ITS DEPLOYMENT EVALUATION

Executive Briefing

Highlights

- The NIST Cybersecurity Framework (NIST CSF) provides TMCs with best practices to manage physical and software system cybersecurity.
- Infrastructure integrating next-generation internet protocol version 6 (IPv6) will be crucial to the future growth of connected vehicle networks and secure and trusted communications.
- The three U.S DOT Connected Vehicle Pilots sites employed encryption and certificate management techniques to facilitate trusted communications in a connected environment.

This brief is based on past evaluation data contained in the ITS Databases at: www.itskrs.its.dot.gov. The databases are maintained by the U.S. DOT's ITS JPO Evaluation Program to support informed decision making regarding ITS investments. The brief presents benefits, costs and best practices from past evaluations of ITS projects.

U.S. Department of Transportation
Intelligent Transportation Systems
Joint Program Office

ITS Cybersecurity

Introduction

Today's transportation sector is becoming increasingly connected and dependent on information systems and networks. The advent of Intelligent Transportation Systems (ITS) communications technologies such as vehicle to vehicle, infrastructure, pedestrian, and others are improving the safety, mobility, and environmental impacts of how people travel. However, with increased connectivity there is increased risk of cybersecurity attacks, and agencies that collect and analyze data for critical system operations are particularly vulnerable. Transportation Management Centers (TMCs) and ITS devices no longer function as closed systems, increasing the risk of cyber threats to transportation facilities and infrastructure. Figure 1 below describes current classifications of cyber threat actor and respective threat levels.

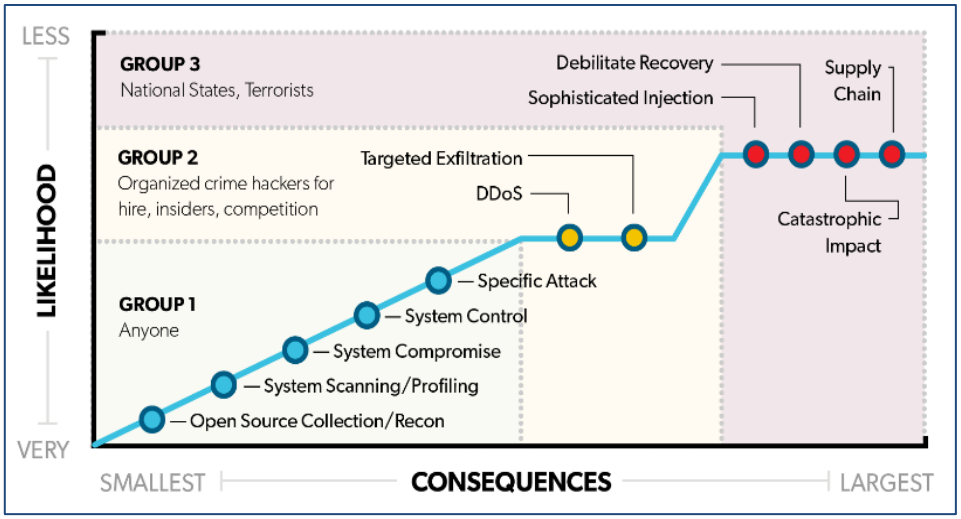

Figure 1: Cyber Threat Actor Classification (Source: U.S. DOT)

To address these risks, transportation agencies have implemented the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) to harden physical and software system security and protect communications from malicious attacks, unauthorized access, damage, and disruptions that might interfere with system performance or functions. The CSF provides voluntary guidance based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk [1].

Top cybersecurity control measures used by TMCs to conform to the NIST cybersecurity framework and CIS (Center for Internet Security) Top 20 Controls currently include: routinely scanning networks to identify attached devices, isolating vendor-supported software in a demilitarized zone (DMZ) of a network, and using access control lists (2021-L01016). A DMZ works by restricting remote support access to the DMZ itself and not to the enterprise/business network. Restricting access by remote vendors limits risk exposure and the potential attack surface on the most critical infrastructure/systems. Access control lists limit outside access to specific machines or services, so that access is granted only to the devices/networks that need. This also helps to manage insider vulnerabilities.

As connected vehicle (CV) applications increase in popularity, DOTs will need to protect more than just TMC infrastructure, back-office systems, data hubs, and communication links to field equipment. Large-scale deployments will require DOTs to support and protect massive amounts of bidirectional data flow between vehicle onboard units (OBUs) and roadside infrastructure (2019-L00891). To secure these data flows, Security Credential Management Systems (SCMS) were developed by the U.S. DOT using Public Key Infrastructure (PKI) concepts. PKI involves the creation and management of digital certificates that ensure the validity of messages, enabling users to trust one another and the system as a whole. A PKI allows for users who are unknown to each other to communicate securely with one another and with a back-end security system that produces digital certificates. This enables trusted communications between vehicles, and between vehicles and field devices that have had no prior interaction.

