NAVIGANT
RESEARCH

RESEARCH REPORT

Autonomous Automotive Cybersecurity

The Need to Protect Automated and Connected Vehicles

Published 3Q 2016

Commissioned by Karamba Security

Sam Abuelsamid
Senior Research Analyst

Section 1
EXECUTIVE SUMMARY

1.1 Introduction

The transportation ecosystem is on the verge of its most significant transformation in more than a century. For the first time since Karl Benz took his first drive in 1886, connectivity, automation, and services have the potential to virtually eliminate automobile crashes, fatalities, and injuries. However, before that goal can be achieved, manufacturers must ensure that everything possible is done to minimize the possibility of malicious actors interfering with the 21st century mobility ecosystem and to mitigate the impact of any interruptions that do occur. Whether they are abused by criminals, vandals, or terrorist organizations, the same technologies that have the potential for societal benefits also provide a means to sow destruction or chaos.

Security solutions that can be implemented quickly, reliably, and without a performance impact on both current and future products are essential. Protecting vehicles, occupants, and bystanders will require holistic approaches to design, implementation, and response when the unexpected does happen. This Navigant Research report examines why cybersecurity solutions that can function autonomously are needed and what the overall system requirements should be.

Section 2
THE NEED TO SECURE THE VEHICLE

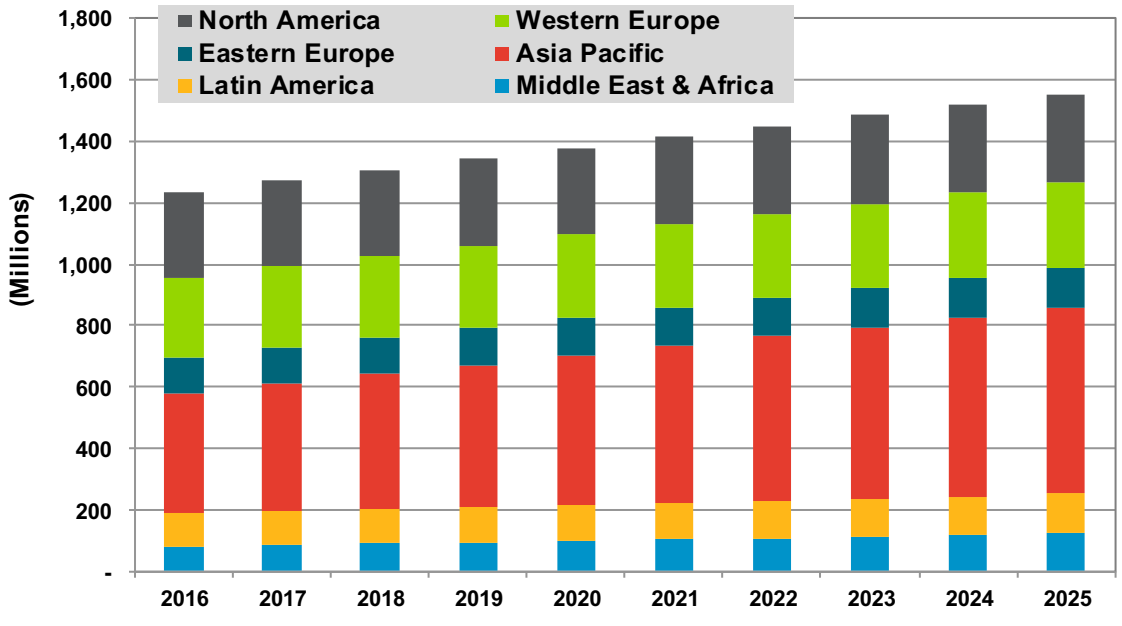
2.1 The Changing Nature of Transportation

For the first time in a century, the nature of how we use motor vehicles is on the verge of a fundamental change. In the coming decade, an increasing number of travelers will go from directly manipulating vehicle control inputs for accelerating, braking, and steering to simply entering a destination and sitting back for the ride. Before that happens to any significant degree, the people using connected and automated vehicles must be able to trust that vehicles are adequately protected from malicious actors trying to do physical or financial harm via cyber attacks.

