EDITORS: Rick Kuhn, US National Institute of Standards and Technology, kuhn@nist.gov
Tim Weil, Scram Systems, tweil.ieee@gmail.com

VPKI Hits the Highway

Secure Communication for the Connected Vehicle Program

Tim Weil, *SCRAM Systems*

This article presents a condensed account of the 10-year effort to develop and deploy *vehicular public-key infrastructure* (VPKI) as a security infrastructure for vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) intelligent transportations systems (ITS). Most conversations about future generations of connected vehicles and ITS begin with a litany of statistics for crash avoidance and improving road and driver safety:

> Connected vehicle safety applications could potentially prevent 25,000 to 592,000 crashes, save 49 to 1,083 lives, avoid 11,000 to 270,000 Maximum Abbreviated Injury Scale (MAIS) 1–5 injuries, and reduce 31,000 to 728,000 property-damage-only crashes annually.[1]

Realizing these kinds of safety improvements for the ITS smart highway requires national-level architecture and technologies (http://itsarch.iteris.com/itsarch/). When you look "under the hood" at current US Department of Transportation (USDOT) Connected Vehicle pilot programs—VPKI as an industry proof of concept and academic topic—the design of this secure communication solution has many branches:

- security for ITS automotive systems (smart highways);
- threat vectors and car hacking;
- the complexity and sophistication of a security standard (IEEE 1609 Wireless Access in Vehicular Environments, or WAVE, standards);
- encryption research (elliptic curve cryptography, butterfly keys, and so on);
- privacy impacts and mitigations; and
- the complexity and scalability of VPKI—the USDOT Security Credential Management System (SCMS) Proof of Concept is 550 pages! (See www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf.)

As a practitioner, writer, and sometime educator in the field of vehicular networks, I am here to report on the use of VPKI for the USDOT Connected Vehicle Pilot Deployment Program, now in the design and deployment phase (www.its.dot.gov/pilots). A 2014 *Federal Register* solicitation described an SCMS designed as a VPKI system to provide a secure communication system for three national Connected Vehicle transportation testbeds—the Wyoming I-80 corridor, New York City, and the downtown Tampa Hillsborough Expressway Authority (THEA):

> Pilot deployments shall make appropriate use of the latest ITS standards for trusted information exchange. Pilot sites will be expected to connect to an SCMS. The SCMS encompasses all technical, organizational, and operational aspects of the V2V security system that are needed to support trusted, safe/secure V2V communications and to protect driver privacy appropriately.[2]

Only a few years ago (2011), I was a contributing author to the

 Published by the IEEE Computer Society

seminal paper, "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards, and Solutions" for *IEEE Communications Surveys & Tutorials*.[3] At the time of that study, Dedicated Short-Range Communication (DSRC; IEEE 802.11p) seemed like the only game in town, and research was focused on prototypes and trials for the WAVE protocol stack.[4] For US-based programs, the Connected Vehicle pilot programs were still emerging, and much of the research had developed from the earlier USDOT Vehicular Infrastructure Integration (VII)/Intellidrive programs. Fast-forward five years to a 2015 *Wall Street Journal* article, "Automakers Tackle the Massive Security Challenges of Connected Vehicles," and the validation that SCMS in the automotive industry presents large-scale challenges and opportunities:

> During the first year that new vehicles are equipped with communications technology, the security credential management system (SCMS) will only need to scale to a few million equipped vehicles. That will require roughly 30 high-end servers and is comparable to the scale of existing IT systems. But 25 years after connected cars are mandated, there will be roughly 300 million equipped vehicles on the road, according to an August 2014 NHTSA report.[1] "When it is fully operational, this PKI system will be the largest in the world in terms of the number of certificates generated per year and the number of equipped devices," [says] Dr. Mike Shulman (technical leader in Ford's Active Safety Research Department).[5]

What makes this activity exciting is the convergence of government, industry, and academia in bringing the promise of vehicular networks as ITS into the reality of the 21st century.

