CSE201: Introduction to Security Credential Management System (SCMS)

Table of Contents

1. Module Description

This module is part of the Intelligent Transportation System (ITS) set of learning modules. It explains how ITS deployments should plan for interactions with a Security Credential Management System (SCMS) operator to enable roadside and road-using components in the system to trust each other.

The SCMS is a critical component of ensuring trust while maintaining privacy in a vehicle-to-everything (V2X) ecosystem. In contrast to other types of safety technologies currently found in the vehicle fleet, connected vehicle applications are cooperative—meaning, system participants (i.e. applications running on devices) must exchange messages with each other and act on them in real time to realize the benefits of the system. The correctness and reliability of messages being transmitted between participants is of critical importance as it impacts the outcomes and effectiveness of safety applications based on them. Message senders need to digitally sign their messages, and message receivers need to verify the signature before acting on it. To protect the privacy of vehicle owners, the certificates used to sign the messages contain no personal or equipment-identifying information but serve as system credentials so that other users in the system can trust the source of each message. The SCMS also plays a key function in protecting the content of each message by identifying and removing misbehaving devices, while still maintaining privacy.

The following prerequisites are recommended for students taking this course:

- CV262: Vehicle-to-Vehicle ITS Standards for Project Managers
- CV261: Vehicle-to-Infrastructure ITS Standards for Project Managers
- CV265: Introduction to IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments

2. Introduction/Purpose

The SCMS is a form of Public Key Infrastructure (PKI) that issues and manages the security certificates that form the basis of trust for V2X communications. The SCMS is distinguished from traditional PKI in several aspects—its size and the balance among security, privacy, and efficiency. V2X devices enroll into the SCMS after completing device certification processes that validate the devices as trusted players in the system. The applications on those devices then obtain security certificates from certificate authorities (CAs) and attach those certificates to their transmitted messages as part of a digital signature. As well as authorizing baseline application activities, these credentials provide special permissions to privileged participants (e.g., first responders) to prioritize their V2X messages.

The SCMS also plays a key function in protecting the system as a whole by identifying and removing misbehaving devices, while still maintaining privacy. With misbehavior, field devices (Onboard Units (OBUs), Aftermarket Safety Devices (ASDs), or Roadside Units (RSUs)) can report back to the SCMS if they perceive that other vehicle devices are transmitting invalid or untrustworthy messages. Misbehavior detection capabilities remove misbehaving devices from the system, so they do not interfere with safety and transportation critical operations.

After taking this course, participants will be able to understand the application of a transportation-oriented SCMS and how the security certificates provide the mechanism for devices to exchange messages in a trustworthy and privacy-protected manner. This course will help participants in understanding the standards used to ensure the security of the V2X communications exchanges, including the interoperability among devices operating in a connected vehicle environment. Finally, participants will understand technical and organizational challenges associated with obtaining credentials for use by devices that participate in deployments and will be positioned to specify implementation or deployment requirements related to SCMS-based certificate management.

The target audience for this module include:

- Private and public sector users including manufacturers and vendors
- Decision makers
- Procurement managers/specification writers
- Public sector IT and CV project managers
- Traffic management and engineering staff
- Transportation planners
- Traffic management center/ITS operations staff
- System developers/integrators
- Transit system managers and operators

3. Reference to Other Standards

1. IEEE Draft Standard P1609.2.1, Wireless Access In Vehicular Environments (WAVE) – Certificate Management for End Entities, https://standards.ieee.org/project/1609_2_1.html.
2. IEEE Std 1609.2-2016™, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages.
3. IEEE Std. 1609.2a-2017, IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages - Amendment 1.
4. IEEE Std. 1609.2b-2019, IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages - Amendment 2--PDU Functional Types and Encryption Key Management.
5. SAE J2945/1, On-Board System Requirements for V2V Safety Communications, https://www.sae.org/standards/content/j2945/1_201603/.
6. SAE J2945/5, Service Specific Permissions and Security Guidelines for Connected Vehicle Applications, https://www.sae.org/standards/content/j2945/5_202002/.
7. S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, Internet Engineering Task Force (IETF) Request for Comments (RFC) 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

