LESSONS LEARNED: SECURITY AND PRIVACY IN SAFETY PILOT MODEL DEPLOYMENT

André Weimerskirch, Scott Bogard, Debby Bezzina
University of Michigan Transportation Research Institute
2901 Baxter Road
Ann Arbor, MI 48109
+1-734-936-1046, andrewmk@umich.edu
+1-734-936-1069, sbogard@umich.edu
+1-734-763-2498, dbezzina@umich.edu

Abstract: Safety Pilot Model Deployment successfully demonstrated field-operational testing of connected vehicles. The Model Deployment comprises over 2,800 vehicles equipped with dedicated short range communication on-board units, 32 road-side units to establish communication to IT infrastructure, and several servers and a backbone network to store and evaluate test results. The demonstration of cyber-security and privacy for connected vehicles was a major objective of Model Deployment. This technical paper will provide an overview of the cyber-security and privacy design and the security concept of operation, and an evaluation of the results of Safety Pilot Model Deployment in terms of security performance.

Keywords: safety pilot model deployment, cyber-security, privacy, vehicle-to-vehicle communication, vehicle-to-infrastructure communication

OVERVIEW

Safety Pilot Model Deployment (MD) successfully demonstrated vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication safety applications in Ann Arbor, Michigan. More than 2,800 vehicles were equipped with on-board units (OBU) and 32 road-side units (RSU) were deployed to gather results for potential deployment in the USA. There are several types of OBUs including vehicle awareness devices (VAD) that only broadcast but do not receive; aftermarket safety devices (ASD) for passenger vehicles using audible warnings to the driver, that broadcast and receive messages; retrofit safety devices (RSD) for commercial trucks and transit that use a display for visual and audible warnings to the driver and that are connected to the vehicle's data bus; and integrated safety devices (ISD) that are connected to the vehicle's CAN and that are fully integrated in the vehicle to provide haptic, visual and audible warnings. This article will focus on VAD and ASD since they accumulate to more than 90% of all deployed OBUs. Proper communication security and privacy are considered major requirements for deployment and were therefore thoroughly tested during MD. The MD was conducted by the University of Michigan Transportation Research Institute (UMTRI).

SECURITY DESIGN AND CONCEPT OF OPERATION

V2V communication security requires a supporting Public-Key Infrastructure (PKI) to provide all devices (OBU and RSU) with security credentials that are then used to protect the communication. A PKI called Security Credential Management System (SCMS) for V2V

communications safety applications was deployed. The SCMS design [1], [2] protects privacy of end-users and carefully accounts for the limitations of vehicle electronics (e.g. limited connectivity to IT infrastructure, limited communication bandwidth, and limited in-vehicle computing resources) and safety applications (e.g. computational delay, channel congestion, and availability). OBUs and RSUs were loaded with security software and security credentials. The security services include the enrolment of new OBUs, the request for security credentials, download of security credentials by wire or over-the-air, sending of misbehavior reports, and download of certificate revocation lists (CRL). Note that automatic detection of vehicle misbehavior, both due to defects and malicious acting, was not implemented but the mechanism to send misbehavior reports with test data was implemented. CRLs were implemented to allow revocation of misbehaving OBUs if misbehavior is detected manually, by informing all devices of the revoked device. The security of MD comprises three main pillars:

1. *Communication security of V2V and V2I connections*: communication security between on-board units and between on-board unit and road-side unit was implemented based on an interim version of the IEEE 1609.2 standard [3]. Interoperability of devices was tested and ensured in various interoperability tests before start of MD. The implemented services include single-hop broadcast of basic safety messages (BSM) by OBUs, single-hop broadcast of Signal Phase and Timing (SPaT), Traveler Information Message (TIM), and Geometric Intersection Description (GID) messages by RSUs, and encrypted communication between OBU and SCMS via RSUs to update security credentials, send misbehavior reports, and download CRLs.
2. *Security Credential Management Server (SCMS)*: The SCMS [1] provides all security services that are necessary to support secure V2V and V2I communication. The SCMS consists of a Certificate Authority (CA) to issue certificates, a Registration Authority (RA) to receive, expand and shuffle requests before forwarding to the CA in order to introduce privacy protection, Linkage Authorities (LA) 1 and 2 to generate linkage values in order to enable efficient revocation of nodes, and a Misbehavior Detection Authority (MDA) to receive misbehavior reports from OBUs.
3. *Security concept of operation*: VADs and ASDs use one certificate per 5-minute interval and require 288 certificates per day, i.e., 105,120 certificates per year. The 5-minute certificates are also called pseudonym certificates since they do not include any real-world identifiers that could identify the sender device or the device owner, and since the frequent certificate change protects devices and device-owners against tracking.
   A Local Certificate Distribution System (LCDS), consisting of several server instances, bootstraps and requests certificates on behalf of VADs. The LCDS requests these ahead of time and once the certificates are available they are loaded to a removable drive (e.g. SD Card) and insert to the VAD. Certificates are encrypted on the removable drive using a global VAD encryption key. Certificates worth 2 years were loaded. The security credentials on the removable drive are not linked to the VAD so that VADs security credentials can easily be updated by replacing the removable drive. Note that in a deployment scenario, there has to be a strong security link between any device and security credential, and it must not be possible to interchange certificates.
   ASDs were enabled to connect over-the-air via RSU to the SCMS in order to request and load certificates, request a CRL, and report misbehavior. ASDs ran bootstrap at suppliers' location before shipping and bootstrap was protected with a device specific password that

