# Car Hacki

# Preparing For The Future Now

By Donald W. Dunphy

**THE DRIVER PLACES HIS** foot on the gas in order to pass a driver in the left lane. He holds it in a comfortable 65 mph range. Suddenly the speed spikes, the motor revs harder, and the vehicle bolts forward and out of control. He takes his foot off the gas, and as he does so, the brakes slam, bringing the wheels to a screeching halt. The car immediately behind him runs headlong into the bumper. He never applied the brakes. The car "decided" to do so independently.

It is a terrible thought for anyone who drives – that feeling of losing control of the vehicle you are using. Far worse is the possibility that someone else, nowhere near that car, was in control instead. Our world, including vehicles, is connected to the Internet in ways that once seemed impossible, and therein resides the temptation for those who might manipulate them.

"There are a lot of definitions of the Internet-Of-Things, but we are including basically anything that was not traditionally connected to the Internet in the past," said Johan Sys, Managing Principal for Identity and Access Management from Verizon. He is part of the team that has developed the Managed Certificate Services (MCS) Security Platform, which utilizes a sophisticated digital certificate protocol similar to that used for websites with online banking or other security-intensive websites.

Sys' platform is designed to add a layer of protection not solely to vehicles, but other objects in our linked world, from climate controls and thermostats, all the way up to medical devices and remote-operation surgical units. The goal is to keep bad code from breaching the vulnerabilities found in these items. While widespread cyber-attacks on such items are not yet prevalent, designers and programmers are trying to disrupt such events proactively.

Patrick T. Barrett, CAFM®, is Director of University of Nebraska Transportation Services, and he also suggested that now is the time to make security a priority consideration, before those decisions become unavoidable. "Hopefully, 'car hacking' as a frequent practice never becomes a reality, but if you think about it, not that many years ago we didn't password protect personal computers, and nobody imagined computer viruses. With this in mind, I believe now is the time to start protecting our fleets from the future we hope never occurs."

### The Future Now

At DEFCON 21, a convention for computer hackers held in Las Vegas in 2013, the duo of Charlie Miller, a Security Engineer at Twitter, and Chris Valasek, Director of Security Intelligence at the Seattle consultancy IOActive, demonstrated current vehicle vulnerability. They showed how they could take control of primary functions of a 2010 Toyota Prius and 2010 Ford Escape and command it wirelessly with a laptop computer. They were able to kill the engine of the Ford Escape in mid-usage, and made the Prius brake at 80 miles an hour. They even had remote control of the steering wheel.

"We started the project not really knowing how any of these cars worked. We're both computer guys," Valasek said. "We found out that all of the computers in a car communicate in a broadcast fashion where every computer on one segment of the automobile on the CAN Bus (Controller Area Network involving a distinct set of conductors carrying data and control signals within a computer system) can hear all others.

"Depending on what computer is on which segments of the network -- a lot of the time all on the same network -- you

# ng

*"I BELIEVE NOW IS THE TIME TO START PROTECTING OUR FLEETS FROM THE FUTURE WE HOPE NEVER OCCURS."*
***—PATRICK T. BARRETT, CAFM®, DIRECTOR, UNIVERSITY OF NEBRASKA TRANSPORTATION SERVICES***

could control a lot. We realized that if you ever breached a computer network, there are very good odds that you could control physical aspects of an automobile if it had a certain degree of technology," Valasek said.

**Good News First**

Car hacking requires three things beside the know-how to execute a takeover: the money to afford the tools, the time it takes to carry out the job, and the effort necessary to follow the plan through. "You have to buy the automobile (type)," Valasek said. "Each car is different and they have different ways of communicating via these proprietary messages. The messages a Ford might send to turn the wheel of a car is different than a message a Toyota sends.

"You also would need to make sure the car has technology features that will let you do things like control the wheel. Not all cars do," Valasek said, referring to technologies like 'drive-by-wire' where a car's steering wheel no longer has direct linkage, but is operated by digital communication. "Drive-by-wire is going to become very popular because the computer is going to be doing (the work), and that's something we want. Computer-enabled steering provides very quick auto-corrections and things of that nature.

"When we start considering terrorism, the return-on-investment turns out to be pretty low. You buy all the automobiles (that correspond with those you would choose to take over), and then have to pay a very skilled researcher to dissect it."

Stefan Savage is a Professor at the Department of Computer Science and Engineering at the University of California, San Diego. He also does not think the first problems we'll see will be the sexy cyber-terrorism scenarios. "The first, which already exists to some extent, is to enable sophisticated theft – particularly for vehicles in which anti-theft measures are driving the need for a more sophisticated entry and engine-start capability (e.g, immobilizers, etc.).

"Beyond this I can imagine a scenario where a disaffected character (or a 'prankster' without much empathy) might simply think it was funny to 'brick' cars (i.e., disable them to the point where they would need to be towed to the shop)," Savage said. "Correctly changing the function of the systems reliably is quite difficult. However, just making them not work is much easier and thus doesn't need as focused or strong a motivation to carry out."

Miller and Valasek accessed the system through the OBD-II (on-board diagnostic) plug-in port regularly used by mechanics to read car data from the internal computer. That required a physical breach to gain access, and the common response would be, "Deny access to vehicles from strangers. Problem solved." Only, that's not entirely possible.