Benefits

Critical infrastructure TMC applications that support Advanced Traffic Management (ATM) systems are of particular concern because they can directly impact system performance. Recently, researchers demonstrated through simulation efforts that real-time cyber threat monitoring systems can effectively assess if an ATM system is behaving as expected in response to prevailing traffic conditions, or if a possible cyberattack that could potentially shut down a congested corridor is underway. Findings suggest these monitoring systems can preempt the severest of consequences of a cyberattack by enabling compromised ATM networks to automatically revert to a default operational state where nominal corridor performance can be maintained (2019-B01346).

Currently, SCMS applications that improve security between vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications continue to be implemented, with potential benefits of SCMS becoming available as commercial applications expand. SCMS provides several benefits, including:

- Ensuring integrity—so users can trust that the message was not modified between sender and receiver.
- Ensuring authenticity—so users can trust that the message originates from a trustworthy and legitimate source.
- Ensuring privacy—so users can trust that the message appropriately protects their privacy.
- Helping achieve interoperability—so different vehicle makes and models will be able to talk to each other and exchange trusted data without pre-existing agreements or altering vehicle designs [2].

Costs

The costs to establish and maintain ITS communications include upgrades to ITS backhaul and communication protocols (i.e., IPv4 to IPv6 transition) as required to support SCMS, the deployment of back-office data analytics platforms, and information management strategies that ensure trustworthy messages are available and can be exchanged between vehicle OBUs, roadside equipment, and TMCs. The following table includes example system cost data for cybersecurity and data management systems deployed in the United States (2022-SC00514).

Table 1: Cybersecurity Element Cost Data Reported by DOTs

Cost Component	Cost Data Reported by DOTs
Security Credential Management System (SCMS)	Minnesota DOT (MnDOT): The cost for a SCMS to support a 22-signal Connected Corridor project along Hwy 55 in the Twin Cities region was estimated at $100,000 with ongoing consultant support estimated at $15,000 per year. MnDOT spent approximately $43,000 to upgrade its corridor communications from IPV4 to IPV6 improving security and enabling Roadside Units (RSUs) to request and download new certificates from the SCMS.
	University of Michigan Transportation Research Institute (UMTRI) and U.S. DOT: The cost of a third-party production SCMS was estimated at $150,000 for three years (2015-2018) to support secure communications between 5,000 connected vehicles and roadside equipment at 45 street locations and 12 freeway sites in the City of Ann Arbor.
	Georgia DOT (GDOT): The cost to implement a SCMS for full deployment of connected vehicle infrastructure at 1,700 intersections in metro-Atlanta was estimated at $240,000.
Back Office TMC Data Analytics Platform	MnDOT: The cost to deploy a back office analytics platform to support a 22-signal Connected Corridor project along Hwy 55 in the Twin Cities region was estimated at $367,000.
	UMTRI and U.S. DOT: The cost to upgrade a connected vehicle analytics platform to support the Ann Arbor Connected Vehicle Test Environment was estimated at $762,000.
	GDOT: The cost to plan and design a back office analytics platform to support a partial deployment of connected vehicle applications for roughly 650 of 1,700 intersections in the metro Atlanta area was estimated at $85,000.

Best Practices

A comprehensive resource developed by the U.S. DOT Cyber Security Action Team to support the Department's Incident Response Capability Program, "Improving Critical Infrastructure Cybersecurity," is available in Executive Order 13636. The team leveraged U.S. transportation system security threat and vulnerability assessments and research conducted by the Federal Highway Administration (FHWA) to examine strategies of potential attackers, common cyberattack processes, and potential

Figure 2: Cybersecurity team examining strategies of potential attackers (Source USDOT).

points of TMC vulnerability to prepare TMC managers and operators to respond to incidents.

Best practices that improve cybersecurity for critical infrastructure are summarized below (2019-L00857).

Stop Breaches

- Review the Industrial Control Systems Cyber Emergency Response Team's Cyber Security Evaluation Tool (CSET)
- Train TMC management and staff to identify and defend against social engineering
- Develop an IT and Information Security policy, which TMC operators should understand and follow
- Implement network segmentation, proper firewall deployment, and best practices in edge device communication

Disrupt Scans and Network Mapping

- Encrypt communication on the control network
- Implement an Intrusion Detection System (IDS) on the TMC's internal network
- Use a honeypot to help trap and collect information on intruders in accordance with agency legal department

Limit the Effects of Exploitation and Lock the Gate

- Maintain TMC operator and IT support team vigilance
- Monitor TMC data traffic between trusted partners to prevent operational partners from becoming a source of unprotected backdoor attacks
- Limit data connections and connection types into the internal TMC network
- Conduct and protect frequent backups of critical applications and databases