4. Glossary/Abbreviations

Term	Definition
ACA	Authorization Certificate Authority

Term	Definition
AES	Advanced Encryption Standard
ARC-IT	Architecture Reference for Cooperative and Intelligent Transportation
ASD	Aftermarket Safety Device
BSM	Basic Safety Message
CA	Certificate Authority
CRL	Certificate Revocation List
CTL	Certificate Trust List
CV	Connected Vehicle
DC	Distribution Center
DES	Data Encryption Standard
DOT	Department of Transportation
DSRC	Dedicated Short-Range Communications
ECA	Enrollment Certificate Authority
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
EE	End Entity
FIPS	Federal Information Processing Standard
GPS	Global Positioning System
ICA	Intermediate Certificate Authority
IEEE	Institute of Electrical and Electronics Engineers
IOO	Infrastructure Owner and Operator
ITS	Intelligent Transportation System
KP	Key Point
LO	Learning Objective
MA	Misbehavior Authority
MAP	Map
NIST	National Institute of Standards and Technology
NYCDOT	New York City Department of Transportation
OAEP	Optimal Asymmetric Encryption Padding
OTA	Over the Air
PKI	Public Key Infrastructure
PP	Protection Profile
PSID	Provider Service Identifier
RA	Registration Authority
RSA	Rivest–Shamir–Adleman
RSU	Roadside Unit
SAE	Society of Automotive Engineers
SCMS	Security Credential Management System
SMOC	Security Management Operating Concept
SPaT	Signal Phase and Timing
TIM	Traveler Information Message
TMC	Traffic Management Center
USDOT	United States Department of Transportation
V2X	Vehicle-to-Everything

5. Other References

1. National Security Credential Management System (SCMS) Deployment Support, 2018, USDOT www.its.dot.gov/index.htm, https://www.its.dot.gov/resources/scms.htm.
2. Security Credential Management System Proof–of–Concept https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf.
3. W. Whyte et al., "A Security Credential Management System for V2V Communications," Proc. IEEE Vehicular Networking Conf. (VNC), 2013; http://ieeexplore.ieee.org/document/6737583.
4. Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) Service Package SU02: Core Authorization, https://local.iteris.com/arc-it/html/servicepackages/sp12.html#tab-3.
5. Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) Service Package SU08: Security and Credentials Management, https://local.iteris.com/arc-it/html/servicepackages/sp63.html#tab-3.
6. Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) Service Package SU09: Device Certification and Enrollment, https://local.iteris.com/arc-it/html/servicepackages/sp206.html#tab-3.
7. European Commission C-ITS Platform Phase II, Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1.1 June 2018.
8. European Commission C-ITS Platform Phase II, Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS), Release 1 December 2017.
9. Connected Vehicle Pilot Deployment Program Phase 1 -- Security Management Operating Concept –New York City -- Final Report —May 18, 2016 FHWA-JPO-16-300 https://rosap.ntl.bts.gov/view/dot/31725/Share.
10. SCMS CV Pilots Documentation, https://wiki.campllc.org/display/SCP.
11. IEEE Draft Standard P1609.2.1, Wireless Access In Vehicular Environments (WAVE) – Certificate Management for End Entities, https://standards.ieee.org/project/1609_2_1.html.

6. Study Questions

1. In terms of the security models they enable, what do communications with websites on the internet have in common with V2X communications?
    a) The sender's identity is important.
    b) Both parties have access to an online database that they can use to determine what permissions someone has.
    c) <u>An end-user may sometimes interact with a service provider that they have never interacted with before.</u>
    d) Decisions need to be made in less than a tenth of a second.

2. Which of the following is not a security functional requirement for the system?
    a) There must be a way of determining that devices are valid before they are issued with credentials.
    b) If devices send bad data, the damage they do to the system should be detected and mitigated.
    c) Credentials should identify what a sending device's permissions are.
    d) Devices should be able to use other device's credentials to improve system robustness.

3. Which of the following is not a performance requirement for the security system?
    a) The system must work even if devices have very limited connectivity to the internet.
    b) The system must work even when channels are congested and there is limited capacity for each participant.
    c) The system must work for broadcast messages.
    d) The system must minimize power consumption when the vehicle is running.

4. Which of the following statements about privacy is not true?
    a) There are many ways to track drivers on the road.
    b) To preserve privacy, consideration must be given both to how data is created and transmitted, and also to how it is stored and managed.
    c) Protecting privacy uses both technological and policy approaches.
    d) The V2X system must always completely protect the anonymity of drivers.

5. Digital signatures should be used when
    a) We want to prevent an eavesdropper from learning the message.
    b) We want to protect the data from machine or communication errors.
    c) We want to be sure that the message came from the right sender.
    d) Both b and c apply.

