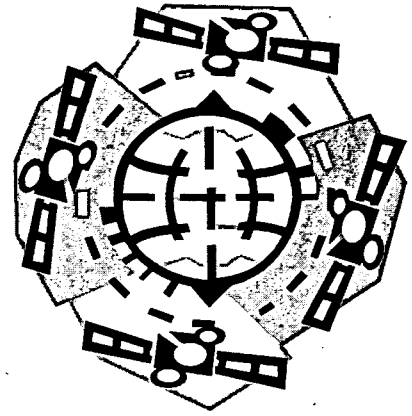
Jamming: easy to build a noisy rf transmitter (complete information is on the Internet); not surreptitious.

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

Physical attacks: appear to be easy, too.

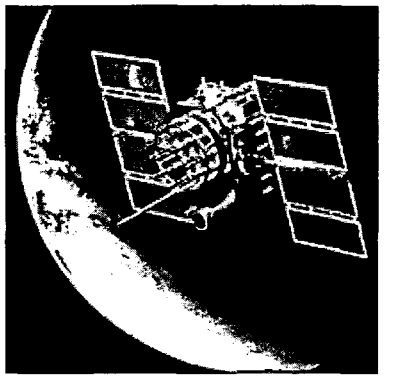


GPS Vulnerabilities



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

GPS Vulnerabilities



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

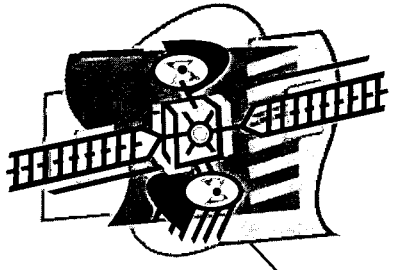
- Many national networks are somewhat prepared for jamming, but not for spoofing, which is easy and would crash the networks.

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

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

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.

Contingency Planning & Management
CPM
The Leader in Global Business Continuity
2004 WEST

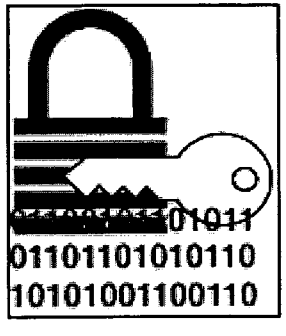
Spoofing GPS Receivers

- 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.

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)

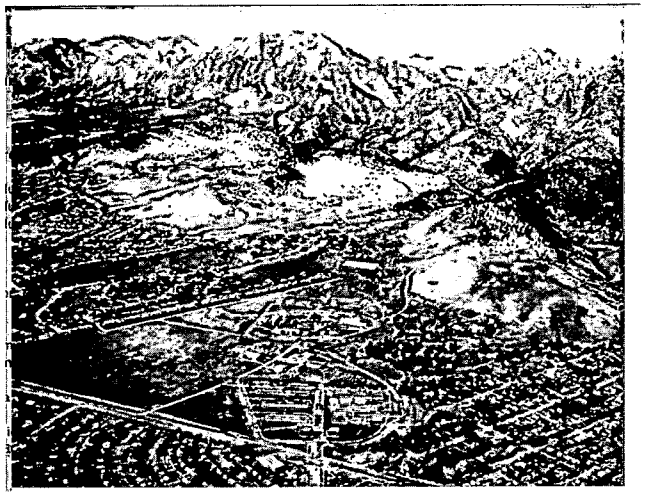
Spoofing Countermeasures

Cost for Retrofitting

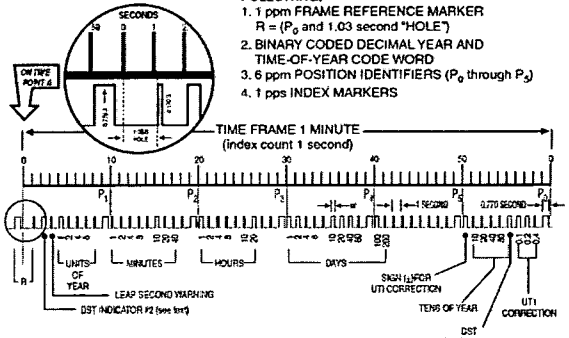
$15 per GPS receiver in quantity?

(The cost is low because most GPS receivers already have access to far more information than they use.)

NIST Time Standard



WWV and WWVH TIME CODE FORMAT



MODIFIED IRIG H FORMAT IS COMPOSED OF THE FOLLOWING:

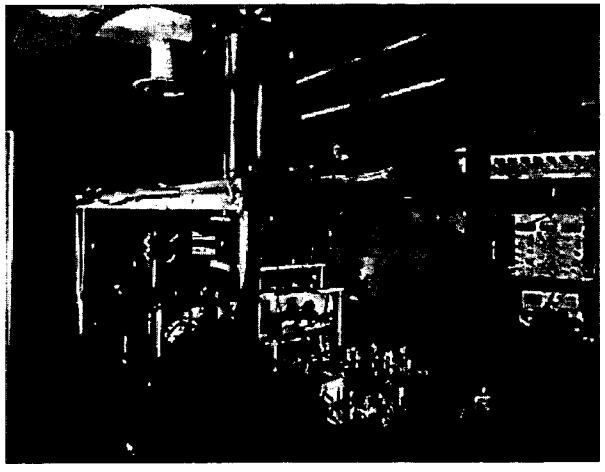
1. 1 ppm FRAME REFERENCE MARKER
   R = (P_0 and 1.03 second "HOLE")
2. BINARY CODED DECIMAL YEAR AND TIME-OF-YEAR CODE WORD
3. 6 ppm POSITION IDENTIFIERS (P_0 through P_5)
4. 1 pps INDEX MARKERS

(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

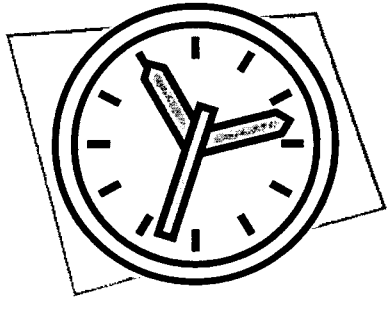
NIST-F1 Cesium Fountain Atomic Clock

The Primary Time and Frequency Standard for the United States



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.