**Shock of the New**

A team of researchers at the University of Washington and the University of California, San Diego, including Professor Savage, found they could wirelessly penetrate the same critical systems Miller and Valasek targeted using a car's OnStar-type cellular connection, Bluetooth bugs, a corrupted Android app tied in with the car's network from the driver's smartphone, or even something as innocuous as a compromised audio file on a CD in the car's stereo system.

The key remained in gaining access to the vehicle's CAN Bus through the OBD-II, where much of the data information overlap exists. That could be how someone would compromise data integrity with code transmitted over a Wi-Fi connection... or with a song downloaded from an illegal file-sharing site.

"In the end, we were able to demonstrate that existing vehicular systems were highly brittle. Once compromised, this usually provided sufficient access to where we could eventually take over all systems in the car (engine, brakes, lights) and control remotely without any prior physical access to the car," Savage said. "We carried out some attacks where we compromised a vehicle, sight unseen, via cellular over 1,000 miles away. That's not much access."

Savage added, "Other modes of compromise might require more access... ranging from being within 100 miles, to hacking the driver's phone, having the car go in for service, getting the driver to play a song off the Internet, etc., up to physical access to the interior of the vehicle."

He did not think there was any singular eureka moment in their tests since his team was constantly expanding what they knew from one experiment to the next, but recognized that the results were not solely of academic interest. The key stakeholders (OEMs and regulators) needed to know the findings so that they could responsibly move forward.

Valasek agreed, saying, "(Charlie Miller and I) were looking to open a dialog between security researchers and the automotive industry. We are in a society that has the Internet-Of-Things. Almost everything will eventually be connected, with cars being one of them. You're going to want security researchers investigating these types of issues and communicating with manufacturers to make a better product for the end consumer."

Savage indicated that telematics might present an additional attack surface for entry into the vehicle (typically via cellular data) and enables a wide range of threats since it allows interactive control and surveillance at an arbitrary standoff distance. "By design, telematics systems must touch a wide array of a vehicle's systems and thus are difficult to isolate and yet must also be controllable from afar," he said.

Revenue-bearing services involving the telematics platform are creating a parallel concern. "This is driving the

creation of an 'app' platform on the car that can't help but increase the attack surface of the vehicle," Savage said. "At the same time, there has been some good work of late in trying to lock down the sets of interactions and messages that a telematics head-end can emit onto the car's buses to at least limit the capability of an attacker to what the system's designed capabilities are (although these might be significant since systems like OnStar allow remote stop for example)."

**Risk Management**

It is impossible to accurately structure a risk management policy to cover a risk that hasn't presented itself in full yet. Fleet presents a significant challenge in that a single car or truck could have many individuals involved with its care and usage, from multiple drivers to multiple mechanics, to the people monitoring digital equipment from afar. Given the hypothetical situation where that line has now been crossed, the experts considered what appropriate steps might look like.

"You're going to want to make sure you can check the code on a car's computer, making sure it is what was originally put there by the manufacturer," Valasek said. "If you find someone has overwritten or changed any of these that could potentially signal that something malicious is being planned."

"Just as organizations have computer security/network policies in reaction to known threats, initiating a car hacking policy to eliminate or prevent a potential threat may be justified," said Patrick Barrett. He said that the University of Nebraska-Lincoln vehicle security policy would require augmentation to include this futuristic threat, which would include language like:

*Car Hacking – Vehicle security is as much about knowledge and behavior as it is about hardware and software. On board computer security and subsequent safety, is best accomplished by implementing multiple levels of solutions to help protect and prevent car hacking.*

- *All University vehicles must have their OBDII port capped to prevent easy access.*
- *If available, all University vehicles must have antivirus software installed and enabled.*
- *Vehicles equipped with drive-by-wire systems, will have their factory sound systems, and GPS systems replaced with aftermarket systems which operate independently from factory on-board computers.*
- *If vehicle is equipped, Blue Tooth must be disabled.*
- *If available, all University vehicles will be regularly accessed, scanned for potential threats, and repaired if a threat is detected.*

Barrett cautioned that this policy update, for now, is purely speculation, and added, "Much research is required to develop a realistic policy, but a proactive approach is better than a reactive approach if car hacking becomes reality."

In a landscape where car hacking becomes less rarified, limits to vehicle access would likely spell the end of the personal-use fleet vehicle. Savage said, "It is definitely the case that cars held at home with reduced physical security would have greater risk of being hacked via direct access to the OBD-II port. In this scenario the attacker may not need to find a compromise at all, but just enough knowledge to convince a firmware update tool to overwrite the existing car's Engine Control Units (ECU)."

While personal use is not permitted at any time with University of Nebraska vehicles, Barrett said that by no means excludes the possibility of unsupervised access. "Our vehicles travel to all lower 48 states, and our campus in Nebraska runs border to border. Even though our campus is the entire state, they are not under our direct control. If car hacking became prevalent or more feasible, we'd have to address the issue on where vehicles are kept after hours."

"We're hoping that manufacturers start thinking about security from an external and an internal perspective," Valasek said. "You want to test and make sure there are a minimal amount of remote vulnerabilities in your car. I think we all know there's no such thing as perfect code. Manufacturers should plan on trying to diagnose and on alerting drivers – or at least alert the automobile – if something crazy is happening on the car's network."

"Unfortunately right now," Valasek said, "we're in the infant stages of all this. We're just now starting to talk with people about the types of things that need to be done. There's no real solid set of risk assessment criteria that can be done with a car (in this circumstance). Right now, it's about trusting the manufacturer hasn't made a flaw." ■