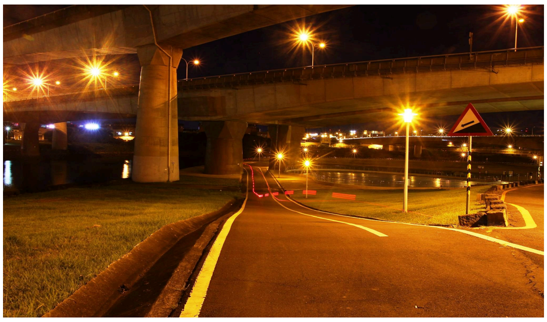
Is Your Vehicle Controlled by You?

Fu-Hau Hsu
National Central University
hsufh@csie.ncu.edu.tw



Abstract — **To increase the vehicle security and the comfort of drivers and passengers, many electronic devices, embedded systems, and vehicle computers have been added to automobiles to control the automobiles and various devices. However, ironically, research shows that attackers can take over the control of a moving vehicle from its driver through wireless networks by compromising these electronic devices or vehicle computers. Even though the anti-virus industry and security researchers have developed many approaches, such as anti-virus software and patches, to defend a system against malware and computer attacks, these approaches are not suitable for vehicle computer security, because they are not able to provide real-time defense and achieve zero-tolerance upon false positives and false negatives. In this new battlefield, for security researchers and security industry, there are plenty of tough battles ahead of them.**

Keywords — **Vehicle Security, Vehicle Computer, Car Hijacking.**

When security industry is doing their best to provide a secure and reliable environment for desktop, laptop, and smartphone users, a much more vital security problem, *vehicle computer security*, is emerging, which may not only cause life-threating problems but also become a powerful tool for terrorists or criminals.

In a demonstration [1] made in 2015, Charlie Miller and Chris Valasek showed that through Internet and wireless connections, they can easily remotely control a Jeep Cherokee driven by a human user. In other words, just using a laptop, they remotely disabled a driver's capability to control his Jeep and got full control of the dashboard functions, steering, brakes, and transmission of that car. Besides, they also obtained the Jeep's GPS coordinates, which leaked the positions of the Jeep. This demonstration proves that Checkoway *et al.* [2]'s 2011 work is not paranoid speculation and can be further enhanced.

In the above demonstration, Miller and Valasek utilized the vulnerability in an electronic control unit (ECU) of a Jeep to rewrite the firmware of a chip with their own code. Based on the instructions issued by them, the code used the CAN bus [3, 4] to send commands to the physical components, such as the engine and wheels, to hijack the Jeep. As vehicles incorporate more electronics to provide more functions to their users, more vulnerabilities are also unwittingly introduced to vehicles. As a result, nowadays, car thieves can utilize a completely different approach [5] to steal cars, especially keyless cars. For example, a car thief can use a device to physically access a car's OBD (on-board diagnostics) connector to collect unsecured key code. With the key code, the thief can quickly create a new car key and use the new key to star the car engine and drive it away.

Even though the above situations have inspired lawmakers' intention to make related bills and set new digital security standards for cars and trucks [6], the fundamental solution still should come from technology. However, due to having different hardware, software, and communication protocols in an automobile and zero tolerance upon false negatives, the traditional antivirus models or patch mechanisms may not be suitable for vehicle computers or vehicle embedded systems. First of all, in a traditional antivirus model, it may take a couple of weeks to obtain a signature of a zero-day malicious program. And it may take several months to find a vulnerability of a program. Besides, extra time is required to obtain related patch. However, this time period is too long for vehicles. After all, an unfixed vehicle is vulnerable to car hijack. A hijacked car may result in life-threating problems and cause huge panic upon the public. Moreover, even if a signature or a patch is created, it is not easy to dispatch them to all related antivirus systems or software on automobiles. Automobile manufacturers usually recall faulty cars and ask their technicians to use special devices to fix problems. However, the recall-and-fix pattern means that some cars may remain unfixed because their owners may ignore or do not know a recall. The patterns also means that it needs to take a much longer time to fix software vulnerability or add a malware signature to an antivirus system in a vehicle. As a result, if we do not develop new approaches to handle vehicle computer security problems, it is very likely that cars with unpatched software or cares with un-updated antivirus software may be full of the streets, which creates a serious security problem.

We believe that Checkoway *et al.*, Miller, and Valasek just unveiled a new type of critical security threats that will last for a long period of time. In this new battlefield, for security researchers and security industry, there are plenty of tough battles ahead of them.

REFERENCES

[1] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[2] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," USENIX Security, San Francisco, CA, USA, August 10–12, 2011.

[3] Steve Corrigan, "Introduction to the Controller Area Network (CAN)," http://www.ti.com/lit/an/sloa101a/sloa101a.pdf

[4] AA1Car, "How to Diagnose a Controller Area Network (CAN)," http://www.aa1car.com/library/can_systems.htm

[5] Bill Howard, "Hack the diagnostics connector, steal yourself a BMW in 3 minutes," http://www.extremetech.com/extreme/132526-hack-the-diagnostics-connector-steal-yourself-a-bmw-in-3-minutes

[6] Dan Goodin, "Senator: Car hacks that control steering or steal driver data way too easy," http://arstechnica.com/security/2015/02/senator-car-hacks-that-control-steering-or-steal-driver-data-way-too-easy/

Fu-Hau Hsu received his Ph.D. degree in Computer Science from Stony Brook University, New York, USA in 2004. He is an associate professor in the Department of Computer Science and Information Engineering at National Central University, Taiwan, R.O.C. His research interests include system security, smartphone security, web security, information hiding, operating system, and networking.