CYBERSECURITY PRIMER FOR DEPLOYMENT OF CAV TECHNOLOGIES

Prepared for:

NCHRP Project 03-127
Cybersecurity of Traffic Management Systems

Prepared by:

Marisa C. Ramon
Ben A. Abbott, Ph. D
Cameron R. Mott
SOUTHWEST RESEARCH INSTITUTE®
Intelligent Systems Division
Post Office Drawer 28510, 6220 Culebra Road
San Antonio, Texas 78228-0510

(October, 2019)

The information contained in this report was prepared as part of NCHRP Project 03-127, National Cooperative Highway Research Program.

Acknowledgements (include in report)

This study was conducted with funding provided through the National Cooperative Highway Research Program (NCHRP) Project 03-127, *Cybersecurity of Traffic Management Systems.* The NCHRP is supported by annual voluntary contributions from the state Departments of Transportation. Project 03-127 is developing guidance for state and local transportation agencies on mitigating the risks from cyber-attacks on the field side of traffic management systems (including traffic signal systems, intelligent transportation systems, vehicle-to-infrastructure systems (V2I), and closed-circuit television systems) and, secondarily, on informing the agency's response to an attack. This document summarizes a variety of efforts applicable to the objective and will be updated throughout the life of the project. The report was prepared by Ben Abbott, Ph. D, Marisa Ramon, and Cameron Mott of the Southwest Research Institute. The work is being guided by a technical working group and managed by Ray Derr, NCHRP Senior Program Officer.

EXECUTIVE SUMMARY

The Connected and Automated Vehicle (CAV) market is expanding rapidly, and the technology that drives these advancements will be increasingly interacting with Infrastructure Owner Operator (IOO) equipment. This primer informs readers about:

- Existing security standards for CAV technology
- Recommendations for security best practices to protect safety-critical CAV deployments

Attacks against traditional vehicles without connected or automated features have been demonstrated, and their impacts are fairly well understood. The addition of CAV technology and supporting infrastructure equipment increases the availability of attack surfaces. If an attack occurs, it will be vitally important for an IOO to be ready to assess the impact of the situation and respond accordingly. The information in this primer can help to prepare for that scenario. It is expected that the reader is familiar with previous reports from NCHRP 03-127.

TABLE OF CONTENTS

1. INTRODUCTION

With more than 300,000 Traffic Signal Systems (TSS) across the United States and 2,550 added each year, based on the U.S. Census Bureau forecast of future population growth[1], Traffic Management Systems (TMS) have increasing cybersecurity risks. All these signalized systems contain varying levels of network access and embedded security. Traffic managers and government stakeholders may be unaware of the cybersecurity risks to field systems and other connected devices that relay data between systems and third parties or understand the likelihood of a cyber-attack occurring in one's network. Field systems and other connected devices introduce potential cybersecurity vulnerabilities that may be overlooked or not well understood by traffic managers and government agencies.

To help state and local agencies address cybersecurity risks on current transportation systems and those posed by integration of Connected and Automated Vehicles (CAV), Southwest Research Institute® (SwRI®) is currently researching cybersecurity weakness in TMSs as part of the program from the Transportation Research Board (TRB). The TRB is part of the private, nonprofit National Academies of Sciences, Engineering, and Medicine.

SwRI is leading the two-year project with support from Praetorian and, over the course of the program, the team has conducted a security assessment of high-risk traffic management systems and developed a web-based guide to help transportation agencies learn to safeguard equipment.

1.1 Project Background

The objective of the overall research effort is to develop guidance for state and local transportation agencies for mitigating risks from cyber attacks and responding to cyber attacks on the field side of traffic management systems (including traffic signal systems, intelligent transportation systems, Vehicle-To-Infrastructure systems (V2I), and closed-circuit television systems). The guidance will address the vulnerability of field equipment (e.g., traffic signal controller, changeable message signs, and V2I roadside units), field communications networks, and field-to-center communications. It will not address vulnerabilities within a traffic management center, within center-to-center communications, or insider risk (accidental or intentional).

