# Wireless tire pressure monitoring systems in cars may compromise privacy, pose security threat

August 12 2010

New wireless technologies in cars may compromise a driver's privacy and pose a security threat, warn researchers at Rutgers University.

Modern automobiles are increasingly equipped with wireless sensors and devices, such as systems that monitor air pressure inside tires and trigger dashboard warnings if a tire's pressure drops. The Rutgers researchers have shown that these wireless signals can be intercepted 120 feet away from the car using a simple receiver despite the shielding provided by the metal car body.

Since signals in tire pressure monitoring systems (TPMS) include unique codes from each wheel sensor, this raises concerns that drivers' locations could be tracked more easily than through other means, such as capturing images of license plates.

The Rutgers researchers and their collaborators at the University of South Carolina are presenting results of their work this week at the USENIX Security Symposium, one of the premiere academic computer security conferences. The researchers are experts in wireless communication and computer networking security.

TPMS wireless transmissions also lack security protections common in basic computer networking, such as input validation, data encryption or authentication. The researchers demonstrated how a transmitter that

mimics, or "spoofs," the sensor signal can easily send false readings and trigger a car's dashboard warning display. This could prompt a driver into stopping his or her car when there is actually nothing wrong with the tires.

"We have not heard of any security compromises to-date, but it's our mission as privacy and security researchers to identify potential problems before they become widespread and serious," said Marco Gruteser, associate professor of electrical and computer engineering and a member of the university's Wireless Information Network Laboratory (WINLAB).

He notes that tire pressure monitoring is the first widespread use of in-car wireless networking, and because of the increasing cost and complexity of wired electronic systems, it's reasonable to expect other aspects of automobile operation to come under wireless control.

"A spoofed signal could potentially cause serious safety concerns if stability control or anti-lock braking systems relied on the data," he said. "So we are sounding the alarm right now."

Gruteser acknowledged that intercepting and spoofing signals is not a casual effort. But the fact that people with college-level engineering expertise could carry out those actions using publicly available radio and computer equipment costing a few thousand dollars shows that systems are vulnerable.

Tire pressure monitoring was widely implemented starting around 2000 using systems that measure and compare wheel rotation speeds. A mismatch infers that a tire is underinflated. This method wasn't accurate enough to meet U.S. regulatory requirements that took effect later in the decade, so automakers started installing systems that directly monitor air pressure inside the tires and transmit that information to a control unit.

The two systems that Rutgers examined are commonly used in vehicles manufactured during the past three years.

"While we agree this technology is essential for driver safety, more can be done to improve security, such as using input validation or encryption," said Wade Trappe, a collaborator on the project who is an associate professor of electrical and computer engineering and associate director of WINLAB.

The researchers' South Carolina collaborators, led by Wenyuan Xu, a former doctoral student at WINLAB and now an assistant professor at the University of South Carolina, were able to intercept a signal more than 30 feet from the car using a simple antenna and more than 120 feet away by adding an amplifier. They were able to analyze the radio signal and reverse-engineer the code using common laboratory instruments. With that knowledge, they built a transmitter that spoofed a sensor's wireless message.

In tests using their own cars, the researchers were able to send false signals from one car and trigger a "low tire pressure" light in another while driving next to each other at 35 miles per hour. They were also able to trigger the dashboard "check tire pressure" light while driving next to each other at 65 miles per hour.

The researchers also found that at least one tire pressure system could be damaged through spoofed wireless signals.

Provided by Rutgers University