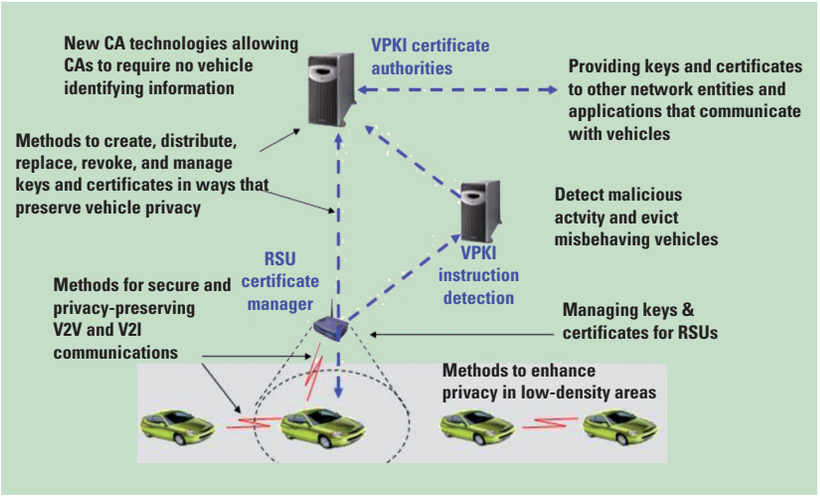

Figure 1. Vehicular public-key infrastructure (VPKI) certificate authority model.

VPKI Principles: Contributions in Research

At the 2007 IEEE GLOBECOM Symposium on WAVE, Tao Zhang (then with Telcordia) presented his vision on "Technologies for Privacy Preserving Vehicular Communications for VII" to examine basic VPKI challenges and solutions, including

- which certificates to use and how,
- how to determine which certificate should be revoked,
- how to replace an expired or revoked certificate (rekey),
- how to distribute certificate revocation lists to vehicles,
- how to determine which certificate requests should be accepted or rejected, and
- how to eliminate any single entity with sufficient information for vehicle tracing.

For the USDOT VII/Intellidrive program (2006–2009), Telcordia, in partnership with Raytheon, Booz Allen, and USDOT, developed a prototype certificate authority (CA) manager component to the VII program (see Figure 1 based on the emerging WAVE security standard (IEEE 1609.2; http://ieeexplore.ieee.org/document/7426684).

As a project manager, I was given the job of making sure it all worked. Our efforts generated a significant volume of reporting that validated the operability of this privacy-preserving VPKI solution based on IEEE 1609.2 in conjunction with field trials using on-board equipment (OBE), roadside units (RSUs), and digitally signed application, safety, and low-level system messages.[6]

As an occasional contributor to the IEEE Working Groups on WAVE standards, I later developed a series of IEEE GLOBECOM seminars (from 2007–2009) on the topics of WAVE security and providing secure communication of managed services. In conjunction with Luca Delgrossi (Mercedes Benz R&D), Zhang (now with Cisco) went on to publish *Vehicle Safety Communications—Protocols, Security, and Privacy*,[7] with significant research in VPKI addressing many of the topics he presented back in 2007—including cryptographic mechanisms, PKI for vehicular networks, privacy protection with shared certificates, and IEEE 1609.2 security services.

