Transportation Security in the Era of Autonomous Vehicles: Challenges and Practice

Sandip Ray
NXP Semiconductors
Austin, TX 78735. USA.
sandip.ray@nxp.com

ABSTRACT

The Transportation Sector is one of the Critical Infrastructure Sectors identified by the United States Department of Homeland Security. Developing robust, secure, and resilient designs for Transportation Sector components is particularly challenging since it requires significant, real-time coordination with automotive, marine, and aviation systems that are themselves undergoing transformative changes in electronic complexity. In this paper we provide a general overview of security challenges in the Transportation Sector, focusing in particular the Highways and Roadways sub-sector. We discuss current and emergent challenges in this area arising as a result of increased autonomy (and hence complexity) of automotive systems, and point out key research needs.

Keywords

critical infrastructure, highways and roadways, side channel, V2X, vehicle security

1. INTRODUCTION

Autonomous cars are upon us. Self-driving cars are already on road in California, Texas, Washington, Pennsylvania, and Michigan, albeit restricted to specific test areas and driving conditions [7]. Given the trends, it is getting increasingly clear that driverless cars will become a mainstream reality in a not too distant future, with its arrival estimated between 2020 and 2035. The phenomenon of autonomous automotives is anticipated to have momentous consequences on our economy and our way of life, with effects on city infrastructure, commute overhead, energy efficiency, and security. It is therefore crucial to comprehend these effects, identify the components which can potentially incur prohibitive risk, cost, and overhead to our well-being, and take appropriate mitigatory actions while enabling and facilitating the positive effects.

In this paper, we consider one specific critical effect of the era of autonomous automotives, *viz.*, the security challenges incurred to the transportation infrastructure. Transportation security is acknowledged to be a key component of national security, *e.g.*, the United States Department of Homeland Security lists Transportation Security as one of the nation's critical infrastructures whose security affects the "backbone of our nation's economy, security, and health" [1]. Unfortunately, transportation security is also highly complex, requiring deep comprehension and delicate balance between highly divergent constraints from real-time requirements, connectivity, reliability, and environmental concerns.

The purpose of this paper is to provide a general overview of problems in transportation security, explain the current state of the practice in developing secure transportation infrastructure, and the gap between the current practice and needs of the area. Research in this area is quite nascent with various unknowns and uncertainties, providing for a fertile field for emergent technologies. Our goal is to foster that process by providing a consolidated account of the challenges and trade-offs that must be considered to create viable solutions.

The remainder of the paper is organized as follows. Section 2 provides a general overview of the scope of transportation sector, and Section 3 discusses the security spectrum. Sections 4 and 5 focus more narrowly on the cybersecurity challenges a specific sub-sector of the transportation infrastructure, *viz.*, Highways and Roadways. We discuss how these challenges are accenuated in the environment of autonomous automotives. We conclude in Section 6. Note that the paper does not offer a new solution for a specific problem. Rather our goal is to provide a flavor of the challenges and considerations that must be accounted for in order to develop resilient, secure solutions in the Transportation Sector.

2. ELEMENTS OF TRANSPORTATION SECTOR

The transportation sector is designated by the Department of Homeland Security as one of the sixteen critical infrastructures [1] in the United States. The scope of transportation infrastructure as defined in that context encompasses all of the national infrastructure that facilitates transportation of goods and services across the country and the world [2]. It includes the following sub-sectors.

- **Aviation:** This sub-sector encompasses aircraft, air traffic control systems, airports (civil and military), heliports, sea plane bases,and landing strips. It includes commercial and recreational aircraft (manned and unmanned) as well as a wide variety of support services, such as aircraft repair stations, fueling facilities, navigation aids, and flight schools.

- **Highways and roadways:** This sub-sector encompasses transportation across roadway, bridges, and tunnels that carry automotive traffic, vehicle and driver licensing systems, traffic management systems, electronic systems for operational management, etc.

- **Maritime Transportation:** This sub-sector consists

978-1-5386-3093-8/17/$31.00 ©2017 IEEE

of the coastline, ports, waterways, and intermodal landside connections that allow the various modes of transportation to move people and goods to, from, and on the water.