was distributed by encrypted email. ASDs requested certificates worth 3 months and ASDs were able to switch to a fall-back certificate if they ran out of 5-minute pseudonym certificates. ASDs requested and eventually downloaded certificate batches from the SCMS, each worth one month, that were encrypted. ASDs then requested the corresponding decryption key from the SCMS.
RSEs received certificates worth one year. To protect devices physically, standard security means were implemented, including physical access control and hard-disk encryption of all SCMS components and of LCDS, and tamper evident seals as well as regular visual inspection for OBUs and RSUs. CRLs were limited to OBUs and were generated weekly.

Figure 1 provides an overview of the functional partitioning of the SCMS. The figure describes the individual components of the SCMS (explained in detail in [2]), the LCDS to provision certificates to VADs, and the remaining devices, such as ASD, that communicate with SCMS via RSU. The SCMS runs on several physical servers. There are SCMS instances to serve VADs (via the LCDS), an instance to issue RSU certificates, and an instance to serve the remaining devices that connect by Internet, typically via RSU.

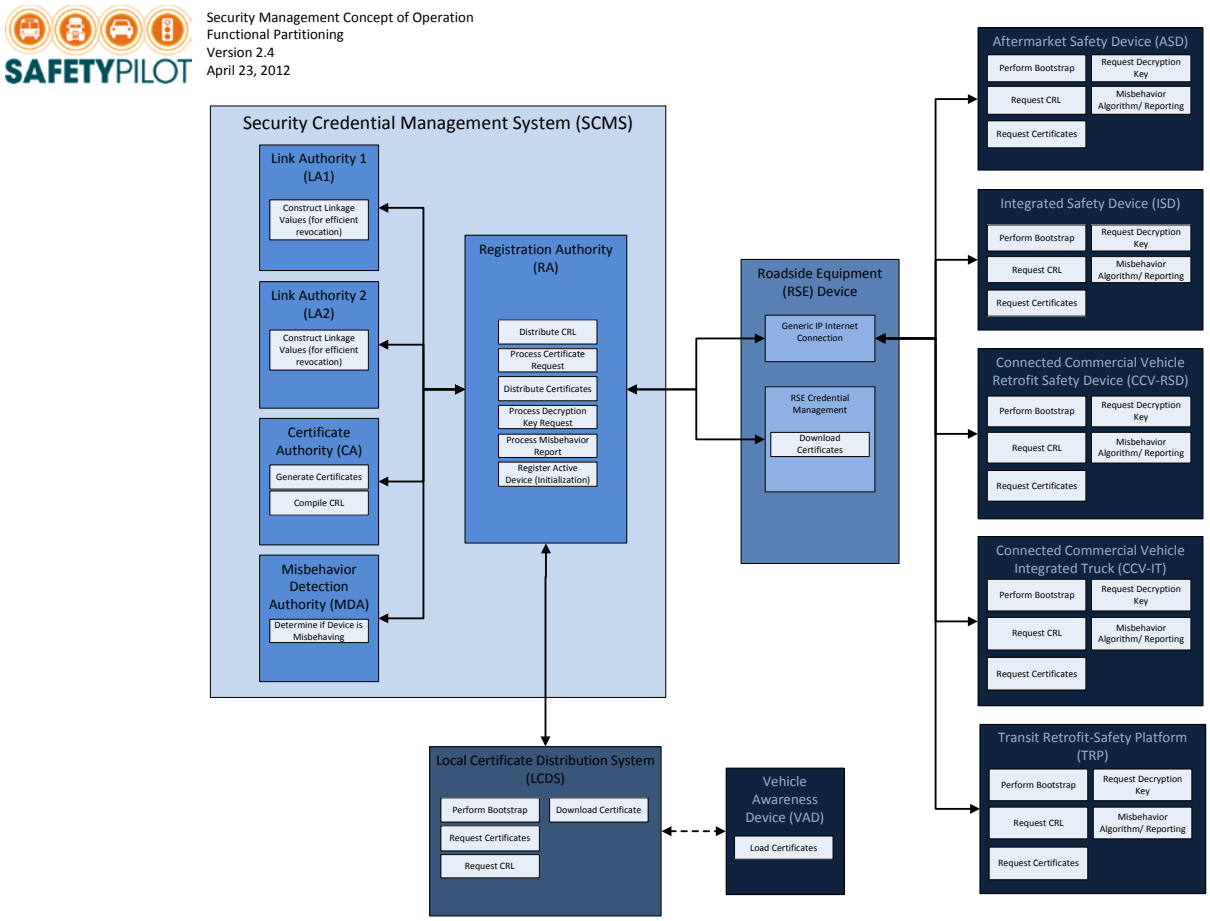

Figure 1: Functional Partitioning of the SCMS

RESULTS

MD ran August 2012 – August 2014, with millions of trips, around 25 million miles driven, and billions of messages broadcast over-the-air. A wide variety of data was collected during MD, comprising V2V over-the-air broadcast messages as well as V2I messages. VADs do not communicate over-the-air with the SCMS and therefore we focus on ASDs here. Note that there were 319 vehicles deployed with ASDs that were provided by three suppliers. We analyzed the SCMS protocol files ranging from February 2013 to mid-April 2014. Obviously faulty sessions were excluded (e.g. sessions in which the ASD requested certificates dozens of times within a short time period). The results are summarized below:

1. The SCMS registered the bootstrap of 381 ASDs overall. Bootstrapping an ASD after the initial bootstrap is comparable to a hard-reset. Repeated bootstraps which account for the difference of 381 ASDs and 319 deployed vehicles were likely performed to test a device before it was eventually deployed in MD.
2. The ASDs established 1,383 sessions with the SCMS of which 940 (68%) were executed successfully. A session can include bootstrap, request of certificates, repeated request to download of certificates, the actual download of certificates, request of the encryption key, and download of the encryption key. Sessions are not successful if the ASD eventually gives up after repeatedly trying to pick-up the session (e.g. if the ASD gives up after repeatedly trying to download certificates). This might happen if the ASD leaves the transmission range of an RSU, if the connection is faulty, or if time-outs occur.
