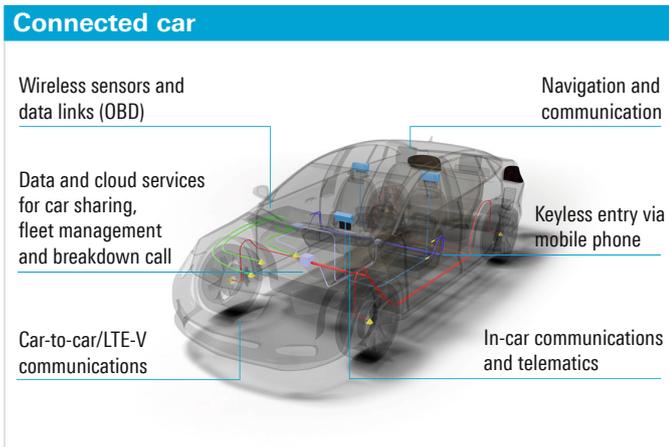


Testing the IP connection security of telematics units

The IP connection security analysis solution for the R&S®CMW500 platform identifies IP connection vulnerabilities in telematics units at an early stage of development.



Your task

The Internet is becoming an integral part of our vehicles. An increasing number of vehicles are equipped with cellular and non-cellular wireless modules to exchange data, monitor measured values or even remotely control a system. The amount of IP traffic between the vehicle and the network is expected to drastically increase over the next few years, for example in automotive applications such as navigation, multimedia and firmware updates. A considerable number of vehicles will be connected to the Internet using non-cellular technology such as WLAN or a cellular network such as LTE/LTE-A.

When designing connected vehicles, IP connection security becomes an important topic, particularly when the device will manage sensitive data or is connected to control systems. The term IP connection security originates from the IT world and describes the procedure used to secure the communications channels between two devices, typically by using authentication and encryption. Authentication and encryption are required for all communications channels to the Internet in order to secure the information exchanged.

Most of today's telematics platforms are proprietary. This could be the reason why security gaps in telematics units' IP connection security are frequently reported in the news.

Developers need to focus on testing and identifying weak spots in their telematics applications at an early stage of development. This presents a challenge since measurement solutions for telematics units' IP connection security under fully controlled non-cellular and cellular network conditions are rather rare.

T&M solution

Rohde & Schwarz is the first to offer a solution. The company has integrated IP connection security analysis into its established R&S®CMW500 wideband mobile communication tester. The R&S®CMW-KM052 option detects and analyzes IP data traffic in realtime. It is a powerful add-on to the R&S®CMW500 realtime tester that supports all common cellular radio standards such as LTE, WCDMA and GSM as well as non-cellular standards such as WLAN in a single unit.

For the test, the R&S®CMW500 simulates the relevant network, including country and mobile network codes, and establishes a connection to the telematics device. The integrated data application unit (DAU) takes over IP configuration and establishes the IP connection. The DAU also provides internal services such as web servers, file transfer servers or an IMS server if required by the DUT. It is also a gateway to the Internet and establishes the connections required for communications.

The R&S®CMW-KM052 captures and analyzes the data streams of the DUT's established IP connections and visualizes the data streams as well as relevant IP connection security parameters, including:

- Certificate-based authentication details
- SSL/TLS handshake
- Encrypted versus unencrypted traffic

It is also important to ensure that the telematics unit has no unwanted open ports to the Internet and that it does not transmit passwords or user-relevant data unencrypted.

The R&S®CMW500 offers comprehensive capability for:

- Open port analysis
- Clear text keyword matching analysis

It is also possible to determine the location and domain name of the endpoint to which communications have been established. This is done by analyzing the:

