Tire-pressure monitors vulnerable, researchers say

September 2 2010

(PhysOrg.com) -- Wireless tire pressure monitoring systems designed to alert drivers to problems with low tire pressure can be intercepted or forged, causing possible security or privacy threats, according to research at the University of South Carolina and Rutgers University.

Dr. Wenyuan Xu, an assistant professor in the department of computer science and engineering at USC and the lead investigator on the project, said tire pressure monitoring communications systems in many new cars are not properly secured, allowing anyone to eavesdrop on the wireless communication and send false messages to drivers. Most new cars manufactured or sold in the U.S. after 2007 are equipped with the tire pressure monitoring system.

As technology evolves and more wireless sensors and devices are introduced into cars, Xu said carmakers need to pay more attention to securing wireless communication before more serious vulnerabilities emerge. For example, although not a reality yet, if the tire pressure reading is used to assist the stability control, then sending a forged message with the wrong tire pressure could be dangerous.

USC researchers and their colleagues at Rutgers University studied tire-pressure monitoring systems (TPMS), the devices that monitor air pressure inside tires and trigger a dashboard warning if a tire's pressure drops. Researchers were able to intercept the wireless signals 120 feet away from the car using a simple receiver.

“Hopefully, as a result of our project, the security and privacy concerns from consumers will push the car industry to design in-car wireless networks with security and privacy in mind,” Xu said.

Virtually all new cars use direct TPMS, which relies on wireless technologies. Since wireless communication is prone to eavesdropping and malicious hacking, the researchers wanted to analyze the security and privacy aspects of the first widely used wireless systems, Xu said. “Since the wireless communication contains unique identifiers of each car, it is possible to track vehicles by listening to the tire pressure monitoring system’s wireless communication,” Xu said. “Further, we have shown that we can transmit false messages to make the car trigger the ‘low pressure warning light’ on the dashboard while all tire pressures are normal. We managed to ‘damage’ the tire pressure monitoring system by sending false messages.”

More information: Xu is a co-author of the paper, “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study,” and presented it at the USENIX Security Symposium in Washington, D.C., earlier this month.

Provided by University of South Carolina