2.2 Why Not Just Drive in Isolation?

The automobile transformed the way humanity moves about during the course of the 20th century. It provided a freedom of movement and choice of where to live, work, and play that was unparalleled in human history. But the automobile also created unprecedented problems. By 2014, for the first time in history, more than half of the world's population of 7.2 billion people was living in cities, and an estimated 1.2 billion vehicles were on the road. From London to Manhattan to Beijing, traffic congestion was costing drivers time, while pollution and crashes were killing more than 1 million people a year.

Chart 2.1 Light Duty Vehicles in Use by Region, World Markets: 2016-2025

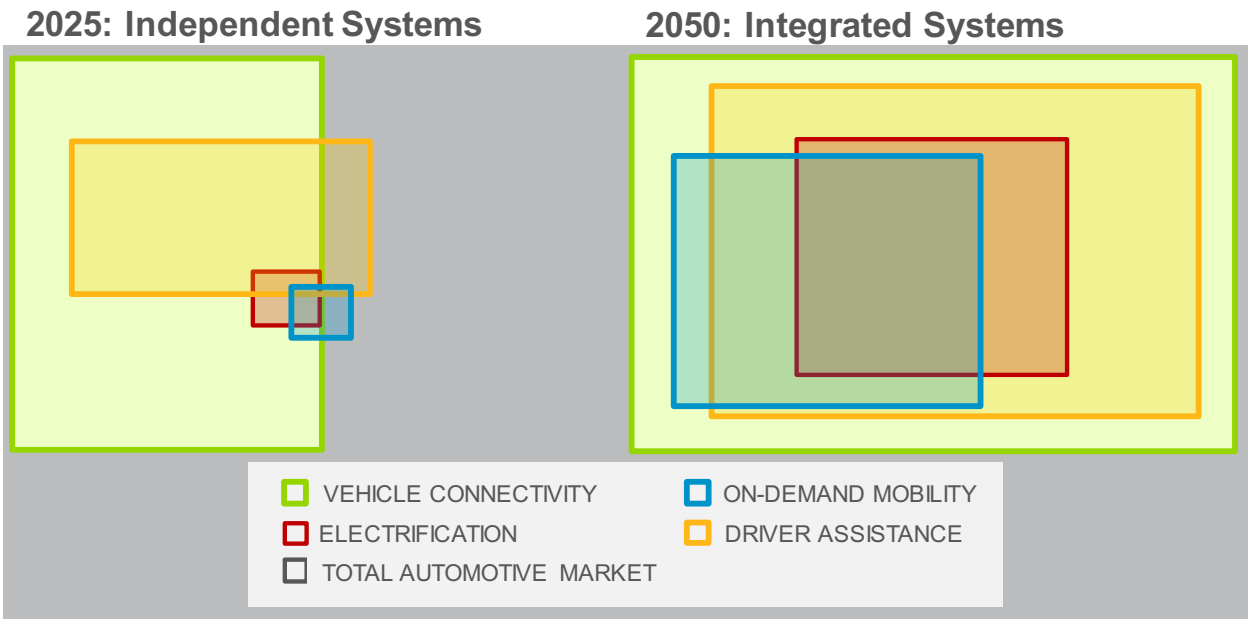


(Source: Navigant Research)

By 2050, the United Nation's *World Population Prospects* report forecasts that the global population will grow to nearly 10 billion people, with as many three-quarters residing in cities. Having everyone drive around in manually controlled, unconnected vehicles would make transportation safe from cyber attack, but this is an unsustainable approach in the modern world. New modes of mobility are needed for 2020 and beyond.

