Memo on applicability of “Software and OS Security” Document

This memo concerns the “Software and OS Security” document that was provided by the NYC Connected Vehicle Pilot Deployment project to CAMP and subsequently reviewed and edited by the CAMP SCMS POC project.

# Background

**Introduction**. For certificates to be issued to a device, the SCMS must have a guarantee that the device’s implementation is “secure enough” in terms of protecting against hardware attacks, malware, and software-based unauthorized access to keys. It is therefore important to have two things:

1. A definition of the physical, hardware and software requirements that make a device “secure enough”.
2. A certification program so that the SCMS can have assurance that any given device actually meets those requirements.

The main focus of this memo is on step 1, defining the security requirements. We touch briefly on step 2, certification, at the end.

**Need for these requirements**. Defining these requirements is urgent for two reasons. First, the SCMS will be issuing certificates for the Pilot Deployments in the relatively near future. Second, GM is deploying DSRC-enabled vehicles in 2017 and other OEMs may follow suit and deploy before the mandated date. Suppliers must know what the security requirements are early in the development process as the security requirements may significantly constrain or dictate fundamental design choices.

**Device classes**. There will not be one single set of requirements, especially for the Pilot Deployment devices. Requirements may vary according to the type of device (RSE, OBE, ASD and Personal Information Device (PID) operate in different threat environments); they may also vary according to the actions the device is intended to take (a police OBE that can send signal preemption messages is a more high-value target than a standard OBE that can only send BSMs). The V2I Cybersecurity analysis project run by Iteris under contract to FHWA has proposed that there are five “security classes” of device, depending on their Confidentiality, Integrity and Availability requirements, with OBEs falling into the lowest class of these devices, class 1, and other device types falling into higher classes. This approach, of categorizing devices into the FHWA device classes, is the approach that the Pilot Deployments have been asked to follow.

**Current status**. The missing step between defining the device classes based on requirements and issuing certs to those devices is to define the exact set of security properties a device must have to meet the requirements of its class. Currently, there are the following attempts to define security properties:

* SAE J2945/1 section 6.6.5, “Hardware Security”, defines physical security as a profile of Federal Information Processing Standard (FIPS) 140-2.
* The Car2Car Communications Consortium has been developing a potential Common Criteria Protection Profile (PP) for OBEs in the European system. This is not yet published.
* A project carried out by Booz Allen under contract to NHTSA developed a Common Criteria Protection Profile with potential applicability to OBEs in the US system. This has also not yet been published.
* The V2I Cybersecurity project is developing a set of security controls for devices in each class based on NIST Special Publication (SP) 800-53. This has also not yet been published.

None of these approaches meet the needs of the Pilot Deployment or of pre-mandate OBE deployment:

* Since the text in SAE J2945/1 was written, there has been further analysis of the security requirements and the text in SAE J2945/1 is not believed to be complete. For example, it doesn’t address malware protection or access by unauthorized users. Additionally, it only applies to OBEs
* None of the other four approaches are currently public, and of the four only the V2I Cybersecurity project deliverable applies to devices other than OBEs.

**Origin and originally intended use of the “Software and OS Security” Document**. The “Software and OS Security” document was originally developed by the NYC CVPD project to provide a guide to best practices for suppliers to NYC CVPD. It was subsequently provided to and reviewed by the other CV Pilot Deployment sites and to CAMP. It therefore represents the consensus opinion among a wide range of stakeholders as to what security requirements are appropriate for the Connected Vehicle environment.

The Software and OS Security document is not a formal document: it does not follow a standard template for security requirements. However, it provides a readable overview of the security requirements, and it is concrete enough to allow meaningful conformance statements to be made (of the form “This device complies with the requirements in paragraphs A, B and C but not D”).

The intent in NYC CVPD was that this document would be provided to suppliers with the goal that suppliers would attempt to provide devices that completely complied with all of its requirements. However, NYC CVPD understood that given the short timescales it would not be possible to set up formal conformance testing, and it might not even be possible for suppliers to conform with all the requirements in the document. NYC CVPD therefore proposed a conformance approach where suppliers would provide documentation stating, for each requirement in the document, (a) whether or not it was implemented and (b) if it was implemented, an overview of how it had been implemented; NYC CVPD would then take it on good faith that the stated implementation was in fact what the supplier had tried to do and that they had implemented it correctly.

Note that these requirements are the ones that NYC CVPD believe (and other stakeholders also believe) met its security requirements for Pilot Deployment. In other words, a device that meets these requirements is “approved for use in NYC CVPD”. That is not necessarily the same as “approved by the SCMS to receive certificates”. At the moment there is no statement from the SCMS Manager (currently NHTSA) as to what the requirements are to receive certificates IS THIS TRUE, though it is understood that OBEs must comply with J2945/1.

**Device classes and permissions in certificates**. In the 1609.2 security model, permissions are expressed in certificates by indicating what application activities a certificate holder can carry out (for example, “send BSM”, “send SPaT”, “request signal preemption”). These permissions are encoded via Provider Service Identifiers (PSIDs) and Service Specific Permissions (SSPs). Certificates do not directly include the device’s security class. Instead, the application specification identifies what device class is necessary for a device to be allowed to take a particular action, and the SCMS issues a certificate indicating permission to take that action once the SCMS has determined that the device is of the appropriate class. If a device is intended to run multiple applications, its required security level is at least the maximum security level of any of the individual applications.

# CAMP proposal

CAMP proposes two uses of the Software and OS Security document.

First, the text in the document that defines the requirements for Class 1 devices, i.e. OBEs, should be incorporated into J2945/1, replacing the current text in section 6.6.5. This will give a complete set of security requirements for suppliers of OBEs under the mandate to implement to.

Second, CAMP proposes that the document be adopted by NHTSA and formally published as the device security requirements to be conformed to by devices seeking certificates from the SCMS. This will ensure that the security requirements of the SCMS are consistent with the security requirements that are being developed by the Pilot Deployment projects.

# Future work and conformance testing

CAMP considers that in future it will be useful to have a formal security requirements document such as a Common Criteria protection profile for all five of the device classes identified in the V2I Cybersecurity report. This will allow formal conformance testing by existing test labs, for example Common Criteria test labs accredited under NIST’s National Information Assurance Program (NIAP) (see <https://www.niap-ccevs.org/Documents_and_Guidance/cctls.cfm)>

While enabling this conformance testing will be valuable, CAMP does not yet have a position on whether this conformance testing should be mandatory, especially for OBEs. On the one hand, formal conformance testing is expensive and time-consuming, and can be inflexible with respect to different versions of the same device, requiring extensive re-testing for minor changes. On the other hand, the more Connected Vehicle devices follow existing formal conformance practices, the greater opportunity we have to take advantage of existing institutional knowledge and provide assurance of secure implementations.

Therefore, nothing in this memo should be taken as a proposal for how conformance to the security requirements is to be tested. CAMP considers that question still to be open.

# Conclusions

CAMP proposes that the Software and OS Security document is integrated into J2945/1 as a statement of security requirements for BSM-sending devices. (Note that other changes to J2945/1 may also be necessary – for example, J2945/1 does not currently mandate support for peer-to-peer certificate distribution).

CAMP proposes that the Software and OS Security document is referenced by the RSU v4 specification.

CAMP proposes that the SCMS Manager formally adopts the Software and OS Security document as a statement of security requirements for devices that request certificates.

CAMP encourages an open discussion about the appropriate certification testing regime, both for Pilot Deployments and pre-mandate devices, and for OBEs subject to the mandate.