ITU activities on secure vehicle software updates

8th meeting of IWG ITS/AD

9 March 2016

T. Russell Shields, Co-Chair, Collaboration on ITS Communication Standards
Martin Adolph, Programme Coordinator, ITU
Outline

1. Draft Report on secure over-the-air vehicle software updates - operational and functional requirements
2. Draft Standard on secure software update capability for ITS communications devices
3. Other ITS communications related activities in ITU
4. Supplementary material
Report on secure over-the-air vehicle software updates - operational and functional requirements

• Objectives:
  – The principal objective of the report is to provide supportive information to the groups working on the technical specifications for a FOTA/SOTA telecommunications standard.
  – A secondary objective of the report is to provide background information to the vehicle manufacturer groups working on their internal processes aimed at delivering a vehicle-manufacturer-specific end-to-end FOTA/SOTA update solution for their own vehicles.
Report on secure over-the-air vehicle software updates - operational and functional requirements

• Status of Report:
  – Reviewed in two meetings of the Collaboration on ITS Communication Standards (2015/12; 2016/03)
  – Submitted to ITU-T Study Group 17 (Security; meeting late 2016/03) and ITU-T Study Group 16 Multimedia; meeting 2016/05) for adoption as ITU-T Technical Paper
  – ITU-T Technical Papers are available on the ITU website, free of charge
Standard on secure software update capability for ITS communications devices

- Objectives of “ITU-T X.itssec-1”:
  - Assessment of security threats, risks and vulnerabilities
  - Provision of common methods to update vehicle software by a secure procedure
  - Security controls and protocol definition

- Note:
  - ITU-T standards (“Recommendations”) have non-mandatory status until they are adopted in national laws
  - This standard is aimed to provide a guideline for baseline security for networked vehicles
Standard on secure software update capability for ITS communications devices

- Status of “ITU-T X.itssec-1”:
  - Initiated in 2014/09
  - Draft achieved a certain level of maturity through discussions with some vehicle manufactures and suppliers
  - Draft is to be “determined” as an ITU-T Recommendation, the final stage of standardization, during the meeting of ITU-T Study Group 17 (Security), Geneva, 16-23 March 2016
  - ITU-T Recommendations are available on the ITU website, free of charge
Other ITS communications related activities ITU

• An up-to-date list of ITS related work items in ITU is available at http://www.itu.int/en/ITU-T/extcoop/cits/Documents/ITS%20work%20items.xlsx
Supplementary Material
Report on secure over-the-air vehicle software updates - operational and functional requirements

Structure

1. Introduction
   - Executive Summary
   - Objectives
   - References
   - Acronyms and Definitions

2. The Automotive Context
   - Are we ready for OTA Updates?
   - Use Cases
   - Conditions
   - National Standards Regulation and Type Approval Regulation Compliance
   - National Standards Initiatives for Security Risk Mitigation

3. Operational Requirements
   - Update preparation
   - Regulatory approvals
   - Permissions to perform update
   - End-to-end update management
   - Confirm receipt and proper functioning
   - Perform administrative tasks

4. Functional Requirements
   - Recall
   - Non-recall Operation Updates
   - Improvements to Performance
   - Security Risk Corrective Action
Report on secure over-the-air vehicle software updates - operational and functional requirements
Report on secure over-the-air vehicle software updates - operational and functional requirements

• A properly designed system that provides for as high a level of security as is possible must protect each of the four levels of vehicle electronics systems that could be addressed by OTA software updates:
  • Information and entertainment systems
  • Fail safe body function systems
  • Fail safe driving and vehicle dynamic function systems
  • Fault functional driving and vehicle dynamic function systems
Conducted threat analysis for each step in the procedure.
Impersonation of VMG

- Software information on every ECU in the vehicle is improperly collected

Impersonation of ECU

- Improper software information is uploaded to VMG
- DoS attack against VMG by sending forged data (e.g., enormously huge data)

Tampering/eavesdropping/replay of a message

- Improper software information is uploaded to VMG
- Software information on every ECU in the vehicle is improperly collected
- DoS attack against VMG by sending forged data (e.g., enormously huge data)
X.itssec-1: Security controls for the software update

✓ **Message verification**
  - Threats: tampering, eavesdropping and replaying of messages
  - Measure: message verification mechanism based on Message Authentication Code (MAC) or digital signature method

✓ **Trusted boot of ECUs**
  - Threats: tampering of software in ECU
  - Measure: hardware Security Module (HSM) to verify software modules in ECUs’ boot sequences

✓ **Authentication of communication entity**
  - Threats: impersonation of the entities
  - Measure: authentication of both client and server of each communication based authentication protocol such as SSL/TLS
X.itssec-1: Security controls for the software update

✓ **Message filtering**
  - **Threats:** DoS attack against VMG or update server
  - **Measure:** message filtering based on white listing of senders and frequency limitation of received messages, etc.

✓ **Fault tolerance**
  - **Threats:** DoS attack against VMG
  - **Measure:** measures such as auto-reboot for recovery of normal state, safe suspension of operation should be taken if something irregular is detected on the operation of VMG.
X.itssec-1: Procedure definition (Phases)

1. diagnose phase

2. diagnose (request)
3. diagnose (report)
4. diagnose (submit)
5. diagnose (receipt)

6. update_check phase

7. update_check (request)
8. update_check (response)

9. update phase

10. update (notification)
11. update (confirmation)
12. update (application)
13. update (report)

14. update_report phase
15. update_report (submit)
16. update_report (receipt)
X.itssec-1: Example of a message: diagnose (submit)

Structure of diagnose (submit) message

Practical expression of a diagnose (submit) message (example: XML)