

## **Today's Vehicle Security Risks Being Driven by High Tech Threats**

### **A Primer for Secure Transportation and Protection Practitioners**

The response in the executive protection community to an episode of CBS's "60 Minutes" which aired On February 8, 2015 has been pretty overwhelming and as is often the case, some of what has been put out there is not necessarily accurate and, in some cases, has led to more questions than answers. The episode, which was titled "DARPA: Nobody's Safe on the Internet", showed a vehicle being hacked into and controlled remotely by an engineer from DARPA (Defense Advanced Research Project Agency). In this instance, the engineer launched a very sophisticated attack on the car's onboard cellular phone system that allowed a malicious string of code (computer language for operating instructions) to be introduced into the vehicles electronic control system. Once the code was installed, the engineer was able to remotely engage the car's horn, windshield wipers, and brakes. While conducting an attack of the kind demonstrated in this instance would require the resources of a large private sector company or government agency, protection practitioners should recognize that most vehicle systems can be hacked - and controlled - by a moderately determined, resourceful person who is computer savvy. The bottom line for the security professional is that with today's tech laden vehicles hacking is a very real threat.

While detecting and defeating a sophisticated hacker's attack on the principal's vehicle may be just as challenging as launching the type of attack seen in the *60 Minutes* episode, as with most security challenges the first step in defeating the threat is to understand it. So we've taken some of the most frequently asked questions we have fielded from clients and their protection practitioners, both before and after CBS' coverage of this emerging threat along with some of what is being discussed about these types of threats in the tech community to provide those in the executive protection field a better understanding of the risks they may face from a malicious hacker's attack on their principal's vehicle.

Perhaps the question we get most often is whether not the principal's car can be hacked and controlled remotely, possibly from hundreds or even thousands of miles away. According to Stephan Savage, a professor in the Computer Science and Engineering Department at the University of San Diego, "We can remotely stop the brakes on a car from 1,000 miles away, but it's not a clear and present danger today." From the perspective of an academic it stands to reason that, at least in his world, remotely hacking a car's computer is not a real danger. After all who would *want* to hack into *their* car's computer systems?

However, if we look at things from an executive protection perspective, vehicle hacking absolutely *is* a "clear and present danger". Perhaps even more so as it is becomes increasingly evident that vehicle manufacturers and automotive safety "experts" are ignoring not just security

risks posed by malicious attacks on a vehicle's computer systems, but the life safety issues as well. The risk is also not just limited to a handful of specific high profile individuals living and working in technologically advanced countries. If the right technology and resources "fell into" the hands of, or was made available to, the wrong people, security professionals could very quickly find themselves dealing with an expansive global threat. One which is much different from the traditional threat paradigm, as once a vehicle's systems have been hacked the attacker can use those very systems themselves against the vehicle....and the people in it. It goes without saying that an unseen attacker with control over the principal's vehicle could very easily have fatal consequences.

In order to understand the magnitude of this potential threat the security practitioner doesn't need to have a degree in Computer Science, he or she just needs to have a very basic understanding of modern automobiles and the systems that operate them. Today's vehicles utilize Electronic Control Units (ECU) to control various parts of the vehicle, which operate either independently or as a component of a larger network. Examples of ECUs include; the Powertrain Control Module, Body Control Module, Speed Control Unit, Brake Control Unit, and the Telematics Control Unit. All of these, as well as many other electronic components and systems communicate over one common network, or what is referred to as a CAN bus, to effectively manage and control the vehicle's operations within some preprogrammed parameters. Depending on the make, model and options it comes equipped with, a vehicle today might have dozens of ECUs. Once access is gained to one ECU, access is potentially available to all of the ECUs, thereby allowing a hacker to work his or her way into the systems that control critical functions like acceleration, braking, transmission and steering.

While a vehicle may be hacked by remotely accessing the Telematics ECU, which records, stores and sometimes even transmits vehicle performance data, or even the cellular or radio systems if the vehicle is equipped with Bluetooth and Wi-Fi systems, if it is so equipped, a hacker may also gain access to critical systems through a vehicles diagnostic port, USB port, or some other connection to the vehicle's computer system. The protection practitioner should note that Bluetooth, a short-range wireless standard, is available in nearly all new vehicles today not just the higher end luxury vehicles the principal is driven in so virtually any vehicle they may drive could be vulnerable to a remote hacking attempt . Accessing a vehicle's Bluetooth is as simple as pairing a Bluetooth capable device, such as a smartphone, with the vehicle. Most vehicle's come with a very simple, pre-programmed password for the Bluetooth and Wi-Fi systems, and few people ever re-program that password, which leaves this remote access point particularly vulnerable to hacking Once an attacker has established a connection he or she may have the full access needed to upload a malicious code into the onboard system and compromise the telematics ECU. This type of attack was described in a paper published by the University of California and

the University of Washington, titled *Comprehensive Experimental Analyses of Automotive Attack Surface*, which simply stated that “We modified the Bluetooth exploit code on the telematics ECU”.

