Car Security

Author:
Tiina Turban

Supervisor:
Dominique Unruh

December 16, 2013


1 Introduction

Cars these days are becoming more and more computerized. The electronics in the vehicle makes our drive safer and more comfortable, for example Anti-lock braking system (ABS) allows us to keep better control of a vehicle without manually pumping the breaks or bluetooth capability, which makes it possible to play music from our phones. It certainly has its benefits, but like in most cases, where there are advantages there are also disadvantages. In this paper I will concentrate on the security issues that have arisen with having lot of electronic components embed in cars.

My work is mainly based on three papers [1,3,5]. In 2010 various attacks were demonstrated, e.g. disabling breaks [3]. It was also shown how, by having compromised one electronic control unit, it is possible to gain control over the entire car. However they got a lot of criticism about those attacks being unrealistic, because for an attacker with physical access performing mechanical attacks might be easier, e.g. tampering with breaks. This lead the Center for Automotive Embedded Systems Security researchers to write another paper exploring the external attack surface a year later [1]. Miller and Valasek contribute by providing all the tools and details of their attacks [5]. Their goal was to make the further research of car security easier.

I will start off with explaining some of the essential concepts in computerisation of cars, namely the Electronic control unit (ECU) and internal communication network. Then we shall look at how it is possible to gain access and compromise the car. The fourth section features examples of experimentally verified attacks from various sources. After which a quick peak into attack methodology and mitigating factors is given. In the end I hope to answer the question if all the electronics in the car is really making our life safer or would we be better off with the old-fashioned mere mechanical vehicles.

2 Background

The electronic components in cars these days come from many different contractors, as its cheaper that way. On the positive side these companies that are specialised in making just this one part are probably quite good at it and their software is relatively safe. The problem in many cases however comes from the integration of those components together into a working whole system, which is done by the car manufacturers. What makes matters worse is that contractors legitimately do not give out their source code, making it even more difficult to security check this glue code and the system working as a whole.
Electronic control unit (ECU). Modern cars embed millions of lines of code, which is spread across more than 50 independent computers, called Electronic Control Units [3]. ECU was originally a term for Engine Control Unit and helped to reduce the pollution and increase performance by controlling the air/fuel ratio. But as these self-contained embedded systems are now used more widely also for lights and entertainment, the term ECU had to be generalised. The electronic control units in a car are shown in figure 1.

Internal communication network. Vehicle bus is an internal communication network used inside vehicles to connect all those independent ECUs together. An ECU can send packets to other ECUs in this network. One of the most commonly used protocols in the car is Controller Area Network (CAN), which is a message-based-protocol, designed specifically for automotive industry.

A typical car these days has multiple CAN buses, e.g. one high-speed and the other low-speed. The first might control more important features like breaks and engine, while the latter controls radio, heating etc. It would be more secure if HVAC (the ECU responsible for heating, ventilation, and air conditioning) would not be able to send messages to EBCM (Electronic Brake Control Mod-
ule), however in reality we cannot fully separate safety critical systems. In fact the separation was originally done due to bandwidth and integration concerns. The need for broader connectivity can be seen from the Central Locking Systems (CLS), which needs to monitor the physical locks and react to wireless signals for keyless entry. But additionally we want the doors to be unlocked after a crash, so the ECU must get information from safety critical systems. To summarize the ECUs are commonly divided into groups and placed into different digital buses, but bridged where necessary.

3 Gaining Access

Back in the days, when cars were mere mechanical devices, one could only think of physically accessing a car. As automotive vehicles are becoming more and more computerized, the attack surface is also widening [1]. Drivers can connect their phones to the car via Bluetooth to enable hands-free calling, but an attacker might also be able to maliciously pair her device too. In this section we will look at four categories: direct and indirect physical access, short and long-range wireless access. Figure 3 summarises the ways one can take control over a car, which are covered in this section.

From a compromised ECU to others [3, 5]. Lets assume we have compromised an electronic control unit in the car, lets see where we can go from there. Packets on the CAN bus are broadcast, which makes it possible to eavesdrop from any compromised ECU. Another thing that makes attacks easier is the fact that there is no source identifier field, so an ECU can pretend to be any other ECU and send messages. The only authentication is implemented via challenge-response sequence, but that is done with fixed seeds and keys to keep the encryption algorithm from ending up in wrong hands. In other words manufacturers are using security via obscurity and in reality most of the algorithms are known to the community. Moreover each key is only 16 bits and reattempt is allowed every 10 seconds, hence the authentication can also be brute forced within 7.5 days and ECUs can be hacked in parallel.

