Anritsu envision:ensure

WP.29/2020/79-Mandated Method for Evaluating Cyber-Security Weakness of Vehicles using Cellular Communications

Signalling Tester MD8475B

Increasing Importance of Connected Car Cyber Security

Recently, more automobile equipment is using cellular communications, expanding both services for remote monitoring of traffic conditions and smartphone applications. Automobile and in-vehicle equipment manufacturers are providing these applications to help assure more comfortable and safer driving. However, although the services make the automobile more useful, they also create cyber-attack security problems, which has increased the importance of automobile cyber-security penetration testing.

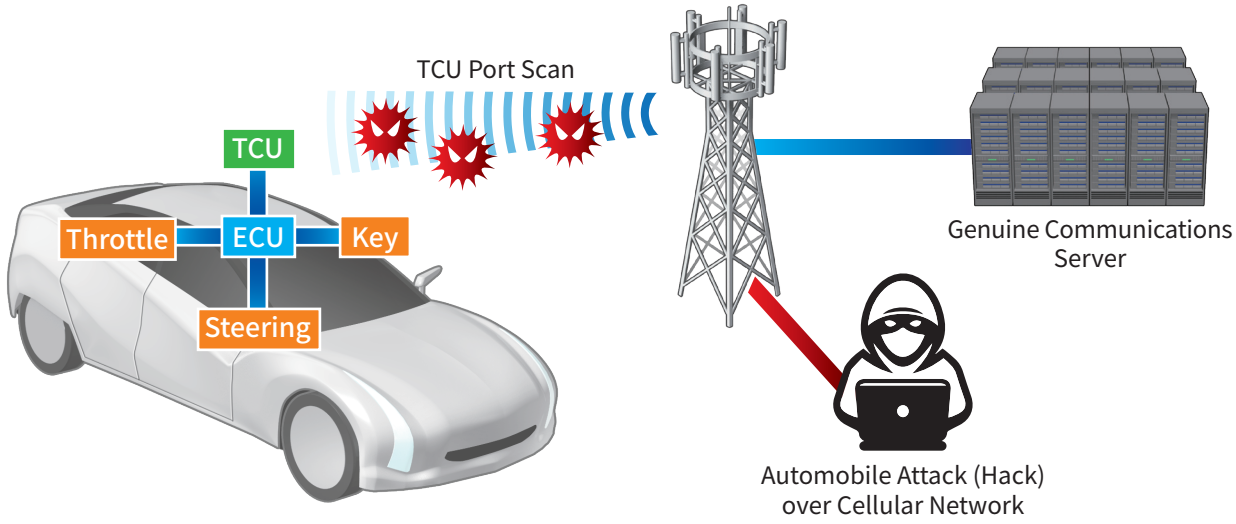


Figure 1: TCU Port Scanning Cyber Attack

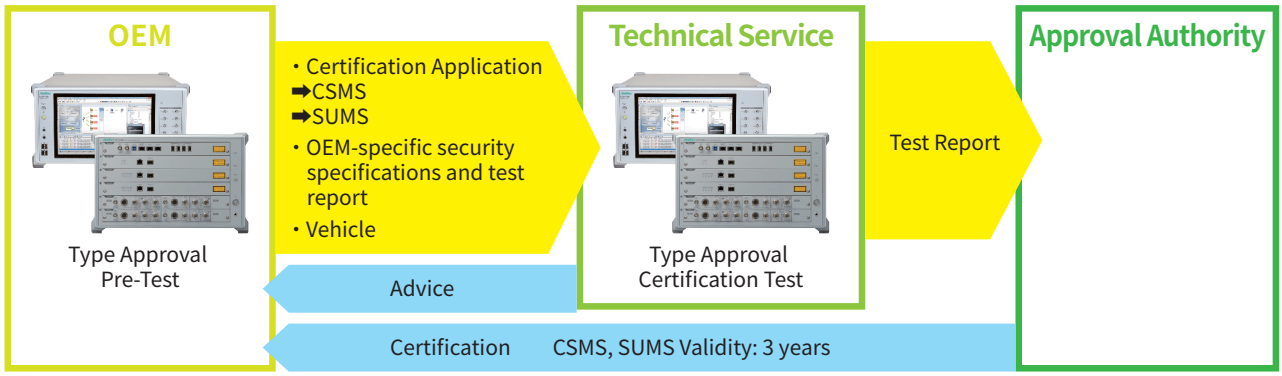
Common cyber-attacks pose a risk of hijackers taking control of the automobile by scanning the Telematics Communication Unit (TCU) for vulnerable ports. Two typical hacks over cellular communications are listed below.