- **Mass Transit:** This includes terminals, operational systems, and supporting infrastructure for passenger services by transit buses, trolleybuses, monorail, subways or metrosâĂŤlight rail, passenger rail, and vanpool or rideshare.

- **Pipeline Systems:** This sector consists of more than 2.5 million miles of pipelines spanning the country. The pipeline systems carry nearly all of the nation's natural gas and about 65 percent of hazardous liquids, as well as various chemicals. Above-ground compressor stations and pumping stations are also included.

- **Freight Rail:** This consists of the over 138,000 miles of active railroad, over 1.33 million freight cars, and approximately 20,000 locomotives.

- **Postal Systems:** This sector encompasses transportation of letters and packages, and includes large integrated carriers, regional and local courier services, mail services, mail management firms, and chartered and delivery services.

Obviously, the sector itself is massive in scope and scale. Note that the United States have several million miles of roadway and hundreds of thousands of bridges, a diverse traffic consisting of automotives, trucks, other commercial vehicles including commercial motor-coaches and school buses, a hundred thousand miles of coastline, 25000 miles of waterways, and a public transportation infrastructure that enables billions of passenger trips every year. Furthermore, a disruption in this sector affect other critical infrastructure sectors.

- The Critical Manufacturing Sector relies on transportation network to move goods and services.

- The Energy Sector requires transportation of fuel (*e.g.*, coal, petroleum products, natural gas, etc.) through maritime, freight rail, and pipeline systems.

- The Defense Industrial Base uses air, maritime, rail, and highway networks to move material and personnel in support of military operations.

- The Financial Services Sector and Government Services Sector rely on mass transit systems for employees to access the workplace.

Correspondingly, the functioning of the Transportation Systems Sector is also directly dependent on its effective coordination with other sectors.

- The Energy Sector produces fuels to power transportation systems.

- The Information Technology Sector is essential in the transmission of information necessary for the efficient operation of the transportation network.

3. SECURITY WITHIN THE TRANSPORTATION SECTOR

The Transportation sector, like any other critical infrastructure sector, must account for a wide-ranging spectrum of security challenge including natural disasters, accidents, and terrorist attacks. However, ensuring security for Transportation sector while maintaining and expanding free flow of trade, commerce, and commute convenience, is more complex than many other infrastructures for a variety of reasons. Here we summarize some of these complexities. The goal is not to be complete but to provide a flavor of the diversity of challenges involved.

- **Asset Proliferation:** A critical challenge for securing the transportation sector is the sheer number of assets, components, and communication involved. Note that the assets are widely distributed geographically, can be both static (*e.g.*, airports, rail yards) or dynamic, and can be used both as weapons and as targets.
- **Stakeholder Proliferation:** The Transportation Sector has a large diversity of stakeholders with orthogonal (and even conflicting) interests and incentives. These include government agencies (Federal, State, and Local) as well as the private sector.
- **Complexity of Connectivity:** The transportation infrastructure today to a large extent comprises of interconnected, interdependent communication networks. While this model has increased the efficiency and effectiveness of communication, it has also resulted in a complex operating model involving significant interaction and coordination among interdependent components.
- Moving Target Adversaries: A key challenge in developing security solution is to ensure defense against a human adversary (*e.g.*, terrorism). While terrorists may rely on a distinct set of attack methods, they can adjust their attack strategies based on past responses. As a result, unlike natural disasters or accidents, the time and place (or even strategy) of terrorists can specifically account for the defense and mitigatory mechanisms developed against security threats. Consequently, defense against terrorism is a moving target, played on as an increasingly sophisticated arms race between attack and mitigation strategies.

