Standards Integration Review Workshop – Security

Workshop Summary

5 October 2016
Ann Arbor, MI

Workshop Introduction

CVTA's Standards Integration Review Workshop was held on 5 October 2016 in Ann Arbor, Michigan. The workshop was intended to consider end-to-end security standards integration for the connected vehicle ecosystem:

- What standards are already available/in progress across the ecosystem?
- Where are the gaps and opportunities for collaboration in development, demonstration, testing of these standards?
- What should we be doing to ensure that our standards suite is sufficient to enable our ecosystem?

There were 30 attendees, which included key experts from AUTOSAR, GENIVI, IEEE, SAE, and 3GPP, along with a cross-cutting group from OEMs, Tier Ones, Security, Testing, and Privacy specialists, Consumer Electronics firms, Infrastructure Owner/Operators, and Universities.

The event was organized in two parts. First, the group collaborated to build a picture of current standards activities. The exercise sparked a lot of good discussion, and it was clear that there were opportunities to improve the conversation and process around standards development in this area. In particular, there is a lot of fragmentation as each industry sector (e.g., automotive OEMs, telecoms, etc.) focuses on their own issues without always having the opportunity to integrate across sectors.

Next, the group talked about ways to address these challenges, and identified a small set of focus areas which we can build on:

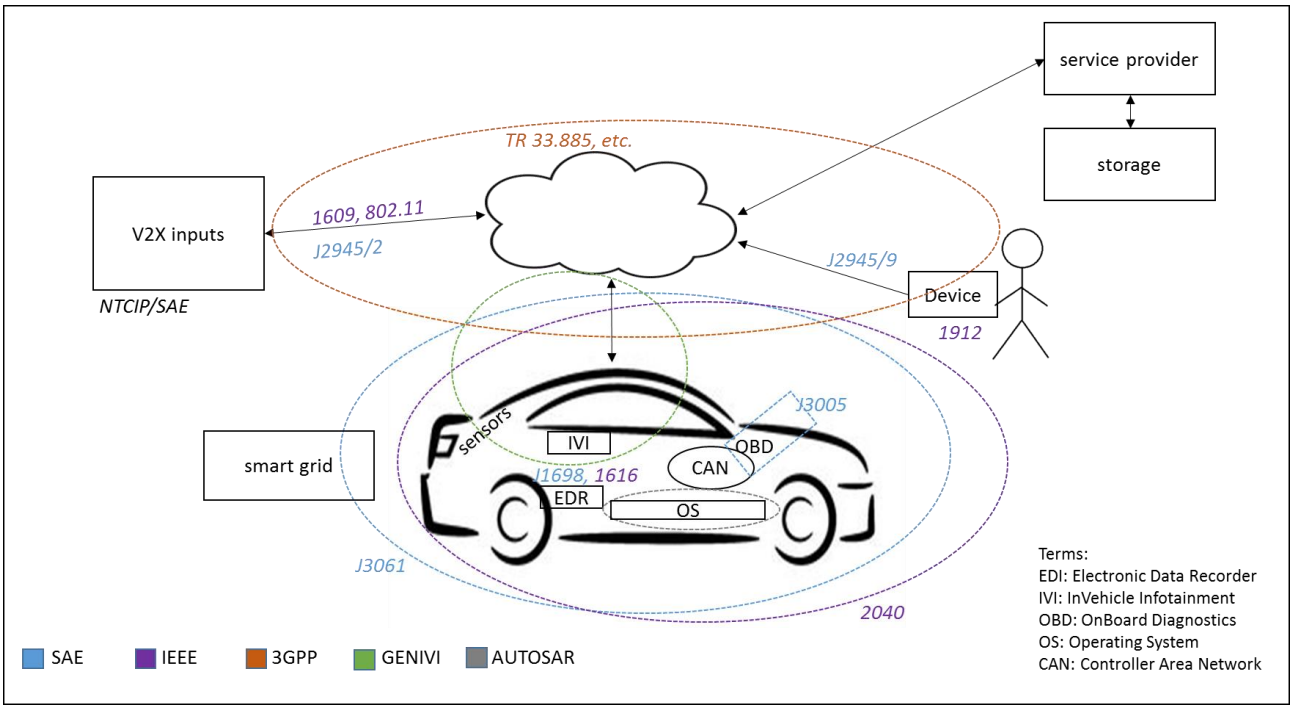
- Develop a System/Holistic Perspective.
- Share Hazard and Risk Assessments.
- Run a Cross-SDO Use Case "test".
- Develop Shared Terms and Definitions.