The Road to SCMS

In 2006, USDOT joined together with a partnership of automotive

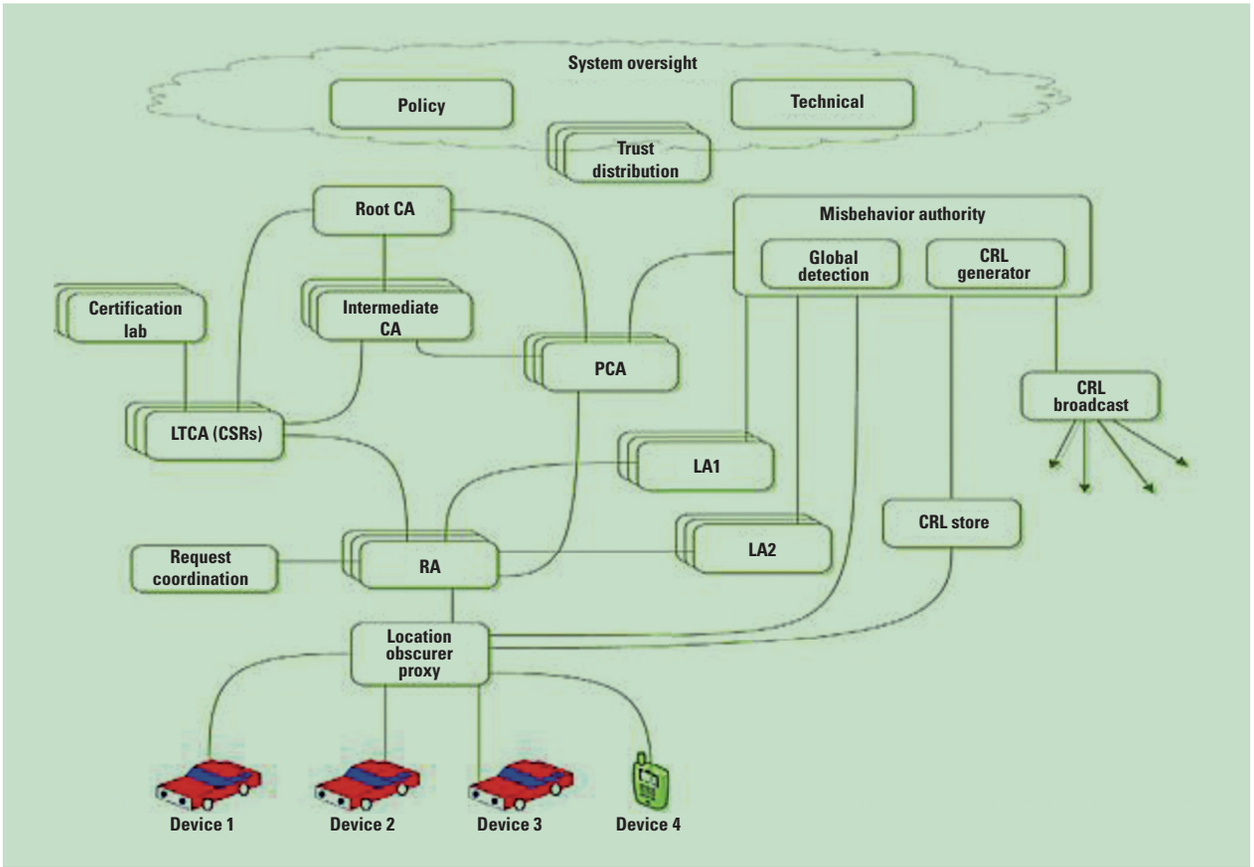

Figure 2. Security credential management system deployment model (see http://tinyurl.com/jozqn4l).

manufacturers, the Crash Avoidance Metrics Partnership (CAMP), to develop and test prototype V2V safety applications (CAMP includes Ford, General Motors, Honda, Hyundai-Kia, Volkswagen, Mercedes-Benz, and Toyota). At that time, the overarching goal was to determine whether this technology would work better than existing vehicle-based safety systems, such as adaptive cruise control, to address imminent crash scenarios. The CAMP consortium continued to oversee work on the SCMS/VPKI security infrastructure through the 2013 Connected Vehicle Safety Pilot.

Coincident to the VPKI research of that era (federal and academic articles on vehicular ad hoc networks and PKI), a formal model of the SCMS system (Figure 2) was developed by USDOT partner Security Innovations (www.securityinnovation.com/products/aerolink/automotive-v2v-resources) in what would become the Connected Vehicle Safety Pilot program (www.its.dot.gov/pilots/pdf/TechAssistWebinar_Template_SCMSIIv4.pdf).[8,9]

Beginning in 2014 with the Connected Vehicle Safety Pilot program in Michigan,[10] USDOT began supporting, contracting, and deploying the SCMS as the de facto security infrastructure solution. As noted in the 2014 National Highway Traffic Safety Administration (NHTSA) report, *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*,