As mentioned before, any ECU including a malicious one can send CAN packets to any other, hence only the security checks implemented in the receiving ECU matter, but how should the unit displaying speed know if 50 km/h is a reasonable speed to display at the moment. Additionally it was shown that it is possible to gain control over all ECUs even from an ECU from the low-speed CAN bus [3]. This was done by first attacking an ECU that was on both CAN buses (the telematics unit) and then from there gain access to the ECUs that are only on the high-speed bus.
Furthermore CAN packets have an identifier for priority, so more important messages will get routed faster. As the packets were broadcast, one can flood packets, which leads the whole internal communication network to be vulnerable to denial-of-service attacks. To summarize gaining access over any ECU can be used to compromise the entire car.

**Direct physical access.** This is the easiest way to access the vehicle to influence its behaviour. Direct physical access can be obtained by the owner, her friends, mechanics or via a break-in. Once inside the car a relatively cheap cable can be used to connect a laptop to the car’s standard On-Board Diagnostics II (OBD-II) port, which is typically located under the dash, see Figure 2. This provides a way to interact with the vehicle’s CAN bus [3, 5]. On the one hand the requirement for prior physical access makes this surface unrealistic for larger scale malicious attacks. On the other hand it is handy during research.

![Figure 2: Direct physical access via cable [5]](image)

**Indirect physical access [1].** Routine maintenance diagnostics or ECU programming is commonly done via the same OBD-II port. At the dealership the computers being used are typically laptops with internet access. There are many ways to compromise a personal computer and afterwards one can alter the service. Electric vehicles might be also vulnerable during charging.

Another example of indirect physical access is using the media player. In 2011 a group of researchers [1] were able to create a WMA file that, when played in a PC works nicely, but in the car radio made it possible to send arbitrary packets over the CAN bus. This non trivial vulnerability was exploited due to a buffer overflow in the WMA parser. Once found, this attack could be easily used on large scale, at least to the same car model, as it would just require spreading a malicious music file.
Short-range wireless access. Modern vehicles have many additions to make our life more comfortable and safe. Some examples include Bluetooth for hands free calling, Remote Keyless Entry — so that with a click of a button we can lock or unlock the car doors, Tire Pressure Monitoring Systems to alert the driver and therefore gain better road safety. Newer cars might even have WiFi over the cellular network.

As mentioned in Section 2 it is most probable that vulnerabilities lie in the integration of different components. That is where a security hole was found. One can write a Trojan Horse Application for the Android platform that, when being paired and connected to a car’s telematics unit, takes control over that ECU [1]. This Trojan could hide itself behind a game and then be distributed in the Android Market. Alternatively as the mobile industry evolves so does malware and an infection could spread to thousands of phones, from where it could affect cars.

The previous attack worked only with paired devices, but a group of researchers were able to pair their Bluetooth device with the car [1]. That required quite a bit of work, first they needed to sniff the car’s MAC address and then brute force
the PIN, which took them about 8-9 hours at an average. Additionally the engine had to be running. However many cars can be attacked in parallel, for example at least a few cars leaving a popular parking lot will be brute forced within minutes.

Newer technology also poses more likely to have vulnerabilities. A paper about Tire Pressure Monitoring System [6] reveals that it could be used for eavesdropping from up to 40 meters. Worse, it was possible to falsify the tire pressure and via extensive reverse-engineering even compromise an ECU [1]. In this case the manufactures either did not see a threat in tire pressure reporting or naively hoped on security via obscurity and did not reveal much information about the protocol. Unfortunately signals can be eavesdropped and math with reverse engineering applied to use it against car owners.

Long-range wireless access [1]. Some channels allow access from kilometres away. The first that comes to mind is the radio, either digital or satellite. Another example of broadcast channels is the Global Positioning System (GPS). Modern safety features also include anti-theft via remotely tracking and disabling a car and crash reporting via cellular network in case of an accident. The same telematics unit is the one offering cellular capabilities (voice help calls, location services for directions). In 2011 at least two vulnerabilities were found one in the authentication and another in the glue code between client and aqLink software modem that made it possible to compromise the car. They created an audio file, called the car and played it, see Figure 4. Furthermore the attack was not detectable by the driver as incoming call to the car’s cellular phone number was not displayed anywhere. A scary example of exploiting this long-range wireless access was to connect the car or cars to an IRC client and send commands to either one, selected or all the compromised vehicles.

Figure 4: Compromising a car over cellular network with a special audio file
4 Attacks

Now that we have seen various ways how to gain control over the car (see Section 3), let's see what can be done with that control.

