Security experts warn of risky attacks on tech-loaded cars

August 20 2012, by Nancy Owano

(Phys.org) -- Now that tiny computers and electronic communications systems are being designed into cars, hackers can look toward the car, like the PC, as potential roadkill. If cars are to become computers on wheels, a number of security experts are expanding their focus on car security systems and sources of security threats. U.S. computer scientists from California and Washington state have already identified ways in which computer worms and Trojans are carried over to automobiles. Conduits include onboard diagnostics systems, wireless connections and even tainted CDs played on radios systems.

Experts point out that the numerous computers known as electronic control units, or ECUs, require tens of millions of lines of computer code to manage interconnected systems. These range from engines,

brakes and navigation to lighting, ventilation and entertainment. The same wireless technologies that power cell phones and Bluetooth headsets are in cars and in turn are vulnerable to remote attacks.

Unlike PCs, though, the attacker's goal with cars may not be to rob the victim of information but to steal the car, or spy on in-car conversation, or cause the vehicle to crash.

McAfee, a subsidiary of Intel and known for its security work to remedy PC viruses, are conducting research on car security at a Beaverton, Oregon garage. Bruce Snell, a McAfee executive, confirmed that automakers are not blind to risks of cyber attacks and are aware of auto system-hacking repercussions far different from seeing laptop data swiped and wiped. McAfee, a subsidiary of Intel, issued a report on automotive systems security with a title that reveals what it sees as the coming risks: "Caution: Malware Ahead."

Researchers of the University of California, San Diego, and the University of Washington have already figured out how to hack into a modern car using a laptop. The same research team extended the scenario to remotely mount attacks via Bluetooth. According to the McAfee paper, another attack scenario was presented by researchers of the University of South Carolina and Rutgers. They demonstrated it was possible to mount an attack on a vehicle and compromise passengers' privacy by tracking Radio Frequency Identification (RFID)tags using long-distance readers at around 40 meters; the RFID tags are used in tires for sensor data over wireless short-distance communication to the vehicle.

Reports do not single out vendors because the issues are relevant to the entire industry; automakers use common suppliers and processes. Nonetheless, a Reuters check of vendor initiatives shows concern in responses.

Major U.S. automakers did not say if they knew of any instances in which their vehicles had been attacked with malicious software or if they had recalled cars to fix security vulnerabilities. At the same time, nothing is impossible and they are working to keep their systems as safe as possible.

Ford has its security engineers working on SYNC in-vehicle communications and entertainment system to ensure it is as resistant as possible to attack, according to the Reuters report. Toyota Motor Corp, the world's biggest automaker, said it was not aware of any hacking incidents and that hacking was at least close to impossible. A Toyota source said the vehicles are designed to change their coding constantly. Chrysler is joining industry groups and outside organizations to tackle car security.

As noted in *Car and Driver*, as more people start to access car networks, the auto industry will beef up relevant security. That may also mean something all too familiar to the PC industry, a relentless skirmish between hackers and automakers.

Citation: Security experts warn of risky attacks on tech-loaded cars (2012, August 20) retrieved 25 April 2024 from https://phys.org/news/2012-08-experts-risky-tech-loaded-cars.html