Fortunately, technologies now in development have the potential to address those problems while at the same time making safer and more efficient mobility available to even more people. The convergence of electrification, connectivity, automation, and cloud services that have until now evolved somewhat independently will take root in the coming years to provide the on-demand mobility that allows drivers to make more efficient use of natural resources, infrastructure, and time.

Figure 2.1 Transportation Landscape: 2025 to 2050



(Source: Navigant Research)

2.3 Defining the Problem

The automobile used to be essentially an isolated mechanical device. Like an individual device of any type, it could be tampered with, but only if someone had direct physical access. Even then, only one vehicle could be modified at a time, so any attacks that did occur tended to be highly targeted. However, we are now in an era where the technology exists for attackers to remotely target millions of vehicles simultaneously.

If attackers were to discover a vulnerability that made such an attack possible, the results could vary over a broad range. A potential best case scenario would be a ransomware

attack. In such a case, a malware infection could be used to disable anywhere from tens of thousands to millions of vehicles, releasing them only when a sum of money is paid to the attackers. This case would be costly and disruptive, but might not threaten human lives. In the worst case scenario, an infection of those same millions of vehicles could be used to remotely manipulate the vehicle control systems, causing crashes and leading to a catastrophic loss of life.

"Potential access to vehicle control systems could be used against us to undermine the very safety the technology was designed to provide," said John Carlin, US Assistant Attorney General for National Security during a keynote address at the 2016 SAE World Congress in Detroit in April 2016. "There is no Internet-connected system where you can build a wall that's high enough or deep enough to keep a dedicated nation-state adversary or a sophisticated criminal group out of the system."

Fortunately, no one has yet succeeded in demonstrating or executing such an attack. It is imperative that automotive OEMs, suppliers, and regulators do everything possible to make vehicles both as secure and as resilient as possible in the event of a cyber attack.

2.4 Real-Time Control

Microprocessors, software, and sensors have been the key technologies enabling the automotive industry to meet increasingly stringent emissions, fuel economy, and safety requirements in markets around the world. Without the ability to perceive what is happening, make decisions, and control actuators in real-time, the advances in improving air quality while slashing fatalities and injuries would not have been made.

Today's most advanced vehicles have nearly 100 discrete electronic control units (ECUs) and in some cases more than 100 million lines of code, a significant portion of which makes up advanced driver assist systems (ADASs). Moving toward the 2020s, ADASs will become increasingly sophisticated and eventually morph into full-blown autonomous driving systems.

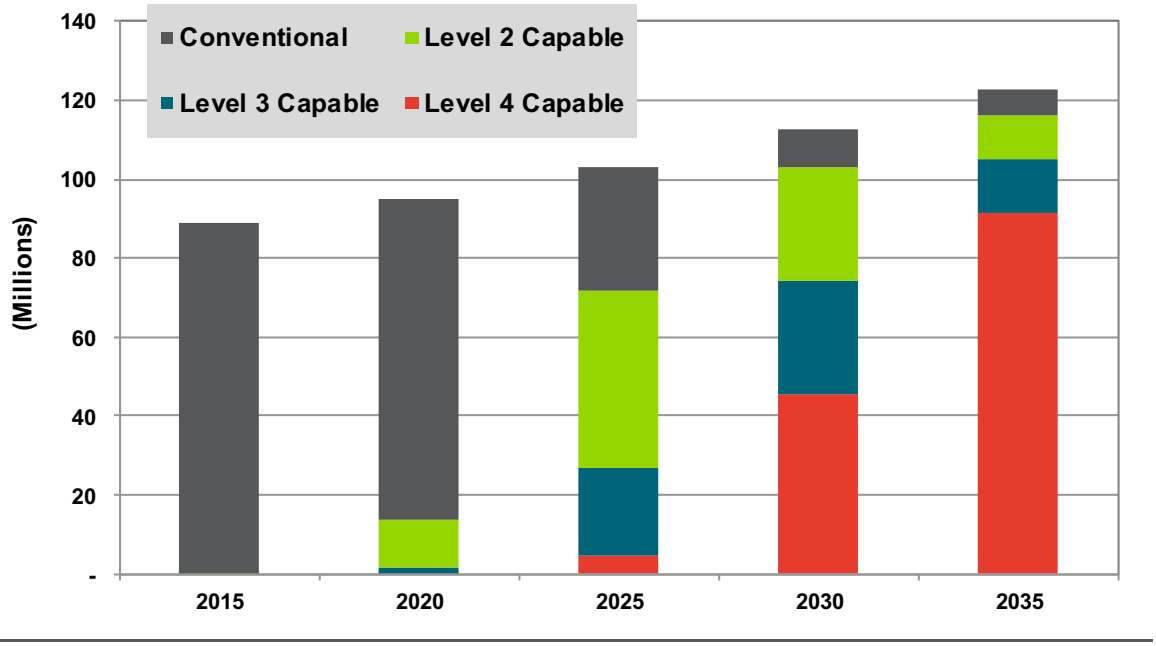
Navigant Research's *Autonomous Vehicles* research report forecasts that sales of vehicles of Level 2 through Level 4 autonomy will grow from 14 million annually in 2020 (about 15% of annual car sales globally) to nearly 72 million annually in 2025, accounting for nearly 70% of the 103 million light duty vehicles expected to be sold that year. By the mid-2020s, it is expected that more than 245 million vehicles with at least Level 2 autonomous capability will be on the road globally.