The decision not to include traffic management centers within the scope of this project rests on the fact that the attack surface of a traffic management center is the same as a conventional network. Traffic management centers consist of devices such as workstations, servers, and network equipment, typically with Internet connectivity. The best practices to secure such environments are well understood, with multiple frameworks and guidelines being available to guide traffic management organizations. As such, the research team focused on addressing the unknowns of best practices to secure traffic management field equipment.

1.2 Project Goals

The goal of this entire project is to improve the cybersecurity of TMS by:

- Performing a strategic literature review and investigation of ongoing security efforts

[1] https://www.access-board.gov/guidelines-and-standards/streets-sidewalks/144-public-rights-of-way-guidelines/regulatory-assessment

- Review state of the art technologies across multiple disciplines
- Assess representative TMS and equipment
- Perform penetration testing on high-risk equipment
- Develop guidance for state and local agencies that aid in identifying:
    - Risks to their current field networks
    - Recommended changes they may implement to reduce those risks
    - Implications of the Connected Vehicle (CV) and Automated Vehicle (AV) technologies on the field networks
- Promote adoption and industry participation

This report is one of the several tasks performed under this project working toward the overall project objective.

1.3 Purpose of this Document

This document provides insight into existing state of the technology and provides guidelines and best practice for CAV deployments.

2. OT VS. IT CYBERSECURITY

As transportation agencies are updating and developing new road infrastructure systems (including infrastructure for CAV deployments), there are operational needs, cyber-physical impacts, and other considerations that must be addressed. Information Technology (IT) and Operations Technology (OT) cybersecurity have similar goals however require different approaches.

The IT Cybersecurity field has served as a foundational inspiration for the emerging OT Cybersecurity field. IT security is typically focused on protection of information, while OT security is focused on the protection of the device and the users. While the first is data-centric, the latter tries to balance enabling connectivity and control while maintaining physical safety and operations. IT prioritizes the detection and response to an incident (including recovery such as restoring from back-ups) while OT security prioritizes prevention. TMS, like Industrial Control System (ICS) networks has thousands of simple devices out in the field providing sensory data. These simple field devices are becoming increasingly connected and capable, especially with the evolution and deployment of CAV. With these advancements must come the advancement of cybersecurity protection, beyond the typical data-centric focus of IT Cybersecurity. For additional references on these topics, readers are encouraged to read some of the existing research including:

- "Emerging Consensus for an ICS Security Approach" by Courtney Schneider, Cyber Policy Research Manager, Waterfall Security Solutions

  https://static.waterfall-security.com/Emerging-Consensus-on-ICS-Cyber-Security_Whitepaper.pdf

- "Cybersecurity risks of TMS and the implications of CAV" by Marisa C. Ramon and Daniel A. Zajac, Southwest Research Institute

  https://static1.squarespace.com/static/59c3ed7b197aeabbd2a51a3b/t/5b2a52552b6a2875afd5e7c1/1529500246026/TS17_Paper15556.pdf

3. STANDARDS AND SPECIFICATIONS

There are several established standards and specifications that contribute heavily to the state of CAV technology.

3.1 Standards

3GPP Cellular Vehicle-to-Everything (C-V2X) or Long Term Evolution V2X (LTE-V2X) Standard

Through efforts under 3rd Generation Partnership Project (3GPP) standards organization, the Cellular Vehicle-to-Everything (C-V2X) standard was defined in 2016 (Release 14) with the goal of standardizing V2X capabilities integrated with LTE. C-V2X and Dedicated Short Range Communication (DSRC) are competing technologies and research results can be found that favor DSRC[2] and others that favor C-V2X[3]. C-V2X standardized the use of Cooperative-ITS (C-ITS) short-range technology referred to as 3GPP LTE-V2X PC5 (or LTE side-link). These Peer-to-Peer (P2P) connections enable low-latency and high-reliability communication between links that are within communication range. Range can vary on a number of environmental factors for both technologies including Line of Sight (LoS), weather and interference from other devices. LTE side-link and DSRC (IEEE 802.11p) both operate in the 5.9 GHz wireless radio frequency, though with incompatible modulation schemes (DSRC uses Orthogonal Frequency Division Multiplexing (OFDM) while PC5 uses Single Carrier Frequency Division Multiplexing (SC-FDM)). The applications that are enabled through each technology are essentially the same. While DSRC has been deployed by traffic authorities in cities throughout the U.S. over the past decade, vehicle OEMs have only deployed a small amount of vehicles equipped with DSRC. Now, as C-V2X equipment becomes more readily available, vehicle OEMs and traffic authorities are weighing the value of both technologies before deciding on which to use.