A more detailed summary of results from these discussions is included below. This summary is a collection of highlights which does not necessarily represent consensus of all attendees at the workshop. This document also includes a Resource section with materials contributed by the participants.

Workshop Results

Part One: Standards Activities Review

The group started with a picture of the basic V2X infrastructure on a whiteboard, starting from basic sensors and working outwards within the vehicle, across the airlink, and to the services/databases beyond. Each participating SDO then built on that picture to explain where their security efforts are currently focused. The resulting picture was quite complex. A summarized version is shown below:



Specific highlights from each SDO include:

- GENIVI's security efforts are focused on telematics data coming into and out of the car which flow through the in-vehicle infotainment (IVI) middleware. This includes car to cloud and sensor to cloud interactions. The goal is to prevent malware from coming in and creating issues at the middleware level. Efforts include encryption and parsing, as well as secure software updates.
- IEEE's activities cover a range of items, from electronic data recorders (EDR) and DSRC communications standards to consumer device privacy and connected vehicle

architecture. The device privacy effort is working to develop templates for standards on access, storing and sharing of consumer IoT data. The DSRC technology standards include digital certificate mechanisms for permissions and privacy, credential management solutions, etc. This set of security services can be applied at any level.

- 3GPP standards focus on securing the connection into the cellular radio network from the vehicle/device and the application servers; and between radio network components. This includes work on replay protection, authentication, confidentiality, privacy, tracking, etc. The PROSE standard was noted as an example of peer to peer cellular security that is being handled by this group. For more detail on 3GPP connected vehicle standards, see Appendix.

- SAE security work covers a broad spectrum as well. Specific items of interest to this discussion include: OBD port security for cars and heavy trucks, recommended practices for designing cybersecurity into the vehicle (which are currently being expanded at the ISO level), and performance requirements for vehicle communications by application area. For more detail on SAE cybersecurity standards, see Appendix.

- AUTOSAR works to standardize in-vehicle systems. A new adaptive platform for a LINUX-based Operating System (OS) is planned for release Q1 2017 and SOA for that platform is in the near term plan. Security efforts in AUTOSAR are currently focused on authentication, and there are additional security features planned for Q4 2017 releases, including crypto interfaces and credential management. They are also working on end to end protection within the vehicle.

Part Two: Opportunity Review

The group discussion highlighted the fact that, while most of the SDOs were aware of some of the work going on in other areas, there had been limited opportunity for cross-SDO discussion of the entire system. As a result, the initial review of standards activities generated a substantial list of items for further discussion. These included:

- Regulatory issues. Each SDO works with in the regulatory boundaries of its industry sector, but these often have conflicting requirements. For example, the telecom community must comply with federal wire-tapping rules, while the DSRC communications system has built-in privacy to avoid identification of users. Similarly, regulations surrounding OBD port access and vehicle data availability (e.g., right to

repair laws) create related challenges. As these technologies come together into a single, connected vehicle environment, these issues will have to be navigated.

- Privacy in managed and peer to peer communications environments
- The current lack of standards focus on detection/mitigation/resilience
- The need to better include the transportation infrastructure owner-operators (IOOs) in security discussions. It was noted that IOOs have to handle unique physical security hazards (e.g., roadside equipment), in addition to public data availability rules.
- The challenges of ensuring both data and functional security in the automotive environment. This was tightly related to another item: security/vehicle lifecycle management. Security management is an ongoing process, but there is currently no way to ensure that individual vehicles are updated over time. In addition, it is currently possible for individuals to modify major vehicle functions. Secondary and tertiary owners have no visibility into these modifications.
- Unintended consequences caused by lack of understanding across major system components
- The need for work on sensor security and associated standards.

Next Steps

During the discussion, quite a number of ideas were put forward for action, and the participating SDOs agreed to consider how they might contribute. Four Key Opportunities rose to the top:

- Develop a System/Holistic Perspective. We need better ways for everyone to think about the whole system when defining security solutions. The group identified a couple of existing standards activities where this discussion might thrive, including SAE's J3061 activity.
- Share Hazard, Threat and Risk Assessments. We should share information about how hazard assessments are handled by each group to help make sure everyone is looking at all of the required perspectives. Both transportation system level (catastrophic) and individual level threats are of concern. This might be initially addressed in a one day workshop which allows key experts to compare notes. This might also fit into the J3061 work effort.

