LAUR-03-2384 The Journal of Security Administration 25, 19-28 (2002).

A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing

Jon S. Warner, Ph.D. and Roger G. Johnston, Ph.D., CPP
Los Alamos National Laboratory
Los Alamos, New Mexico, 87545
jwarner@LANL.gov

Introduction

The Global Positioning System (GPS) is a powerful navigational tool. In our experience, however, security managers using GPS for cargo security and tracking applications often believe that GPS offers high security. This is incorrect: the civilian GPS is not inherently secure. The Department of Transportation (DOT), for example, has raised concerns about GPS vulnerabilities, and about the over reliance on GPS for critical safety and security applications [1]. As a warning, the DOT GPS vulnerability report states that, "As GPS further penetrates into the civil infrastructure it becomes a temping target that could be exploited by individuals, groups or countries hostile to the United States. The potential for jamming exists. The potential for inducing a GPS receiver to produce misleading information exists [1]."

We undertook a simple experiment to test how easily a civilian (non DoD encrypted) GPS receiver could be spoofed, i.e., sent false information. Discussions of the civilian code GPS system and its vulnerabilities are fully unclassified [2]. The experiment performed was done on a very limited budget in a short timeframe. With better funding and more time, we believe we could have demonstrated a much more sophisticated attack.

Background

GPS, which is operated by the Department of Defense (DoD), is one of the most impressive and important navigational tools in use today. Originally designed by the Air Force in the 1970's, the civilian signal (C/A course acquisition code) was added to the original design only as an afterthought [3]. The GPS constellation of 27 satellites (24 active and 3 standby) in 6 separate orbits reached full official operational capability status on July 17, 1995 [4].

Like the Internet and the personnel computer, the number of civilian GPS users and applications exceeded the expectations of the original designers. GPS users have the ability to obtain a 3-D position, velocity and time fix in all types of weather, 24-hours a day. GPS users can locate their position to within ± 18 ft on average or ± 60-90 ft for the worst case 3-D fix [5].

GPS applications include public safety services such as police, fire, rescue and ambulance. The cargo industry, buses, taxis, railcars, delivery vehicles, agricultural harvesters, private automobiles, spacecraft, marine and airborne traffic also use GPS systems for navigation. In fact, the Federal Aviation Administration (FAA) is in the process of drafting an instruction requiring that

all radio navigation systems aboard aircraft use GPS [1]. Additional uses include hiking and surveying, as well as being used in robotics, cell phones, animal tracking and even GPS wristwatches. Utility companies and telecommunication companies even use GPS timing signals to regulate the base frequency of their distribution grids. In short, anyone who wants to know their exact location, velocity, or time might find GPS systems useful.

The cargo and trucking industries are major users of GPS technology. The GPS tracking industry has experienced a 30% growth rate per year since 1995. In 1997, it was estimated that 16% of all the GPS systems sold are being used in the trucking industry [6]. More recently, Mike Russell of the American Truckers Association stated that 70% of all long haul trucks are fitted with some type of GPS system [7]. GPS tracking system benefits include shipment tracking, real time routing, just-in-time inventory optimization, lower insurance rates, vehicle operation and maintenance scheduling and vehicle systems monitoring

How Does GPS work?

Each GPS satellite broadcasts two signals, a military signal and a civilian signal. Only the civilian code GPS signal can be used by the vast majority of GPS users (including most DoD users). The civilian code is made up of two main data signals and a carrier wave as shown in Figure 1. The Nav/System data provides the GPS receiver with information about the position of the satellites as well as precise timing data from the atomic clocks aboard the satellites. Each satellite has a unique identification code (C/A code) that is repeated every millionth of a second. The Nav/System information is combined with the C/A code and then modulated within a carrier wave.