Defend Against Denial-of-Service (DOS) Attacks

- Stop an attack at the Internet Service Provider (ISP) connection
- Consider moving frequently attacked servers such as those that support traveler information systems to a separate network that is protected by additional firewalls to prevent attacks from affecting core TMC functions

Have a Plan

- Develop and maintain an IT infrastructure protection plan that clearly identifies resources and agency roles
- Use the CSET tool to understand the TMC's current vulnerabilities, and institute continuous evaluation and monitoring of the configuration and health of the TMC's IT infrastructure
- TMC operators within a jurisdiction encompassing a national security facility may want to reach out to the facility to determine whether the TMC's risk exposures are elevated. TMC owners should determine the damage potential from a breach, considering potential immediacy and breadth of disruption and TMC complexity

- Ensure both TMC and IT team members know how to execute the plan

Success Story

Connected Vehicle Pilot Deployment Program Driving Towards Deployment

Figure 3: Recipients of federal funding to implement a suite of connected vehicle applications and technologies (Source: USDOT).

In September of 2015, U.S. DOT selected the New York City Department of Transportation (NYCDOT), Wyoming Department of Transportation (WYDOT) and Tampa Hillsborough Expressway Authority (THEA) as the recipients of a combined $42 million in federal funding to implement a suite of connected vehicle applications and technologies tailored to meet their region's unique transportation needs under the Connected Vehicle Pilot Deployment Program. Following the award, each site spent 12 months preparing a comprehensive deployment concept to ensure rapid and efficient connected vehicle capability roll-out. The sites next completed a 24-month phase to design, build, and test these deployments of integrated wireless in-vehicle, mobile device, and roadside technologies. As of 2021, the New York City and Wyoming pilot sites are in the operate and maintain phase, where system impact is being monitored on a set of key performance measures, while Tampa has completed Phase 3 and is currently performing follow-up work focused on spectrum testing and interoperability capabilities with device manufacturers.

The following lessons address changes agencies may have to make to their existing systems and operations to accommodate the security needs of CV technology. Emphasis is particularly placed on the utilization of a SCMS that uses PKI to employ encryption and certificate management to facilitate trusted communications between the vehicles and the surrounding infrastructure (2019-L00889).

Address security in all aspects of the CV and agency systems. Recognize that the security requirements of the system extend to the agency's networks and computer systems and will likely require changes to existing systems and operations. To address the security needs of CV technology, the Pilot sites made numerous changes to their security procedures regarding:

- Operations – password control (strength) and expiration, physical access to facilities such as TMCs, and encryption of databases
- Communications – upgrades to the ITS environment to provide increased security – especially where National Transportation Communications for ITS Protocol (NTCIP) standards are concerned; Virtual Private Network (VPN) tunnels, Datagram Transport Layer Security (DTLS) and Transport Layer Security (TLS) protocols using x.509 digital certificates; and disabling local access ports without security.
- Maintenance – requiring authentication of field personnel in real time when replacing failed devices; devices have a collection of enrollment certificates; and keypad interactions to use USB access to reload and re-initialize the device.

Implement a credential management misbehavior detection feature to address vulnerabilities to cyberattacks, spoofing and malfunctioning equipment. A standard Misbehavior Detection and Certificate Revocation List (CRL) distribution mechanism should be designed to limit front loading of certificates to minimize the potential impact of compromised OBUs.

Identify all Provider Service Identifiers (PSIDs) for all applications being implemented prior to enrollment in the SCMS. Since each enrollment certificate is associated with a particular application that is mapped to a particular PSID it is important to determine what applications the device will need to support and the corresponding PSIDs before enlisting in enrollment. If additional applications are added later, additional security measures may require that the device be physically delivered to a secure facility for re-enrollment.

Implement proper certificate change requirements to prevent vehicle tracking. Certificates need to be changed at time intervals as required, but exceptions involving "absolute distance" from the previous certificate change location should also be considered. With an absolute distance assumption of two kilometers, a vehicle traveling within an urban grid network (such as a taxi in New York City) may operate in a large area for an extended time period and not trigger the certificate change mechanism. In New York City, the CV Pilot team decided to implement a change mechanism that required certificates to change every two kilometers traveled or every five minutes – whichever occurred first.

References

[1] National Institute of Standards and Technology (NIST), "Cybersecurity Framework (CSF)," *nist.gov*, 2021. [Online]. Available: https://www.nist.gov/cyberframework.

[2] U.S. DOT ITS JPO, "Security Credential Management System (SCMS)," *U.S. DOT ITS JPO Resources Website*. [Online]. Available: https://www.its.dot.gov/resources/scms.htm.