ITU Workshop on Security Aspects of Intelligent Transport System

Geneva, Switzerland, 28 August 2017

Session 1: Understanding current threats and security requirements

Takeaways and Conclusions

1. Cyber security and data protection are the immediate challenge for ITS/IVS.WP.29 initiates task force on this regard. Product lifetime considerations need to be emphasized.
2. Aeronautic, automotive, railways domains would benefit from a common cybersecurity architecture model to mitigate security threats.
3. Vulnerabilities in a vehicle cannot be overlooked. Security requirements for vehicle accessible devices should be the first priority.
4. IoV is facing multi-dimentional security threats which need a comprehensive security solution to address them. IoV security standardization is active in both SDOs and regulartory agencies.

Suggestions to SG17

- ❑ To coordinate with WP.29 and other SDOs on ITS security standardization.
- ❑ To develop common cybersecurity architecture framework for ITS.
- ❑ To identify threats and security requirements of vehicle accessible external devices.
- ❑ Identify risks and security requirements for IOV.

Session 2: ITS security standardization Overview

Takeaways and Conclusions

1. WP29/TFCS activities (high level and detailed threats assessment) were recognized.
2. Q13/17 activities including ongoing X.itssec-2 were also recognized.
3. Collaboration with WP29/TF was recommended.

Suggestions to SG17

1. (General) Security Guidelines for Secure ITS should be developed in ITU-T SG17 jointly with ISO/TC 204 (and TC 22);
2. Secure Software Update Procedures (X.1373) should be refined to be utilized for Car OEM vendors jointly with ISO/TC 204. We need to consider the activities in WP29/TFCS OTA (software update);
3. Security Guideline for V2X (draft X.itssec-2) should be actively collaborate with experts in ISO/TC 204 and OEM vendors;
4. Threats assessment in ITS environment should be conducted in ITU-T SG17 based on the results of WP29/TFCS. How to utilize the output from WP29/TFCS-OTA should be also considered in ITU-T side… Collaboration with WP29/TFCS should be strengthened.
5. Specific Security Guideline should be also developed for Major modules (GW, NW, IDS, App…), Components (such as onboard unit…) venders. It is also worthwhile for Q13/17 to discuss and study on use of “Lightweight Cryptography” in ITS environment.

Session 3: Mitigating security threats to automotive systems

Takeaways and Conclusions

1. Connected cars present tons of opportunities, but lacked with tons of risk.
2. The amount of legislation shows that governments are serious about regulating cars in the future.
3. An adaptive security strategy is crucial to mitigate risk to the automotive industry.
4. In emerging automotive/ITS services, protection of automotive sensor data is critical to system reliability and privacy concerns.

Suggestions to SG17

- ❑ Establish secure architecture prior to connecting anything to the outside.
- ❑ Mitigate external attacks against the secure architecture once connections have been established.
- ❑ Authenticate critical endpoints and users.
- ❑ Lightweight cryptography has great potentials for this purpose on resource-constrained devices such as sensors and their control ICs.

Session 4: Panel discussion – Future directions on ITS standardization activity

Takeaways and Conclusions

1. Cybersecurity of Intelligent Transport (CTI).
2. Hacker effect on Human Life.
3. Focus on the “Telecom”-centric “external communications” elements.

Suggestions to SG17

- ❑ Develop Common Architecture Framework.
- ❑ Towards a common cybersecurity process (a shift from Driver Distraction to cyber threats on ITS).
- ❑ Q13 as lead, with support for Collaboration with other SDOs through CITS.