CYBER THREAT BRIEF:

Security Concerns Around Self-Driving Cars and Other Innovations in the Auto Industry

Sector	Automotive
Topics	Autonomous automobile industry
Companies Developing Autonomous Driving Technology	Ford, General Motors, Toyota, Tesla, BMW, Baidu, Daimler, ZF, Uber, Hyundai, Delphi, PSA, Volvo, Waymo, nuTonomy, Honda, Renault-Nissan Alliance, Volkswagen Group[1], Apple[2]
Security Concerns	Sensor jamming and blinding, DoS/DDoS, Forged vehicle communications, Leaked data, Physical attacks

Summary

Autonomous vehicles promise to provide numerous benefits to mankind. These include increases in productivity due to drivers being freed up during commutes, improvements in safety due to less accidents caused by driver error, more transportation options for the elderly or disabled who otherwise can't drive themselves, and more. As with every other major advance in technology, creating vehicles that can drive autonomously introduces new issues and concerns that must be overcome. The two biggest challenges beyond the achievement of autonomous driving itself are security concerns and appropriate legislation and regulations. This document explores the security concerns of self-driving technology. Rest assured, companies developing autonomous driving technology are devoting serious thought into these very issues and more..

[1] http://www.businessinsider.com/the-companies-most-likely-to-get-driverless-cars-on-the-road-first-2017-4/#1-ford-18

[2] http://www.dailymail.co.uk/sciencetech/article-5167597/Apple-gives-rare-private-demo-driverless-car-system.html

Stages of Self-Driving Technology

According to SAE International, there are six levels of driving automation, ranging from no automation to complete automation (depicted below)[4]. Features in the level 1 range are fairly common in current model year vehicles. An increasing number of vehicles from several manufacturers already have level 2 features. Within just a few years, vehicles achieving level 4 autonomy will be available. Despite this progress, level 5 is still a good number of years away due to the complexity in automating responses to the many possibilities encountered when driving in various situations and conditions.

Level 0 – No self-driving features.

Level 1 – Some driver assistance; Examples: adaptive cruise control, automatic emergency braking, active lane control.

Level 2 – Increased driver assistance; Ability to control speed and steering with little or no driver input in specific situations. Driver awareness still required. Example: Tesla's autopilot feature.

Level 3 – Conditional autonomy; Ability to automatically control the car but reverts back to human driving if there are problems or unforeseen situations.

Level 4 – High automation; Car controls and navigates itself and is programmed to pull over and stop if there is a problem. While a driver isn't necessary, there are limited scenarios where vehicles that operate at this level can operate autonomously. This makes this level ideal for vehicles operating in predictable urban areas.

Level 5 – Complete autonomy; Vehicle is able to completely control itself in nearly any set of conditions. There is no ability for the driver to control the vehicle.

Security Concerns

Self-driving technology for automobiles necessarily involves a complex array of sensors and communication systems. All of this creates a substantial attack surface for potential misuse or malicious manipulation. Security issues with autonomous cars can lead to monetary theft by spoofing toll identities or altering vehicle monitoring for cheaper insurance. In more serious cases, security issues can affect the safety of passengers or others. Some primary security concerns are included here for consideration..

Sensor Jamming, Spoofing, and Blinding

Current approaches to self-driving automation leverage a variety of cameras, lasers, GPS, radar, and other sensors to give the vehicle necessary environmental and situational awareness. Each of these types of sensors can be blinded or jammed, thereby hindering the vehicle's ability to retain full awareness of environmental conditions or potential obstructions. As cars begin to lean more and more on these sensors for driving and navigation, the appeal of abusing these systems will inevitably grow.

> *"Autonomy … will make mobility more efficient, but will also open up greater possibilities for dual-use applications and ways for a car to be more of a potential lethal weapon that it is today."*
>
> *FBI report on autonomous cars*[3]

Specific threats:

- GPS Spoofing.
- Blinding cameras with bright LED lights or lasers.
- Laser jamming.

Potential mitigations:

- Infrared filters on cameras designed to detect only visible light.
- Lenses that can dim or adjust aperture in very bright light.
- Protections against GPS spoofing (cryptography, signal-distortion detection, and direction-of-arrival sensing)[5].
- Lean on secure communications from nearby vehicles to share clean imagery.
- Infrared and laser jamming countermeasures[6].

