technology review
Published by MIT

Thursday, January 6, 2011

Carjacking by Antenna

Researchers beat automatic locking and ignition systems.
By Erica Naone

Car thieves of the future might be able to get into a car and drive away without forced entry and without needing a physical key, according to new research that will be presented at the Network and Distributed System Security Symposium next month in San Diego, California.

The researchers successfully attacked eight car manufacturers' passive keyless entry and start systems—wireless key fobs that open a car's doors and start the engine by proximity alone.

Srdjan Capkun, an assistant professor of computer science in the system security group at ETH Zurich in Switzerland, who led the work, says he was inspired to investigate the security of keyless entry and start systems after buying a car that had one. Capkun and Aurélien Francillon and Boris Danev, both researchers in the same institution, examined 10 car models from the eight manufacturers. They were able to access all 10 and drive them away by intercepting and relaying signals from the cars to their wireless keys. While they could relay the signals from the key back to the car as well, usually they did not need to because the key transmits its signals up to around 100 meters. The attack works no matter what cryptography and protocols the key and car use to communicate with each other.

Normally, when a wireless key is within a few meters of the right car, it detects a low-powered signal that causes it to issue a command that opens the car enable the ignition. The researchers used a pair of antennas to transmit these signals from the car to the key when the key was farther away, tricking the car into opening without the ordinary authorization. One antenna needs to be very close to the car, and one needs to be within eight meters of the key.

The researchers came up with two versions of the attack. In one, they ran a cable from near the car to near the key and used it to transmit the signals. They conducted the other wirelessly. Francillon says that the materials for the wired attack cost about $50, and those for the wireless attack cost between $100 and $1,000, depending on the electronic components used.

The researchers tested a few scenarios. An attacker could watch a parking lot and have an accomplice watch as car owners as entered a nearby store. The accomplice would only need to be within eight meters of the targeted owner's key fob, making it easy to avoid arousing suspicion. In another scenario, a car owner might leave a car key on a table near a window. An antenna placed outside the house was able to communicate with the key, allowing the researchers then to start the car parked out front and drive away.

A car won't open or start if the signal from its key takes too long to arrive, so the researchers devised a way to speed communication between their antennas. Most relay attacks require the signals to be converted from analog to digital and back, which takes time. The researchers were able to keep the signals in analog format, which reduced their delay from microseconds to nanoseconds and made their attack more difficult to detect.

The researchers suggest things that car owners and manufacturers can do to protect themselves. Car owners can shield their keys when they're not in use, to prevent attackers from communicating with them. Alternatively, manufacturers could add a button to fobs that would allow owners to deactivate and reactivate them. Capkun worries, however, that these types of solutions detract from the convenience that makes passive keyless entry systems worthwhile.

Ultimately, he says, manufacturers will need to add secure technology that allows the car to confirm that the key is in fact nearby. "I don't see a way around it," Capkun says. His group is actively working on protocols that would accomplish this.

David Wagner, a professor of computer science at the University of California at Berkeley who has

studied the cryptographic systems used in keyless entry systems, says the research "should help car manufacturers improve auto security systems in the future."

Wagner doesn't think the research ought to make car owners anxious. "There are probably easier ways to steal cars," he says. But, he adds, a "nasty aspect of high-tech car theft" is that "it doesn't leave any sign of forced entry," so if a thief did use this method to steal a car, he says, it might be hard for police and insurance companies to get sufficient evidence of what happened. Wagner believes that manufacturers, police, and insurance companies all need to prepare for this eventuality.

"Automobiles are a key example of a system that is pervasively computerized," so they need to be thoroughly examined to ensure they are secure, says Tadayoshi Kohno, an assistant professor of computer science at the University of Washington. Kohno helped form the Center for Automotive Embedded Systems Security, which is dedicated to identifying and solving security problems with car security systems before they cause problems in the real world.