3. 600 of the 940 sessions targeted the renewal of security credentials (i.e. request and download of new certificates to replace certificates that will expire soon). Out of these 600 certificate renewal sessions, 500 sessions (83%) were executed in time so that ASDs always had access to security credentials without a gap, and 100 sessions were executed after the last valid certificate had already expired (in which case the ASD should have switched to using the fall-back certificate). The average gap length, i.e. the time an ASD had to use a fall-back certificate if it were turned-on, was around 946 hours (39.41 days) and the median gap length was around 329 hours (13.7 days). Note that this statistic is blurred since some ASDs were used temporarily for testing without being installed in a vehicle. The significant difference between average and median gap points to a few ASDs that highly contributed to these errors. In fact, the maximum gap was around 5,158 hours (214.9 days), and there were 9 cases of gaps of more than 3,000 hours, 3 cases of gaps of more than 4,000 hours, and one case of a gap of more than 5,000 hours.

No problems with security of V2V and V2I communications during MD are known. The security layer did not disturb communication, i.e., all devices were able to use a security certificate (either 5-minute or fall-back certificate) to sign broadcast messages and all receiving devices were able to verify incoming messages. Future work will include the analysis of recorded over-the-air broadcast messages and match those results to the results presented in this work that were gained from the SCMS protocol files.

CONCLUSIONS

Cyber-security and privacy is an essential part of the V2V safety communication system and it was thoroughly tested during Safety Pilot Model Deployment in Ann Arbor, Michigan. A

security server, the SCMS, was deployed to provide security credentials to devices. Security on the communication layer was implemented to authenticate BSMs and infrastructure-originating messages. A security concept of operation defined physical security, security parameters, and security mechanisms to deploy. The security layer did not disrupt the V2V and V2I communications applications, and the SCMS was able to provide security credentials to devices. Note that the SCMS is currently refined [2] and that the refined design is much more efficient and less resource and memory demanding. For instance, the refined design requires 1,040 certificates per week instead of 105,120 certificates, thus reducing the memory requirement from 30 Mbyte to less than 150 Kbyte to hold one year's worth of certificates. Also the use of decryption keys for certificate batches was discarded. The smaller memory storage requirement and the discarding of decryption keys allows storing several years' worth of certificates, thus reducing the number of required certificate renewal sessions and the complexity of the SCMS design. Therefore the successful deployment of a very resource demanding SCMS in MD can be considered a strong indicator for the feasibility of the refined SCMS in a real-world deployment scenario.

REFERENCES

[1] Anonymous, "Defensive Publication," [Online]. Available: priorartdatabase.com/pubView/IPCOM000210877D.

[2] W. Whyte, A. Weimerskirch, V. Kumar and T. Hehn, "A Security Credential Management System for V2V Communications," in *Vehicular Networking Conference (VNC) 2013*, Boston, MA, 2013.

[3] IEEE Vehicular Technology Society, "IEEE Std 1609.2-2013: IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," IEEE, 2013.