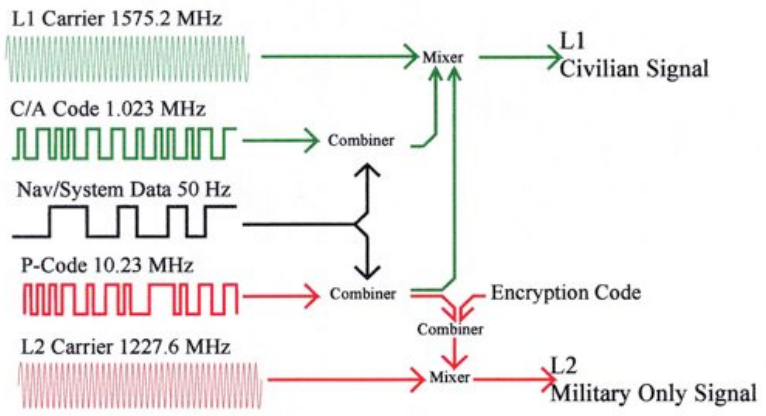


Figure 1: GPS signal structure.

The GPS receiver locks onto the signal from several GPS satellites simultaneously, but for simplicity we will focus on a single satellite lock. The receiver knows the C/A identification string associated with each satellite. The receiver continuously listens for the GPS signals from space.

When the GPS receiver picks up a GPS satellite signal it looks to the C/A code to determine which satellite it is listening to, and then generates an internal C/A code to match the satellite. This internally generated code is matched against the repeating C/A code from space. This technique is used to determine the travel

time of the signal (Figure 2). Once the travel time (ΔT) has been determined, the receiver can then calculate its distance to the satellite (Distance = ΔT x Speed of Light).

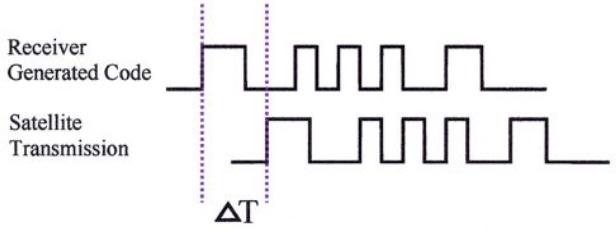


Figure 2: Example of GPS signal time delay.

Knowing the distance to a single satellite is not all that helpful. Even if you know the position of the satellite precisely, all this tells you is that you are somewhere underneath the satellite (albeit at a fixed distance). Instead, it is much more helpful to know the distance from several satellites at once.

Notice in Figure 3 that the measured ranges to the satellite measured by the GPS receiver do not overlap at a single point. The measured and true ranges differ due to clock errors in the GPS receiver. The clock in the receiver is far less expensive and precise than the atomic clocks found in the GPS satellites. This results in a distance error seen by the receiver.

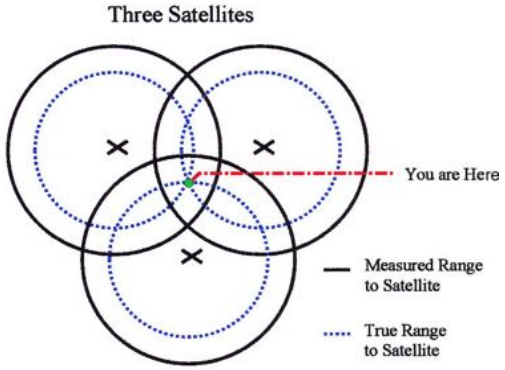


Figure 3: 2-D representation of finding a position.

Figure 3 shows an area of overlap associated with the three incorrect ranges. The receiver interpolates this area of overlap to find the center which then gives two important pieces of information; 1) what your position is and 2) the clock error of the receiver. The more satellites involved, the smaller the area of overlap the better the position fix will be. The position is initially found in an X,Y,Z Earth centered/Earth Fixed co-ordinate frame and then converted to Latitude, Longitude and Altitude.

GPS as Security?

A paradigm and misconception that appears to have emerged is that GPS is high-tech and therefore must be high security. Civilian GPS, however, was never

meant for security applications. One aspect that has been gaining in popularity is the use of GPS for security and cargo tracking. Vehicle theft and recovery systems are becoming increasingly popular. The idea is that if a vehicle is stolen, the tracking device on the vehicle can report its exact position to authorities. Geo-fencing is another popular aspect in tracking. This is where a map is displayed on a computer at headquarters (or elsewhere). On the map, tracking information for a given vehicle is displayed and if the vehicle deviates from its intended route by more than some preset limit, an alarm will sound.