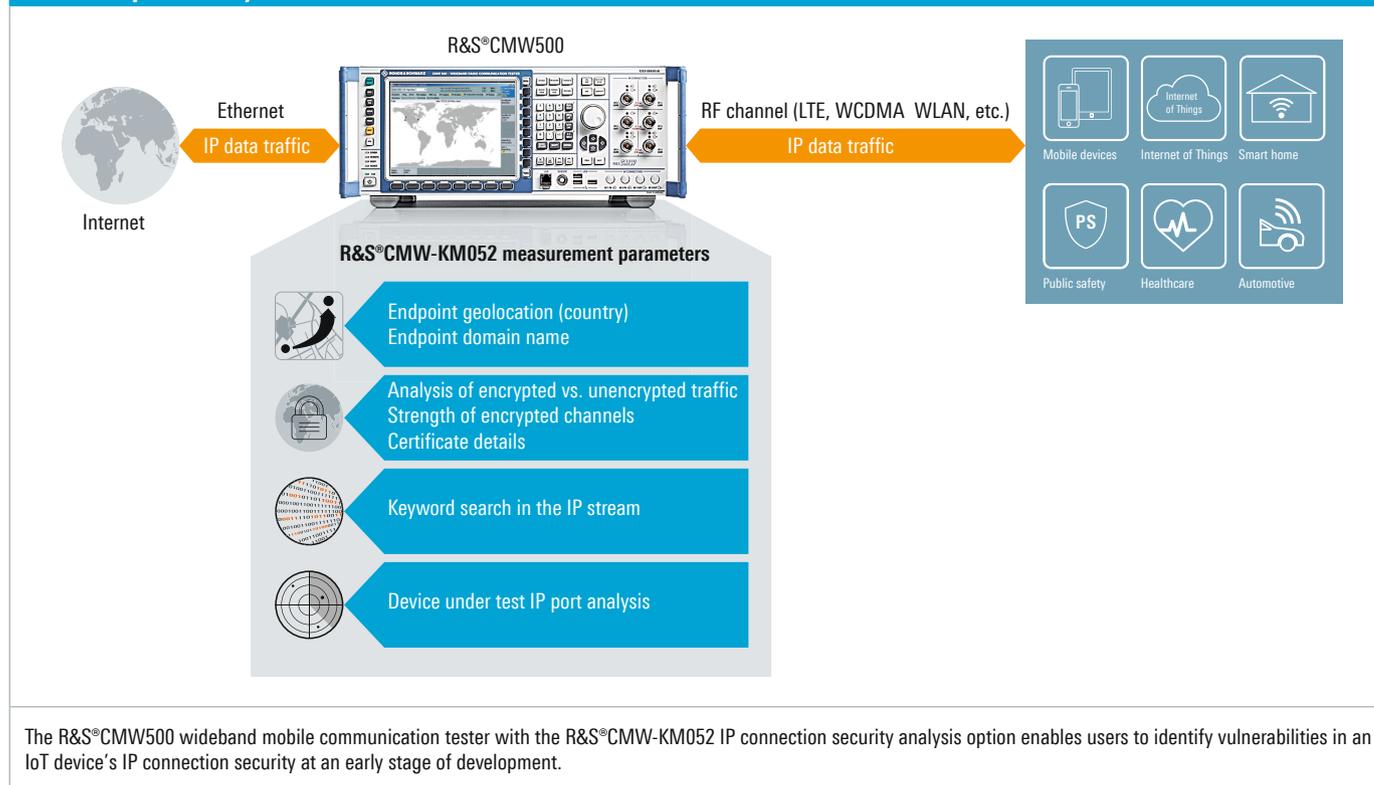
- Endpoint's geolocation (country)
- Endpoint's domain name

The R&S®CMW500 tester's new analysis functionality enables telematics unit manufacturers to identify vulnerabilities in the IP connection security under controlled network conditions in the lab. Development engineers can now improve the IP connection security of their devices at an early stage of development. Especially the combination with cellular technologies such as LTE/LTE-A, WCDMA and GSM makes the R&S®CMW500 with the R&S®CMW-KM052 option a unique and powerful test solution.

See also

www.rohde-schwarz.com/CMW

Test setup to analyze IP data traffic of mobile devices



The R&S®CMW500 wideband mobile communication tester with the R&S®CMW-KM052 IP connection security analysis option enables users to identify vulnerabilities in an IoT device's IP connection security at an early stage of development.

Rohde & Schwarz GmbH & Co. KG

Europe, Africa, Middle East | +49 89 4129 12345
 North America | 1 888 TEST RSA (1 888 837 87 72)
 Latin America | +1 410 910 79 88
 Asia Pacific | +65 65 13 04 88
 China | +86 800 810 82 28 | +86 400 650 58 96
www.rohde-schwarz.com
customersupport@rohde-schwarz.com

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG
 Trade names are trademarks of the owners
 PD 5215.3256.92 | Version 01.02 | August 2017 (he)
 Testing the IP connection security of telematics units
 Data without tolerance limits is not binding | Subject to change
 © 2017 Rohde & Schwarz GmbH & Co. KG | 81671 Munich, Germany



5215325692