6. Message authenticity and confidentiality are distinct features, so combining them won't be useful/practical
    a) True
    b) False

7. Which of the following is good practice for a CA?
    a) Share its private key with the authorities to assist with legal investigations of hackers.

b) Issue certificates to anyone who pays a fee.

c) Require end entities to submit a copy of their private key before receiving a certificate.

d) <u>Ensure that certificate requesters meet minimum standards for security and are entitled to the requested certificate.</u>

8. What type of end entities can request certificates from the SCMS?

a) Vehicle onboard units.

b) Roadside units.

c) Aftermarket safety devices.

d) <u>All of the above.</u>

9. To get the authorization certificates it uses to sign messages, the end entity contacts the …

a) Root CA.

b) Enrollment CA.

c) Authorization CA.

d) <u>RA.</u>

10. If an RSU wants to send both signed SPaTs and signed WAVE Service Announcements …

a) It needs one certificate for SPaT and one certificate for WSA.

b) It must use the same certificate to sign both messages.

c) <u>It can do either a or b.</u>

d) A device is not allowed to run two applications, so this situation does not arise.

11. How long does it take to revoke a device after the first report of its misbehavior?

a) One week.

b) It depends on how bad the misbehavior is.

c) It depends on whether it's reported by an ordinary vehicle or a police car.

d) <u>Currently there is no well-defined answer to the question.</u>

12. The activities that the SCMS Manager is responsible for include:

a) <u>Defining and updating the certificate policy.</u>

b) Approving requests to create intermediate CAs.

c) Updating IEEE 1609.2.

d) Defining functional safety requirements for new cars.

13. Which of the following statements about certification labs is true?
    a) The system design only allows there to be one certification lab.
    b) <u>There may be multiple certification labs and the SCMS Provider indicates which labs are acceptable for security certification.</u>
    c) There may be multiple certification labs and the device provider decides which labs are acceptable for security certification.
    d) There may be multiple certification labs and any lab that is accredited by a third-party accreditation body is acceptable.

14. Which of the following is true?
    a) A deployment manager should never run an SCMS or an SCMS component.
    b) <u>A deployment manager should run an SCMS component only if they have experience at operating a PKI and secure provisioning.</u>
    c) A deployment manager should run an SCMS component if they have a secure facility to host it.
    d) A deployment manager should in general plan on operating a full instance of the SCMS.

15. What is the minimum number of root CAs that must be supported in a deployment?
    a) Zero.
    b) <u>One.</u>
    c) Two.
    d) All existing root CAs.

16. If a deployment wants to use centrally generated messages…
    a) <u>… the deployment manager should work with the SCMS provider to understand requirements for signing centrally.</u>
    b) … the messages should be generated on an air-gapped server at the Traffic Management Center.
    c) … it should instead sign the messages on the RSUs.
    d) … it should distribute the messages to an app on participants' phones.

17. Which of these is not a characteristic of secure boot?
    a) If a device boots successfully it means any changes were carried out through an authorized mechanism.
    b) If a device boots successfully it means that all access control mechanisms will function as intended.

c) If a device has been tampered with then some security-critical code will not run.

d) <u>If a device has been tampered with then a network security center will be alerted.</u>

18. Which of these is a way of assessing the security of hardware security modules?

a) Common Certification Protection Policy.

b) ISO 26262.

c) AES.

d) <u>FIPS 140.</u>

19. Which of these is true of OmniAir certification?

a) Suppliers are required to demonstrate OmniAir certification before they can ship devices.

b) Deployment sites with USDOT funding have a flowdown requirement from DOT to require OmniAir certification for any device included in their deployment.

c) SCMS operators have all signed up to a policy that requires OmniAir certification before devices can be issued with certificates.

d) <u>There is no regulatory or policy requirement to use OmniAir certification, but it has become informally established as industry best practice and individual deployment sites that choose to require it will have access to the widest range of correct implementations.</u>

20. Which of these issues can be addressed by revocation?

a) An attacker jamming the channel with white noise.

b) An attacker replaying previously sent messages.

c) An attacker creating messages with random signatures that do not verify and attaching someone else's certificate to the message.

d) <u>An attacker creating fake messages and signing them with a valid but compromised certificate.</u>

21. Which of these is a correct statement about data collection and management?

a) Only vehicles can produce personally identifying information.

b) Individuals must give consent to their data being collected.

c) If there is concern that data may reveal driver behavior that violates the law, it should be immediately shared with law enforcement.

d) <u>Data must be managed in a manner consistent with local data protection regulations.</u>

7. Icon Guide

The following icons are used throughout the module to visually indicate the corresponding learning concept listed out below, and/or to highlight a specific point in the training material.

1) **Background information:** General knowledge that is available elsewhere and is outside the module being presented.

2) **Tools/Applications:** An industry-specific item a person would use to accomplish a specific task, and applying that tool to fit your need.

3) **Remember:** Used when referencing something already discussed in the module that is necessary to recount.

4) **Refer to Student Supplement:** Items or information that are further explained/detailed in the Student Supplement.

5) **Example:** Can be real-world (case study), hypothetical, a sample of a table, etc.

6) **Checklist:** Use to indicate a process that is being laid out sequentially.