Article published on December 14th 2011 | Internet

Many of us know that it is easy for criminals to hotwire cars â€“ particularly the older models. Criminals would just open the car's steering column, connect battery wires and then attach starter wires until the car comes to life. Newer models of automobiles may be harder to steal, but high-tech thieves have some ways to accomplish their dark deeds. As a matter of fact, automobiles today can be unlocked and also started by using cellular phones or using the Web â€“ all that is needed is the data of the system and the password.

We know that automobiles are very expensive and it is among the largest purchase a person could make. Indeed, automobiles are very expensive, but newer models have something that is more important and valuable than the vehicle â€“ the important information of the owner. The personal data that are found in the car's system could be compromised and this is known as car hacking.

Indeed, cars today have different innovative features; embedded devices that can control virtually everything â€“ from the engine to even the performance of the breaks. There are systems that monitor the alertness of the driver. Features may have become more impressive and because the digital connectivity these cars bring like infotainment, Internet connectivity, and hands-free access to mobile phones, consumers don't look for safety and the reliability of cars anymore. Cars are now more sophisticated thanks to the mobile computers embedded on them. Just like any regular computer, the systems in cars can be compromised. In fact, the connectivity of cars to the Internet could lead to vulnerabilities that can be exploited.

Whenever there are personal credentials that is involved, then that means money can be made from those. Cars may have systems that could easily provide access to voicemail, email, and any Internet application and service and all of these offer valuable information that could be stolen and then exploited. Systems inside cars could even be hacked using Bluetooth access and attacks can be performed to track the vehicle and compromise the privacy of those who are inside the car. The signals that are transmitted from the car which is needed for the car's systems can easily be intercepted. This could be used in compromising the passenger's privacy.

Even police cars are vulnerable, according to one master in information security expert, it is easy to hack the onboard system of police cars, access the video storage and copy or delete files. In fact, it is easy to access these systems by using the default password in the car's DVRs, password that happens to be available in the Internet. Additionally, according to the same ms information security expert, hackers can even record the driving behavior of the driver since the system itself is not protected. Hackers can even use the vulnerabilities of the system to pinpoint the location of the victim and stalk them, understand their behavior pattern or disable their cars.

It is very important to protect personal credentials and in the event that auto manufacturers fail to defend their systems, then sooner or later they will face recalls as well as fines that would be costly. Manufacturers must secure the vehicles before any safety issues and also brand-damaging exploits could even happen. Security is an important element in the new breed of innovative and intelligent cars. In fact, people will prefer malware on their laptop than having that malware inside their car.

Luckily, drivers need not to be totally tech-savvy in order to protect their systems because there are technologies that are available. These technologies can be used by automakers and manufacturers to secure the systems inside their cars. Possibly, the best and cost effective way to protect the

systems inside automobiles is implementing security solutions that will feature useful application like whitelisting and technologies in change control.

Whitelisting feature will create sets of dynamic applications that are authorized in the embedded device of the car. It can be automatically applied in all the devices of the car. When it comes to change control, this feature will prevent unwanted changes in the system of the car. The authorized modifications in the car can be tracked according to who changed it, where and also when it happened. Every change will be logged and the administrators will be alerted. In fact, drivers won't need to become masters degree information security graduates just to use these features.

Article Source:
http://www.articleside.com/internet-articles/the-new-wave-of-crime-the-car-hacking.htm - Article Side

Eccuni - About Author:

EC-Council University is a licensed university that offers degrees and master's degrees on Security Science online. The degrees are recognized worldwide and may be used in any employment worldwide as well as the graduate certificates that they offer. With excellence and dedication as the core values, many professionals and degree holders have benefitted from undergoing the programs in this university.

More information about master's degrees in information security available at www.eccuni.us, a master in information security, a ms information security, a masters degree information security

Article Keywords:
Car hacking, ms information security, master in information security, masters degree information security, hotwire cars, automobiles, embedded devices, vulnerabilities, personal credentials, Bluetooth, password, victim, manufacturers, malware, security so