The technology and data made available through the Telematics control unit is found in popular systems such as *OnStar*, which is used in GM vehicles, and Ford’s versions branded as *SYNC* and *Uconnect*. These systems, as well as those offered by other manufacturer’s, operate over a cellular connection and may even provide WI-FI access from within the vehicle. This makes the vehicle highly vulnerable to the type of attack demonstrated in the “*60 Minutes*” segment.

In fact, in that same report stated that “ We have found that an attacker who has compromised our car’s telematics unit can record data from the in-cabin microphone (normally reserved for hands-free calling) and exfiltrate that data...” The fact that researchers have demonstrated the ability to control the vehicle remotely using the on-board cellular connection is certainly cause for concern, but when you consider the possibility that someone could remotely activate the vehicle’s in-cabin microphone and listen to the conversations being had it becomes downright frightening. A good rule of thumb for practitioners to keep in mind is that if a vehicle has the capability to connect to the internet, it is subject to the same risks and vulnerabilities a home computer is when used to access the internet

Another system that creates vulnerability is, of all things, the Tire Pressure Monitoring System (TPMS). This system utilizes four sensors, one inside of each tire, to broadcast data from its location to the vehicle. Given that the sensors each have a unique ID and the capability to wirelessly broadcast a signal approximately 130 feet from its location, it is possible that an attacker who has captured that devices unique signal could use as a remote trigger for, say, a roadside bomb. While the fact that TPMS sensors currently only send data once a minute may make staging such an attack more challenging, it is not entirely out of the realm of possibility. It is also possible to utilize those sensors to track a specific vehicle, as discussed in a paper titled *Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring Case Study*, which stated: “...show that eavesdropping is easily possible at a distance of roughly 40m from a passing vehicle...messages can be easily triggered remotely, which raises privacy concerns as vehicles can be tracked through these identifiers”.

It’s not just remote access that the executive protection professional needs to be concerned with either. There is always the potential for a hacker to physically access to the vehicle, which affords the attacker access to the On Board Diagnostic (OBD-II) port and other “hard” connections to the cars computer control systems. In fact, an article in *Forbes* in August of last year highlighted this sort threat, “They’re using sophisticated electronic “scanner boxes” to deduce the radio frequency

codes and pop the locks on the burgeoning number of late-model cars equipped with remote keyless entry systems”

While older vehicles are typically equipped with Remote Keyless Entry (RKE) systems, which means the user must press a button on a fob to send a unique Radio-frequency identification (RFID) signal to the lock controller to activate or deactivate the locks, more modern vehicle’s – particularly high end luxury makes and models – are equipped with Passive Keyless Entry (PKES). This technology combines a UHF transmitter with RFID technology to provide the ability for these “smart keys’ to perform a variety of functions, such as engaging the starter activating and deactivating door locks, opening or closing windows, unlocking the trunk, , etc.) Regardless of which system the vehicle is equipped with, they operate over standard frequencies, which makes them particularly vulnerable to compromise. With the PKES systems, research has proven that by using an inexpensive, readily available radio relay device, its possible for someone to unlock an PKES-equipped vehicle from more than 150 feet; the attacker only needs to be within 25 feet of the PKES ”smart key’ to intercept and duplicate its signal and *does not* need line of sight to the vehicle to activate or deactivate the vehicle’s systems. A published report of one study, *Relay Attacks on Passive Keyless Entry and Start Systems on Modern Cars*, reported that “...tested 10 recent car models from 8 manufacturers and show that their PKES systems are vulnerable to certain types of relay attacks. Our attack allowed us to open and start the car while the true distance between the key and car remained large... It worked without physically compromising the key or raising any suspicion of the owner,”

One important fact that all security professionals should be aware of is that while RKE or PKES systems usually incorporate some sort of immobilizer function or system that requires the presence of the actual key fob to activate and deactivate, vehicles equipped with remote start capabilities are at a greater risk because the RKE or PKES also deactivates the immobilizer when the starting sequence is initiated. While the scenarios that accompany a vehicle hacking attack are probably only limited by the bad guy’s imagination, the one that might be the most concerning is a simple scenario in which the attacker jam’s the RFID signal after the intended target (and/or their protection) exits the vehicle. This would prevent the signal from ever reaching the vehicle and prevent the doors from locking, giving someone full access to the vehicle. Or they could initiate the attack when the intended target (and/or their protection) returned to the vehicle. Jamming the signal at that point could prevent the automobile from recognizing the key, which, in turn, would prevent the immobilizer system from being deactivated. At that point the car couldn’t be started be started and, quite possibly, the doors couldn’t be locked...or unlocked.

