Increase the IP connection security of your IoT device

The new IP connection security analysis solution for the R&S®CMW500 platform identifies IoT and mobile communications devices' IP connection vulnerabilities in an early stage of development.

Your task

The Internet is becoming more integrated into our lives with an increasing number of connected devices equipped with cellular and non-cellular wireless modules to exchange data, monitor measured values or even remotely control a system. The number of things communicating with each other is expected to drastically increase over the next years, for example in the automotive, health care and robot control industries. A considerable number of IoT devices will be connected to the Internet using non-cellular technology such as WLAN or the cellular network such as LTE/LTE-A.

When designing innovative IoT devices, IP connection security becomes an important topic, particularly when the device will manage sensitive data or 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 IoT platforms are proprietary since standardization is still in progress and technical specifications are not yet ready for implementation. This could be the reason why security gaps in IoT devices' IP connection security are frequently reported in the news.

Developers need to focus on testing and identifying weak spots in their IoT applications at an early stage of development. This presents a challenge since measurement solutions for IoT devices' 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, and 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 the IP data traffic in realtime and 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 radio network, including country and mobile network codes, and establishes a connection to the IoT device. The integrated data application unit (DAU) takes over the 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.

ROHDE&SCHWARZ

Application Card | Version 02.00

Increase the IP connection security of your IoT device

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

In addition, it is important to ensure that the IoT device has no unwanted open ports to the Internet and also that it doesn't transmit passwords or user-relevant data unencrypted. The R&S®CMW500 offers detailed analysis capabilities for both:

- 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 has been established. This is done by analyzing the:

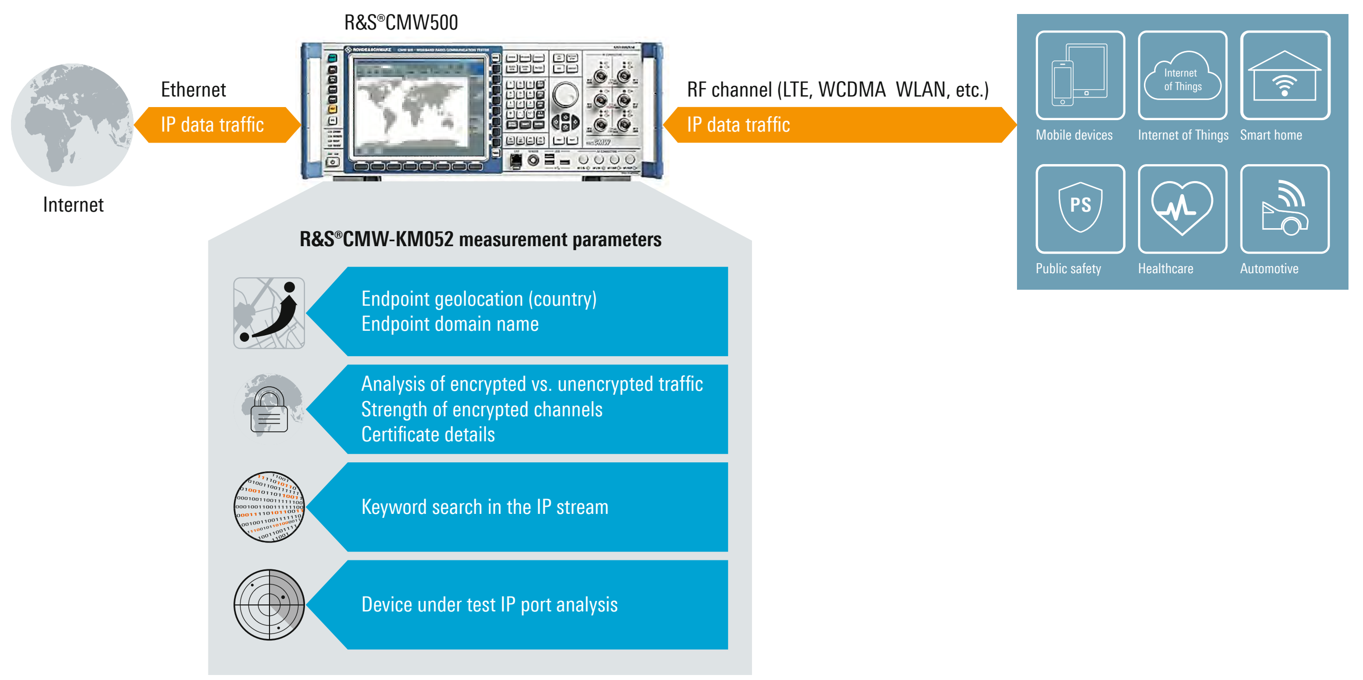
- Endpoint's geolocation (country)
- Endpoint's domain name

The R&S®CMW500 tester's new analysis functionality enables mobile and IoT device manufacturers for the first time 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


R&S®CMW500
Ethernet
IP data traffic
Internet
RF channel (LTE, WCDMA WLAN, etc.)
IP data traffic
Internet of Things
Mobile devices
Internet of Things
Smart home
PS
Public safety
Healthcare
Automotive
R&S®CMW-KM052 measurement parameters
Endpoint geolocation (country)
Endpoint domain name
Analysis of encrypted vs. unencrypted traffic
Strength of encrypted channels
Certificate details
Keyword search in the IP stream
Device under test IP port analysis

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

PD 5214.9021.92 | Version 02.00 | April 2017 (as)
R&S®CMW500; Increase the IP connection security of your IoT device
Data without tolerance limits is not binding | Subject to change

5214902192