Leaflet

Anritsu envision : ensure

Automobile Cellular Communications Cyber-Security Penetration Testing

Signalling Tester MD8475A/B

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.

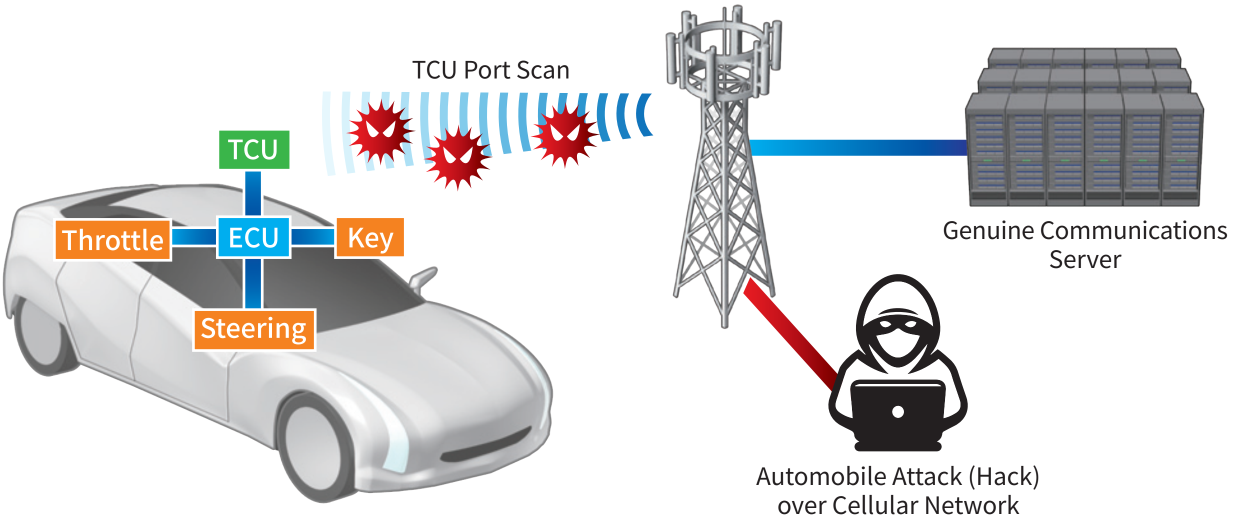
TCU Port Scan
TCU
Throttle
ECU
Key
Steering
Genuine Communications Server
Automobile Attack (Hack) over Cellular Network

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**

As self-driving vehicle technologies progress, these cyber-security problems are becoming increasingly important in the automobile business world. Consequently, automobile and in-vehicle equipment manufacturers are placing heavy emphasis on prior cyber-security penetration testing.

Security Penetration Testing using Anritsu Base Station Simulator MD8475A/B

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 MD8475A/B to perform penetration tests of the vehicle's cellular communications cyber security. Combining the MD8475A/B 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 MD8475A/B for penetration testing.

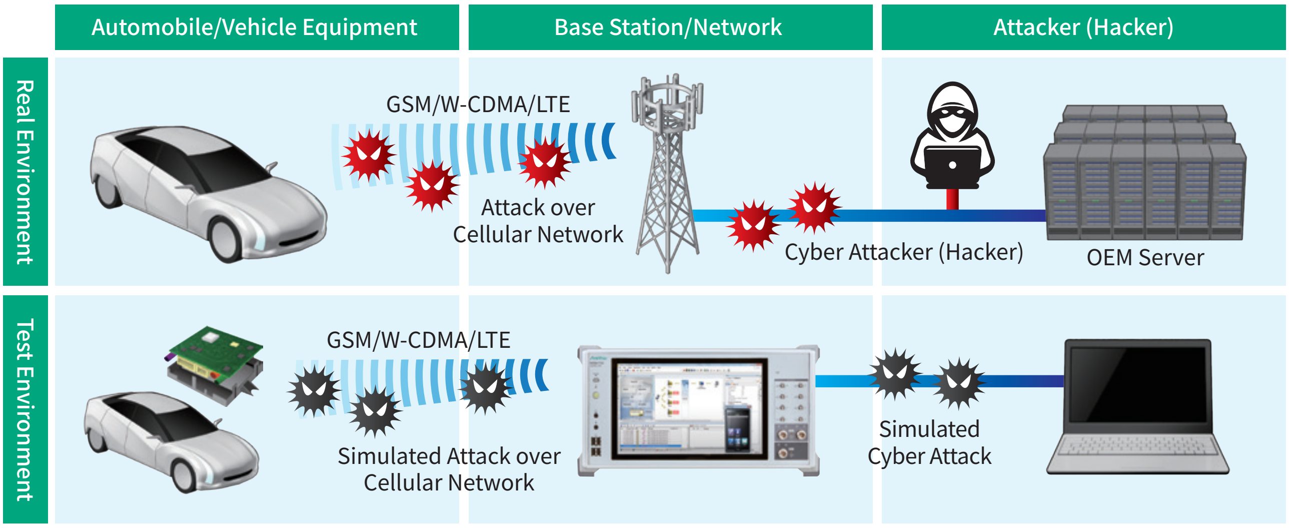

Figure 2: Real and Test Environments

Other Cyber-Security Evaluation Applications

The MD8475A/B 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.

ANRITSU CORPORATION
https://www.anritsu.com