- **Automobile remote operation using SMS via self-diagnostics port dongle**
- **Hijack voice calls and SMS by abusing CS (Circuit Switched) fallback**

Mandatory WP.29/2020/79 Certification Process

Cyber security is becoming an increasingly important issue following advances in self-driving automobile technologies. Working Party (WP29) of the World Forum for Harmonization of Vehicle Regulations established as a UN/UN ECE working group has enacted the cyber-security related ECE/TRANS/WP.29/2020/79 rules defining concrete standards as ISO/SAE 21434. Automobile and on-board unit manufacturers are required to build an organization and system that complies with laws and standards. And vehicles are required to obtain type approval.

- It is necessary to create a corresponding organization and system
- Vehicle certification must be obtained for the car



Security Penetration Testing using Anritsu Base Station Simulator MD8475B

The sale of vehicles with cyber-security weaknesses can lead to serious issues and accidents. These risks can be mitigated beforehand by using Anritsu's Base Station Simulator MD8475B to perform penetration tests of the vehicle's cellular communications cyber security. Combining the MD8475B with software for simulating a cyber-attack (hack) under the same conditions as actual usage can help manufacturers evaluate the resistance of their products to cyber-attacks via cellular communications.

⁎ Consult our sales representative for software products to use with the MD8475B for penetration testing.

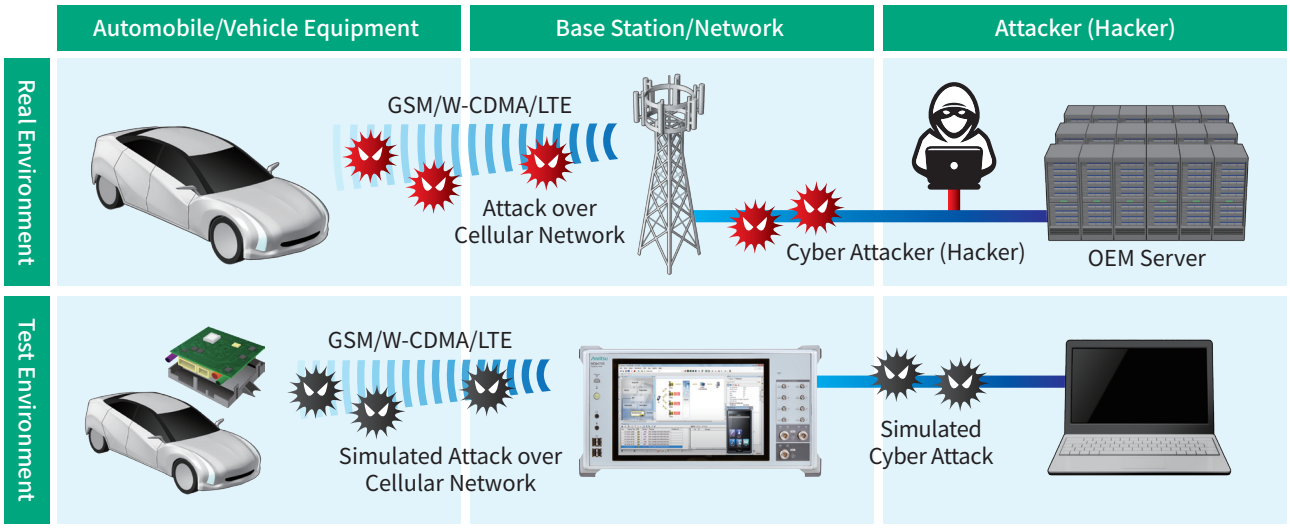


Figure 2: Real and Test Environments

Other Cyber-Security Evaluation Applications

The MD8475B can also be used in combination with various other security evaluation systems for cyber-security penetration tests not using port scans. Currently, Anritsu supports penetration testing simulating DoS attacks, SMS spoofing, firmware tampering, etc., under various wireless environments.