Infotainment Systems or Infotaintment Systems? How Dancing Pigs are Ruining Cars

Obaid Farooqui

Fall Comp 116 Final Project

Mentor: Prof. Ming Chow

Abstract

The modern car buyer expects advanced infotainment systems that offer a lot of amenities to the driver and passenger. These features are often built into or have access to the onboard computers that handle mission critical functions relating to braking, accelerating, and steering.

The infotainment systems inherently require communication with the outside world. Navigation systems need to communicate with GPS and with cellular networks, satellite and AM/FM radios need to communicate via radio channels, and many other features need require access to the internet. Not to mention the fact that many infotainment systems allow users to plug in their own devices into the car via USB ports, Bluetooth, and even with good old fashioned CD's.

All of these, while they serve legitimate purposes, open up a number of attack surfaces, or interfaces that can be hacked to communicate with the car in unintended and potentially dangerous ways. By exploiting vulnerabilities in the infotainment systems, attackers can gain access to the car's computer, and through that to the controller area network (CAN bus), and once an attacker has access to that there are few, if any, functions of the vehicle he or she cannot control. This paper will explore these exploits in more detail, and will discuss possible precautions and defenses against these types of attacks.

Connected Cars for a Connected World

Modern cars are little more than networks of computers on wheels these days. Onboard computers and processors control most functions of the vehicle, collect data on usage, and communicate with outside systems for navigation, entertainment, and safety reasons. Long gone are the days when a car was the sum of its mechanical parts, cut off from the outside world and contained within its doors. It is estimated that by 2013, the total number of cars that are capable of sending and receiving information to and from external services has reached 45 million, with that count expected to grow tenfold before the decade is up [1]. A report on automobile safety written by the staff of Massachusetts Senator Ed Markey has found just about all cars manufactured today incorporate some kind of wireless communication [2].

There are legitimate reasons for our cars to communicate. Services like GPS navigation and OnStar (a feature that automatically calls for help when it detects an the vehicle has been involved in an accident) require access to the outside world and are fast becoming, if they have not already become, standard offerings. But there are other features that are there purely for entertainment purposes. The ability to play CDs, listen to traditional and satellite radio, connect devices to the car via Bluetooth, and in some cases to use the car as a WiFi hotspot, all represent interfaces between the car and external inputs. All of these greatly improve the

driving and riding experience, and it is difficult to imagine cars without them being marketable at all to today's consumers.

Attack Surfaces

The problem with these interfaces between the car and the outside world is that once an attacker gains access to the car through any system, they can gain control to the CAN bus, and through that they can gain control of the vehicle as a whole. As Checkoway and his colleagues write in their paper, through their attacks through they were able to obtain full control of the vehicle [3]. They explore a number of creative attack surfaces: they were able to cause a malicious firmware update through a CD that had a special WMA song with the update on it, and they exploited buffer overflow vulnerabilities through the both Bluetooth and WiFi connections. While it is true that there are additional attacks surfaces not touched by these researchers, what is so worrisome is that all of the attack surfaces they dealt with had to do with the infotainment system, a part of the vehicle that arguably has no business being connected to the CAN Bus and through it to the mission critical parts of the car.

Charlie Miller and Chris Valasek explain in detail in their paper how they were able to remotely hack into a Jeep Cherokee [4]. In this particular vehicle (as in plenty of others), the telematics, applications, and entertainment systems are all physically together as part of the Uconnect system. Fortunately, this system is not on the CAN

bus itself; less fortunately, it does have the ability to connect to the CAN bus through a microcontroller (Renesas V850) and its associated package. To be fair, this in and of itself is not the end of the road, as the packets that are exchanged through the CAN bus are not always readily identifiable. However, with a little bit of work, it is possible to distinguish normal CAN messages which affect a lot of the signals and the locks, from diagnostic CAN messages, which control the engine, brakes, and steering. There are safeguards that surround the diagnostic CAN messages—for instance, they can't be sent if the car is moving faster than roughly 10MPH. However, once an attacker has figured out the normal messages, it is relatively easy to spoof speed and other data to work around these safeguards, and from that point on the attacker can wreak havoc on a moving vehicle.