SAE J2735 Dedicated Short Range Communication (DSRC) Message Set Dictionary establishes the information and encoding/decoding format that is communicated between connected vehicles and infrastructure devices. This ensures interoperability for CVs at the application level and enables applications such as forward collision warning, emergency vehicle alerts, and traveler information messages.

SAE J2945/1 On-board Minimum Performance Requirements for V2V Safety Communications is an SAE standard that sets the minimum performance requirements and the standard features for Over-The-Air (OTA) communication. This provides interoperability at the interface level for CVs and infrastructure devices[4].

IEEE 1609.3-2016 Standard for Wireless Access in Vehicular Environments - Networking Services is an IEEE standard which defines the network and transport layer services. These services include routing and addressing and work together to provide secure Wireless Access in Vehicular Environments (WAVE) data

---

[2] https://www.nxp.com/docs/en/white-paper/ROADLINK-TECH-WP.pdf

[3] https://5gaa.org/news/an-assessment-of-lte-v2x-pc5-and-802-11p-direct-communications-technologies-for-improved-road-safety-in-the-eu/

[4] https://www.its.dot.gov/press/2016/standards_deployment.htm

exchanges. Additionally, IEEE 1609.3 defines Wave Short Messages, enabling IPv6 over an efficient WAVE-specific interface that can be directly supported by end applications. The Management Information Base (MIB) is also defined for the WAVE protocol stack[5].

IEEE 1609.2, IEEE 1609.4 and IEEE 1609.12 also further define DSRC and WAVE security standards, within the IEEE standards effort.

ISO/SAE 21434 Standard for "Road Vehicles – Cybersecurity" is developing a global standard for cybersecurity development of automotive systems. The key objectives are to define common terminology and key aspects of cybersecurity such that companies applying the standard can demonstrate responsible handling of automotive system development and cyber-threat prevention, ensuring security was adequately considered. The European Union (EU) is creating an EU Cyber Security Regulation in parallel with this standard and, in coordination with the United Nations Economic Commission for Europe (UNECE), is preparing a certification for a "Cyber Security Management System" (CSMS) as part of a task force on cybersecurity and OTA issues under a working party for automated/autonomous and connected vehicles (GRVA)[6]. This standard is currently under commenting and review. The ISO/SAE 21434 standard is anticipated to be available, if approved, on SAE's website in 2020.

SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems[7], while not a standard, it is guidance that establishes a comprehensive and systematic process and recommendations for designing cybersecurity into the cyber-physical vehicle system including product design, validation, deployment, and communication tasks. This guidance covers the complete lifecycle process to ensure cybersecurity is built in to the design and carried throughout product development and includes monitoring and incident handling in the field, along with addressing vulnerabilities in service and operation.

Under **IEEE ISTO, the Uptane Alliance**[8] is working on completing a standard for protecting remote Software-Over-The-Air (SOTA) updates for automotive Electronic Control Units (ECU). This standardization effort will provide the necessary requirements and recommendations for suppliers, Original Equipment Manufacturers (OEM), and solution providers to deploy a secured software update process similar to the methods that are protecting updates for non-embedded computing platforms[9]. Security measures similar to these may protect field-deployed equipment in the future.

