New defenses sought against GPS spoofing attacks

January 17 2018

Yongqiang Wang, right, and Muaz Ahmad look at a smart phone that has been tricked through GPS spoofing into thinking it was four days earlier than the actual date. Credit: Pat Wright, Clemson University

Cyberattacks with the potential to expose sensitive information and

cripple basic services could start with what would seem to be the most harmless of computer functions.

Timekeeping.

It's a vulnerability that has raised growing concerns as more homes, businesses, utilities and other critical services rely on the internet and GPS to function and each week brings news of another devastating cyberattack. But new defenses could be on the way with the help of Clemson University.

Yongqiang Wang, an assistant professor of electrical and computer engineering, is leading a team that is receiving $1 million from the National Science Foundation to fortify computers and devices against cyberattacks associated with timekeeping.

The research could have wide ranging effects from making cell phones more secure and protecting the power grid against terrorism to ensuring that scientific data remains sheltered. The team's focus will be on "GPS spoofing" and attacks on Network Time Protocol, commonly called NTP.

"The impact of our research will be to make sure the timing service is more reliable," Wang said. "In a network where time has to be aligned, such as the internet, cellular communication networks, and power systems, if the time on one device goes wrong, then there could be catastrophic consequences. So we want to provide secure timing solutions, by securing the two most commonly used time distribution approaches,GPS receivers and NTP."

Rolling back time on a computer can make it relatively easy for hackers to break open encrypted documents, he said. They could also access accounts with login information that should be expired, Wang said.

Muaz Ahmad, a master's student in Wang's lab, demonstrated how simple GPS spoofing can be. All he needed was a software-defined radio purchased available on a popular shopping website for about $300.

With a few taps on a keyboard, Ahmad had the software-defined radio send signals to a smart phone sitting on the desk next to him. The GPS chip in the phone interpreted the signals as GPS signals beamed from satellites.

Ahmad was able to trick the phone into thinking it was four days earlier than the actual date and that it was sitting about a mile away from its actual location.

"This is what we're trying to prevent," Wang said.

The experiment was harmless, but GPS spoofing carries the potential for devastating consequences. The same GPS system built into smartphones and cars also helps guide ships, trucking fleets and intelligent cars.

As recently as last year, GPS told two vessels that they were at Sochi Airport in Russia, but they were actually in the harbor 12 miles away, USA Today reported.

Wang and his team plan to counteract GPS spoofing by setting up a server at Clemson University.

Every 10 seconds, two GPS receivers in Clemson and Anderson will sample secret code embedded in GPS signals and upload them to the server. Users elsewhere in the United States will be able to access those samples to verify that the signals they are receiving actually come from the genuine satellite source.

Researchers plan to test their server on several battery-powered sensors

that have been deployed along the Savannah River to measure flooding and water quality as part of the Intelligent River Project.

At the same time, researchers will be working to defend against attacks on NTP. One of the oldest computer protocols still in use, NTP helps computer systems synchronize clocks.

It's an increasingly important function as more infrastructure ranging from the power grid to water systems rely on computer networks to keep them functioning smoothly. Each system typically has facilities in different locations, and time accuracy at each location is critical, Wang said.

For example, a flood gate that opens to soon or too late could have catastrophic consequences.

As crucial as it is, NTP is among the vulnerabilities in denial-of-service attacks, Wang said. Those attacks flood computer systems and servers with traffic, making it difficult for legitimate users to access them.

Wang and his team plan to combat NTP attacks by creating a complement to NTP they call "pulse synch protocol." It would be a secure way of cross-checking whether computers are closely synchronized under NTP.

The team plans to test its pulse synch protocol by synchronizing clocks of five weather stations deployed around Clemson's campus.

Daniel Noneaker, chair of the Holcombe Department of Electrical and Computer Engineering, said the grant is well deserved.

"The research that Dr. Wang and his team are doing will help advance the technologies and techniques that protect cyberinfrastructure in

academia and beyond," he said. "It's a critical challenge as the cyberinfrastructure ecosystem becomes more interconnected, even as resources are distributed in different locations."

The team plans to use the research in the classroom, including a new graduate class, Secure Network Science. Researchers also plan to start a new Creative Inquiry course aimed at undergraduates and a new cybersecurity program that will be part of the Project WISE summer camp for middle school girls.

Co-principal investigators on the grant, all from Clemson University, are Kuang-Ching "K.C." Wang, professor of electrical and computer engineering; Kumar Venayagamoorthy, professor of electrical and computer engineering; and Christopher Post, professor of environmental information science.

Anand Gramopadhye, dean of the College of Engineering, Computing and Applied Sciences, said that the grant will help secure cyberspace, one of the grand challenges facing society in the 21st century.

"I congratulate Dr. Wang and his team on the grant," he said. "The amount of the award is a testament to the strength of their approach and the urgency to develop new ways of protecting our cyberinfrastructure."

Provided by Clemson University