A perfect storm of ever-increasing technological capability, decreasing cost and systemic vulnerabilities has made defending computer networks one of the most pressing challenges facing industries and governments worldwide. Another area where the same conditions exist—and where the potential problem is of comparable magnitude—is in the growing reliance on GNSS (Global Navigation Satellite Systems).

Equipment capable of interfering with systems such as GPS is widely available for approximately the price of a smartphone and is becoming increasingly popular with criminals. The problem is not confined to those who use GNSS for geolocation or navigation purposes: Industries, including telecommunications and finance, rely on GPS’s timing functions to synchronize automated processes. The potential disruption to critical infrastructure from an attack on GPS is considerable.

“We’ve come from a position where almost nobody understood the vulnerability of GPS to a position where it’s almost universally understood by engineers,” says David Last, a former president of the U.K.’s Royal Institute of Navigation and a consultant engineer specializing in radio navigation and communication systems. “It is in the domain of policymakers and politicians where the understanding is slowest. But, country by country, that understanding is changing.”

A wake-up call was sounded this year, when problems arose during the decommissioning of GPS satellite SVN23. The spacecraft, the oldest in the GPS constellation, was taken out of service on Jan. 26 by the 50th Space Wing of the U.S. Air Force but during the process, an error of 13.7 microseconds was introduced into the coordinated universal time (UTC) signal. This eventually affected 15 satellites, according to Charles Curry, founder of the British timing monitoring company Chronos Technology Ltd.; impacts included disruption to landline communications and a lengthy outage to the BBC’s digital radio service.
“At [2 a.m.] our network operations center got a call from a major fixed-line telecom operator saying, ‘My screen’s gone all red and my GPS receivers have failed,’” Curry says. “We had some operators with over 1,000 alarm events around the world. It took our team four days to correct it, and we weren’t an isolated case.”

High-frequency trading is synchronized using GPS; telecom networks align nanoseconds-long timeslots to digital traffic packets to maintain frequency stability and data throughput. Yet the very low power of GNSS transmissions makes them very easy to jam.

GPS jammers are offered for sale online, often from companies located in China that will ship worldwide. Users include individuals wishing to disable GPS or cellphone coverage in their immediate location. Curry cites examples of drivers who use low-power jammers that are designed to fit in vehicle cigarette lighters to prevent employers from monitoring private use of company vehicles, and the pastor of an American church who installed a GPS jammer to stop cellphones from interrupting his sermons.

Using a jammer is illegal in the U.K., but buying and owning one is not; jammers are illegal to buy, sell, own or operate in the U.S. GPS jamming technology has been used by organized criminal gangs in the U.K. for at least 18 months. Jammers have been discovered fitted to the batteries of stolen cars, preventing location-tracking while the vehicles are loaded onto containers and shipped overseas.

“Almost all the jamming we’re seeing is either accidental or intentional at a level of minor criminality up to organized crime gangs. What we have yet to see is jamming with intent by terrorists who are technically literate,” says Last, who has appeared as an expert witness in several jamming-related court cases in the U.K. “It’s perfectly possible to take out all of the communications across a substantial city if you know how to do it—and it isn’t very difficult.”

Another type of attack, known as spoofing, is moving from laboratory theory to practical reality, thanks to the widespread and low-cost availability of software-defined radios and the online distribution of programs for them that enable relatively unskilled users to broadcast counterfeit GPS signals. Like jamming, spoofing exploits the low power of GNSS signals, but instead of merely preventing receivers from accessing the information, the technique broadcasts false data. All receivers in a given area would be affected, with the zone of disruption dependent on the power of the transmitter being used.

“I watched a spoofer demonstration in an English country pub recently, and not only did it alter the position that the GPS receiver gave, it altered the time,” says Last. “At one point, the receiver was set back two years, and
all of the software on the smartphone collapsed.”

Military need is driving development in GPS alternatives, with a number of Darpa programs looking at different aspects of technologies to solve precision-navigation challenges in GPS-denied environments. These include the Timing and Inertial Measurement Unit (TIMU) program, which is investigating chip-scale gyroscope and accelerometer technologies, and Precise Robust Inertial Guidance for Munitions (Prigm), which is attempting to build and flight-test a microelectromechanical guidance system capable of navigating a munition from launch to target.

For commercial users, the options are limited. Mitigation against GNSS jamming and spoofing is available but costly. The real alternative, Curry argues, is to revive an older navigation and timing technology and operate it as a complementary service.

Enhanced Loran (eLoran), a development of the Loran and Loran-C long-range maritime navigation systems originally built during World War II, offers geolocation capabilities accurate to ±8 ft. and a comparable timing capability to GPS, with diurnal variation in the order of around 50 nanoseconds. Instead of a low-power satellite transmission, the signals are high-powered and sent from large transmitters built on land. This makes the signal very difficult to jam or disrupt, short of a kinetic strike on the transmission stations.

The adoption of eLoran as a global GNSS backup is technically feasible: Curry has established a new joint-venture company, Taviga (for which Last acts as a consultant), with UrsaNav, a Massachusetts-based position, navigation and timing provider, and he is positioning it to deliver a commercial eLoran service. But to build a persuasive business case, the company needs guarantees from governments over provision of an eLoran signal. And despite widespread interest in a GPS backup, some countries that were originally on board now seem to be backtracking; Loran transmitters have been turned off in several countries.

The Taviga partners are in discussion with an as yet undisclosed U.K. government department. The aim is to agree on a viable plan for eLoran across Europe, utilizing decommissioned Loran C sites where antennas have not yet been dismantled and repurposing them as eLoran transmitters. The U.K. government partially funded operation of a German Loran station the island of Sylt. The Russian Loran equivalent, Chayka, is potentially interoperable with eLoran, and a number of Loran stations still exist in the U.S.—though several more have had their antennas dismantled. Additional stations will have to be built, but Taviga and UrsaNav co-founder Chuck Schue argues that the costs are manageable.

“It’s not a technology problem to move the system forward—it’s a will-of-governments problem,” says Schue. “We can install and operate a fully capitalized eLoran position, navigation and timing solution for the lower 48 United States for 20 years for less than the cost of one GPS-3 satellite.”

The concern is that GNSS resilience may be in the same position today that computer network defense was in the early years of the century. The threats were real, growing and understood by specialist professionals, but it was not until hacks, leaks and cybercrime became high-profile and high-impact problems that governmental resources began to be funneled toward the sector.

“Some of us who work deeply in this space are very aware that there could be a major incident,” says Curry. “No one is really prepared for it. Our mission is to highlight the concerns and make sure that appropriate resiliency techniques are incorporated.”

Source URL: http://aviationweek.com/defense/vulnerabilities-satellite-navigation-systems