Lessons Learned from Hacking a Car

Charlie Miller
Cruise Automation

Editor's note:
In 2015, Miller and Valasek demonstrated one of the most celebrated hacks on automotive systems, when they managed to remotely compromise a 2014 Jeep Cherokee. They showed how to exploit a vulnerability in head unit to control the physical aspects of the driving subsystem, including steering and braking. In this article, with the hindsight of over three years, Miller reflects on the lessons learned from this experience.

—Sandip Roy, University of Florida

In 2015, Chris Valasek and I demonstrated the remote compromise of my 2014 Jeep Cherokee. We exploited a vulnerability in the head unit that was produced by the supplier Harmon Kardon (Figure 1). After this initial exploitation, we reprogrammed a gateway chip in the head unit to allow it to send arbitrary controller area network (CAN) messages. Upon some further research, we were able to control physical aspects of the car such as steering and braking at speed (Figure 2).

In many ways, this was the worst scenario you could imagine. From my living room, we could compromise one of any of 1.4 million vehicles located anywhere in the United States. This required no user interaction or special setup on the vehicles—the only prerequisite for the attack was that the vehicle was on. The attack was nearly invisible to the driver and left behind almost no forensic evidence. It was an excellent demonstration of why automotive cyber security is such an important topic.

Now that over three years have passed, I've had time to reflect on this experience and draw conclusions. One insight is the importance of code signing in verifying the software on the electronic control units (ECUs) in the vehicle. In both our attack and an exploit demonstrated later against a Tesla Model S, there was a gateway preventing the compromised head unit from directly sending CAN messages. In both cases, the attackers were able to simply reprogram the gateway since it did not do any verification of the code that was used to reprogram it. Had the gateway been performing verification of the code, it would have made an end-to-end attack significantly more difficult to achieve. In fact, it would have been so much more difficult, I doubt Chris and I would have continued the research beyond this point and would have only shown compromise of the head unit without demonstrating how to physically affect the vehicle by sending CAN messages.

Another point that becomes clear with reflection is that, no matter how hard we try and how complex we make the security solutions on vehicles, it is impossible to make something perfectly secure and unhackable. Therefore, a vehicle's security should not rely solely on preventing attacks, but should also design systems that can detect attacks and take appropriate actions. While doing the Jeep research, we successfully attacked the Jeep hundreds of times, reprogrammed ECUs tens of times, and disabled various functionalities of the vehicles more times than I can remember. Despite all of this anomalous behavior, the Jeep never contacted Chrysler to report a problem or take any significant defensive action at all. Ideally, if an attack was detected, the driver could be notified and actions could be taken by the vehicle such as automatically

Digital Object Identifier 10.1109/MDAT.2018.2863106
Date of current version: 31 October 2019.

Figure 1. Interior of the Jeep Cherokee. The head unit has the large screen in the center of the dashboard.

disabling some advanced features that are especially susceptible to manipulation.

This leads to the next point regarding cybersecurity of automobiles. I would love to see more communication between the auto manufacturers and outside researchers in academia and industry. For example, after the exploitation of the Tesla Model S by the group of researchers from the Keen Security Lab, Tesla added code signing to their gateway. It would be great to know how many other manufacturers have also added code signing to their electronic control units (ECUs), and furthermore, how many of their different ECUs require code to be signed before reprogramming. Similarly, how many automobile manufacturers have gateways between their head units and steering, how many have gateways between the obdii port and steering, and how many have any kind of anomaly detection on their CAN bus? This is data that are not available to us and probably isn't even shared between manufacturers. The publishing of this information could help encourage manufacturers to add security while also providing lessons learned by both success and failure of these technologies. It would also provide insight to consumers attempting to purchase the vehicle that is most resilient to cyberattack.

Figure 2. After remotely attacking the Jeep and turning the steering wheel, we had to get it towed out of a ditch.

While the demonstration of the Jeep vulnerability seems to have spurred a lot of discussion of automotive cybersecurity, in some ways, it was not a complete success. The biggest disappointment in the time since we started doing automotive research is the lack of similar research being carried out by other groups. Chris and I released a number of papers, totaling over 300 pages, as well as all of our tools that we used. We hoped this would jumpstart a number of researchers into this important space. We looked forward to a number of papers about how to physically control other vehicles using CAN messages as well as other ways to remotely exploit vehicles. Sadly, the only group that has produced similar work seems to be the Keen Security Lab from China which exploited the Tesla discussed above in 2016. The field of offensive automotive security research has not progressed significantly in the past few years. Until we understand attacks better, it will be difficult to effectively design defenses. I understand that automotive security research has a large barrier of entry, but I still hold out hope that in the future more people will continue to do research in this field.

In the end, the good news is that we don't need new fundamental ideas or technologies to secure automobiles. We can treat vehicles as small networks of computers and apply the technologies and techniques from the world of enterprise security to secure vehicles with well-established concepts, including minimizing attack surface, verifying code running on systems, segregating networks, and detecting anomalies. We don't need new ideas, instead we need to focus and apply security mechanisms we already know but thoroughly and carefully. After all, if we fail to secure automobiles, the result won't be limited to credit card information being stolen. ■

References

[1] K. Koscher et al., "Experimental security analysis of a modern automobile." [Online]. Available: http://www.autosec.org/pubs/cars-oakland2010.pdf

[2] S. Checkoway et al., "Comprehensive experimental analyses of automotive attack surfaces." [Online]. Available: http://www.autosec.org/pubs/cars-usenixsec2011.pdf

[3] C. Miller and C. Valasek, "Adventures in automotive networks and control units." [Online]. Available: http://illmatics.com/car_hacking.pdf

[4] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces." [Online]. Available: http://illmatics.com/remote%20attack%20surfaces.pdf

[5] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," 2015. [Online]. Available: http://illmatics.com/Remote%20Car%20Hacking.pdf

[6] C. Miller and C. Valasek, "CAN message injection," 2016. [Online]. Available: http://illmatics.com/can%20message%20injection.pdf

[7] S. Nie, L. Liu, and Y. Du. "Free-Fall: Hacking Tesla from Wireless to Can Bus." [Online]. Available: https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf

[8] Keen Security Lab. "Experimental Security Assessment of BMW Cars: A Summary Report." [Online]. Available: https://keenlab.tencent.com/en/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf

Charlie Miller is a Security Researcher interested in the security of connected and autonomous vehicles. He is also a Principal Autonomous Vehicle Security Architect at Cruise Automation, San Francisco, CA, USA. He received a PhD in mathematics from the University of Notre Dame, Notre Dame, IN, USA.

■ Direct questions and comments about this article to Charlie Miller, Cruise Automation, San Francisco, CA 94103, USA; e-mail: cmiller@openrce.org.