To The Community

A natural question to ask is why we as a community should care. The attacks using physical attack surfaces, such as CD or connecting directly using USB, are not necessarily any more dangerous than traditional car tampering; after all, anyone who has physical access to a car's CD player or USB port can conceivably do a lot more damage a lot faster with the use of an ordinary sledgehammer. As for the remote attacks demonstrated by the aforementioned security researchers, these were highly skilled attacks, the product of years of hard work and thousands of dollars in funding. We have yet to see hackers using these attack surfaces for

malicious activities in the wild, and it seems for the time being that conducting such attacks is more trouble than it's worth.

First of all, it is only a matter of time before we start to see these kinds of attacks in the wild. Already, nearly half of automobile thefts in the UK this year have been the result of hacking keyless entry systems [5], something that would have been unthinkable just a few years ago. Furthermore, conducting these types of attacks does not require lots of extra or expensive equipment, and the equipment needed can easily be got from any electronics store [6]. All that's needed is the know-how, and as the security community knows all too well, information about exploits is not particularly difficult to find. This qualification of technical knowledge serves as a barrier to entry for amateur would-be car hackers, but it certainly is not prohibitive.

The value for attackers in these hacks is that once an attacker is able to access and control a vehicle, the possibilities of what he/she might be able to do are endless. Of course, he could take over a moving vehicle and cause an accident, as Miller and Valasek demonstrated, and it goes without saying that losing control of a moving vehicle is just about the worst situation a driver can find himself in. But there's far more to it than that. They could brick a car remotely, holding it for ransom—a dealership employee recently did just that after he was laid off, abusing a system that the dealership had to remotely disable the ignition system or honk the horns of cars for which late payments were due [8].

But this is just the beginning. Vehicle to vehicle communication is coming, and will be of more significance as self-driving vehicles start hitting the streets [7]. Gaining access to one vehicle, then, could simply be an entry point through which to gain access to others, using modified worms or viruses. Even before our cities become fully automated networks of cars, using the techniques mentioned above could lead trailblazing hackers to attack multiple cars at once. Terrorists could use tools to remotely control multiple cars at once, haphazardly causing accidents all over a congested metropolitan area, turning innocent commuters' vehicles into lethal weapons of choice. Going back to theft, as Checkoway and his colleagues write, it is possible for attackers to scan all the cars in an area and only go after the most valuable ones, or perhaps to even monitor areas and sell this information to others who might then steal select cars [3]. They mention that the progression of attacks on cars could very well follow the trajectory of desktop attacks, which also began by exploiting individual machines, moved to using viruses and worms to infect networks of machines, and has progressed now to black markets that sell access to exploited systems.

The best part about all of this for the attackers is that they can do this all remotely; it provides distance, and makes tracing the crime back to the perpetrator harder for law enforcement, especially because most automakers cannot recognize or respond to such infiltration in real-time [2].

We've thus far been so focused on the physical loss or manipulation of a vehicle through these methods that we have completely ignored the enormous elephant in the room, namely that cars nowadays possess the equivalent of modern day cyber-gold: troves upon troves of driving data. As the Markey report finds, nearly all car manufacturers record usage data that includes driving habits, location, speed, settings, and a host of other personal information [2]. While some manufacturers store all data on the vehicle and only download it for diagnostic purposes when the car comes into the shop, many program the cars to send reports back to the mother ship frequently, if not constantly. A hacker who gains access to a vehicle does not necessarily have to physically take control of the vehicle to do evil; he could steal the stored data, or have the car send data to him (or to others) in addition to wherever it already sends it, thereby allowing the hacker to keep complete tabs on the location and habits of the owner. It's obvious that such a serious security breach could have disastrous effects, and the options of using or selling this data for nefarious purposes are both incredibly dangerous for car owners, and represent serious privacy and security threats.

We are fortunate that we are in the early days of car security, and we know from our experience with desktops, mobile phones, and web apps at large what happens when we engineer things without regards to security. We have the opportunity to not repeat the same mistakes, to proceed with caution and purpose as we bring in the next generation of the automobile. While it may seem that the above scenarios are far-fetched and worries for a later time, they are already within the realm of the

possible; what remains for us to do is to fix them before they enter the realm of the normal.

Action Items

There are a number of things that car manufacturers should consider when implementing security features, but the biggest one with regards to infotainment systems is the separation of essential and non-essential systems.

It's a first step to keep the infotainment system separate from the CAN bus, but as Miller and Valasek demonstrated, this is useless if it is still possible to access the CAN bus [4]. Furthermore, while it may be useful for some infotainment system features to access messages from the CAN bus to display relevant information to the driver—in the case of showing engine signals or assisted parking, for instance — doing so presents an attack surface that can be exploited.