Level 2 systems are those that are able to manage both vehicle steering and acceleration simultaneously. Vehicles with Level 3 automation are capable of fully autonomous control under limited conditions, such as in geo-fenced areas or when weather conditions permit; the human driver must take over the remainder of the time. Level 4 automation and above indicates a vehicle is capable of operating without human intervention under virtually all

conditions. Annual sales of vehicles with Level 4 autonomy are expected to approach 5 million units by 2025. By the mid-2030s, nearly 85 million self-driving vehicles are expected to be sold every year, and more than 20% of the world's vehicle parc will be expected to be able to operate without a human driver.

While these vehicles with higher levels of automation pose the greatest cybersecurity risk, even conventional vehicles on the road now and well into the next several decades are potentially vulnerable. Any vehicle with a built-in telematics system or aftermarket connectivity via an OBD-II adapter or smartphone connection could potentially be compromised.

Chart 2.2 Vehicle Sales by Autonomous Driving Level, World Markets: 2015-2035



(Source: Navigant Research)

Executing all of these functions requires precise timing between the reading of the sensor inputs, making control decisions, and finally firing off the actuators. The software running on a general purpose machine such as a desktop computer or mobile device can be installed or altered by end users, and processor resources are shared among the nearly infinite variety of tasks that are possible. No such end user manipulation of the software should be possible in the vehicle.

Critical safety systems have a well-defined set of tasks that do not change unless there has been a firmware update from the manufacturer. As a result, these systems often run on a fixed time schedule loop with deterministic results. Anything that attempts to operate

at runtime that is not part of that pre-defined task list can be assumed to be either a hardware malfunction that alters the storage or malware.