To address these challenges, the National Infrastructure Protection Plan (NIPP) has developed a risk management framework for the purpose of developing secure, robust, and resilient infrastructures. Given the security goals of a sector, the NIPP framework involves addressing five key components: (1) identifying the critical assets across sectors; (2) identifying and assessing risks; (3) normalizing, analyzing, and prioritizing study results; (4) implementing protective programs; and (5) measuring effectiveness. Each critical infrastructure creates a Sector-Specific Plan (SSP), which describes how the NIPP risk management framework is implemented within the context of the unique characteristics and risk landscape of the sector. The Transportation SSP identifies the following three key goals:

- Deter and prevent terrorist and criminal activities before their occurrence without disrupting normal transportation activities, civil liberties, and trade.

- Improve the resilience of a transportation system by increasing its ability to accommodate and absorb damage from natural disasters or terrorist attacks without catastrophic failure.
- Facilitate cost-effective resource utilization, *viz.*, by minimizing duplication of efforts, improving effort coordination, and aligning resources to the highest risk.

Each of these goals can be broken down into lower-level objectives and action items, *e.g.*, the requirement of resilience involves reducing the risk associated with key nodes, links, and flows within critical transportation systems to improve overall network survivability as well as enhancing the capacity for rapid and flexible response and recovery to all-hazards events.

Cybersecurity is, obviously, a key component of security requirements for each of the critical infrastructures. The relevant component of NIPP risk management that pertains to cyber threats is defined by the National Institute of Standards and Technology (NIST). For Transportation Sector, the Department of Homeland Security provides a *Transportation Systems Sector Cybersecurity Framework Implementation Guidance* [3] to help reduce cyber risks and align cybersecurity goals of organizations with NIST framework. The goal of the implementation guidance is to define the following tenets for organizations pertaining to any of the sub-sectors of transportation security:

- Characterize their current cybersecurity posture.
- Identify opportunities for enhancing existing cyber risk management programs.
- Find existing tools, standards, and guides to support Framework implementation.
- Communicate their risk management issues to internal and external stakeholders.

The implementation guide defines a 3-phase cybersecurity strategy: (1) estanblishing a risk profile; (2) establishing priorities; and (3) actual implementation of the solution. The guidance is expected to be incorporated into the culture and methodology of the organizations. For organizations that do not have a formal cybersecurity risk management program, the role of the guidance is to help comprehend, evaluate, and establish the organizations cyber-risk priorities. For organizations with existing formal risk management program, the guidance provides additional mechanisms to review existing programs and identify areas for improvement, while aligning their organizational goals to the overall cybersecurity goals of the sector.

4. VEHICLE SECURITY AND TRANSPORTATION INFRASTRUCTURE

Having developed a background on the scope and challenges involved in Transportation Security in general, we will delve in this and the following sections into technical challenges towards developing robust cybersecurity solutions. To keep the discussions grounded, for the remainder of the paper we focus primarily on the Highways and Roadways sub-sector, specifically as we move into the era of autonomous automobiles. Nevertheless, much of the discussion is applicable for other sub-sectors as well.

Why is transportation security so challenging, and what even within the narrow context where we consider transportation through motorized vehicles? The unique feature of the sector is that the transportation agents involved (*e.g.*, automotives) are themselves highly complex electronic systems. Indeed, electronics and software provide the key distinguishing factors to a modern automobile. A car today includes more than 100 electronic control units (ECU), between 3 and 5 in-vehicle networks, and several hundred megabytes of software. Furthermore, the trend is for this complexity to increase, — indeed, increase on a much sharper gradient than ever before. For instance, National Highway Traffic Safety Administration lists five levels of automation, with Level 0 representing no automation and Level 5 representing full automation [12]. Our current automobiles on road belong primarily to Level 2. On the other hand, a jump from one level to the next represents an increase in electronic and software complexity by over an order of magnitude: replacing a specific human driving function by an automatic component (*e.g.*, obviating the need for eyes on the road as required to move from Level 3 to Level 4,) would require significant increase in a diversity of sensors to detect environmental stimulus, computing elements responsible for data processing and analytics (*e.g.*, inferring from various sensory data that there is an obstacle or pedestrian on the way), and control mechanism for reacting and controlling the automotive to the environment (*e.g.*, pressing the brake or steering away from the pedestrian). Unfortunately, these complexities induce serious security concerns as well. Vehicle security, of course, is a topic whose concerns are orthogonal to the security of transportation infrastructure; another paper [11] explains some of the challenges in vehicle security and current practice in that area. Here we only summarize two key aspects of vehicle security that directly relate to the transportation infrastructure.

