Assessing Risk:

Identifying and Analyzing Cybersecurity Threats to Automated Vehicles

ANDRÉ WEIMERSKIRCH
Lead, Mcity Cybersecurity
Working Group
Vice President, Cybersecurity,
Lear Corporation

DERRICK DOMINIC
Graduate Student Research Assistant,
Robotics, University of Michigan

Contents

INTRODUCTION

It's no secret that developers of automated vehicles face a host of complex issues to be solved before self-driving cars can hit the road en masse, from building the necessary infrastructure and defining legal issues to safety testing and coping with the vagaries of weather and urban environments. In addition, developers face huge risks if they neglect the vital issue of cybersecurity in automated vehicles.

Driverless vehicles will be at least as vulnerable to all the existing security threats that regularly disrupt our computer networks. That could include data thieves who want to glean personal and finance information, spoofers who present incorrect information to a vehicle, and denial-of-service attacks that move from shutting down computers to shutting down cars.

Cybersecurity is an overlooked area of research in the development of driverless vehicles, even though many threats and vulnerabilities exist, and more are likely to emerge as the technology progresses to higher levels of automated mobility. Although no over-arching solutions are obvious at this point, Mcity researchers have developed the first tool and methodology for assessing cybersecurity risks in automated vehicles. This marks not only an important step in solving these problems, but also presents a blueprint to effectively identify and analyze cybersecurity threats and create effective approaches to make automated vehicle systems safe and secure.

There are the new cybersecurity threats unique to automated vehicles, including hackers who would try to take control over or shut-down a vehicle, criminals who could try to ransom a vehicle or its passengers and thieves who would direct a self-driving car to relocate itself to the local chop-shop.

Also, there are security threats to the wide-ranging networks that will connect with automated vehicles, from financial networks that process tolls and parking payments to roadway sensors, cameras and traffic signals to the electricity grid and our personal home networks. Consider the seemingly nonthreatening convenience of an automated car that gets within 15 minutes of your home and automatically turns on your furnace or air conditioner, opens the garage and unlocks your front door. Any hacker who can breach that vehicle system would be able to walk right in and burglarize your home.

Researchers affiliated with the University of Michigan's Mcity connected and automated vehicle center are finding that the complex and wide-ranging issue of cybersecurity specific to automated vehicles and the infrastructure that will support them is just beginning to be recognized, and will become more important as the development of these vehicles progresses. Without robust, sophisticated, bullet-proof cybersecurity for automated vehicles, systems and infrastructure, a viable, mass market for these vehicles simply won't come into being.

UNDERSTANDING THE VULNERABILITIES

The threats to automated vehicles can come through any of the systems that connect to the vehicle's sensors, communications applications, processors, and control systems, as well as external inputs from other vehicles, roadways, infrastructure and mapping and GPS data systems. In addition, the control systems of each vehicle for speed, steering and braking are exposed to attacks.

Each individual automated application will require its own unique threat analysis that maps its vulnerabilities and assesses the level of risk presented. New work by researchers working with Mcity on adapting existing automotive threat models demonstrates how employing this approach to risk assessment can identify potential threats and solutions. Mcity researchers propose a new customizable threat model based on existing approaches. This was created by combining the strengths of threat models from the National Highway Traffic Safety Administration (NHTSA) and the European Commission's E-safety Vehicle Intrusion Protected Applications (EVITA) automotive threat models and expanding on them. These existing models are good, comprehensive examinations that look at automotive applications and their vulnerabilities, but omit considerations about specific sources and actors behind security threats, their motivations, and how they weigh the risks involved in considering an attack.

MCITY THREAT IDENTIFICATION MODEL

In this proposed model, each threat consists of a threat agent (attacker), one or more system components that could be attacked (attack surfaces), and one or more attack models for each component.

- Threat agents are reviewed by their motivations and capabilities to determine the potential likelihood of an attack. While two different attackers might focus on a vehicle's self-parking capabilities, for example, the threat of a lone car thief trying to steal a single vehicle would be significantly different from an organized group of dedicated hacktivists looking to hurt a manufacturer by disabling a huge number of vehicles.

- Potentially vulnerable components of automated driving applications – such as sensors, GPS systems or databases that receive over-the-air updates – are analyzed according to their characteristics and potential for attack. Combined with the attack method and the targeted application, this allows researchers to estimate the resources required for the threat agent to make an attack successful.

- The attack methods used in the researchers' analysis follow the STRIDE classifications developed by Microsoft: Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.

- Attack potential examines the difference between the threat agent's ability to execute a successful attack and the system's ability to withstand the attack, taking into account such factors as financial requirements, time needed to create and execute an attack, technical expertise of the attackers, and other factors.

- Motivation, which captures both the motivations and deterrents for the threat agent to execute the attack, including risk, passion to carry out the attack, and any potential financial gains.

- Impact looks at the potential level of loss to the stakeholders, including financial loss, privacy and safety.

The resulting analysis can be captured within a matrix that is weighted by likelihood, producing a result that can be customized to assess different assumptions. This table captures the threat assessment to automated vehicles with automatic parking:

See table on page 5.

