Dan Bednar
Software Secuirty Article 4:
Could Hackers take your car for a ride?
IEEE Security and Privacy Magazine

The one place I had always thought I would be safe from hackers is my car. Being one who knows a fair portion about what is behind the scenes in my own car I know almost everything I do feeds into a computer. Even the gas and brake pedals on my RAV4 are completely computerized. I almost feel silly for never thinking that these systems could be taken over. My laptop can have hardware implanted on it so a hacker could take over anytime, anywhere so why not my car?

The threat itself comes from the rise in networks that are being built into cars. Many manufacturers are creating on-demand help systems such as OnStar that can control a vehicle no matter where it's located. Research has even shown that special CDs can be used to upload malicious programs into a car through a disguised MP3 or WMA disk. Adding to this is a large number of devices that can plug into the ODB-II diagnostic port which can contain their own vulnerabilities.

10 years ago, people would hack their own cars. However this hacking is more like what computer people would consider over-clocking. The cars would be modified to improve engine performance or change vehicles settings

According to the article, there has only been one case of "carhacking" that has been recorded. A former car dealership employee from Austin Texas used a stolen password to log into a remote immobilizer system used by the dealership to disable cars when the purchasers missed a payment. This employee disabled around 100 cars that were purchased from the dealership. This does raise my own questions as to what is hidden on my own car that I might not be aware of. Would a dealership put this on every car they sell regardless of their credit worthiness? Assuming they do how much of a risk am I at of someone doing this to me?

This also leads to the question of privacy. A device like that can find my car anywhere it is. Why can't it track and record all of my movements. What would prevent the same guy from above from taking the device information and putting that into some tracking software instead of shutting the cars down? Now they can study my patterns and know when I won't be home to defend my home.

Many cars now have built-in wireless and Bluetooth systems that can be exploited. These systems, like all other must pass through an internal computer to route the data. Like the malicious CDs I mentioned before this kind of attack must be mounted from within the car itself. The true risk here is the architecture (or lack thereof) of the computer systems. There is no isolation of services in a car's computer systems according to the article, which means compromising one system compromises them all.

Some attacks can be mounted remotely as well. Researchers have found a weakness in the way cars receive messages from the remote assistance services. Messages can be intercepted and then re-created. Any laptop that has the appropriate radio can do this. To identify vulnerable vehicles, the hacker just needs to do what is called "war texting". When war texting, the hacker sends out malicious SMS messages and looks for a vehicle that responds to it. Once a vehicle is found the hacker can control anything within the car.

Researches were able to prove this in their tests. Once a car was found, they were able to mimic the smart-phone functionality that allows users to unlock or start their car from anywhere. Their abilities went beyond what would allow them to gain easy access to valuables. The attacks also allowed the hackers to mimic the diagnostics systems and report a tire problem to the car's dashboard.

The article ends with a little reassurance. With the exception of the former employee in Austin, carhacking has only been done in labs. The authors attribute this to the time-consuming nature of finding a vulnerable car and finding the holes in the car's system. Companies such as Ford are taking actions to redesign their systems for security. They are using threat modeling and documenting areas of possible vulnerability to help them in these efforts.

An outstanding question remains. What happens to cars that are already out on the market when these attacks are perfected and made quicker? Will Toyota, Ford, GM, and everyone else update their systems to prevent their older cars from being taken advantage of? I prefer to hope so, but being a money-making business, I doubt they'll consider spending the time and money on updating the software on older systems.