The workaround to this is to have two different systems that do not communicate with each other: one that is responsible for the operation of the car and has access to the CAN bus, and the second that is purely for entertainment purposes. The entertainment features, and especially the ones that interact with the user through any number of input channels, including CDs, Bluetooth, WiFi, and radio, should not have access to the CAN bus. This way the damage that can be done

through these attack surfaces is limited to the entertainment functions of the vehicle, and cannot put the car physically at risk.

To divorce the entertainment system from the rest of the mission critical components of the car makes sense, but how then to deal with the information systems—the gauges and alerts that drivers rely on to know when there might be a car in their blind spot or if a door is open or when they're desperately in need of an oil change? The answer is to have these gauges and alerts be a part of the first system, living separately from the entertainment system. Additionally, they should only be able to receive messages from the CAN bus, not send them.

One might argue that having dual systems would destroy the beauty of a unified car system, especially when say the same dashboard screen that a driver might use to choose songs to play from their iPhone would also be the natural place to display information and critical alerts, such as a blown tire or statistics on gas usage. However, as convenient as it might be to lump all of the systems together and as tempting as it is to allow communication between different parts, the ramifications of such connectivity, as shown through the hacks by security researchers, is far too great. These information displays and systems must necessarily communicate with the operational components of the car, and for that they must have access to the CAN bus, but there is no reason why these should be lumped together with the entertainment systems that have no need for communication with the CAN bus. If treating the entertainment system, with its

myriad user inputs and attack surfaces, as a separate entity from the rest of the vehicle will improve car safety, then it is absolutely worth the trouble that building such systems might present.

Conclusion

The automobile industry, much like the rest of the tech industry, is at crossroads where it must make engineering choices to reflect the balance between connectivity and security. The features that are being shipped with new cars are revolutionizing the driving experience, but we must be careful not to allow the thirst for these to open drivers and passengers up to new and unforeseen vectors of attacks, against not only the physical cars themselves but the data that they collect and store as well. The infotainment system in particular has a large number of interfaces between the outside world and the car's operational components, and separating the two is necessary to prevent attackers from gaining control of a vehicle and its data through exploiting vulnerabilities in these secondary entertainment systems.

Edward Felton and Gary McGraw remarked that consumers will always pick dancing pigs over security, and the dancing pigs that are infotainment systems aren't going anywhere. But ignoring vulnerabilities in the digital world could leave drivers and passengers alike vulnerable to real world attacks, and it is the responsibility of the auto industry to prevent the dancing pigs from becoming wild boars.

References

[1] "Car Hacking | Argus Cyber Security." Argus Cyber Security RSS. N.p., n.d. Web. 15 Dec. 2015. <http://argus-sec.com/car-hacking/>.

[2] "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk." (2015): n. pag. Ed Markey, United States Senator for Massachusetts. Web. 15 Dec. 2015. <https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf>.

[3] Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Andersin, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." (n.d.): n. pag. Autosec. Web. 15 Dec. 2015. <http://www.autosec.org/pubs/cars-usenixsec2011.pdf>.

[4] Miller, Charlie, and Chris Valasek. "Remote Exploitation of an Unaltered Passenger Vehicle." (2015): n. pag. 10 Aug. 2015. Web. 15 Dec. 2015. <http://illmatics.com/Remote%20Car%20Hacking.pdf>.

[5] Crilly, Rob. "Thousands of Cars Vulnerable to Keyless Theft, According to Researchers." The Telegraph. Telegraph Media Group, 18 Aug. 2015. Web. 15 Dec.

2015. <http://www.telegraph.co.uk/news/uknews/11808814/Thousands-of-cars-vulnerable-to-keyless-theft-according-to-researchers.html>.

[6] "How to Hack a Car | VICE | United States." VICE. N.p., n.d. Web. 15 Dec. 2015. <http://www.vice.com/video/how-to-hack-a-car>.

[7] "Car Hackers Handbook." (n.d.): n. pag. Open Garages. Web. 15 Dec. 2015. <http://opengarages.org/handbook/2014_car_hackers_handbook_compressed.pdf>
.

[8] Poulsen, Kevin. "Hacker Disables More Than 100 Cars Remotely." Wired.com. N.p., n.d. Web. 15 Dec. 2015. <http://www.wired.com/2010/03/hacker-bricks-cars/>.