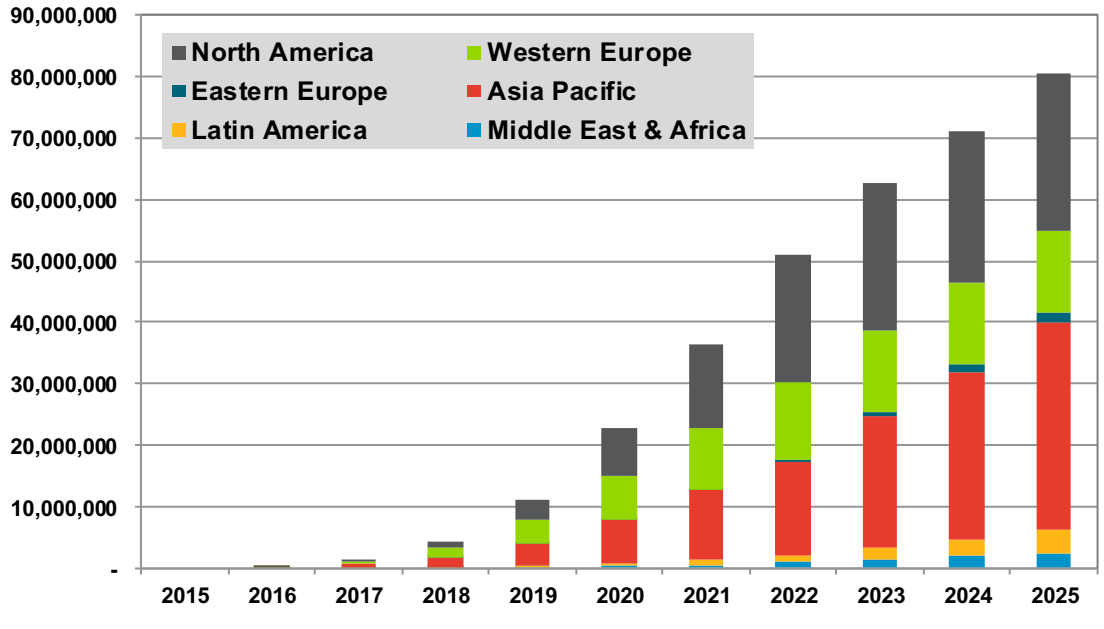
Safety critical systems work under stringent latency and response time requirements. Any security protection mechanisms that are implemented must be able to function with an absolute minimum of additional performance and storage overhead.

2.5 Over-the-Air Commands

In order to truly harness the power of vehicle automation, vehicles need to be connected to each other, to infrastructure, and ultimately to users. A vehicle capable of driving itself without the ability to communicate is of far less value to society than one that can drop off a set of passengers and then pick up others in need of a ride. Future vehicles will also need to communicate in multiple ways.

Vehicle-to-external (V2X) communications using dedicated short-range communications (DSRC) technology adds an extra layer of low-latency, real-time situational awareness that is not possible through sensing technologies alone. Navigant Research's *Connected Vehicles* report forecasts that by 2025, more than 80 million new vehicles annually will be equipped with the ability to communicate directly with other vehicles, infrastructure, cyclists, and pedestrians.

Chart 2.3 Annual OEM DSRC LDV Sales by Region, World Markets: 2015-2025



(Source: Navigant Research)

2.6 Connectivity Increases Fatality Risks

For nearly half a century, there has been an intense focus on safety in transportation, and tremendous progress has been made in reducing injuries and fatalities on the world's roads. In 1967, when the first Federal Motor Vehicle Safety Standards were adopted in the United States, nearly 51,000 people died on the nation's roadways at a rate of 5.26 per 100 million miles traveled. By 2014, Americans more than tripled the miles they drove every year, growing from less than 1 trillion to more than 3 trillion miles, and the number of fatalities had dipped to below 33,000, a rate of 1.08 per 100 million miles traveled. Unfortunately, those fatality numbers are on the rise again, with more than 35,000 roadway fatalities in 2015, and an even greater number is expected in 2016.

One of the primary goals in adopting new technologies such as connected vehicles and autonomy is to drive the fatality rate toward zero. However, that can only happen if those technologies work as intended and malicious actors are prevented from tampering with the systems. Unfortunately, it is impossible to guarantee that any complex code base is absolutely free of logic errors, and there is a significant probability that some number of those errors will lead to security vulnerabilities. With hundreds of millions of connected and automated vehicles expected to be on the road in the coming decades, the likelihood of attacks from vandals, thieves, and those with political motivations that may exploit those security vulnerabilities for mass attacks increases exponentially.

