LAUR-03-6178

"Cargo Tracking and Security", *Transport Security World*, Sept. 1, 2003,
http://www.transportsecurityworld.com/Tmpl/article.asp?CID=24&AID=21027&SCID=162&TCode=FT.

Think GPS Cargo Tracking = High Security? Think Again.

Roger G. Johnston, Ph.D., CPP & Jon S. Warner, Ph.D.
Vulnerability Assessment Team
Los Alamos National Laboratory
Los Alamos, New Mexico, 87545, USA 505-667-7414
rogerj@lanl.gov

Introduction

The Global Position System (GPS) is being increasingly used for a variety of critical applications. These include public safety services (police, fire, rescue and ambulance), marine and aircraft navigation, cargo security, vehicle tracking, and time synchronization for utility, telecommunications, banking, and computer industries.

While people tend to think about GPS as being high-tech and thus high security, the fact is that the satellite signals used in most GPS applications are not secure. The civilian GPS signals—the only ones available to private industry and the vast majority of the federal government—are neither encrypted nor authenticated. They are thus easy to counterfeit, unlike the military GPS signals.

The use of GPS is only going to increase in the future. 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.

How Does GPS work?

Operated by the U.S. Department of Defense (DoD), GPS is one of the most widely used tools for navigation and timing in use today. The GPS constellation of 27 satellites (24 active and 3 standby) in 6 separate orbits reached full official operational status on July 17, 1995. Plans are underway to upgrade the existing GPS system, though this will not significantly improve security for most users.

GPS receivers have the ability to obtain a 3D 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 a worst-case 3D fix. Because of these abilities, GPS has been found to be useful in a variety of applications.

Each GPS satellite broadcasts two signals, a civilian unencrypted signal and a military encrypted ("coded") signal. All private companies and most of the federal government (including most of DoD) must use the civilian GPS signal. The civilian GPS signal was never intended for security applications, and is relatively easy to counterfeit. The DoD reserves the military encrypted GPS signal for critical military applications, such as cruise missiles and smart bombs.

A GPS receiver continuously listens for the GPS signals from space. The GPS receiver locks onto the signals from several GPS satellites simultaneously. Usually, signals from 4 or more satellites are needed to determine position on the Earth's surface. Position is determined by a kind of triangulation, where the location of the each satellite, plus the time it takes the radio signal to reach the GPS receiver, is used to determine the exact location of the GPS receiver.

Attacking Civilian GPS

A typical GPS radio signal has a strength of about 0.0000000000000001 ($1x10^{-16}$) Watts at the Earth's surface. This is roughly equivalent to seeing a 25-Watt light bulb in Tokyo from Los Angeles. An adversary, such as a cargo thief, can easily block the signal by breaking off the GPS antenna, or covering it with metal. He can also jam the weak satellite signals using a radio transmitter at the same frequency, but having greater strength. Jammers are inexpensive to make, and instructions are available on the Internet.

Blocking or jamming, however, are not the greatest security risks, because the GPS receiver (and user) will be fully aware that the GPS satellite signals are not being detected. He will thus be alerted to the fact that there is a problem.

A more pernicious attack involves feeding the GPS receiver fake GPS signals so that it believes it is located somewhere it is not. This “spoofing” is most easily accomplished by using a GPS satellite simulator. The simulator produces fake satellite radio signals that are stronger than the real signals coming from outer space. Most current GPS receivers are totally fooled, happily accepting these stronger signals while ignoring the weaker, authentic signals.

GPS satellite simulators are readily available to cargo thieves. They are legitimately used to test new GPS products being developed by various companies. GPS satellite simulators are available from nearly a dozen different manufacturers, and can be easily purchased ($10K-$50K), rented (few $K per month), or stolen. No authorization is required to purchase or rent a GPS satellite simulator, and the vendor usually asks no questions. It is also possible to build a GPS satellite simulator from scratch—complete information is available on the Internet—but this requires a sophisticated knowledge of electronics.

We have demonstrated just how easy it is use a GPS satellite simulator to spoof a GPS receiver, such as that used for cargo tracking. Many simulators are remarkably user-friendly. An adversary using a GPS satellite simulator to spoof a GPS cargo tracking system needs to understand very little about electronics, computers, or even GPS itself. We were spoofing GPS receivers within minutes of turning on a GPS satellite simulator for the first time.

GPS cargo tracking systems, such as those used on trucks, typically send the information from the onboard GPS receiver to headquarters several times an hour. Other information about the status of the truck may also be sent. If headquarters sees the truck going off the planned route, action can be taken, such as contacting the truck driver or alerting the police.

Manufacturers and vendors of GPS cargo tracking systems often go to great lengths to emphasize the sophisticated encryption methods used to secure these transmissions. The best encryption in the world, however, is useless if the raw data prior to encryption (the GPS location) isn’t trustworthy.

We also believe that many GPS cargo tracking systems are susceptible to simple physical attacks. These would allow an adversary to tamper with the GPS data without needing a GPS satellite simulator. Some knowledge of electronics, however, would be needed.

We are unaware of any examples of GPS spoofing being used for criminal activity, including cargo theft. We believe, however, that it is only a matter of time.

Cargo Theft Scenarios

To hijack a truck using GPS spoofing, an adversary must decide whether to remove the driver before or after spoofing (assuming the driver himself isn't the cargo thief). The risk with taking out the driver first, is that he may be able to signal for help. The authorities can then descend upon the truck based on its most recent GPS coordinates. If no alarm is sounded, however, the truck hijackers can place their GPS satellite simulators on the truck, and begin generating fake GPS signals. When they drive the truck off the authorized route, the truck's own GPS receiver will be sending data back to headquarters several times an hour, falsely indicating that the truck is proceeding along the approved route. Headquarters will thus be unconcerned.

Alternately, if the truck hijackers are worried about the driver possibly getting off a panic alarm, they may instead want to feed his GPS cargo tracking system fake signals. They can have the truck wrongly report back to headquarters that it is 10 or 20 miles farther along, or farther behind, the planned route than it truly is. When the hijackers then attack the driver, any panic alarm he can get off will cause the authorities to descend on the wrong location. The truck hijackers can drive the truck off without fear of being apprehended.

Countermeasures

Current GPS receivers are relatively stupid. They eagerly accept fake GPS satellite signals that are thousands of times stronger than any real satellite could possibly produce. Current GPS receivers also overlook certain abnormal, artificial characteristics of GPS signals generated by standard GPS satellite simulators.

We believe that simple software changes to most GPS receivers would permit them to detect relatively unsophisticated spoofing attacks. In some cases, the addition of small and inexpensive electronics would also assist in spotting attacks. Most current GPS receivers could be readily retro-fitted with such software and/or hardware for under $20 in quantity.

Ultimately, very sophisticated spoofing attacks would be hard to detect. We believe the immediate goal, however, should be to make simple-minded spoofing attacks detectable, at least for the most critical cargo.

Conclusion

Civilian GPS was not designed, and was never intended, for security applications. If you are relying on GPS cargo tracking systems for high level security, you should be aware they are vulnerable to a number of different kinds of attacks, including blocking, jamming, spoofing, and physical attacks. Relatively unsophisticated adversaries can successfully execute all of these attacks. We believe that effective, inexpensive countermeasures are possible, but they require modifying (or redesigning) the GPS receivers.

Disclaimer

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