- **Real-time and Connectivity Requirements:** A key requirement of a car is its need for real-time response to an emergency situation, *e.g.*, a pedestrian on its course, an approaching vehicle etc. Much of these communications are performed by V2X communications, *i.e.*, communication of the vehicle with another vehicle or infrastructure. A key challenge with real-time requirements is that messages in the communication must be processed quickly: authentication mechanisms that are highly computation-intensive or require significant message exchanges are obviously inapplicable. On the other hand, with millions of cars on road, it is likely that a significant fraction of the communication is indeed from malicious or otherwise compromised vehicles. The infrastructure system must account for such communication without the benefit of extensive authentication, with limited computation, and while ensuring that the infrastructure system is not excessively "overwhelmed" and thereby unavailable.
- **Security/Privacy Trade-offs:** One of the requirements of secure cyber-communication is to ensure security and privacy. Unfortunately, in the domain of transportation security, these two requirements can be in conflict. Consider a highway system communicating with a multitude of vehicles. It is important for the infrastructure to perform some form of authentication

to trust the identity of the vehicles (the challenges in the above bullet notwithstanding). On the other hand, this can violate privacy constraints; a third party listening to this communication can track the location, direction, and identity of the communicating vehicles. Note that since there is no *a priori* coordination between the vehicles on road and the transportation infrastructure it is difficult to create a trusted communication channel between them that accounts for such man-in-the-middle attacks.

In addition, of course, there are security challenges associated with a complex supply-chain [10, 9], multitude of available side-channels, and the challenge of introducing secure cyber systems on top of an aging physical infrastructure.

5. EXTENSIBILITY ISSUES

Aside from the communication, connectivity, and real-time requirements, developing robust, secure architectures for the transportation sector requires another critical consideration, extensibility. The point of extensibility is to ensure that any solution developed today can be easily updated in future to adapt to changing needs. Extensibility is a particularly relevant component of infrastructure architectures because of the long life of critical infrastructures. Bridges, highways, and roadways are built to last for several decades. In contrast, common electronic systems only last a few years. On the other hand, the usage patterns, security needs, etc. of the infrastructures continue to evolve and often change drastically in the course of this long life. Consequently, any architecture or solution pertaining to infrastructures must have built-in adaptation capabilities that enable potential drastic changes in response to changing needs. This problem is particularly vexing at the current point of time in the transportation sector since automotive systems and connectivity paradigms are undergoing drastic and highly uncertain changes as well. For instance, at the time of this writing, it is difficult to fully anticipate the connectivity and real-time response provided by 5G network [8] when deployed ubiquitously and required to transmits gigabytes of real-time data. However, the quality of these features will be a crucial factor in the architecture of key features (including, but not limited to, security) of automotives. For example, there are two alternative approaches to V2X features:

- **Centralized Approach:** In this approach, vehicles send as much of the sensory information as possible to data centers in the cloud, where advanced analytics can be performed with a global view (based on information about the entire traffic) to compute a suitable response.
- **Distributed Approach:** In this approach, each individual vehicle performs analytics based on the local view of traffic provided by its own sensors as well we V2X communications with nearby vehicles.

There are clearly advantages and disadvantages to each approach. In particular, the first approach critically depends on the ability of communication network to carry large amounts of low-level sensory data reliably and securely to the cloud and the ability of the cloud to perform real-time analytics over this massive scale; on the other hand, the second approach requires significant "local data mining" at each vehicle based on incomplete and imperfect sensory information and communication. From the perspective of transportation infrastructure, too, the challenges imposed by the two modes would be very different, *viz.*, the centralized approach may require large communication between the highway infrastructure and cloud while the distributed approach would require significantly larger real-time communication with individual vehicles. Consequently, architectural trade-offs would be different. It is crucial then that the architectures we develop for infrastructures today be easily upgradable for effective performance with either approach. Another similar concern is readiness for post-quantum cryptography, *e.g.*, to ensure that the cryptographic implementations can be easily upgraded to implementations that are robust against quantum computers in case quantum computing becomes a reality in the next few decades.