2.7 Machine Learning and Pattern Recognition

Using general purpose computer operating systems, it would be nearly impossible to predict all of the normal cross-system operation permutations. Therefore, developers of malware detection and protection systems for vehicles have created heuristic algorithms that monitor the behavior of the software that is running across the car ECUs on the car's controller area network (CAN) bus. These algorithms have adaptive functions that can detect what appears to be anomalous actions. However, just as humans sometimes err and misrecognize a voice or a face, heuristic algorithms sometimes flag perfectly normal activity as malware.

With a general purpose computing device, false positives are very common and generally do not disrupt the normal course of operation. Mistakenly blocked packets can be resubmitted by the servers to eventually reach their destination, even if an unnecessary packet blocking and delay was introduced to the packet flow. Users of general purpose computers can also be alerted when a malware detection that may be a false positive occurs and are given the opportunity to review it.

2.8 False Positives Are Not Acceptable on the Road

The same is not true of the automotive environment. Navigant Research's *Transportation Forecast: Light Duty Vehicles* report projects that global vehicle parc will grow by more than 50% to more than 1.8 billion units in 2035. Introducing the risk of false positives to

cars due to misrecognition of an innocent packet as malware can disrupt the functionality of safety critical systems. It can also further exacerbate traffic congestion if vehicles become erroneously disabled. That scenario could conceivably negate the benefits of driver assist and automation systems, leading to an increase in crashes, injuries, and fatalities.

Moreover, the probability of having false positives varies between 2% and 5% (i.e., at least every 2 out of 100 packets that are blocked on the car's CAN bus network will be mistakenly prevented from reaching their destination). The fatality risk of such frequent blocking of valid operations is something that the automotive industry cannot tolerate.

2.9 Deterministic Security

To avoid the risk of false positives, the ideal security approach in vehicles should be as deterministic as their control strategies. Car ECUs do not change from their factory settings. Even when car companies introduce app stores to enable third-party application downloads to their infotainment systems, such stores should be provisioned and inspected by automotive OEMs. Third-party apps should be hardened as another branch of the infotainment factory settings.

At runtime of the vehicle, all potential control permutations should be predictable based on the code that was built into the binary files. A similar method applies for updated versions of the ECU software, which are received as an update from the manufacturer as part of service checks or over-the-air updates. There should be no surprises.

Attackers have two primary means of performing nefarious actions in the vehicle: Through dropping in new binary code that did not come from the factory, and through in-memory attacks that manipulate processes that are already running in-memory in ways that those programs were not designed to perform. All automotive cybersecurity systems should have mechanisms to protect against both of these attack vectors, which are destined to compromise ECUs as a way to gain entry into a vehicle's CAN bus.

2.10 Pre-Production Protection

Protecting any computing system—including a vehicle—from malicious attack requires a multi-layered protection approach. From requirement definitions to field maintenance, every aspect of the process must be architected with security and resilience at the forefront.

The teams developing the architecture should always be asking themselves if there are any ways to exploit their systems. Processes should also be developed to validate and audit these systems to ensure that they meet performance requirements and do not introduce any potential vulnerabilities. Robust version control, reviews, and auditing are key components before software is even compiled.

2.11 Autonomous Security

From a security perspective, one of the key features that makes protection in the vehicle simpler than on individual-use general purpose platforms is the static nature of the applications that run. From the factory floor, until authorized software updates are complete, the binaries and operations running on the ECU should never change from their factory settings. Once the vehicle leaves the factory, the security of the onboard ECUs must be autonomous, with no intervention or outside connectivity required to block attacks at any time.

Including a process that runs locally on the ECU to validate the authenticity and accuracy of the binaries and in-memory operations is part of the deterministic security that should work well in the automotive environment. If an attacker has utilized either physical access to the vehicle or a remote attack through one of the communication surfaces to inject unauthorized code, it should be possible to detect those changes at runtime. Anything that does not belong should be prevented from executing. Since the applications and functions running in the vehicle computing platform are a known quantity, it should also be possible to know every possible control permutation before the vehicle ever runs.