It's important to note that, while these threats are

[3] https://www.theguardian.com/technology/2014/jul/16/google-fbi-driverless-cars-leathal-weapons-autonomous
[4] http://www.sae.org/misc/pdfs/automated_driving.pdf
[5] https://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation
[6] http://spie.org/newsroom/5614-ir-imaging-seekers-may-be-very-resistant-to-laser-jamming?SSO=1

possible, the likelihood of the average person developing a sufficient technological attack along these lines is currently scarce (beyond repurposing commercially available tools). Police laser jammers that work against LiDAR, very bright LED or IR spotlights, or home-built transmitters are the likely extent of threats that would actually be encountered. Designers should take these threats into account when developing autonomous driving systems and build in sufficient mitigations and redundancy to address these.

DoS/DDoS

Autonomous cars will be fitted with a number of communications systems that are designed to receive and share information necessary for safe navigation and driving. Depending on implementation, these communications systems could include Vehicle to Satellite (V2S), Vehicle to Vehicle (V2V), Vehicle to Road (V2R), Vehicle to Internet (V2I), Vehicle to Motorcycle (V2M), or others. There is also communication within the vehicle itself via the Controller Area Network (CAN). Disruption of any of these methods of communication can degrade the ability of the car to operate appropriately.

Specific threats:

- Radio Frequency (RF) jamming or interference.
- Signal blocking materials or devices.
- Overwhelming systems with too many messages.
- Crafted messages or signals that exploit vulnerabilities in a specific service or function.

Potential Mitigations:

- Systematic redundancy designed to overcome individual system or process failures.
- Use of cryptography to protect messages and transmissions.
- Intrusion prevention and/or firewalls designed to drop errant or malformed messages.
- Access controls to prevent unauthorized communication.

Due to limitations of vehicle-based resources and communication methods, the ability to offload communication from a DDoS attack would be limited if at all feasible. Systems that only allow accepted types of communications may provide adequate defense but additional research into other vehicle-based solutions against DoS and DDoS attacks should be conducted.

Forged Vehicle Communications

Another risk involving communications would be the ability to forge vehicle communications to spoof hazards that don't exist or attempt to cause a vehicle to behave in ways it isn't designed or intended to. Due to the variety of communications that autonomous cars will engage in both within itself and externally with other systems, many different protocols and methods may be used. This is both a boon and a bane for various reasons. One potential problem revolves around protocols that lack cryptographically sound integrity checks. These protocols may be vulnerable to spoofing depending on their implementation and communication methods.

Specific threats:

- Spoofed messages from a compromised vehicle or to a vehicle from another source in an attempt to force changes in vehicle behavior.
- Social engineering against human passengers (where communication messages can be sent directly to onboard messaging for passengers) in which the attacker's goal can either be compromise of the vehicle or of the passenger's other devices and accounts. Spoofing may allow for concealing the attacker's true source in this instance.
- Spoofed messages aimed at soliciting a response from the receiving vehicle where the response is actually the attack against another vehicle. For example, an attacker could send messages to a large number of vehicles in an area around the intended target, spoofing the target's address as the source of the messages. When all the vehicles respond to the spoofed messages, the resulting deluge could overwhelm the targeted vehicle's messaging system, thereby potentially denying any legitimate messages from being received or processed. This is essentially a smurf attack[7]. There could be additional fallout from this type of attack depending on how robust the vehicle's connected systems are.

[7] https://usa.kaspersky.com/resource-center/definitions/smurf-attack

Potential mitigations:

- Access controls to prevent unauthorized communication.
- Cryptographic controls to guarantee message integrity and validate message sources.
- Intrusion prevention and/or firewalls designed to drop messages from unauthorized sources.
- Use of protocols with built-in integrity checking.

Leaked Data

Autonomous cars will, by nature, have a significant amount of data about the travels and potentially some of the communications of its passengers. Additionally, personalization features as well as other functionality may necessarily store sensitive information about passengers such as payment details and other Personally Identifiable Information (PII). If the vehicle is compromised in some way, this information could be leaked to an attacker.

Specific threats:

- Capture of sensitive passenger or owner information as a result of vehicle compromise.
- Leaking of sensitive information due to an attacker spoofing communication from a trusted source.
- Making the vehicle appear to be someone else's vehicle by spoofing identifying information.
- Information leakage through third-party access or compromise.

Potential mitigations:

- Carefully protect any stored sensitive information via encryption and cryptographic access control.
- Ensure information is not shared except with trusted entities through appropriate encrypted and signed channels.
- Any communication designed to identify the vehicle should be cryptographically secure and validate the authenticity of the source.

Physical Attacks

Certain attacks could be carried out by those with physical access to the vehicle. Vehicular systems that are exposed to passengers such as USB ports or OBD-2 ports might provide mechanisms to allow for malicious use or exploitation. As with other technological systems, physical access often bypasses controls that are specifically in place to prevent remote exploitation.