Unfortunately, extensibility is not easy to achieve. In addition to requiring significant creativity to anticipate which components of the architecture are There are two crucial factors that make extensibility challenging, optimization and verification. An architecture developed with the goal of extensibility is typically *required* to be modular, which, while leading to robust, hierarchical designs, often precludes low-level optimization. This is particularly crucial for transportation components that impose hard real-time constraints. Correspondingly, extensible designs typically involve more behaviors and configurations than necessary for current use cases. This poses additional burden on verification since those behaviors can become sources of security vulnerabilities.

There has been work to address these challenges. Emergent research on security architecture [13, 4, 5, 6] have been exploring means to develop systematic implementation of security requirements while facilitating optimization and verification needs. In spite of this, a significant gap remains between the state of the research and the needs of the practice.

6. CONCLUSION

We have discussed the scope and spectrum of security challenges in transportation infrastructure, focusing in particular in the sub-sector of highways and roadways as we move towards the era of self-driving autonomous vehicles. We discussed security challenges coming out of interaction between the infrastructure and transporting agents, and crucial challenges in V2X, real-time requirements and extensibility. We also provided a flavor of the state of the practice in automotive security architecture today, and how they are limited in the degree of genericity and extensibility for the expected requirements of tomorrow's automotive systems. While there has been some research progress, the area is still nascent with ripe possibilities and uncertainties.. A comprehensive solution will require a re-thinking of the architecture, and comprehending and accounting for the trade-offs necessary among various stakeholders' interests.

7. REFERENCES

[1] Critical Infrastructure Sectors. See URL https://www.dhs.gov/critical-infrastructure-sectors.

[2] Transportation Systems Sector. See URL https://www.dhs.gov/transportation-systems-sector.

[3] Transportation Systems Sector Cybersecurity Framework Implementation Guide. See URL

https://www.dhs.gov/publication/tss-cybersecurity-framework-implementation-guide.

[4] J. Backer, D. Hély, and R. Karri. Secure and Flexible Trace-Based Debugging of Systems-on-Chip. *ACM TODAES*, 22(2):31:1–31:25, 2017.

[5] A. Basak, S. Bhunia, and S. Ray. A Flexible Architecture for Systematic Implementation of SoC Security Policies. In *Proceedings of the* 34*th International Conference on Computer-Aided Design*, 2015.

[6] A. Basak, S. Bhunia, and S. Ray. Exploiting design-for-debug for flexible SoC security architecture. In *DAC*, 2016.

[7] Forbes. 10 Million Self-Driving Cars Will Hit The Road By 2020. See URL https://www.forbes.com/sites/oliviergarret/2017/03/03/10-million-self-driving-cars-will-hit-the-road-by-2020-heres-how-to-profit.

[8] International Telecommunications Union. ITU towards IMT for 2020 and beyond - IMT-2020 standards for 5G. See URL http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx.

[9] E. Messmer. RSA security attack demo deep-fries Apple Mac components, 2014. See URL http://www.networkworld.com/news/2014/022614-rsa-apple-attack-279212.html.

[10] G. Ramamoorthy. Market Share Analysis: Semiconductor Design Intellectual Property, Worldwide, 2012. See URL https://www.gartner.com/doc/2403015/market-share-analysis-semiconductor-design.

[11] S. Ray, W. Chen, J. Bhadra, and M. A. A. Faruque. Extensibility in Automotive Security: Current Practice and Challenges. In *DAC 2017*, 2017.

[12] SAE. Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems (Std. J3016). See URL http://standards.sae.org/j3016_201401/.

[13] M. R. Sastry, I. T. Schoinas, , and D. M. Cermak. Method for enforcing resource access control in computer system. US Patent 20120079590 A1.