> Eleven years of research (that is, examination of different security approaches, technical architecture and configuration decisions, testing of prototypes, and development of an operational and organizational structure) have resulted in the current security design concept for a V2V system (SCMS). Between 2015 and 2016, CAMP worked in support of the Department of Transportation (DoT) to create a proof-of-concept SCMS. The CAMP team included a number of subcontractors. Green Hills Software was responsible for developing the system, while Security Innovation provided protocol-level support to mature the IEEE 1609.2 specification. Leidos provided independent test and evaluation of the system, including functional and security testing. The proof-of-concept was successfully developed and ready for use in pilot deployments.[1]

Since the 2014 USDOT Safety Pilot, aftermarket safety device (ASD) manufacturers who have developed SCMS PKI technology

include companies such as Thales Security for Connected Vehicles[11] and Leidos (http://modot.org/team/2015/documents/02ConnectedVehicles_000.pdf), both of which have partnered with USDOT on this SCMS VPKI solution. In 2016, Green Hills began offering a managed V2X certificate solution (http://finance.yahoo.com/news/integrity-security-services-delivers-certificates-213400792.html).

Table 1. Certificate types for testing.

Issued to	Certificate name	Purpose
OBU*/ASD	Enrollment	Initializes the OBU to allow communication with the SCMS
OBU/ASD	Pseudonym	Used to sign all basic safety messages generated by an OBU
OBU	Authorization	Used to identify public sector vehicles for specific apps
RSU	Enrollment	Initializes the RSU to allow communication with SCMS
RSU	Application	Used to sign messages generated by the RSU

**OBU: onboard unit; ASD: aftermarket safety device; RSU: roadside unit; SCMS: Security Credential Management System*

Secure Communication for the Connected Vehicle Pilot

The complexity and requirements of the VPKI systems developed for the current Connected Vehicle Pilot go well beyond the scope of this article. A good summary of SCMS functionality is given in a recently published Cloud Security Alliance white paper on "Observations and Recommendations on Connected Vehicle Security" (available via http://bit.ly/2hkZf1Q):

> SCMS is a tailored public-key infrastructure (PKI) that is designed to provision PKI certificates to vehicles and infrastructure. The tailoring of the SCMS is focused on implementing robust privacy controls that guard against both message manipulation and casual tracking of vehicles (and by extension their owners) by outsiders. This includes tracking by potentially rogue insiders that operate components of the SCMS itself (for example, the insider threat). The SCMS employs components such as location obscurer proxies (LOPs) that shield vehicle identities from PKI components and by extension operators. Vehicles themselves employ a concept of rotating certificates taken from a pool, and then used to digitally sign messages.

In the USDOT briefing, "Preparing a Security Operational Concept for Connected Vehicle Deployments" (http://bit.ly/2gugD84), specific certificate types to be tested were given (see Table 1).

In the current Connected Vehicle Pilot, the SCMS use cases to be trialed and some of the test criteria include the following:

- *Bootstrapping of an OBU/ASD device*. This involves initializing and enrolling an OBU/ASD device with SCMS certificates, and preventing the SCMS from issuing certificates to unauthorized devices.
- *Provisioning of certificates*. These include pseudonym certificates issued by in-vehicle devices transmitting basic safety messages; pseudonym certificate requests for devices requesting ECC Butterfly Seed Pairs and start/end times for certs; application certificates issued by devices transmitting infrastructure messages (Traveler Information Message, Signal Phase and Timing, MapData, and so on; see www.sae.org/events/ces/2016/attend/program/presentations/misener.pdf); and the creation and verification of digital signatures for application message signing.
- *Misbehavior detection*. This involves bad actor detection and reporting; and Location Obscurer Proxy (LOP) and Global Detection System (GDS) SCMS misbehavior components.
- *Certificate revocation list (CRL) distribution*. This requires the CRL request and response with the most current CRL; it allows a maximum of 10,000 CRL entries (40 bytes each).