Currently in its experimental stages is a method of turning the engine off in a stolen or fleeing vehicle with a GPS tracking system. Another experimental system allows a thief to break into a vehicle, where the vehicle then locks its doors and drives itself to the nearest police station. There are of course many more security systems than we can address here but the underlying principle is the same in all of them, GPS allows us to know our location, or the location of assets of interest.

The 3 Main Ways to Attack a GPS Receiver

Blocking: This involves preventing the satellite signal from reaching the antenna. This can be accomplished by, for example, simply ripping the antenna off the receiver.

Jamming: This is preventing a receiver from tracking GPS signals. This type of attack is sometimes referred to as denial of service. The true GPS signal strength reaching the surface of the Earth is about –160dBw ($1x10^{-16}$ Watts). This is roughly equivalent to viewing a 25-Watt light bulb in Japan from Los Angles, California. This weak signal can be effectively jammed by a signal of the same frequency, but greater strength. According to the DOT GPS vulnerability report, "A 1-Watt GPS-Like signal can prevent C/A code acquisition to more than 620 miles (or as limited by the line of sight to the horizon [1]." To make matters worse, "These jammers can be built by people with basic technical competence from readily available commercial components and publicly available information [1]."

Jamming, at least in our view, is a relatively uninteresting attack in that alerts those being jammed that there is a problem (i.e., they cannot get a signal lock). If headquarters notices that they have lost the tracking signal for one (or more) of their vehicles for an extended period of time they should get suspicious and act before the adversary can, for example, divert cargo.

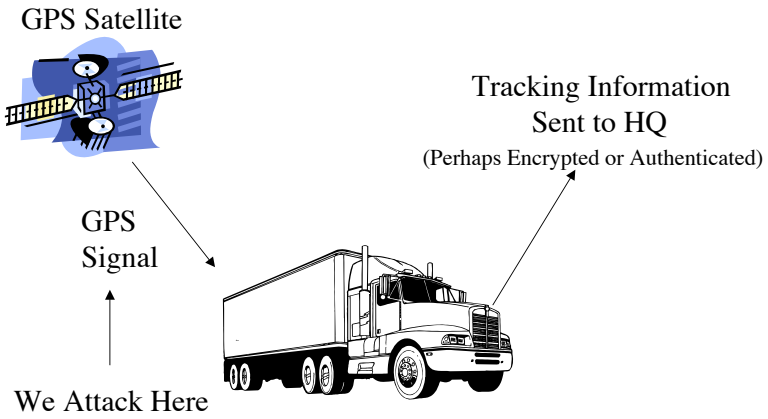
Spoofing: This is the type of attack we demonstrated and discuss in this paper. In this attack, an adversary replaces the true satellite signal from space with a fake signal. Spoofing is a much more elegant attack than either blocking or jamming because it is surreptitious.

Our Spoofing Experiment

There are many GPS tracking devices on the market. They all get their signals from outer space and then report a position to headquarters or some authorized receiver. Some tracking devices use satellites or cell phone technology to

Figure 4: We counterfeit the GPS signal before it gets to the truck.

communicate back to headquarters (HQ). Some tracking companies advertise that their tracking devices use the latest encryption algorithms to secure the data sent to HQ.



However, as can be seen in figure 4, if the adversary controls the signal that the truck is receiving, then the false position calculated by the receiver will be relayed to headquarters regardless of the encryption algorithms or communication protocols used. In other words, garbage in, garbage out.

For our spoofing experiment, we rented a GPS Satellite Simulator for about $1,000/ week. With this device, we can overpower the GPS signal from space. See figure 4. Our simulator was about the size of a desktop computer. (Portable simulators, however, are available). There are many simulators available in the market place and they all do pretty much the same thing.