<table>
<thead>
<tr>
<th>Result</th>
<th>source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable breaks</td>
<td>[3, 5]</td>
</tr>
<tr>
<td>Break (engage right or left front break separately)</td>
<td>[3, 5]</td>
</tr>
<tr>
<td>Steering (not precise enough for remote control)</td>
<td>[5]</td>
</tr>
<tr>
<td>Limited steering</td>
<td>[5]</td>
</tr>
<tr>
<td>Accelerate</td>
<td>[5]</td>
</tr>
<tr>
<td>Kill engine (even while driving)</td>
<td>[3, 5]</td>
</tr>
<tr>
<td>Prevent car from being turned on or off (even if key removed)</td>
<td>[3, 5]</td>
</tr>
<tr>
<td>Hide any evidence of the attack’s existence</td>
<td>[3]</td>
</tr>
<tr>
<td>Wait for an environmental trigger to perform an attack</td>
<td>[1]</td>
</tr>
<tr>
<td>Remotely trigger an attack from IRC (can be broadcast)</td>
<td>[1]</td>
</tr>
<tr>
<td>Send (recorded voice) data over IRC</td>
<td>[1]</td>
</tr>
<tr>
<td>Record voice from in-cabin microphone</td>
<td>[1]</td>
</tr>
<tr>
<td>Get car location, i.e. GPS coordinates (can be done continuously)</td>
<td>[1]</td>
</tr>
<tr>
<td>Adjust lights (including display-, break- and headlights)</td>
<td>[3, 5]</td>
</tr>
<tr>
<td>Lock or unlock doors</td>
<td>[3, 5]</td>
</tr>
<tr>
<td>Control A/C, fans and heat</td>
<td>[3, 5]</td>
</tr>
<tr>
<td>Falsify gauges (including speed, fuel level)</td>
<td>[3, 5]</td>
</tr>
<tr>
<td>Display arbitrary messages</td>
<td>[3]</td>
</tr>
<tr>
<td>Change Radio display and volume</td>
<td>[3]</td>
</tr>
<tr>
<td>Produce other car sounds (e.g. seatbelt warning)</td>
<td>[3]</td>
</tr>
<tr>
<td>Shoot windshield fluid (can be done continuously)</td>
<td>[3]</td>
</tr>
<tr>
<td>Control windshield wipers</td>
<td>[3]</td>
</tr>
<tr>
<td>Open and close windows</td>
<td>[3]</td>
</tr>
<tr>
<td>Open trunk</td>
<td>[3]</td>
</tr>
<tr>
<td>Honk the horn (even after car turned off, can be done continuously)</td>
<td>[3, 5]</td>
</tr>
<tr>
<td>Tighten seat belt</td>
<td>[5]</td>
</tr>
</tbody>
</table>

Table 1: Experimentally verified attacks
4.1 Experimentally Verified Attacks

All the attacks mentioned in this subsection were performed on a real car in active experiments. Even though most of them were tested with having a laptop in the car connected to the ODB-II port, i.e. direct physical access, we saw earlier that this is not the real limitation. See Figure 5 for main results from 2013 research.

Table 1 summarises individual attacks, but there were also the following composite attacks accomplished.

**Self-Destruct [3]** Display countdown on the dash, honking during the last seconds and then kill the engine and lock doors.

**Remote control [1]** 2 cars, that were 1000 miles apart got a command via IRC and made a sound.

**Lights Out [3]** No lights whatsoever (including display-, break- and headlights).

**No visibility [3]** Continuously shoot windshield fluid and disable the windshield wipers.

**Eavesdrop [1]** Monitor car’s location (GPS coordinates) continuously, when it is moving record audio and send it to a server over the Internet.
**Car theft** [1] Electronically get the location and disable all security measures (open doors and start engine), allowing an unskilled partner to drive the car away.

**Influence driving speed** [3] Falsify speed reading to show half of the actual speed when the car is driving faster than 20 miles per hour.

**Steering with game controller** [4] Use a game controller for steering the car, see figure 6.

![Steering the car with a game controller](image)

**Figure 6: Steering the car with a game controller** [4]

### 4.2 Speculated Attacks

All the attacks and ways of gaining access could be combined together, but these are speculations as it has not been tested on the road.

**Cyber war** [1] Disable the brakes of many cars driving at high speed simultaneously.

**Enterprise car theft** [1] First compromise lots of cars, then gather information about their model (Vehicle Identification Number) and location (GPS coordinates). Later sell that information as a service with remotely disabling security. The idea is similar to the way account usernames and password are sold on the web.

**Deliver message** After compromising lots of cars broadcast a command over IRC to display a message in all the cars, e.g. "Follow these instructions or ...". Various other attacks can be used to prove one’s power over the driver.