The **SAE Recommended Practice J3016 (June 2018) "Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles"[10]** lays out the terms and operational domains for automated driving systems. This clarifies the six levels of driving assistance from a fully manually operated to a fully automated vehicle. These terms needed clarification due to the mis-use of the various levels in marketing material. SAE Levels 1-2 (car controls gas, brake, and/or steering) always rely on a human driver and account for virtually all systems on the road today. Some self-driving systems are

---

[5] https://www.standards.its.dot.gov/News

[6] https://wiki.unece.org/pages/viewpage.action?pageId=40829521

[7] https://saemobilus.sae.org/content/J3061_201601/

[8] https://uptane.github.io/

[9] https://theupdateframework.github.io/overview.html

[10] https://saemobilus.sae.org/content/j3016_201806

arguably capable of partial Level 3 (fully automated with human backup) or Level 4 (fully automated without human backup, does not work in all road conditions) but, because they rely on human oversite, are still considered Level 2. Level 5 is reserved for an Automated Driving System (ADS) that operates without any design-based restrictions such as time-of-day, weather conditions, or regional limitations. A Level 5 vehicle would not need to include manual vehicle controls such as a brake pedal or steering wheel. A Level 5 ADS would be capable of detecting road conditions that a human driver would deem "unsafe" such as dense fog, flowing water, and black ice and would achieve a minimal risk condition (such as pulling over to the side of the road) until the condition changes.

3.2 Specifications

Roadside Unit Specification

The Dedicated Short-Range Communications Roadside Unit Specifications document (dated April 28, 2017[11]) specifies the necessary SHALL requirements and SHOULD recommendations for Roadside Units (RSU). While the RSU 4.1 Specification document is not a standard, it is widely recognized as the best practice within the CAV industry. RSU vendors should be following the requirements in order to provide interoperability. In addition, OmniAir certification leverages the RSU 4.1 Specification, and vendors that are seeking certification use the specification as a best practice guide. Efforts to standardize are underway. Prior to standardization and a mandate, adherence to these requirements is mixed.

RSU Bench Test Plan

The Revision to Dedicated Short-Range Communication Roadside Equipment Specification RSU 4.1 Bench Test Plan[12], provides guidance on evaluating RSUs against the United States Department of Transportation (USDOT) RSU Specification 4.1 prior to deployment. The Bench Test Plan evaluates only the basic functionality for an RSU. Beyond the recommendations in the Bench Test Plan, the authors recommend that IOOs verify all equipment against the use cases for the specific deployment. Additionally, implementation details will be a decisive factor for success and system integration efforts are recommended prior to deployment.

RSU and OBU Device Certification

OmniAir offers certification for RSUs and Onboard Units (OBU) through a third-party accredited test lab. Equipment that passes OmniAir certification is listed in a publicly-available database for public consideration. This certification offers assurance of conformance to the requirements against which OmniAir tests, including adherence to many of the standards listed here, as well as interoperability. In addition, the OmniAir Cybersecurity Working Group is establishing detailed test plans and proposed test cases to evaluate the security of OmniAir certified devices. SwRI participates in the OmniAir certification process as contributing technical staff.

---

[11] https://transops.s3.amazonaws.com/uploaded_files/Dedicated%20Short%20Range%20Communications%20Roadside%20Unit%20Specifications.pdf

[12] https://rosap.ntl.bts.gov/view/dot/3621

4. AUTOMATED VEHICLE CYBERSECURITY

Automated vehicles are active on today's roadways in select areas. Since these systems are built on top of modern vehicle architectures, they inherit similar vulnerabilities. In addition, AVs use sensors, drive by wire systems, and automated control algorithms which introduce new attack surfaces. Remote attacks have been demonstrated against several sensors including LIDAR, radar, ultrasonic, Global Positioning System (GPS) and cameras, although some of the demonstrated attacks would be difficult to perform outside of a lab environment. The drive-by-wire system provides control of the vehicle's gas, brake, and steering. These actuators are safety-critical and must be secured from cyber threats. The automated control algorithm that enables automated capabilities also introduces a new vulnerability and must be secured. Integrity checking at startup and during use is highly recommended, and any tampering or misconfiguration should be flagged immediately. Communication between the autopilot system, sensors, and actuators (e.g. gas, brakes, steering) should use authentication to assure the source of transmitted data. If the connections are not secure, another node on the network could transmit messages to manipulate the system.