It must be noted here that simulators are made for testing as well as research and development of GPS receivers. Simulators are not manufactured (yet) explicitly for hijacking cargo trucks. This created some problems for us. Our simulator was designed to feed a GPS signal into a receiver through a cable. We connected an antenna to the simulator output and were able to broadcast a signal. The signal strength output of the simulator was very small, on the order of –130 dBW to –163 dBW. We fixed this by purchasing a GPS signal amplifier (GPS Amplifier, Part #A11, GPS Source) for about $300 and another signal amplifier/re-radiator (GPS L1 Signal Re-Radiating Antenna, Model: RA-46) for about $100. Even with the amplifiers in place, the signal strength was still lower than $1x10^{-10}$ Watts. Such a weak signal does not violate FCC broadcasting guidelines under Part 15 Title 47 of the FCC code [8].

Our simulator, a WelNavigate GS720, was designed to interface to a desktop computer where a suite of programs enabled the end user to input a scenario. A scenario consisted of Longitude/Latitude, speed, heading, altitude and other positional information. The software for the simulator was very user friendly and intuitive. The software took about 10 minutes to learn. Example scenarios were supplied, so a test simulation was running 20 minutes after initially setting up the equipment. Once the scenario was completed, a simulation file was generated and fed into the simulator. The simulator was then able to broadcast the fake GPS signals.

The simulator we rented had the ability to simulate 10 satellite signals at once and could even produce signals that would convince a GPS receiver into believing it was flying at Mach 2 over the ocean, or even that is was a spacecraft orbiting the Earth.

We placed the simulator, desktop PC, and the computer monitor in the cab of a truck. They were all powered with an inverter, which converts the 12 V supplied by the truck into a 120 Volt 1200 Watt supply. The antenna was attached to the grill of the truck. With this setup, we were able to spoof the GPS receiver from about 30 feet away. If our equipment could broadcast a stronger signal, or if we had purchased stronger signal amplifiers, we certainly could have spoofed over a greater distance.

The receivers we spoofed were a DeLorme Earthmate and a Magellan Meridian. These receivers are small handheld units commonly used for hiking and automobile navigation. Due to the short timescale of this project, we were unable to obtain an actual cargo tracking system. That being said, all receivers and tracking devices have pretty much the same receiver circuitry. The main difference between a tracking device and a small handheld unit is what is done with the position information after it has been calculated. All GPS systems (tracking systems, handheld, etc.) expect and receive the same type of GPS signal.

With our simulator, we were able to spoof the GPS receivers into reporting false position information every time we tried it. There were some attempts that took longer than others due to low signal strength, obstructions, etc. Overall however, the attack times ranged from about 20 seconds to 3 minutes with an average spoofing time of 2 minutes. This seems like a reasonable attack time, considering that the typical tracking service updates the position information from a given truck every 15 minutes or so, and sometimes less frequently.

Actual hijacking scenarios were played out during this experiment by using the attack truck (containing the GPS simulator) and another truck as the target cargo truck. One of the GPS receivers was fixed to the back of the target truck (out of convenience, mostly), not on top of the truck where you would usually find the tracking devices antenna. We believe that if the receiving antenna were placed on top of the truck (as it would be in the cargo industry) it would not pose much of a problem to an adversary.

The attack consisted of a three-step process:

1) The existing GPS receiver signal lock must be broken. The adversary could wait until the target truck drove under a bridge, forest cover, or some similar type of obstruction. Alternately, a GPS jammer could be used to break the lock. We instead used a metal wastebasket. Placing the wastebasket over the antenna for about 5 seconds effectively broke the signal lock.

2) The GPS tracking device in the target truck must be locked onto the counterfeit signal. The attack truck was typically parked about 15 feet behind the target truck. This was too far to establish a lock with our simulator alone. To overcome this, we used a GPS signal re-radiator. The re-radiator consisted of an

amplifier and 15 feet of wire. This is the awkward part of the attack (if the adversary has not already overpowered the truck driver, or if the truck is not parked unattended) because the attacker must approach the truck and stand near the antenna for anywhere from 15 seconds to 3 minutes. After several minutes (to be on the safe side), the attacker can then take the re-radiator back to the truck and proceed to the final step.