**Undetected murder** Use the environmental trigger of the car driving faster than 90 kilometres per hour and the time being past nine pm, i.e. it is dark outside.
Put all the lights out and disable the breaks. It is likely that the driver ends up in a tragic car accident. Additionally erase all evidence of the attack taking place.

**Bewitched place** Compromise as many cars as possible in a small area (using short-range wireless access techniques, or location of compromised cars). Then make all of them turn right at the same time. People might start to believe that this place is bewitched or it was just a coincidence as the alternative is too scary to think of.

**Mass scale surveillance** By monitoring car locations it is possible to identify the driver (e.g. most common location at 4 am is probably home and 10 am probably work). Then use the experimentally verified technique to eavesdrop and store all the data in a server.

**Modern car theft** taking the car theft idea further one could make the compromised vehicle drive to a specified location. However currently controlling steering is believed not to be precise enough to accomplish this attack [5].

5 Techniques Used

Here are some of the techniques with examples that were used to exploit the attacks or gain access to the car.

**Gathering information** to know the request-response protocol algorithms details.

**Packet sniffing** to discover the MAC address from bluetooth connections. But also monitor which packets are sent on the CAN bus.

**Fuzzing** to discover new attacks by sending random or partially random CAN packets and seeing what happens.

**Reverse-engineering** to understand how the radio WMA file parser works.

**Social engineering** to convince the driver to do something, e.g. play a WMA file.

**Get copy of hardware or software** to test out the attacks or perform reverse-engineering. It helps to get our hands on the same model car or software used by dealerships.

**Extract firmware** to speed up analysis and reverse-engineering by having the same model car and taking out the software.
Knowledge of common vulnerabilities to notice unchecked assumptions on length causing buffer overflow.

Compromise a device to compromise the car from a compromised dealership laptop or driver’s phone.

Brute-force to find out the key by exhaustive search.

6 Mitigation

We have seen quite many and somewhat really scary attacks, but is the situation really that bad? Should we just abandon electronic components from cars? In this section I will try to answer that question and reason why we have not seen or heard about such attacks in real life.

First let’s look at motivation. Lot of the attacks required substantial reverse-engineering, which demands quite a lot of skills and the equipment has costs as well. If stealing a car electronically takes more resources than just breaking the window and connecting some wires under the dash, then it will probably not become the mainstream way of stealing vehicles. Additionally a person capable of performing complex electronic attacks probably has many great job opportunities elsewhere. Furthermore testing on high speeds is potentially deadly. So the costs seem to outweigh the benefits at the moment.

On a more negative point of view, maybe people just do not recognise the existence of attacks. If one is being monitored how would she even know it? If the breaks in our car suddenly stop working we are more likely to blame ourself or a mechanical error, than speculate over a possible attacker. Also we find it hard to believe those speculations from others. If that would happen to multiple cars at the same time one may label it as coincidence.

The situation in car industry looks a lot like personal computers a few years back [3]. There was no connectivity and the general public was not worried about their computers getting hacked, but with the Internet came a way to compromise thousands of PCs with simple viruses spreading from computer to computer. As time passes more and more vehicles are getting online. But there is one big difference, we have already seen what could happen - if security will not be taken seriously, many attacks will arise. There are many suggestions given in the papers starting from restricting access [3] to detecting CA\N anomalies [5] or removing unnecessary features, such as ftp and vi on ECUs [1]. In conclusion I would not worry too much today about my car getting compromised and I hope that security will be made a top priority, so I would not have to worry tomorrow either.
7 Conclusion

There are lots of electronic components in cars these days, but is it making our life safer. I think it is, at least today. Even though we saw various ways to compromise a car from physically connecting with a cable to calling the car over cellular network. Then there were many attacks that can be exploited and some of those were really scary, e.g. disabling breaks. However designing an attack demands lots of resources and targeting a single car does not seem to pay off. Furthermore why bother reverse-engineering when significant damage could be done through physical means.

An entirely different story is mass scale attacks. Despite the fact that we have not seen many or any attacks so far, it does not mean they are not possible. Quite the opposite actually, as more and more cars are getting connected to the Internet the attack surface only widens and costs decrease. We seem to stand in the same place personal computers were a few years back, before being connected online became the norm.

The manufacturers have been focusing on safety, but one cannot have safety without security [5]. It is good to see research done in this field, especially on external attack surface [1], which addresses the main excuse - why would someone attack electronic components, when she could do more damage physically. I hope we can keep the benefits of electronics in cars, such as collision avoidance, without being afraid of an attacker disabling our breaks and I think it is doable if manufacturers make security a top priority.

References