GLOBECOM 2015: Tie-In to Future Trends

With more than 10 years of development and research, VPKI could one day "hit the highway" as a viable solution for secure vehicular communications. Alternatively, through the rearview mirror of the technology industrial age, VPKI might be seen as the first generation of secure communications for ITS (vehicular networks). Who knows? I'm glad to have a seat at the table watching these sophisticated (and complicated) solutions evolve.

Recently, I had the opportunity to moderate a Vehicular Networks Industry Workshop at IEEE GLOBECOM 2015, surveying current opportunities and challenges with vehicular networks. Presentations described the near-term opportunities for deployment, not only with DSRC but also with evolving concepts in Long-Term Evolution (LTE) and spectrum sharing across unlicensed technologies, up to and including 5G. Other topics included network security and privacy issues, current research in network simulation, vehicular cloud computing, and vehicle telematics.

The challenges and opportunities for security architectures in this field remain (as Zhang suggested) beyond "the firewall garden" are heading quickly toward a model based on ubiquitous communication structures as presented by the Internet of Things. An excellent discussion on this topic is the research on "The Fog Computing Paradigm: Scenarios and Security Issues,"[12] which analyzes threats and defenses in a mixed-mode vehicular network communication system. IT

References

1. J. Harding et al., *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*, report no. DOT HS 812 014, US Nat'l Highway Traffic Safety Administration, Aug. 2014; www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf.
2. "Vehicle-to-Vehicle Security Credential Management System; Request for Information," *Federal Register*, vol. 79, no. 199, 2014; http://bit.ly/2heuRZW.
3. G. Karagiannis et al., "Vehicular Networking: A Survey and Tutorial on Requirements, Architectures, Challenges, Standards, and Solutions," *J. IEEE Comm. Surveys & Tutorials*, vol. 13, no. 4, 2011, pp. 584–616.
4. "Intelligent Transportation Systems Fact Sheet for WAVE Standards," US Dept. of Transportation Research and Innovative Technology Administration, Jan. 2006; www.standards.its.dot.gov/factsheets/factsheet/80.
5. R. King, "Automakers Tackle the Massive Security Challenges of Connected Vehicles," *Wall Street J.*, 25 June 2015; http://on.wsj.com/1SP9FEb.
6. R. Kandarpa, *Final Report: Vehicle Infrastructure Integration (VII) Proof of Concept (POC) Test—Executive Summary*, tech. report, US Dept. of Transportation, IntelliDrive (SM), 2009.
7. T. Zhang and L. Delgrossi, *Vehicle Safety Communications: Protocols, Security, and Privacy*, Wiley, 2012.
8. *Final Report: Vehicle Infrastructure Integration Proof-of-Concept Executive Summary—Infrastructure*, US Dept. of Transportation, Feb. 2009; http:/ntl.bts.gov/lib/31000/31000/31078/14481.pdf.
9. 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/.
10. Connected Vehicle Infrastructure Deployment Considerations: Lessons Learned from Safety Pilot and Other Connected Vehicle Test Programs, US Dept. of Transportation, 30 May 2014; http://bit.ly/2hHlbEf.
11. *Securing the Connected Vehicle*, Thales E-Security white paper, Aug. 2016; http://bit.ly/2het0Ej.
12. I. Stojmenovic and S. Wen, "The Fog Computing Paradigm: Scenarios and Security Issues," *Proc. 2014 Federated Conf. Computer Science and Information Systems*, 2014, pp. 1–8; http://annals-csis.org/Volume_2/pliks/503.pdf.

Tim Weil *is a network project manager at SCRAM Systems. His interests include service management for vehicular networks and vehicular public-key infrastructure. In the areas of vehicular networks, his work includes the IEEE 1609 (WAVE) standards, USDOT VII/Intellidrive, and Connected Vehicle programs, and he's an author and speaker on topics in security for vehicular networks (IEEE GLOBECOM). Weil is an industry-certified security professional (CISSP/CCSP, CISA, PMP) and past chair of the IEEE Denver Communication Society chapter. He's a senior member of IEEE and a Securing IT editor for IT Professional. Contact him at tweil.ieee@gmail.com.*