Symposium on The Future Networked Car

(Geneva, Switzerland, 7 March 2019)

Security issues related to the future Networked Car

Koji Nakao
Distinguished Researcher,
Cybersecurity Research Institute, NICT
ITU-T SG17 WP (Cybersecurity) chairman

Security issues

<Security issues under ITS environment>

1. Observe and Analyze “Threats” & “Vulnerabilities” including emerging IoT threats;
2. Detection of injected Malwares/Mal-functions in vehicle
   - Appropriate Research on detection methods should be studied;
3. Conducting Threat assessment and risk management (for vehicle eco-system) (How to conduct the assessment);
4. Establishment of Remote Software/Firmware update (OTA);
5. Research of Appropriate security capabilities (Data confidentiality, Privacy protection, Authentication. Access control, incl. Lightweight crypto)
6. Remote Maintenance (e.g. Remote Kill Switch) including for IoT devices
7. Global Incident handling and Information Sharing capabilities

ITS security standardization

<For ITS security standardization>

1. Related SDOs should be coordinated and collaborated;
2. Threats assessment methodology for Vehicle eco-system can be standardized (not only for threat assessment on Vehicle);
3. Standards can produce a certain level of security requirements which will be related to "Certification of Vehicle and Vehicle eco-system";
4. Is there any requirements for establishing global incident handling and information sharing scheme? Do we need a capability of AUTO-ISAC?

National Institute of Information and Communications Technology

ITU-T SG17 ITS Recommendations（under development）

X.1373(rev): Secure software update capability for intelligent transportation system communication devices

X.stcv: Security threats in connected vehicles

X.itssec-2: Security guidelines for V2X communication systems

X.itssec-3: Security requirements for vehicle accessible external devices

X.itssec-4: Methodologies for intrusion detection system on in-vehicle systems

X.itssec-5: Security guidelines for vehicular edge computing

X.edrsec: Security guidelines for cloud-based event data recorders in automotive environment

X.fstiscv: Framework of security threat information sharing for connected vehicles

X.eivnsec: Security guidelines for the Ethernet-based in-vehicle networks

X.mdcv: Security-related mis-behavior detection mechanism based on big data analysis for connected vehicles

X.srcd: Security requirements for categorized data in V2X communication