Kiyotaka Atsumi, Adv Automob Eng 2018, Volume 7
DOI: 10.4172/2167-7670-C1-010

5th International Conference and Exhibition on

Automobile and Mechanical Engineering

September 20-21, 2018 | Rome, Italy

Kiyotaka Atsumi

LAC Co Ltd, Japan

Smart CAN cable: Another IPS for CAN BUS network

We propose a new IPS (Intrusion Prevention System) for CAN BUS, one of the popular in-vehicle network. This shape is like a cable with connectors. We call it "Smart CAN Cable." The most important function of Smart CAN Cable is to find a compromised ECU (Electronic Control Units) who sends an illegal message on CAN BUS. A CSIRT (Computer Security Incidence Response Team) must identify a compromised computer and/or network systems at first when they detect that an attacker crack the system. In an office environment, it is to identify a compromised laptop by tracing an IP address. There is a need to solve the cybersecurity problem and to take down the attacker. Many ideas of IDS for CAN BUS were already proposed. Most of them can only detect anomaly CAN message, and they cannot identify which ECU is compromised because any ECUs cannot identify the ECU who sends illegal messages because of the specification of CAN protocol. The Smart CAN cable has two kinds of functions. One is to identify an illegal message; another is to memorize and identify a sender ECU when it sends a message. This paper shows how the Smart CAN cable works, and its advantages and disadvantages.

Biography

Kiyotaka Atsumi pursued his PhD from Toyohashi University of Technology, Japan. He is currently the Director of IoT Technology Laboratory of LAC Co Ltd, Japan, the oldest security vendor in Japan. Currently, he is engaged in research of managed security service for connected-cars and of the threat analysis on model-based development for IoT.

kiyotaka.atsumi@lac.co.jp