Some AVs maintain dual-control of vehicle functionality and allow a manual operator to take control of the vehicle at any time. Level 3 or lower vehicles rely on the manual operator to do so in certain conditions. The manual operator must be familiar with the proper functionality of the AV to monitor for interference through a cybersecurity threat. Currently, responsibility for the safe operation of AVs rests on the safety drivers and the developers/manufacturers. Various DOTs have taken a stance regarding the testing and public use of automated vehicles on their roadways. As one example, California offers three types of permits that can be awarded to organizations. Automated vehicle manufacturers or developers that are operating on California roadways can apply for a testing permit (requires a safety driver), a driverless testing permit, or a deployment (public use) permit. Many agencies have applied and received these permits, and each agency reports specific information to the California Department of Motor Vehicles (DMV). The specific information includes miles traveled while operated by an ADS and the number of human takeovers required (human-initiated Dynamic Driving Task (DDT) fallback). In the report for 2018, there were more than two million miles driven by almost thirty companies[13]. On these drives, there were almost 150 thousand takeovers. This equates to an average of one human takeover per 14 miles[14]. Some agencies are more mature than others, and the technology will continue to improve as long as testing and verification efforts continue.

[13] https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/disengagement_report_2018

[14] https://www.consumerwatchdog.org/privacy-technology/robot-cars-average-required-human-takeover-every-14-miles-driven

5. SECURITY CREDENTIAL MANAGEMENT SYSTEM FOR V2X

The Security Credential Management System (SCMS) Proof-of-Concept (POC) report[15] provides the requirements for securing Vehicle-to-Vehicle (V2V) and V2I communications. The report was authored by the Crash Avoidance Metrics Partners (CAMP LLC) Vehicle Safety Communications 5 (VSC5) Consortium. The scope of the SCMS POC focuses on validating messages over Vehicle-To-Everything (V2X) medium. Because of the privacy concerns for V2X, anonymity is a primary requirement. In contrast, authenticity is needed in order to maintain trust between devices. SCMS proposes a way to bridge that gap, and as such it is not an encryption strategy, it is a message validation process that can authenticate that a message's source is valid and is chained to a trusted root. A Certificate Revocation List (CRL) is maintained that effectively black-lists a source and can flag all messages that are generated using that certificate as invalid. This retains anonymity while still providing a mechanism for ignoring bad actors. A few challenges still remain:

- There are very few commercially-available SCMS deployments
- The volume of certificates that are necessary to support the recommended enrollment is very high (one source cites the possibility of hundreds of billions of certificates[16])
- Advanced research still needs to be completed to perform wide-spread detection of bad actors.

Additionally, due to the small number of potential SCMS providers, two (2) at the time of this report, interoperability is an unknown factor. Each SCMS provider would need to share CRLs and potentially even establish a shared root certificate. Mechanisms exist within the SCMS design to provide for this possibility through electors. While the SCMS protects the privacy of devices that are transmitting data on a broadcast basis, there are existing concerns and security analysis efforts underway at a national level[17]. There are still areas for the misbehavior detection and revocation efforts to grow. Novel cryptographic concepts such as butterfly key expansion help to protect the system but require additional development effort and processing power on embedded devices, which will increase device and overall system cost. In addition, the introduction of novel cryptographic concepts may suffer from a lack of vetting, and security vulnerabilities may be present that have not received a high level of scrutiny. Efforts are underway to address these opportunities, which are drawing interest from the top minds in cybersecurity to solve these remaining items.

[15] https://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf

[16] https://blackberry.certicom.com/en/products/certicom-scms

[17] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8309336

6. RECOMMENDATIONS

Alignment with standards, specifications, and best practices will help protect CAV deployments as they progress through the initial introduction phase. Additionally, there are a number of recommendations that are deemed highly valuable and are indicated below. While not an exhaustive list, these recommendations have the potential to have a high impact on the improvement of a deployment.

6.1 Connect to the Cybersecurity Community

Establishing a connection to the cybersecurity community provides an additional level of knowledge and collaboration. You should be familiar with their activities and they should be familiar with your security approach. Some of the relevant cybersecurity communities are included below:

