The pressure sensors contain unique IDs, so merely eavesdropping enabled the researchers to identify and track vehicles remotely. Earlier in the year, researchers from the University of Washington and University of California San Diego showed that the ECUs could be hacked, giving attackers the ability to be both annoying, by enabling wipers or honking the horn, and dangerous, by disabling the brakes or jamming the accelerator. The Rutgers and South Carolina research will be presented at the USENIX Security conference later this week.

Cars hacked through wireless tire sensors

By Peter Bright

The tire pressure monitors built into modern cars have been shown to be insecure by researchers from Rutgers University and the University of South Carolina. The wireless sensors, compulsory in new automobiles in the US since 2008, can be used to track vehicles or feed bad data to the electronic control units (ECU), causing them to malfunction.

Earlier in the year, researchers from the University of Washington and University of California San Diego showed that the ECUs could be hacked , giving attackers the ability to be both annoying, by enabling wipers or honking the horn, and dangerous, by disabling the brakes or jamming the accelerator.

The new research shows that other systems in the vehicle are similarly insecure. The tire pressure monitors are notable because they're wireless, allowing attacks to be made from adjacent vehicles. The researchers used equipment costing $1,500, including radio sensors and special software, to eavesdrop on, and interfere with, two different tire pressure monitoring systems.

The pressure sensors contain unique IDs, so merely eavesdropping enabled the researchers to identify and track vehicles remotely. Beyond this, they could alter and forge the readings to cause warning lights on the dashboard to turn on, or even crash the ECU completely.

Unlike the work earlier this year, these attacks are more of a nuisance than any real danger; the tire sensors only send a message every 60-90 seconds, giving attackers little opportunity to compromise systems or cause any real damage. Nonetheless, both pieces of research demonstrate that these in-car computers have been designed with ineffective security measures.

The Rutgers and South Carolina research will be presented at the USENIX Security conference later this week.