As was alluded to earlier, simply gaining access to the vehicle may be enough of a reason for some attacker’s to try and capture or duplicate the RFID signal of a particular vehicles’ RKE or PKES system. Particularly in light of what was reported in the study quoted previously,

*Comprehensive Experimental Analyses of Automotive Attack Surfaces*, which stated that “We modified a WMA audio file such that, when burned onto a CD, plays perfectly on a PC but sends arbitrary CAN packets of our choosing when played by our car’s media player. ...” With a little social engineering it’s not out of the realm of possibility that the principal – or even the protector – could become an unwitting accomplice in an attack.

In addition to the CD player, newer vehicles typically have several physical access points that are vulnerable to compromise, to include MP3 connections as well as USB ports and SD slots that are found in the infotainment system. The greatest vulnerability, however, remains the On-Board Diagnostic port (OBD-II). If an attacker is able to access the OBD-II port, which is normally used by automotive mechanics and technicians to diagnose and program automobiles, it can easily be used to introduce malicious code into the system and gain control of any targeted ECU’s. An additional concern is the fact that researches have demonstrated that the computer network that car dealerships and other repair outlets use to diagnose and record data from cars under their care are vulnerable to anyone with access to the same computer network. So, if a potential attacker gains access to the dealer’s network it is possible for him or her to compromise any vehicle the dealer services. According to a piece in *Dark Reading News*, “Toyota and Ford have publicly played down the research. Researchers provided both auto companies with their white paper, but neither firm has promised any fixes. Ford said in a statement for a “Today” show segment featuring this research that “This particular attack was not performed remotely over-the-air, but as a highly aggressive direct physical manipulation of one vehicle ... which would not be a risk to customers.” While we suppose that’s easy enough for someone who is, generally speaking, not directly responsible for the safety and security of those customers, that’s certainly not the case for the protection practitioner.

So while society’s search for convenience and efficiency has created a world of intertwining networks and cyber clouds of data, for the executive protection practitioner it has led to increased threats, vulnerabilities and risks. When you take into account the historical data that indicates the highest risk period of time for a principal is when they are being transported in their vehicle, it places added emphasis on the need for security professionals to understand the vulnerabilities and risks associated with the technology that, quite literally, drives today’s vehicles. Additionally, as technology driven security threats continue to emerge and evolve, what may not be a major concern for the average driver may very well take on added significance for those responsible for protecting others.

Even with the most sophisticated hacking threats, the fundamental best practices for security still hold true, and offer the best protection — gain as much knowledge as possible to understand the threat, and take appropriate steps to reduce vulnerabilities and mitigate or manage potential risks; in the case of a potential “vehicle hacking” threat, the fewer methods of communication and the

fewer remote or physical access points to your vehicles network, the better. While we have spoken to service technicians and managers at a number of automotive dealerships that have stated that it is entirely possible for to simply deactivate a vehicle's Telematics systems and other sensors around the vehicle, thus reducing the risk of hacking, they also indicated that they would not be permitted to do so due to safety considerations. However, there is nothing preventing the owner or operator from deactivating the vehicle's Bluetooth and Wi-Fi systems, and it is strongly suggested that you do so as these are not critical life safety system. In the event of a physical hacking attempt, securing the OBD port is absolutely critical, fortunately there are a number of devices available that cover and lock the port. Or you can simply opt to place tamper evident tape over the standard connector. Other options available to the operator may include disconnecting the antenna for the Telematics system and doing the same for non-essential ECU's., though such decisions are solely the responsibility of the owner and/or operator of the vehicles and should not be taken lightly as, among other things, they may void the vehicle manufacturers warranty.

## **About US**

**Secured Technologies** is a global company that educates, evaluates, and advises on integrating technology with secure transportation and executive protection functions, so the things that clients value most are well protected.

Over 25 years of IT experience in the private and government sectors along with employees that are security professionals with diverse backgrounds as well as recent and relevant experience, provide us with unique insight and capabilities to solve your needs. We can be reached by email [info@secured-technologies](mailto:info@secured-technologies) or phone **(202) 830-0573**