1. Cybersecurity and Infrastructure Security Agency (CISA) [part of the Department of Homeland Security (DHS)]
   CISA provides extensive cybersecurity and infrastructure security knowledge and practices to its stakeholders, shares that knowledge to enable better risk management, and puts it into practice to protect the Nation's essential resources. https://www.cisa.gov/
2. Surface Transportation, Public Transportation, and Over-the-Road Bus ISACs
   The Surface Transportation Information Sharing and Analysis Center (ST-ISAC) provides the Transit and Rail Intelligence Awareness (TRIAD) daily report which focuses on counter-terrorism, suspicious activity reports, and general security awareness. It includes information from the Over the Road Bus ISAC (OTRB-ISAC) and Public Transportation ISAC (PT-ISAC).
   https://www.surfacetransportationisac.org/
3. Multi-State Information Sharing and Analysis Center (MS-ISAC)
   The Multi-State Information Sharing and Analysis Center (MS-ISAC) establishes a community of collaboration around transportation physical and cybersecurity. It is engaging the nation's state, local, tribal, and territorial governments with the help of DHS. https://www.cisecurity.org/ms-isac/
4. Automotive security community (Auto-ISAC)
   The Automotive Information Sharing and Analysis Center (Auto-ISAC) establishes a community of collaboration around automotive cybersecurity. Members are kept informed of the latest in security concerns and are provided with best practices for automotive security. Membership is open to light and heavy-duty vehicle OEMs, suppliers, and commercial trucking companies who are not under government control. Other interested parties such as security vendors, researchers, government agencies, and non-automotive suppliers can participate as partners. Members collaborate through a confidential information portal, with the option of anonymously sharing information, viewing real-time cybersecurity intelligence reports, and live interactions including workshops. Active cybersecurity concerns can be discussed with industry experts through the Auto-ISAC. https://www.automotiveisac.com/
5. Information Technology security community
   The Information Technology ISAC (IT-ISAC) pools information from a diverse community of companies concerned with critical infrastructure security. This ISAC shares knowledge, practices, insights, and cyber incidents that impact the IT sector. https://www.it-isac.org/

6. CV security community
   The CV security community has centered on SCMS and proving the validity of V2X messaging. The OmniAir Cybersecurity Working Group is actively working on detailed test plans and proposed test cases to evaluate the security of OmniAir certified devices.
7. AV security community
   AV cybersecurity is developing rapidly, along with the rapid deployment of AVs. While there are few regulations on the security of AVs, efforts such as the SELF DRIVE Act (passed the House September 2017 but not yet a law) require a cybersecurity plan. "Manufacturers of highly automated vehicles must develop written cybersecurity for sale."[18]
   Standards organizations such as ISO and SAE are working on establishing the standards guidelines for cybersecurity on AVs. Mcity's cybersecurity working group has released a threat identification tool (as a whitepaper) to help readers understand the breadth of cybersecurity challenges that CAVs face[19]. Southwest Research Institute is investing internal funds to perform field-tests of potential AV vulnerabilities[20]. International research organizations such as Horiba Mira are creating physical test environments for CAVs that can identify and address cybersecurity vulnerabilities[21]. Through continued vigilance in this area, AV cybersecurity is a focus of many companies, standards bodies and regulatory agencies and will be growing rapidly.
8. Similar agencies in other regions
   Reaching out to similar agencies in other regions and sharing contact information can help to mitigate the potential impact of security vulnerabilities.

6.2 Secure Entry Points

Minimizing and securing potential entry points is a critical component to protecting the security of CAV technology deployments. These entry points are a direct connection to an otherwise protected network and are critical to maintain control. Equipment deployments to support CAVs may be more physically exposed since they are typically forward deployed into traffic cabinets or power poles at intersections and along roadways. In addition to the recommendations that are outlined in NCHRP 03-127 Task 1[22], the following sections provide some recommendations to help protect these devices.

6.3 Secure Field Devices and Physical Access Requirements and Safeguards

The following sub-sections highlight requirements and safeguards for securing field devices that are a part of CAV technology deployments.

