Driverless cars: A new way of life and a new cybersecurity challenge

Paul Williams, Country Manager, SADC at Fortinet

Cars are an essential part of our everyday life, and are crucial to transporting thousands of commuters on a daily basis through busy towns and cities, and from one country to another. With "smart" vehicles playing such a major role in our day-to-day lives, it's no surprise that semi- and fully-autonomous transportation and the potential for driverless cars have become hot topics. Countries such as the United Kingdom, France, and Switzerland are already testing forms of autonomous cars on public roads. According to Gartner, driverless vehicles will represent approximately 25 percent of the passenger vehicle population in use in mature markets by 2030.

While highways full of driverless cars may be a shining vision of the future for some, from a hacker's perspective they represent yet another opportunity to wreak havoc. Driven home by the rise in increasingly sophisticated cyberattacks and data breaches over the past several years, ensuring driver safety from cyberthreats has become a major development focus and challenge in the automotive and security industries.

A driverless car is a very advanced mode of transportation, possibly even without a readily available steering wheel. They have considerably more electronic components than "traditional" cars, and rely on sensors, radar, GPS mapping, and a variety of artificial intelligence to enable self-driving. These new guidance and safety systems must be integrated into the electronic onboard systems already present in modern day vehicles, connect wirelessly to the manufacturer, and probably even offer third-party services via the Internet. And that's where the problems begin: with hackers remotely accessing a vehicle and compromising one of its onboard systems, resulting in a range of risks from privacy and commercial data theft, to actual physical risks to people and property.

Here are some attacks that are likely to be targeted at highly connected and autonomous cars:

Privilege escalation and system interdependencies: not all systems and in-car networks will be created the same. Attackers will seek vulnerabilities is lesser-defended services, such as entertainment systems, and try to "leap" across intra-car networks to more sensitive systems through the integrated car communications systems. For instance, a limited amount of communication is typically allowed between an engine management system and an entertainment system to display alerts ("Engine fault!" or "Cruise Control is Active") that can potentially be exploited.

System stability and predictability: Conventional, legacy car systems were self contained, and usually came from a single manufacturer. As new autonomous cars are developed, they will very likely need to include software provided by a variety of vendors – including open source software. Information technology (IT), unlike industrial controls systems such as legacy car systems, are not known for predictability. IT systems, in fact, tend to fail in unpredictable manners. This may be tolerable if it is just a matter of a web site going down until a server re-boots. It is less acceptable in the event of a guidance systems being degraded even slightly when an adjacent entertainment or in-car Wi-Fi systems crashes or hangs.

Also expect to see known threats be adapted to this new target, expanding from common Internet platforms like laptops and smart phones an IoT device like an autonomous car. For instance:

Ransomware: Ransomware is certainly on the rise on PCs and mobile phones. But driverless cars represent an almost ideal target. Imagine the following scenario: a hacker uses the in-car display to

inform the driver that his car has been immobilized and that a ransom must be paid to restore the vehicle to normal operation. While a laptop or tablet may be restored relatively easily with potentially no damage, assuming backups are available, a car is a very different story. The owner may be far from home (the ransomware could be programmed to only launch when the car is a predetermined distance from its home base.) Naturally, few dealerships would be familiar with resolving this sort of problem, and specialist help would most likely be required to reset affected components. The cost of such a ransom is expected to be very high, and will likely take time. In the meantime, the vehicle may have to be towed. So the question is, what is the amount of the ransom demand that we expect to see? Estimates are that it is likely to be significantly higher than for traditional computer ransomware, but probably less than any related repair costs so that the car owner is tempted to pay.

Spyware: Perhaps a more attractive target for hackers is collecting data about you through your car. Driverless cars collect massive amounts of data, and know a lot about you – including your favourite destinations, your travel routes, where you live, how and where you buy things, and even the people you travel with. Imagine a hacker, knowing that you're travelling far from home, sells that information to a criminal gang who then breaks into your home, or uses your online credentials to empty your bank account.

