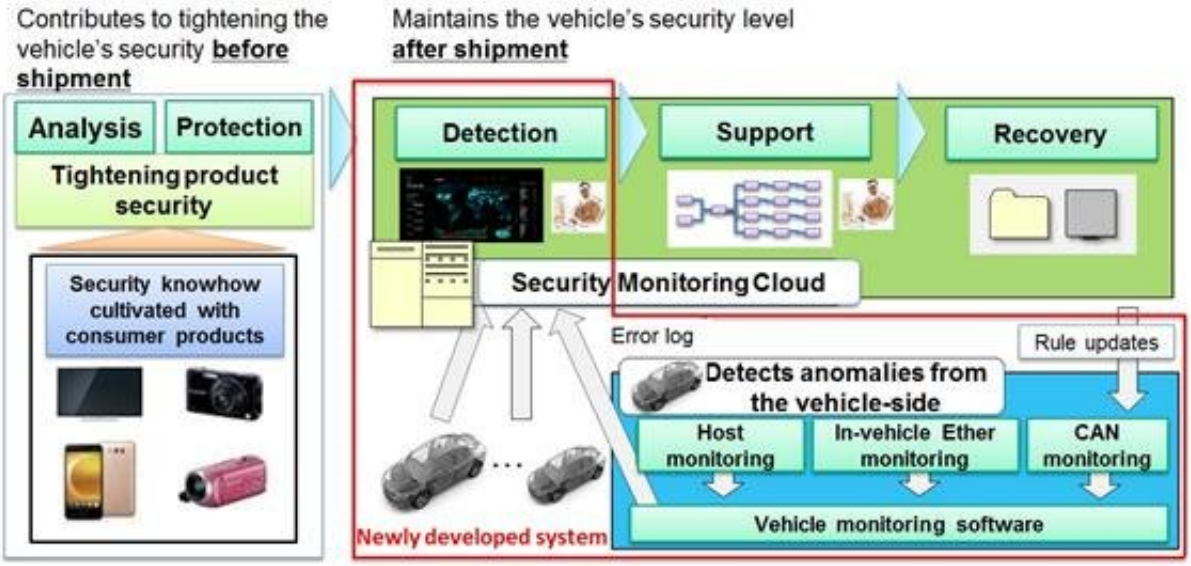
Automotive intrusion detection and prevention systems against cyber attacks

October 10 2017



Credit: Panasonic

Panasonic Corporation announced today that it has developed automotive intrusion detection and prevention systems as a cyber security countermeasure for autonomous and connected cars.

Connected cars are connected to the Internet, so like current IT systems, they have a possibility of receiving cyber attacks from around the world. By using Panasonic's newly developed systems, they are possible to detect cyber attacks in real-time while simultaneously preventing them.

Automobiles have a long product lifecycle, so there is a possibility that they are exposed to attacks that have been evolved compared from attacks that were assumed at the time of factory shipment. By using these systems, they are possible to collect information of the evolved attacks on the cloud side and detect the evolved attacks by distributing and updating the new rules of the countermeasures to the vehicles.

Panasonic's newly developed systems will ensure safe driving with autonomous and connected cars by detecting the intrusion of attacks and viruses to the vehicle system due to cyber-attacks and discarding and disabling them using the prevention system. They will make it easier to comply with future in-vehicle security legislations.

The features of the new systems are as follows.

1. Detects intrusions of attacks from the Internet at an early stage, and additionally detects intrusions to the in-vehicle network as a second step.
2. In addition to the widely used CAN, the systems are also compatible with Ethernet, which is expected to spread in the future as an in-vehicle network, and enables comprehensive detections of intrusions to the entire vehicle.
3. By collecting information from multiple vehicles on the cloud, the systems can detect attacks before they are identified as a true security incident.

The system consists of a vehicle-installed "monitoring module" and a "monitoring cloud" that is linked to the monitoring module. The vehicle-installed monitoring module monitors the entire vehicle based on the monitoring rules. By using the company's newly developed systems, once the attacks that cannot be detected with existing monitoring modules are discovered, the systems can prevent new attacks by updating the monitoring rules from the monitoring cloud. Therefore, it helps to

maintain safety even after the vehicle is released on the market. Also, by grasping signs of attacks before they are identified as true security incidents, they are possible to implement countermeasures in advance so that they can minimize the effects of the attacks.

Technical Features:

1. In-vehicle device-type host intrusion detection technology: This technology detects intrusions from the Internet, which is an early stage of the attacks, and can be installed and used with Internet connected devices (IVI/TCU) In addition to clearly identifying the attacks from the obtainable logs from an OS like Linux and other various security functions, the system can also detect the attacks by combining multiple behavioral information.
2. In-vehicle device-type CAN intrusion detection technology: This technology detects intrusions to CAN communication systems, which is a second stage of the attacks, and can be installed and used with CAN connected devices (ECU) There are two types of CAN monitoring usages, which consist of (1) CAN filter that filter unauthorized CAN commands received by the installed ECU, and (2) CAN monitoring that detects unauthorized commands by monitoring all CAN bus systems that are connected by the installed ECU. Unauthorized commands are judged by taking into consideration various conditions of the vehicle, so it is possible to reduce the number of false positive under specific conditions. Detection of unauthorized commands can be made for each single command, resulting is real-time prevention after detection.
3. In-vehicle device-type Ethernet intrusion detection technology: This technology detects intrusions to Ethernet communication systems, which is a second stage of the attacks, and can be installed and used with Ethernet connected devices (ECU) There is an Ether filter that filters unauthorized Ether frames that are

received or intercepted by the installed ECU (Ethernet Switch ECU, etc.) The system consists of the overlook method, which can lightly determine unauthorized commands by analyzing the frame headers and a detailed method, which has a high-load operation, but can accurately determine unauthorized commands. Flexible detection is possible by combining these methods.

4. Cloud-type vehicle intrusion detection technology: This system analyzes a large amount of logs collected from in-vehicle devices of multiple vehicles through machine learning and can be used by placing it in the cloud. As for the usage, in-vehicle network model that has conducted prior learning, will automatically narrow down the logs that may become potential security risks. After that, the attack analysts will analyze only the selected logs. By linking with various in-vehicle device-type intrusion detection technologies, it is possible to grasp signs of attacks before they are identified as true security incidents.

Provided by Panasonic Corporation