- Run a Cross-SDO Use Case “test”. We need a way to find out whether the set of standards suite we have developed/are developing is actually successful at protecting the end-to-end system. A key first Use Case of interest is over the air software updating (SOTA). This topic sparked some specific discussions about how to achieve this but it is clear that this is a major challenge, as each SDO has a unique perspective on the requirements for such a solution, and the overall system crosses so many standards domains.
- Develop Shared Terms and Definitions. Even within the small group at the workshop, consistent communication was an ongoing challenge. We discussed extending existing standards activities in this area to better serve this need, particularly those activities already underway in ISO and SAE.

This White Paper is intended to serve as a catalyst for those discussions by summarizing the Key Opportunities for further review and action.

Workshop Team

Acknowledgements

Thanks to Steve Crumb, GENIVI; Jack Pokrzywa, SAE; and Jonathan Petit, Security Innovation for their support in establishing this event.

Workshop Chair

Valerie Shuman (SCG, LLC)

Participants

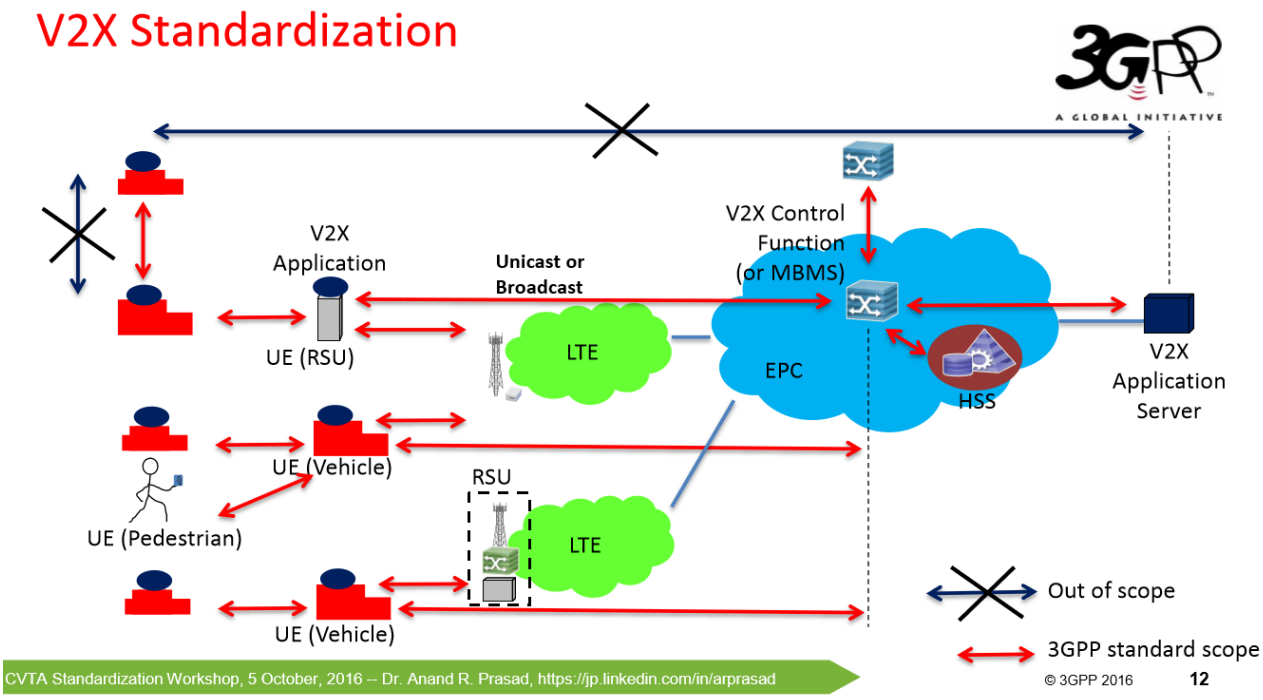
Scott Andrews	Cogenia Partners
Luke Biernbaum	MDOT/ITS Program Office
Benedikt Brecht	VW
Marc Brynczka	SGS Transportation
Matt Clemens	Arxan Technologies
Steve Crumb	GENIVI
Mary Doyle	SAE
Jennifer Dukarski	Butzel Long
Barry Einsig	Cisco
Robert Fust	ESG
John Gonzaga	GM
Bob Gruszczynski	VW
Stacy Janes	Irdeto
Paul Hamburg	VW
Nelson Kelly	Macomb Community College
Ethan Lucarelli	Inmarsat
James J. McCarthy	SGS Transportation
Scott McCormick	CVTA
Jonathan Petit	Security Innovation
Anand Prasad	NEC/3GPP SA3
Kendra Pridemore	UL, LLC
Philippe Robin	Technoveo
Thierry Rolina	Danlaw
Valerie Shuman	CVTA
Mike Stelts	Panasonic
Alessandro Triglia	OSS Nokalva
Mark Vogel	Mitsubishi Electric
Tim Weisenberger	SAE
William Whyte	Security Innovation
Eyad Zeino	Mitsubishi Electric