---

[18] https://www.congress.gov/bill/115th-congress/house-bill/3388

[19] https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf

[20] https://www.swri.org/press-release/system-legally-test-gps-spoofing-vulnerabilities-automated-vehicles

[21] https://www.horiba-mira.com/media-centre/news/2018/11/28/horiba-mira-simulation-and-cybersecurity-expertise-supports-completion-of-uk-cite-project/

[22] http://onlinepubs.trb.org/onlinepubs/nchrp/docs/NCHRP03-127_Cybersecurity_Literature_Review.pdf

6.3.1 Enable Remote Monitoring

- USDOT_RSU-Req_585-v001 is listed as a SHOULD in RSU 4.1 specification and specifies that the FIPS 140-2 Level 3 Physical Security Requirements tamper response mechanism should be supported, such as a network indicator to the backhaul on intrusion. This is a very valuable pre-indicator to an intrusion and is recommended for deployments.
- This should also apply to the enclosure (traffic cabinet) to be aware of a potential physical intrusion that may jeopardize the security of the field equipment and networking equipment.

6.3.2 Segment Access to Broader Network and Operations

Network design should utilize intelligent segmentation, with particular focus on:

a. Protecting the gateways between networks
b. Keeping equipment up to date (firmware, configuration, and even hardware when necessary)

6.3.3 Password Policy

Establish a policy for rotating/expiring passwords and adhere to that policy

6.3.4 Add Multi-Factor Authentication Prior to Deployment

USDOT_RSU-Req_632-v002 and USDOT_RSU-Req_345-v001 establish a SHOULD clause in RSU 4.1 specification which enables multi-factor authentication for Secure Shell (SSH) connections to RSUs. This is a valuable mechanism to protect RSUs from outside intrusion. This should be done prior to field deployment while physical access to the device is available in case of a failure during this process. Establishing multi-factor authentication after deployment incurs additional risk.

6.4 Understand Other Best Practices

Familiarity with similar disciplines and the operations best practices of automotive and energy industries will provide additional understanding for applying secure solutions in the CAV domain. These are recommended:

1. NIST 800-53 Security and Privacy Controls for Federal Information Systems and Organizations
2. Open Web Application Security Project (OWASP)
3. PAS 1885:2018 - The fundamental principles of automotive cybersecurity – Specification

7. CONCLUSION

CAVs are increasingly prolific on public roadways, and it is important for IOOs to understand the impacts and recommendations to protect both CAVs and deployed equipment. Information was provided through this primer regarding existing security standards and specifications for CAV technology. Additionally, recommendations for security best practices to protect safety-critical CAV deployments were provided. While the CAV environment is a target for cybersecurity issues, preparation can help protect deployed equipment. With this primer and some recommended follow-up, an IOO will have a strong foundation to begin assessing the cybersecurity strength of CAV equipment deployments.

APPENDIX A Acronyms

Acronym	Definition
3GPP	3rd Generation Partnership Project
ADS	Automated Driving System
AV	Automated Vehicle
CAMP LLC	Crash Avoidance Metrics Partners
CAV	Connected and Automated Vehicle
CISA	Cybersecurity and Infrastructure Security Agency
CRL	Certificate Revocation List
CSMS	Cyber Security Management System
CV	Connected Vehicle
DDT	Dynamic Driving Task
DHS	Department of Homeland Security
DMV	Department of Motor Vehicles
DSRC	Dedicated Short Range Communication
ECU	Electronic Control Unit
EU	European Union
GPS	Global Positioning System
GRVA	Working party for automated/autonomous and connected vehicles
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IOO	Infrastructure Owner Operator
ISAC	Information Sharing and Analysis Center
ISTO	Industry Standards and Technology Organization
ITS	Intelligent Transportation Systems
LoS	Line of Sight
LTE	Long Term Evolution
MIB	Management Information Base
MS	Multi-State
OBU	Onboard Units
OEM	Original Equipment Manufacturers
OT	Operations Technology
OTA	Over-The-Air

Acronym	Definition
OTRB	Over The Road Bus
OWASP	Open Web Application Security Project
POC	Proof Of Concept
PT	Public Transportation
RSU	Roadside Units
SCMS	Security Credential Management System
SOTA	Software-Over-The-Air
SSH	Secure Shell
ST	Surface Transportation
TMS	Transportation Management System
TRB	Transportation Research Board
TSS	Traffic Signal Systems
UNECE	United Nations Economic Commission for Europe
V2I	Vehicle To Infrastructure
V2V	Vehicle To Vehicle
V2X	Vehicle To Everything
VSC5	Vehicle Safety Communications 5
WAVE	Wireless Access in Vehicular Environment