Threat matrix for automated parking

Attack Scenario

This table looks at the factors involved in evaluating potential cybersecurity threats to a vehicle featuring Parking Assistance with Steering (Level 1) and Key and Remote Parking (Level 2):

Attack Name	Disable Range Sensors (L1/L2)	Spoof or Replay Parking Signal (L2)	Denial of Service Parking Signal (L2)
Threat Agents	Mechanic	Thief	Hacktivist
Attack Surface	Range Sensors	Key/Remote receiver	Key/Remote receiver
Attack Method	Denial of Service	Spoofing	Spoofing
Description	Disable range sensors to degrade the application, requiring further maintenance	Spoof or replay parking signal to initiate parking maneuver without driver's intent	Flood the key/remote frequency to disable the parking signal from an owner's key/remote and, thus, disable the application

Attack Potential (System Withstand)

These next three ratings look at the level of technical skill, equipment, level of motivation, expertise and investment of time and money needed to mount an attack. A low number means the specific threat requires few resources to be successful:

Time Elapsed	Hours (1)	Days (2)	Days (2)
Finances	Low (1)	Low (1)	Low (1)
Expertise	Expert (2)	Proficient (1)	Expert (2)
Knowledge of System	Sensitive (2)	Restricted (1)	Restricted (1)
Window of Opportunity	Long (2)	Medium (1)	Short (0)
Equipment	Specialized (1)	Specialized (1)	Specialized (1)

Attack Potential (Attacker Capability)

Time Elapsed	Hours (1)	Days (2)	Days (2)
Finances	Low (1)	Low (1)	Low (1)
Expertise	Expert (2)	Layman (0)	Multiple Experts (3)
Knowledge of System	Critical (3)	Public (0)	Sensitive (2)
Window of Opportunity	Long (2)	Short (0)	Medium (1)
Equipment	Specialized (1)	Standard (0)	Multiple Bespoke (3)

Motivation (of Attacker)

Financial Gain	Low (1)	High (3)	None (0)
Ideology	None (0)	None (0)	Individual (1)
Passion	None (0)	None (0)	Without Harm (1)
Risk	Low (1)	Moderate (2)	Low (1)

Impact (to Stakeholders)

These numbers indicate the potential severity from damage, with lower numbers indicating less damage:

Financial	Medium (2)	High (3)	Low (1)
Privacy	None (0)	Low (1)	None (0)
Safety Violation	None (0)	None (0)	None (0)

Result Vector

The ratings from all elements above are combined in a weighted scale, with safety and financial loss given priority:

Attack Potential	6	2	6
Motivation	0	1	1
Impact	4	7	2

A CHANGING PERSPECTIVE

The introduction of each new generation of automotive technology presents a new set of security risks. Older, low-tech applications, such as remote starters and locking mechanisms, posed obvious and relatively simple threats – that a thief might bypass the key fob controller in order to break in or steal the car. The introduction of GPS and data recording modules that record speed and where the vehicle went brought data privacy issues to the fore. Drivers feared that stalkers or kidnappers might hack into the systems, or that the data might be used against them by police or insurance investigators.

While data privacy and basic vehicle security will remain issues, each step forward in developing automated vehicles will add another layer of technical complexity – and vulnerability. The 2015 case of hacktivists taking over the controls of an Internet-connected Jeep Cherokee doing 70 mph outside of St. Louis demonstrated the vulnerabilities of onboard control systems, with the hackers able to control the car's radio, ventilation, braking and transmission, ultimately stalling the vehicle on the highway.

A year later, the same hackers demonstrated the ability to control the same car's steering and parking brake systems, bypassing the existing security measures on the vehicle.

Now consider a fully automated vehicle with a feature that allows it to automatically pay for parking. Hackers can not only buy services at the vehicle owner's cost, but also take the car ransom by moving it to another location, steal the car outright, have the vehicle drive itself to a chop-shop, maliciously crash the car into other vehicles or pedestrians or buildings or simply shut the vehicle down, lock the doors and disable the electric windows until the owner pays off the attackers – perhaps after stalling the car in the middle of train tracks.

And that's just a few of the possible outcomes. An unscrupulous mechanic can trigger the car's maintenance alerts to perform expensive unnecessary repairs. Hackers can misdirect the car by either taking over the controls, sending inaccurate information to the vehicle's sensors, or breaching the GPS network. Instead of heading home from work, a passenger suddenly finds himself on a dark desolate road when, suddenly, the car pulls off and the engine dies.

MORE TECHNOLOGY, MORE THREATS

As cars progress from a few automated functions – such as self-parking and lane monitoring – to become fully automated vehicles without any driver controls, the cybersecurity issue will become increasingly complex. Even fail-safe solutions that seem sensible under certain conditions could be problematic, meaning that, with each added piece of automation, all the previous components will need to be re-assessed to see if the new application affects the security and risk factors of the earlier features.

Take a situation where an automated vehicle is programmed so that when it senses it's been hacked, the car slows down and pulls over on the side of the road at the first safe opportunity. That sounds sensible, unless the hackers want to disable your car or want to attack you. Or perhaps the car is programmed so that, in the event of a security breach, it cuts off all external communication, switches into more basic mode, and takes you to a pre-programmed safe destination, such as your home. Once hackers know about such a safety response, they can use it to trigger a breach of security warning every time the driver gets into the car, creating a denial of service attack until a ransom is paid or other conditions are met.