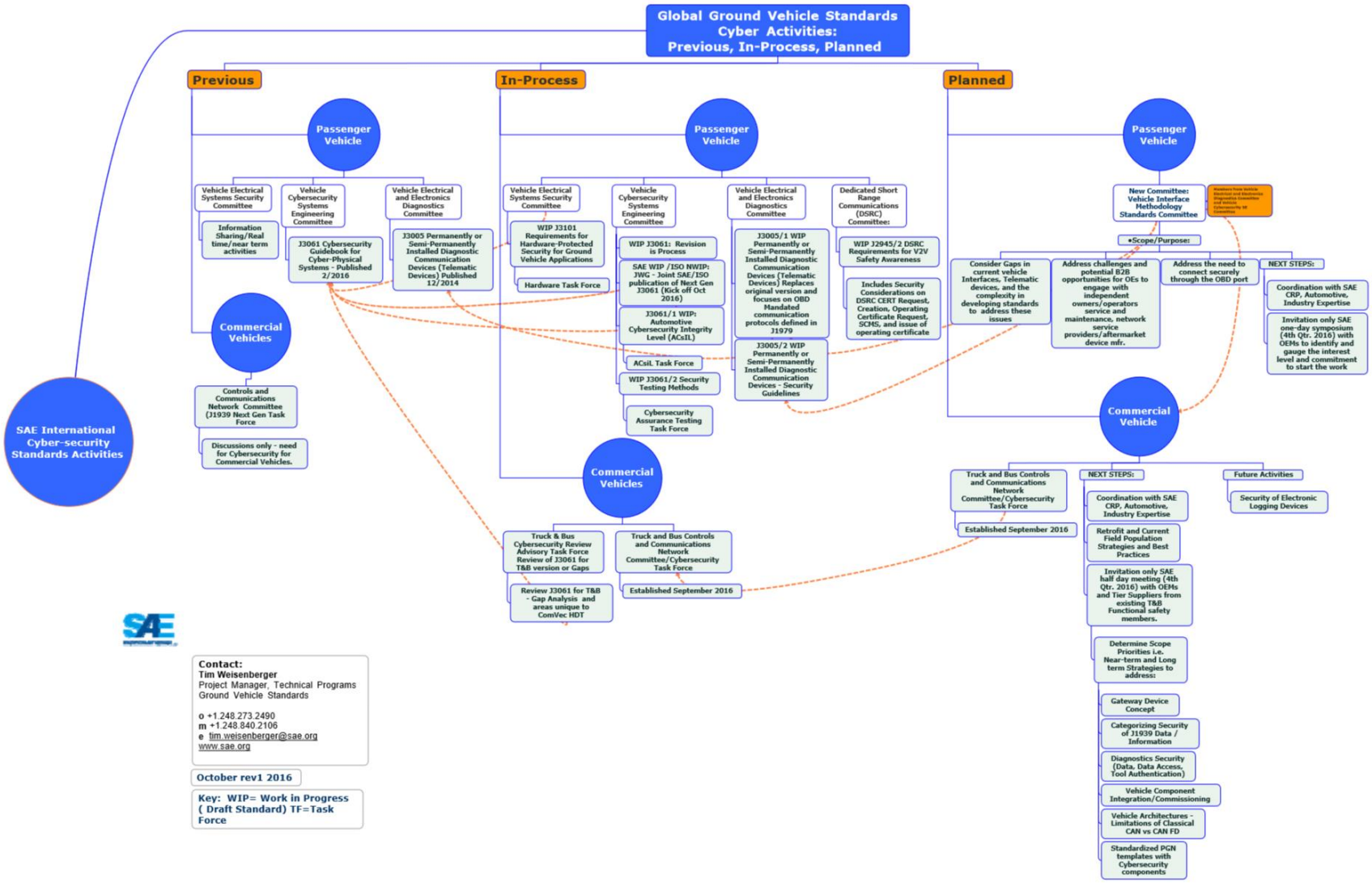
Appendix A: Resources

Resources include:

- http://www.eti-home.org/Telematics/ftp-telematics/Task%20Force/Telematics-Data-Definition-White-Paper-12-10-copy.pdf
- https://www.enisa.europa.eu/topics
- https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-cars
- https://resilience.enisa.europa.eu/carsec-expert-group
- https://asrb.org/

Several participating SDOs provided more detailed views of their activity in the connected vehicle security space – diagrams below:




Global Ground Vehicle Standards Cyber Activities: Previous, In-Process, Planned
SAE International Cyber-security Standards Activities
Previous
In-Process
Planned
Passenger Vehicle
Vehicle Electrical Systems Security Committee
Information Sharing/Real time/near term activities
Vehicle Cybersecurity Systems Engineering Committee
J3061 Cybersecurity Guidebook for Cyber-Physical Systems - Published 2/2016
Vehicle Electrical and Electronics Diagnostics Committee
J3005 Permanently or Semi-Permanently Installed Diagnostic Communication Devices (Telematic Devices) Published 12/2014
Commercial Vehicles
Controls and Communications Network Committee (J1939 Next Gen Task Force
Discussions only - need for Cybersecurity for Commercial Vehicles.
Passenger Vehicle
Vehicle Electrical Systems Security Committee
WIP J3101 Requirements for Hardware-Protected Security for Ground Vehicle Applications
Hardware Task Force
Vehicle Cybersecurity Systems Engineering Committee
WIP J3061: Revision is Process
SAE WIP /ISO NWIP: JWG - Joint SAE/ISO publication of Next Gen J3061 (Kick off Oct 2016)
J3061/1 WIP: Automotive Cybersecurity Integrity Level (ACsIL)
ACsiL Task Force
WIP J3061/2 Security Testing Methods
Cybersecurity Assurance Testing Task Force
Vehicle Electrical and Electronics Diagnostics Committee
J3005/1 WIP Permanently or Semi-Permanently Installed Diagnostic Communication Devices (Telematic Devices) Replaces original version and focuses on OBD Mandated communication protocols defined in J1979
J3005/2 WIP Permanently or Semi-Permanently Installed Diagnostic Communication Devices - Security Guidelines
Dedicated Short Range Communications (DSRC) Committee:
WIP J2945/2 DSRC Requirements for V2V Safety Awareness
Includes Security Considerations on DSRC CERT Request, Creation, Operating Certificate Request, SCMS, and issue of operating certificate
Commercial Vehicles
Truck & Bus Cybersecurity Review Advisory Task Force Review of J3061 for T&B version or Gaps
Review J3061 for T&B - Gap Analysis and areas unique to ComVec HDT
Truck and Bus Controls and Communications Network Committee/Cybersecurity Task Force
Established September 2016
Passenger Vehicle
New Committee: Vehicle Interface Methodology Standards Committee
•Scope/Purpose:
Consider Gaps in current vehicle Interfaces, Telematic devices, and the complexity in developing standards to address these issues
Address challenges and potential B2B opportunities for OEs to engage with independent owners/operators service and maintenance, network service providers/aftermarket device mfr.
Address the need to connect securely through the OBD port
NEXT STEPS:
Coordination with SAE CRP, Automotive, Industry Expertise
Invitation only SAE one-day symposium (4th Qtr. 2016) with OEMs to identify and gauge the interest level and commitment to start the work
Commercial Vehicle
Truck and Bus Controls and Communications Network Committee/Cybersecurity Task Force
Established September 2016
NEXT STEPS:
Coordination with SAE CRP, Automotive, Industry Expertise
Retrofit and Current Field Population Strategies and Best Practices
Invitation only SAE half day meeting (4th Qtr. 2016) with OEMs and Tier Suppliers from existing T&B Functional safety members.
Determine Scope Priorities i.e. Near-term and Long term Strategies to address:
Gateway Device Concept
Categorizing Security of J1939 Data / Information
Diagnostics Security (Data, Data Access, Tool Authentication)
Vehicle Component Integration/Commissioning
Vehicle Architectures - Limitations of Classical CAN vs CAN FD
Standardized PGN templates with Cybersecurity components
Future Activities
Security of Electronic Logging Devices
Contact:
Tim Weisenberger
Project Manager, Technical Programs
Ground Vehicle Standards
o +1.248.273.2490
m +1.248.840.2106
e tim.weisenberger@sae.org
www.sae.org
October rev1 2016
Key: WIP= Work in Progress (Draft Standard) TF=Task Force

Connected Vehicle Trade Association
PO Box 4847, East Lansing, MI 48826
www.connectedvehicle.org

Scott J. McCormick, President
OFC: 734.354.0546
CELL: 734.730.8665
FAX: 734.446.0326
Skype: scott.j.mccormick1
Whats App: Scott McCormick
WeChat: scottm1
sjm@connectedvehicle.org

Valerie Shuman, Vice President of Industry Programs
CELL: 312-972-0220
Skype: vshuman
vs@shumangroupllc.com