MARITIME REPORTER AND ENGINEERING NEWS

Tel 352 692 5493
Fax 352 692 5494

Dennis L. Bryant
Bryant's Maritime Consulting
4845 SW 91st Way
Gainesville, FL 32608-8135

September 2013

GPS spoofing

Dennis L. Bryant

Spoof is defined as "a hoax or swindle". In the world of electronic networks, a spoofing attack is a situation in which one program successfully masquerades as another by falsifying data and thereby gaining an improper advantage. We have all heard of, and possibly fallen victim to, fraudulent card readers (often inserted on self-service fuel pumps). The fraudulent card readers copy security information from the credit card, which is then used to clone an illegitimate credit card and incur improper charges on the victim's credit card account. Most spoofing has a financial object, but that is not always the case.

It is now possible to spoof Global Positioning System (GPS) and other space-based positioning, navigation, and timing (PNT) services. To date (as far as can be determined), intentional GPS spoofing has been limited to research experiments to determine vulnerability. Iranian officials, though, claim that they were able to acquire an American stealth surveillance drone in December 2011 by transmitting false signals to the drone. The claim is almost certainly bogus, but impossible to totally disprove.

The reason that PNT receivers, such as the GPS receiver found on almost every commercial vessel in the world, are susceptible to spoofing is that the signal transmitted by the PNT satellite is of very low power. It does not take much in the way of power from a fraudulent transmitter to overcome that signal. The same is not true of a Loran signal, since it transmits at a much higher power level. Unfortunately, there only a few places in the world where the Loran system remains in operation. It is old technology, not as accurate or efficient as space-based PNT systems, but much more difficult to spoof or jam.

A GPS spoofing attack deceives a GPS receiver by broadcasting a slightly more powerful signal than the real signals, and structured to resemble a set of normal GPS signals. This can be complex because a GPS receiver is usually receiving low-power signals from three or four separate satellites. Spoofing will become more complex in the future as next-generation GPS satellites broadcast more sophisticated signals. The spoofed signals are modified so as to cause the receiver to determine its position to be in a determined location other than where it actually is. Theoretically, this determined location could be anywhere on earth, below it, or above it (at least up to the level of the satellite orbits). If the location determined by the spoofer is initially very far from the actual location of the GPS receiver, though, the users will quickly detect that

E-mail dennis.l.bryant@gmail.com
Internet http://brymar-consulting.com/

something is wrong. Therefore, it is necessary for the initial fraudulent location to be only slightly different from the actual location. The spoofing signal then slowly increases the deviation from the actual location. Many ships and aircraft operate much of the time on auto-pilot. Making the GPS receiver incorrectly determine the position of the ship or aircraft will cause a change in the course of the ship or aircraft to get it back to the programmed trackline. If the spoofing can be extended for a sufficient period, the ship or aircraft potentially can be taken far from its true trackline and destination.

In June 2013, a radio navigation research team from the University of Texas at Austin conducted a "proof-of-concept" demonstration on the 213-foot long luxury yacht White Rose in the Mediterranean Sea. The purpose of the demonstration was to measure the difficulty of carrying out a spoofing attack at sea and to determine whether sensors on the vessel could identify the attack. With the permission of the owner, members of the team boarded the yacht in Monaco en route Rhodes. When the yacht was about 30 miles off southern Italy, they transmitted false GPS signals slightly stronger than the actual ones. The signals were then modified to show that the yacht as slowly moving slightly to starboard. The signal deviation was slowly increased so as not to arouse alarm. The yacht, operating on auto-pilot, slowly adjusted its course to port to bring it to where the GPS receiver computed the yacht should be. The yacht stayed on the fraudulent course for the duration of the experiment.

One can correctly point out that spoofing to any significant extent can be detected by using an alternative means of determining one's position. In the real world, though, this is often not done. We have become so reliant on GPS that we don't question it.

In 10 June 1995, the cruise ship Royal Majesty ran aground in what amounted to a case of accidental spoofing. The ship was returning to Boston from a voyage to Bermuda. At dinner, the master explained to the passenger at his table how groundings were a thing of the past because the ship was equipped with all the latest navigation equipment, including GPS. Unbeknownst to the navigating team on the bridge, as the ship approached the Massachusetts coast, the wire connecting the GPS receiver (located in the chart room) with the GPS antenna came loose and disconnected. Because loss of the GPS signal can occur for various reasons, such as there not being sufficient visible GPS satellites at the moment to obtain a position fix, the GPS receiver automatically switched to the dead reckoning mode. When operating on dead reckoning, the GPS receiver activates a flashing red light. As the receiver was located in the chart room, no one noticed. Besides, the transition from ship's actual position to an estimated position was gradual. The ship continued for some miles on dead reckoning, but was pushed off its intended track by wind and currents. No one noticed until a buoy was unexpectedly seen where there should not have been a buoy. Unfortunately, the buoy marked the Rose and Crown Shoal near Nantucket Island. The navigation team then checked the radar, the fathometer, and the Loran receiver. They quickly determined that the ship was far off course. Unfortunately, the grounding was unavoidable by that time. Fortunately, it was a soft grounding, as these things go. The damage to the ship was relatively minor. The Royal Majesty was refloated by tugs the next day and completed its voyage into Boston, with some hull plating deformation and a lot of embarrassment. Things easily could have been much worse.

In the intervening years, most navigators have become more, rather than less, reliant on GPS. Other space-based PNT systems are now available or coming on line soon, including the Russian GLONASS system and the European Galileo system, as well as ones under development by the Chinese and the Indians. None of them are able to totally avoid vulnerability to spoofing because they all utilize relatively low power transmissions from orbiting satellites. GPS is now fully integrated into electronic navigation charting and the Electronic Chart Display and Information System (ECDIS), as well as other shipboard systems.

In what I consider to be a short-sighted move, the United States shut down its Loran network several years ago, just as that technology was transitioning to the more sophisticated and less manpower-intensive electronic Loran (eLoran) system. The United Kingdom has deployed a small eLoran network, but it is primarily effective only in the vicinity of the English Channel. Until and unless a wide-scale earth-based system such as eLoran is available, ships and aircraft will be vulnerable to spoofing attacks. The same vulnerability is present in unmanned vessels, aircraft, and vehicles. Theoretically, a malicious actor could also use spoofing to alter the timing perception of a GPS receiver, giving the spoofer at least the possibility of disrupting the precise timing required to operate our increasingly interlinked financial, communications, and power grids.

In 2001, the Volpe National Transportation Systems Center conducted a vulnerability assessment of transportation infrastructure relying on GPS. Among its findings was the following: "*As GPS further penetrates into the civil infrastructure, it becomes a tempting target that could be exploited by individuals, groups, or countries hostile to the United States. The potential for denying GPS service by jamming exists. The potential for inducing a GPS receiver to produce misleading information [e.g., spoofing] exists*." It should be noted that this study was completed twelve years ago, and little has improved in the interim.

The take-away here is that GPS and other satellite-based PNT services are susceptible to spoofing (intentional or accidental). It behooves users of these systems to not rely exclusively thereon when making important navigational and operational decisions.