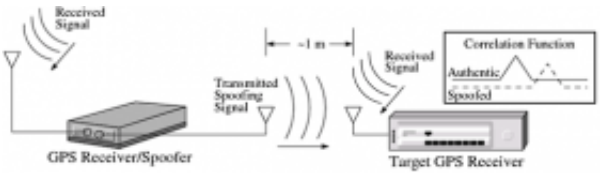
GPS receivers can be 'spoofed,' say researchers

September 22 2008



An illustration showing how a GPS receiver/spoofer would transmit a false signal that a target GPS receiver could mistake for an authentic one.

(PhysOrg.com) -- Just like flat-screen televisions, cell phones and computers, global positioning system (GPS) technology is becoming something people can't imagine living without. So if such a ubiquitous system were to come under attack, would we be ready?

It's an uncomfortable question, but one that a group of Cornell researchers have considered with their research into "spoofing" GPS receivers.

GPS is a U.S. navigation system of more than 30 satellites circling Earth twice a day in specific orbits, transmitting signals to receivers on land, sea and in air to calculate their exact locations. "Spoofing," a not-quite-technical term first coined in the radar community, is the transmission of fake GPS signals that receivers accept as authentic ones.

The Cornell researchers, after more than a year of building equipment

and experimenting in Rhodes Hall, presented a paper on their findings at a meeting of the Institute of Navigation, Sept. 19 in Savannah, Ga.

To demonstrate how a navigation device can be fooled, the researchers, led by Cornell professors Paul Kintner and Mark Psiaki, programmed a briefcase-size GPS receiver, used in ionospheric research, to send out fake signals.

Paper co-authors Brent Ledvina, Cornell Ph.D. '07 and now an assistant professor of electrical and computer engineering at Virginia Tech, and first author Todd Humphreys, Cornell Ph.D. '07, described how the "phony" receiver could be placed in the proximity of a navigation device, where it would track, modify, and retransmit the signals being transmitted from the GPS satellite constellation. Gradually, the "victim" navigation device would take the counterfeit navigation signals for the real thing.

Handheld GPS receivers are popular for their usefulness in navigating unfamiliar highways or backpacking into wilderness areas. But GPS is also embedded in the world's technological fabric. Such large commercial enterprises as utility companies and financial institutions have made GPS an essential part of their operations.

"GPS is woven into our technology infrastructure, just like the power grid or the water system," said Kintner, Cornell professor of electrical and computer engineering and director of the Cornell GPS Laboratory. "If it were attacked, there would be a serious impact."

By demonstrating the vulnerability of receivers to spoofing, the researchers believe they can help devise methods to guard against such attacks.

"Our goal is to inspire people who design GPS hardware to think about

ways to make it so the kinds of things we're showing can be overcome," said Psiaki, Cornell professor of mechanical and aerospace engineering.

The idea of GPS receiver spoofing isn't new; in fact, the U.S. government addressed the issue in a December 2003 report detailing seven "countermeasures" against such an attack.

But, according to the researchers, such countermeasures would not have successfully guarded against the signals produced by their reprogrammed receiver.

"We're fairly certain we could spoof all of these, and that's the value of our work," Humphreys said.

Provided by Cornell University