Abstract

The basis of automated driving systems, information such as high definition map data, data of vehicles, pedestrians, road infrastructure etc., are expected to be obtained primarily from external vehicular networks. Such information will be transferred to vehicle control/information devices to be used for vehicle control in the automated driving system. This could lead to cause cybersecurity issues that did not exist before, in the time of conventional non-connected cars.

"Strategic Innovation Promotion Program (SIP) Phase 2/Automated Driving (Expansion of Systems and Services)/Research on New Cyber-attacks and Countermeasures against New Cyber-attacks " aims to solve such issues through research and analysis on cyber-attack methods as well as its countermeasures, especially Intrusion Detection System (IDS) to protect vehicles in the field against new cyber-attacks. The project also covers research and development of evaluation methods for IDS as well as conducting trial evaluation of the actual IDS product using a vehicle test bed.

In this year, following activities were conducted and summarized into this report: “Research on the Trend of Cyber-attack against Vehicles”, “Research on Cybersecurity Countermeasures such as IDS”, “Research on IDS Evaluation method and Trial Evaluation”, “Development and Documentation of Technical Standard (in collaboration with JASPAR)” and “Investigation on Update Framework of Information Security Evaluation Guideline”

For the “Research on the Trend of Cyber-attack against Vehicles”, the risk values were calculated for the cases reported during 2017 to 2019 at international conferences and other major events. In calculating risk values, methods for analyzing and comparing each reported case with the same criteria were examined since the contents of the reports were inconsistent in the scope and level of detail described depending on the writer and/or publishing organization. For each case, an attack scenario and attack feasibility using a common model of vehicle systems and impact were defined to calculate the risk values.

As for the "Research on Cybersecurity Countermeasures such as IDS ", the service model of the product, detection method, log collection, management system, etc. were investigated through public information and interview with each vendor.

The "Research on IDS Evaluation Method and Trial Evaluation" defined the following four aspects and methods for the evaluation based on the result of interviews with the experts and vendors, public documents, and the result of aforementioned " Research on the Trend of Cyber-attack against Vehicles".

1. Basic specifications: Determine compliance with the objectives and requirements. 2. Implementation (including PoC): Determine the feasibility of implementation to the target system. 3. Operation. Determine the feasibility of regular monitoring and analysis of logs after detection. 4. Detection performance. Determine the basic performance as an IDS.

For “4. Detection performance”, an evaluation method covering five criteria was defined and trial evaluation using the method was conducted to an actual IDS product on a test bed with the cooperation of a IDS vendor.

The five criteria are: 1. No detection during steady state, normal operation or by the events excluded by specification. 2. Detection of unexpected message/activities including injection attacks, etc. 3. Detection of physical connection of unauthorized devices such as fraudulent diagnostic equipment or the addition of ECUs. 4. Detection of malware activity such as malware communications and vulnerability attacks. 5. Detection of abnormality in the protocol such as unexpected use of diagnostic protocols or the injection of anomalous messages.

In "Development and Documentation of Technical Standards", Vehicle ECU penetration testing guideline using the outcome of the “Information Security Field Operational Test” during SIP phase 1 in collaboration with JASPAR Information Security Technology Working Group Testing Team as well as the update framework and method for ensuring to maintain effectiveness of the guideline.