If a previously undetected error in the code is exploited by a malicious actor, it is possible for executable instructions to be included in what appears to be data. This is one of the most common methods of attack on general purpose computing platforms. Demonstrations of this sort of attack in the vehicle have been executed by a variety of methods over the years, including through playing a compact disc with carefully crafted media files or sending modified text messages that trigger a buffer overrun.

Since it is nearly impossible to guarantee that there are no logic errors in any complex computing system, every vehicle is likely to contain at least some vulnerabilities that a skilled attacker may be able to discover and exploit. Based on the deterministic nature of these systems, understanding the possible permutations in advance and blocking any instruction calls that were not projected can prevent in-memory attacks.

If an in-memory attack is detected, the system must also decide how to remediate the problem. Depending on the nature of the attack, it may be as simple as killing a process and continuing on with normal control. If that is not possible, it may be necessary to signal the driver to pull over to a safe place to stop and cycle the ignition, which would reset the memory and wipe out the attack.

The prevention approaches described in this report rely on the deterministic nature of such electronic control systems to provide what is effectively a firewall against malware without any false positives. As a result, these systems can continue to operate as intended uninterrupted.

At a minimum, these security mechanisms need to be applied to the ECUs that manage connectivity to the world outside the vehicle. This includes the V2X, telematics, infotainment, and gateway systems. If these outward-facing attack surfaces are protected, that is likely to be sufficient to protect the downstream critical safety systems from malware infections. Ultimately, all of the electronic control systems, including the sensor input-output, should integrate security mechanisms.

While outward-facing connectivity is expected to be the primary cyber attack surface for vehicles, active connectivity should not be a prerequisite for security mechanisms to function. As anyone that has attempted to use a mobile phone in remote areas or deep within a concrete structure knows, connectivity to a cell tower is never guaranteed, regardless of what provider service maps may indicate. Savvy attackers can nonetheless utilize localized devices such as femtocells or any of the 50 billion Internet of Things devices expected to be deployed by 2020 to connect directly to a vehicle. Thus a local security approach will provide the most robust protection in the vehicle.

2.12 Heuristics in Sensor Signal Analysis

There may still be a place for some heuristic protection in future vehicles, just not necessarily in the same way it has been used in general purpose computing. As vehicles become more automated, they increasingly rely on sensor inputs to understand what is happening around them. A new potential cyber attack vector involves broadcasting inaccurate return messages to sensors such as radar or lidar that confuse the sensors. This is a less precise attack mechanism that is also very localized. However, because it is unpredictable, heuristic analysis could be used to detect anomalous sensor signals and prevent them from being fed into the control algorithms. The remediation in this case would likely require disengaging the driver assist or autonomous control features and returning control to the driver or simply bringing the vehicle to a safe stop.

2.13 Conclusions

Connected and automated vehicles will be coming to the world's roads rapidly in the coming years, and the potential societal benefits they present are enormous. By moving away from driving in isolation, the technology will change the way we interact with these vehicles as users, abstracting people away from the actual act of driving. If done right, many of the more than 1 million lives lost annually on the world's roads can be saved.

The auto industry is among the most competitive business sectors in the world, with very little barrier to prevent customers from switching brands. Customers in the highest volume segments of the industry are also very price sensitive, and costs for manufacturers are rising continuously as they struggle to meet ever stricter regulatory requirements, develop new technologies, and expand notoriously low margins. As a result, manufacturers want solutions to every problem—including security—that have a minimal impact on development and manufacturing cost.

Public demonstrations of automotive cybersecurity vulnerabilities in recent years have raised awareness of the risks of connectivity and automation among the mainstream media and consumers. Moreover, this is not just an issue for future vehicles; tens of millions of vehicles on the road today are equipped with telematics systems and varying degrees of automation and electronic controls.

As researchers such as Charlie Miller, Chris Valesek, and Karl Koscher have shown, these vehicles are already at some degree of risk. Given the long product lifecycles of the automobile, security upgrades that can be applied to work on existing legacy hardware will also have a big advantage over those that require next-generation platforms.