How many ways will there be to mount cyber-attacks on automated vehicles? It's impossible to total every threat to every application and every component made by every manufacturer. As technology improves and becomes more widespread, with more and more people able to understand it and develop expertise in how it works, threats will multiply.

Cybersecurity issues also will change as the industry moves from the beginning phase to more mature operations. Right now, there aren't one or two automation systems that are standard across the industry. Instead, Ford Motor Co., General Motors. Co., BMW, Honda Motor Co., Nissan Motor Co., Toyota Motor Corp., Subaru and more are all working with proprietary systems. That means that any cyber-attack on one of them won't necessarily spread to the others.

But, as systems become more generic – or even move to open-source programming and commonly shared software modules across platforms and car makers – one successful hack could spread across every vehicle that uses the same system, as with the global hacks of the kind seen with Windows computers, such as the WannaCry ransomware attack that shut down more than 300,000 computers in 150 countries during May, at an estimated cost of as much as $4 billion.

Currently, the use of many different suppliers providing just one or two automated vehicle components to a single manufacturer limits the potential scope of any cyber attack. While each component in each of those systems may not have robust cybersecurity protections – if any – the limited deployment of a single component would contain any damage. To create a large-scale attack on driverless vehicles, hackers would need to understand and be able to foil many different security approaches. As systems become more generic and widely adopted, and as cybersecurity standards, approaches and solutions coalesce, these systems will become easier to secure and much more difficult to breach, as all stakeholders focus their security efforts on these common platforms. However, any successful attack that breaks through will have the potential to be hit many more vehicles.

THINKING LONG-TERM

While cybersecurity already receives intense effort in the automotive industry, most developers of automated vehicle technology are working in pursuit of best-case scenarios, with a focus on optimizing vehicle performance that may tend to overlook the specific and new issues that relate to automated vehicles. To be truly effective, teams need dedicated members working on automated vehicle cybersecurity to handle the shifting issues and needs as the industry progresses to higher and higher levels of development. Focusing on automated vehicle cybersecurity issues now is crucial to developing solutions that can expand and change to meet ever-increasing levels of automated driving.

Another reason to consider cybersecurity issues for automated vehicles now as opposed to later is that some automakers already are including semi-automated functions in cars on the road, such as the next Audi 8, which offers Level 3 autonomy, as defined by SAE and adopted by the NHTSA, driving up to 37 mph with no supervision from the driver. While the scope of security threats to semi-automated vehicles aren't as intense as they will be for fully automated vehicles, they do exist and need to be addressed before moving up to Level 4 and Level 5 autonomy, which require little or no driver involvement.

That's why it's crucial to create a thorough risk assessment approach and build long-term security solutions. As each manufacturer and supplier continues to go through this process the industry should be able to move closer to standardized approaches that can speed development of effective, scalable cybersecurity solutions for increasing levels of automated control.

Initial work by Mcity-affiliated researchers in developing practical, flexible threat assessment approaches that can identify potential security breaches and the hackers behind them is just an early step. Beyond this starting point, there is much more work to be done to guarantee the cybersecurity of mass-market automated vehicles.

The automotive industry realizes that the future lies in automated vehicles. Right now, the future of this transformative new technology lies in solving the cybersecurity question.

RESOURCES

S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *Proceedings of the 20th USENIX Conference on Security*, pages 6-6, San Francisco, CA, 2011. USENIX Association.

O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl. Security requirements for automotive on-board networks. In *Proc. Intelligent Transport Systems Telecommunications, (ITST), 2009 9th Int. Conf*, pages 641-646, Oct. 2009.

ISO/IEC. Information technology – security techniques – evaluation criteria for IT security – part 1: Introduction and general model. Technical Report ISO/IEC 15408-1: 2009, ISO, 2009.

K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental Security Analysis of a Modern Automobile. In 2010 *IEEE Symposium on Security and Privacy*, pages 447-462. IEEE, 2010.

C. McCarthy, K. Harnett, and A. Carter. Characterization of Potential Security Threats in Modern Automobiles: A Composite Modeling Approach ((Report No. DOT HS 812 074). Technical Report October, National Highway Traffic Safety Administration, Washington, DC, 2014.

J. Petit, D. Broekhuis, and M. Feiri. Connected Vehicles: Surveillance Threat and Mitigation. In *Black Hat Europe 2015*, Amsterdam, Netherlands, 2015.

J. Petit and S. E. Shladover. Potential Cyberattacks on Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):1{11, 2014.

J. Petit, B. Stottelaar, M. Feiri, and F. Kargl. Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR. In *Black Hat Europe 2015*, Amsterdam, Netherlands, 2015.

About Mcity
Mcity at the University of Michigan is leading the transition to connected and automated vehicles. Home to world-renowned researchers, a one-of-a-kind test facility, and on-road deployments, Mcity brings together industry, government, and academia to improve transportation safety, sustainability, and accessibility for the benefit of society.