That last risk exists because your driverless and connected vehicle is likely to become a gateway for any number of electronic transactions, such as automatic payment of your daily morning coffee, or parking charges, or even repairs. With sensitive information stored in the car, it becomes another attack vector to obtain your personal information. And with RFIDs and Near Field Communications (NFC) becoming commonplace in payment cards, accessing their details through your car would be another way to capture data about you and your passengers.

And last but not least, there are legal and authenticity issues. Can we consider the location data of the car as authentic? That is, if your car reports you opened it, entered it, and travelled to a particular location at a certain time of the day, can we really assume everything happened as recorded? Will such data hold up in court? Or can this sort of data be manipulated? This is an issue that will need to be addressed. Similarly, if cars contain software from several different providers, and spends the day moving from one network to another, who is accountable or liable for a security breech and resulting losses or damage? Was it a software flaw? Was it negligent network management? Was it on-board user-error or lack of training?

So, the question becomes, how do we secure autonomous cars?

The first step must be a greater awareness by the manufacturers of the potential cyberthreats. While manufacturers have vast experience associated with automotive safety, it is reasonable to suspect they have less expertise in the dark arts of cyber compromise and exploitation. A closer alliance with the Internet security industry will benefit everyone. The Automobile ISAC (information Sharing and Analysis Centre) is an interesting precedent.[1]

Next, incorporating more and more technology into a vehicle, whether for improving the customer's driving experience or enhancing the vehicle's performance, must be balanced with the management of their potential threats and risks. Ensuring that appropriate and effective security technologies are implemented within these systems must be a mandatory objective, even if it's not (yet) a regulatory requirement.
Additionally, a growing problem with many IoT devices is that they use common communications programs that have no security built into them at all. As a direct result, an alarming number of IoT devices to date have been highly insecure. We need to achieve better for autonomous cars than what is the current IoT benchmark today.

At the same time, manufacturers must work with their different technology and communications suppliers, across all of the territories where their vehicles are sold, to ensure that any network connections to the vehicles are appropriately hardened.

Automotive security can be addressed as three distinct domains that may make use of similar techniques in some instances, and require novel treatments in others.

1 *Intra-vehicle communications*. Smart vehicles will have several distinct on-board systems, such as vehicle controls systems, entertainment systems, passenger networking, and even third-party systems loaded on-demand by owners. To a certain extent, these systems will need to engage in "cross-talk" to bring new services to life, but this cross-talk needs to be closely monitored and managed by systems such as firewalls and Intrusion Prevention Systems (IPS) that can distinguish between legitimate and normal communications and illicit activity in the car's area network.
2 *External communications*. Many, if not all on-board systems will have reasons to communicate to Internet-based services: for manufacturer maintenance, for software updates, for passenger Internet access, for travel and driving instructions, for service requests, to purchase items or services, or to backup data. External communications will very likely be both "push" and "pull" – they may be initiated either from inside the vehicle, or to the vehicle from a manufacturer or the Internet. This also means that traffic to and from the vehicle will need to be inspected and managed for threats and illicit, defective, or unauthorized communications using firewalls and IPS-like capabilities.
3 Next, *the connectivity infrastructure* used by a vehicle will likely be based on well-established cellular networks, such as 3G and 4G data services, but with a twist. While these cellular services already provide connectivity to billions of smart phones and other devices around the world today, they also suffer from inconsistent security. Smart, driver-assisted, or even driverless vehicles will raise the stakes significantly. A directed attack on or through the cellular network could trigger significant, safety-critical failures on literally thousands of moving vehicles at the same time. Securing cellular networks providing critical vehicle connectivity will require a thorough review in light of such potential catastrophe.

Finally, high-assurance identity and access control systems suitable and designed for machines, not people, will need to be incorporated such that: cars can authenticate incoming connections to critical systems, and internet-based services can positively and irrefutably authenticate cars and the information they log to the cloud, or transaction requests they may perform on behalf of owners – such as service requests or transactions to buy fuel or pay tolls.