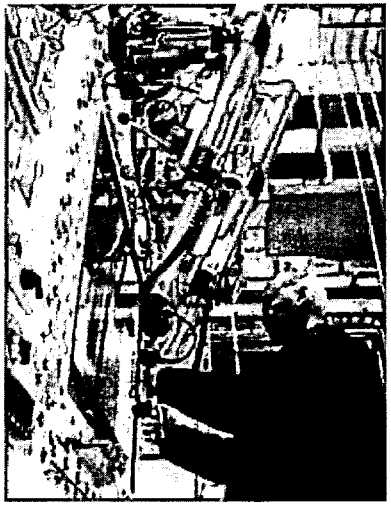


Broader Issues

There are two general lessons here:

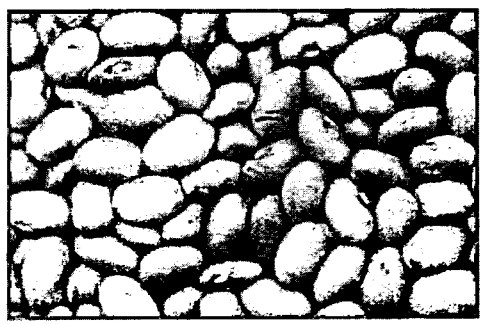
1. We must be careful not to confuse **inventory** functions with **security** functions.

2. High-tech does not guarantee high security.



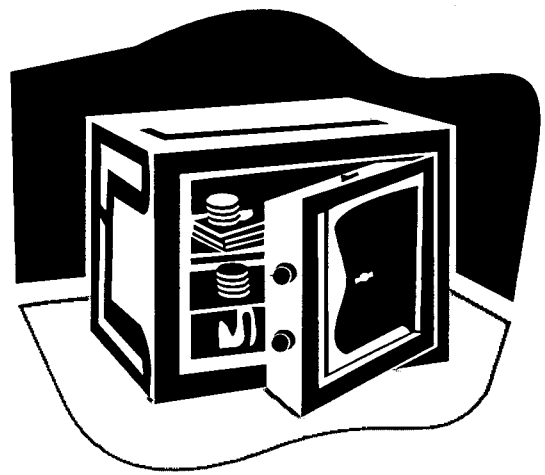
Inventory

- Counting and locating our stuff.
- No nefarious adversary.
- Will detect innocent errors by insiders.



Security

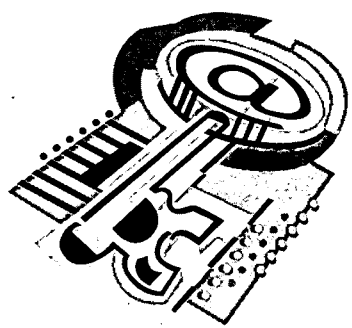
Meant to counter nefarious adversaries, typically both insiders & outsiders.



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 inventory device/system nor the best security device/system.



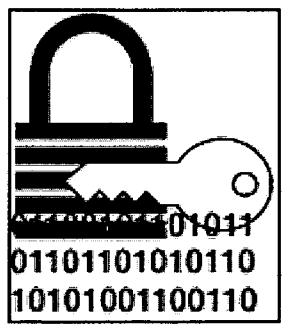
Other examples of inventory or high-tech technologies that frequently fail to provide good security:

- bar codes

- rf transponders (RFIDs)

- contact memory buttons

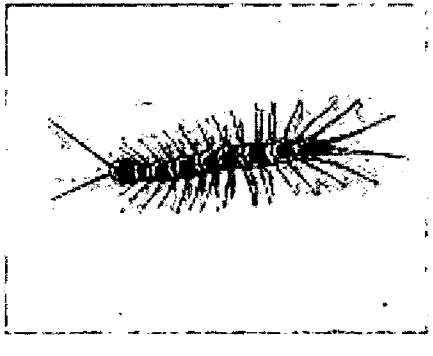
- data encryption/authentication



Contingency Planning & Management
CPM
The Leader in Global Business Continuity
2004 WEST

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

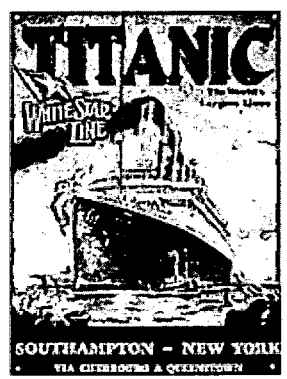
- Still must be physically coupled to the real world
- Still depend on the loyalty & effectiveness of user's personnel
- The increased standoff distance decreases the user's attention to detail
- Many more legs to attack



Contingency Planning & Management
CPM
The Leader in Global Business Continuity
2004 WEST

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

Index to the Proceedings of the 31st Annual ILA Convention and Technical Symposium Washington, DC, October 27-30, 2002 http://www.loran.org/Meetings/Meeting2002/ILA2002CDFiles/A-Index/HTMLBrowserIndex.htm

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)