Security solutions that do not require thousands more engineers to implement or the addition of more or faster ECUs to provide robust protection will be the preferred approach. Ideally, security vendors must provide protection systems with minimal performance overhead that can protect both current and future vehicle platforms.

Mobility systems enabled by connectivity and automation have huge potential societal benefits, but they will not be adopted by consumers that do not trust the technology. The transportation industry must take care not to squander the opportunity provided by next-generation technologies. The new waves of high-tech vehicles need to be designed for both security and resilience against malicious cyber attacks, whether the motive is financial, political, or simply vandalism, and protection systems need to be able to function locally at the vehicle level without active outside intervention.

Autonomous vehicles are a potentially disruptive technology of the magnitude that comes once in every few decades. Autonomous on-demand mobility has the potential to provide a range of enormous societal benefits and quality of life improvements to billions of people around the world. The core technology for this revolution is almost ready, but to thrive, it must be secured. Connected and autonomous vehicle must go hand-in-hand with autonomous cybersecurity to enable safe adoption and to allow the revolution to commence.

Section 3
ACRONYM AND ABBREVIATION LIST

ADAS.....Advanced Driver Assistance System

CAN.....Controller Area Network

DSRC.....Dedicated Short-Range Communications

ECU.....Electronic Control Unit

OEM.....Original Equipment Manufacturer

V2X.....Vehicle-to-External Communications

Section 4
TABLE OF CONTENTS

Section 5
TABLE OF CHARTS AND FIGURES

Section 6
SCOPE OF STUDY

This white paper provides a description of the challenges, opportunities, and solutions of deploying cybersecurity solutions in the automotive environment. This paper draws upon Navigant Research studies of vehicle sales, autonomous vehicles, connected vehicles, mobility services, and cybersecurity.

SOURCES AND METHODOLOGY

Navigant Research's industry analysts utilize a variety of research sources in preparing Research Reports. The key component of Navigant Research's analysis is primary research gained from phone and in-person interviews with industry leaders including executives, engineers, and marketing professionals. Analysts are diligent in ensuring that they speak with representatives from every part of the value chain, including but not limited to technology companies, utilities and other service providers, industry associations, government agencies, and the investment community.

Additional analysis includes secondary research conducted by Navigant Research's analysts and its staff of research assistants. Where applicable, all secondary research sources are appropriately cited within this report.

These primary and secondary research sources, combined with the analyst's industry expertise, are synthesized into the qualitative and quantitative analysis presented in Navigant Research's reports. Great care is taken in making sure that all analysis is well-supported by facts, but where the facts are unknown and assumptions must be made, analysts document their assumptions and are prepared to explain their methodology, both within the body of a report and in direct conversations with clients.

Navigant Research is a market research group whose goal is to present an objective, unbiased view of market opportunities within its coverage areas. Navigant Research is not beholden to any special interests and is thus able to offer clear, actionable advice to help clients succeed in the industry, unfettered by technology hype, political agendas, or emotional factors that are inherent in cleantech markets.

NOTES

CAGR refers to compound average annual growth rate, using the formula:

CAGR = (End Year Value ÷ Start Year Value)$^{(1/steps)}$ – 1.

CAGRs presented in the tables are for the entire timeframe in the title. Where data for fewer years are given, the CAGR is for the range presented. Where relevant, CAGRs for shorter timeframes may be given as well.

Figures are based on the best estimates available at the time of calculation. Annual revenues, shipments, and sales are based on end-of-year figures unless otherwise noted. All values are expressed in year 2016 U.S. dollars unless otherwise noted. Percentages may not add up to 100 due to rounding.

Published 3Q 2016

1375 Walnut Street, Suite 100
Boulder, CO 80302 USA
Tel: +1.303.997.7609
http://www.navigantresearch.com

Note: Editing of this report was closed on September 21, 2016.