

Schrader® Technical Response Q&A – TPMS Security

Subject: Rutgers University & University of South Carolina study on the security of Radio Frequency (RF) based Tire Pressure Monitoring Systems (TPMS).

Rationale: After careful review, Schrader's technical response to the published study which raised uncertainty about the security of RF-based TPMS. While we sincerely respect the opinions of the researchers, we also strongly believe their study makes conclusions which are based on limited knowledge, and in some cases, are incorrect. Schrader invented TPMS technology, and is the global leader in the design, development, and manufacture of TPMS.

Q: Can someone “forge” a TPM sensor and “fool” a vehicle system in thinking it has a low tire?

A. Technically this is possible, however, it is difficult, and certainly not as easy as the researchers suggest. First, it would require a significant amount of time, expensive equipment and knowhow to receive and replicate a proper protocol. Currently, the market has over 147 different protocol variations which would mean an extensive effort would be required before a forger could start to send the correct protocol and vehicle specific ID all before they could create a system disturbance. Next, the forger would have to stay within 25–30 feet of the vehicle for “extended periods of time” to cause the warning light to illuminate to the point of creating a false sense of security. The practicality of a forger following someone around, with the purpose of transmitting a false low pressure simply to annoy them, is questionable.

Q: Can someone use the TPM ID to track a driver's location?

A. This is not only impractical but nearly impossible. TPM sensor transmitters are low signal devices subject to FCC Part 15 and are a Class C device. It is true that the signal is unencrypted but due to the low signal strength, it would be highly unlikely anyone could read the signal from 130 feet away. It would be even more difficult to successfully read the signal when the vehicle is moving past a fixed location. TPM systems operate on multiple frequencies, data speeds, ID lengths, protocol encoding, etc. If someone was successful in decoding one sensor type, there are over 147 different types currently in operation and this number increases every day. The complexity in the market not only makes it difficult for this scenario but also impractical. Even the author admits this: “Xu said that while it is possible to track someone by their tire IDs, ***the feasibility of doing so would be quite low***. Someone would have to invest money at putting receivers at different locations,” she said. “Also multiple tire manufacturers have different types of sensors, requiring different receivers. Each receiver in this test cost \$1,500.”



Q: The researcher suggests, “With such systems, people just try to make things work first, and they don’t care about the security or privacy during the first run of design,” Xu said.

A. Schrader has spent more than 15 years designing and developing TPMS systems. Our product has millions of operating miles in every day field conditions. It is completely incorrect that we “just try to make things work first.” The Automotive Electronics industry has some of the most stringent testing requirements of any industry. Consumer safety and security are first and foremost in the development process and as an industry we do not take short cuts. Similarly, in 2010, Schrader launched a public and industry TPMS communications campaign effort designed to raise consumer awareness about the safety, fuel savings, and environmental benefit of tire pressure monitoring systems. The centrepiece of the initiative is a comprehensive 3-in-1 TPMS website with three role-based sections: TPMSMadeSimple.com for drivers; TPMSMadeEasy.com to address aftermarket-specific training and service needs, and TPMSMadeRight.com to assist original equipment manufacturers with quality and technology-based decisions.

Q: The researcher suggests, “Such messages could also be forged. An attacker could flood the control unit with low pressure readings that would repeatedly set off the warning light, causing the driver to lose confidence in the sensor readings. An attacker could also send nonsensical messages to the control unit, confusing or possibly even breaking the unit.”

A. It is impossible to “break” a transmitter or receiver by sending false or “nonsensical” messages to the ECU. In the hypothetical scenario someone was successful in “confusing” an ECU, these systems are designed to flag such a fault and indicate the system needs to be repaired. This in no way would compromise a consumer’s safety or security.

Summary Conclusion

With all due respect of the researchers, the fact remains that TPM systems, as currently designed, provide a reliable and safe indication of tire pressure. There have been millions of vehicles installed with TPMS over the past 15 years. TPMS is a legislated safety system required on 100% of U.S. vehicles (cars & light trucks under 10,000 gvw) beginning in 2008, and similar legislation is being developed in Europe and the Asia-Pacific countries.

The National Highway Traffic Safety Administration (NHTSA) estimates that 660 fatalities and 33,000 injuries each year are attributable to crashes caused by underinflated tires. TPM systems are protecting drivers and passengers and ensuring safety each and every day.

For more information on TPMS, please visit TPMSMadeSimple.com.