Specific threats:

- Forged but cryptographically valid messages sent from the vehicle.
- Direct compromise of vehicle systems to install malicious code.
- Direct compromise of vehicle systems to install custom code (a jailbreak).
- Use of built-in vehicle cabin microphones and cameras for unauthorized surveillance of passengers (via malicious code).
- Falsification or deletion of vehicle data for fraudulent reasons.

Potential mitigations:

- Expect attempts to compromise the vehicle through available physical connections.
- Disallow access to critical system components via physical ports.
- Restrict access to read-only where possible and only allow access to necessary information for proper port functionality.
- Monitor for potential malicious activity and employ appropriate countermeasures to disrupt or thwart exploitation through physical ports.
- Wrap additional controls around any microphones or cameras in the vehicle to detect or prevent potential misuse.

Conclusion

Autonomous vehicles are coming. In some ways, they are already here as more and more vehicles are sold with elements of automation. Many challenges exist on the path to full automation but so also are the challenges to keeping these vehicles safe and secure. Every new capability or communication stream must be considered carefully for exposure to potential abuse or misuse. Thus far, companies developing this new technology have invested heavily in information security. Despite this, hackers have made headlines by publicly demonstrating exploitation of modern vehicles. It remains to be seen how effective the security measures baked into autonomous vehicle systems are when these are the default vehicles on the road.

The auto industry has built processes around how it handles defects and vehicle recalls but it has yet to be tested in responding to widespread cybersecurity issues. This would be the detection of active exploitation in the wild, diagnosis, and the delivery of an effective patch that, in itself, doesn't introduce other problems. The limited resources available in cars may not yield extensive logging or easy ways to do forensics after there has been a potential security problem. These concerns will have to be explored and tested for companies to be able to properly respond to security incidents involving autonomous vehicles.

Some safety options for autonomous vehicles:

- Safety protocols which can be enabled which put vehicles in "lock-down" mode where attack surface is reduced to the minimum necessary to safely carry passengers to their destination. This could be enabled at times when specific threats are present or likely.
- Ability to push down specific security rules protecting against active threats.
- Sharing of threats and other security concerns via V2V communications.
- Emergency shut-down of vehicles when significant active threats exist. Vehicles could pull-over and stop at a safe location until the threat is mitigated (via emergency update or other solution).

Compromise of individual vehicles is one problem, but attackers will inevitably seek exploitation of large numbers of vehicles at once if they can. Possibilities that could lead to this type of scenario may include accidental backdoors, leaked or stolen private security keys, or attacks to online update processes for vehicles. Third parties that are allowed to share information with vehicles will also be potential avenues for attackers to gain access to many vehicles at once. Imagine fleets of vehicles stopping and unable to go anywhere until a ransom is paid. Unlike other ransom situations, an event such as this could lead to a significant governmental and potentially international response depending on the scope and fallout around the incident. It is these types of scenarios that have made protecting against fleet-wide hacks a priority for Tesla[8] and will expectedly be a top concern for other manufacturers as well.

Some attacks against autonomous vehicles currently require a level of sophistication or access to equipment that is beyond the average person. The most viable threats will come from items and knowledge that are easily accessible. An attack that can be done with a laptop, a USB cable, and some software downloaded from the Internet is more likely to be encountered than a custom built "blinding rig" made of lasers and other components meant to blind the sensors of an autonomous vehicle. This is where it is important for developers and manufacturers to understand the current threat landscape, what is currently being developed by criminals, and who has interests in attacking self-driving vehicles and for what purpose. Governments may develop advanced capabilities in compromising autonomous vehicles for a variety of purposes useful to their goals (and some probably already have). These advanced attacks are unlikely to find their way into the hands of the public but sometimes leaks on this level happen (as has been seen recently with NSA exploits leaked from the ShadowBrokers). Autonomous vehicle technology developers should have plans in place to react to such a leak before it ever happens.

Possible motivations behind attacks against autonomous vehicles could include:

- Carjacking after forcing a vehicle to pull over due to not being able to "see."
- Hacktivism by forcing all cars on certain roads to stop during high traffic periods.
- Creation of vehicular obstacles to hinder law enforcement or other emergency responders.
- Murder or injury to passengers by causing a vehicle to stop in a dangerous location.
- Attacks where the vehicle itself is the weapon (direct it into oncoming traffic, a building, or pedestrians).
- Manipulation of vehicle data to avoid tolls, fees, or higher insurance costs.
- Terrorism.
- Use of vehicular resources for other means (cryptominers for example).
- Vehicle compromise as a means to gain access to otherwise unauthorized locations or resources.
- Government espionage or even assassination.
- Vehicular ransomware.

[8] https://electrek.co/2017/07/17/tesla-fleet-hack-elon-musk/