3) The final step is to continue broadcasting the fake GPS signal from the attack truck. The attack truck can maintain a lock with the target truck regardless of whether the trucks remain stationary or are traveling down the road, as long as the separation distance does not exceed about 30 feet (with our equipment). Of course if the truck driver was first overpowered, the GPS simulator could be operated onboard the stolen truck, instead of onboard the chase vehicle.

With the simulator, we were able to trick the GPS receiver into thinking it was somewhere it was not. This information could then be relayed back to headquarters through the onboard tracking system.

Obtaining a Simulator

There are several methods an adversary could use to obtain a GPS simulator for use in a spoofing attack. If one was so inclined (and understood electronics), a simulator could be built. There are papers available on the Internet, which describe the procedure needed to build a simulator. The parts are readily available and the civilian signal characteristics are public information, available at several government websites.

The second option for obtaining a GPS satellite simulator is to rent or buy one. No clearance or license is needed for civilian simulators, and used simulators can be found on the Internet. At least a dozen companies sell or rent them.

The third method to obtain a GPS simulator is to steal one. Any entity that tests or performs GPS R&D has at least one GPS satellite simulator. If a person (or persons) were willing to steal cargo then perhaps they would not be adverse to stealing a simulator.

The DOT GPS vulnerability report comments on spoofing (that) "There are no practical mitigation methods currently available for this type of GPS disruption,…[there are several theoretical proposals but the expense is too high] [1]."

One type of countermeasure that would be relatively inexpensive for the end user could be realized if the GPS receivers had better clocks. The current state of clocks in a typical GPS receiver is such that highly accurate time stamping is not available. Moreover, the poor quality of the existing GPS receiver clocks permit an adversary to potentially exploit clock error and drift. Higher accuracy clocks—which need not be expensive—could serve to mitigate some of these problems.

Conclusion

Although this demonstration can hardly be considered a thorough or rigorous vulnerability assessment, it certainly does suggest that civilian GPS is indeed vulnerable to simple spoofing attacks that almost anyone could exploit. Simply because GPS is high technology does not mean it offers high security.

Acknowledgements

Anthony Garcia, Adam Pacheco, Ron Martinez, Leon Lopez, and Sonia Trujillo contributed to this work.

Disclaimers

The views expressed in this paper are those of the authors and should not necessarily be ascribed to Los Alamos National Laboratory, or the United States Department of Energy.

References

1 John A. Volpe National Transportation Systems Center, "Vulnerability Assessment Of The Transportation Infrastructure Relying On The Global Positioning System, Final Report.", August 29 2001, pp. 6 - 88, ES3, <http://www.navcen.uscg.gov/gps/geninfo/pressrelease.htm>.

2 Headquarters Air Force Space Command, "NAVSTAR Global Positioning System Operations Protect Guide", Peterson Air Force Base

3 Dr. Neal Lane, Keynote Address, presented at the Institute of Navigation GPS 99 Conference, Nashville, Tennessee, 1999, http://clinton3.nara.gov/WH/EOP/html/9910_6.html.

4 US Coast Gaurd, "GPS - Frequently Asked Questions", 2003, http://www.navcen.uscg.gov/faq/gpsfaq.htm.

5 US Air Force, "GPS Support Center", (2003), https://www.peterson.af.mil/GPS_Support/.

6 Eric Krapf, "New technologies Rev up Transportation Systems", Communications Review, 55 (1997), pp. 55-58,

7 Michael Davis, "Global Positioning Technology Helps Streamline Trucking", Shipping, 2002, <http://www.technologyreview.com/offthewire/3001_19112002_1.asp>.

8 Office of Engineering and Technology Federal Communications Commission, "Understanding the FCC Regulations for Low Power, Non-Licensed Transmitters", October 1993, http://www.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet63/