Connected car, IoT and mobile devices on the security test bench

When it comes to cyberattacks, the focus is usually on devices that communicate with the Internet via fixed networks. Mobile users, however, are at no less risk – a fact that is becoming more critical with the advent of the Internet of Things. A new test solution now covers the network activities of wireless devices, providing important information about security gaps.

The Internet of Things and security

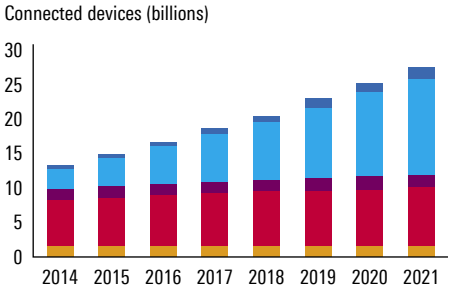
Currently more headline than reality, the Internet of Things (IoT) will soon permeate everyday life through home automation, wearables and connected car technology. It will ultimately have a far greater impact than smartphones do today. An increasing number of devices are being designed with integrated wireless modules in order to exchange (often sensitive) data, transmit measured values and remotely control systems. The number of "things" communicating via the Internet is expected to increase drastically over the coming years, with a major surge predicted after 2020 when 5G provides the necessary network resources (Fig. 1).

The downside of this development is that every wireless device with an IT core becomes a potential target for hackers. The cyber eavesdropping methods recently made public by WikiLeaks have made this threat tangible. Every IoT-connected device represents a potential risk, especially in light of the fact that IoT components are (currently) generally more poorly protected than products originally designed for the IT world. For reasons ranging from price and time pressure to lack of awareness and technical expertise, the security features in many wireless products in which IT plays a secondary or non-existent role (e.g. household appliances) are rudimentary and poorly implemented. Along with absent or weak encryption, open ports (communications channels) and vulnerable firmware, installed apps represent a significant security risk if developers fail to adhere to common IP connection security standards or do not provide regular updates. A single weak point can provide a loophole enabling unauthorized access to one or many devices. A widespread compromised IoT device can create difficulties for network operators and even cause networks to crash.

Companies also at risk

While IoT is still in its infancy, classic wireless communications is omnipresent and extensively used in both professional and personal environments. This becomes problematic for companies when these two spheres intermingle, e.g. when employers follow the "bring your own device" motto and personal mobile devices are used for business purposes.* Unprotected customer and company information poses an imminent risk. Unfortunately, it must be assumed that attackers will attempt to exploit any and all security gaps. Not only operating systems, but the increasing number of apps harbor a security risk. The multitude of helpers found on any well stocked personal mobile phone increase the probability of a poorly programmed or outdated app revealing a security gap. In the worst case, an entire corporate network can be accessed via such a device.

IoT devices – expected growth



	15 billion 2015	28 billion 2021	CAGR* 2015–2021
Cellular IoT	0.4	**1.5**	27 %
Non-cellular IoT	4.2	**14.2**	22 %
PC/laptops/tablets	1.7	**1.8**	1 %
Mobile phones	7.1	**8.6**	3 %
Fixed phones	1.3	**1.4**	0 %

* Compound annual growth rate

* The article on page 70 presents an alternative solution. BizzTrust from Rohde&Schwarz offers a secure solution for mobile devices that are used for business and personal purposes.

Fig. 1: The Internet of Things will soon overtake "classic" Internet use.
(Source: http://blogs-images.forbes.com/louis-columbus/files/2016/07/Internet-of-Things-Forecast.jpg).

Devices become truly susceptible to threats when jailbreaking or rooting manipulates their operating systems and deactivates fundamental security functions. But for attackers, looking for loopholes in allegedly secure original operating systems is a better alternative since there are only two major systems in use worldwide. Fig. 2 shows the percentage of iOS and Android devices in company and government use in selected countries.

New strategies and test methods needed

It must be determined whether a mobile device is at risk and whether the installed apps meet security requirements. The task of the responsible IT team is to verify that any wireless device used in the corporate environment safeguards the confidentiality and integrity of the data it stores and transmits, irrespective of whether it uses WLAN or a cellular connection (it cannot be assumed that malware will behave the same in both environments).

In the past, this task was easier to describe than perform since the communications behavior of the devices could not be readily examined. An analysis of the servers contacted on the Internet, and especially their location, provides essential information about unwanted communications. The server location can be identified using IP geolocation as long as no obfuscation techniques have been used. Any abnormality must be further examined and, if required, the source apps should be banned from devices used within the company. Apps developed specifically for company use, however, must certifiably behave as expected, especially with respect to security.

Security parameters revealed

The R&S®CMW500 wideband radio communication tester can significantly help developers improve the security of IP-based data communications for mobile devices and IoT modules. The new IP connection security analysis reporting module (R&S®CMW-KM052) performs realtime IP data traffic analysis in a controlled test environment (Fig. 3). The R&S®CMW500 also emulates a mobile network or WLAN access point. The data application unit (DAU) is required for security analysis. It provides the DUT with IP addresses and manages the connection with servers on the World Wide Web. The R&S®CMW-KM052 analyzes and logs the security-related parameters of the data traffic. This enables developers to detect and close security gaps early in the design process. It gives IT personnel a tool to determine whether mobile

	Global	France	Germany	Japan	Spain	UK	US	Govt.
iOS	81	50	85	92	33	83	86	82
Android	18	50	14	5	66	16	14	18

Fig 2: Percentage of iOS and Android mobile devices in corporate and government use. (Source: Mobile Security and Risk Review, Second Edition 2016, MobileIron Security Labs).

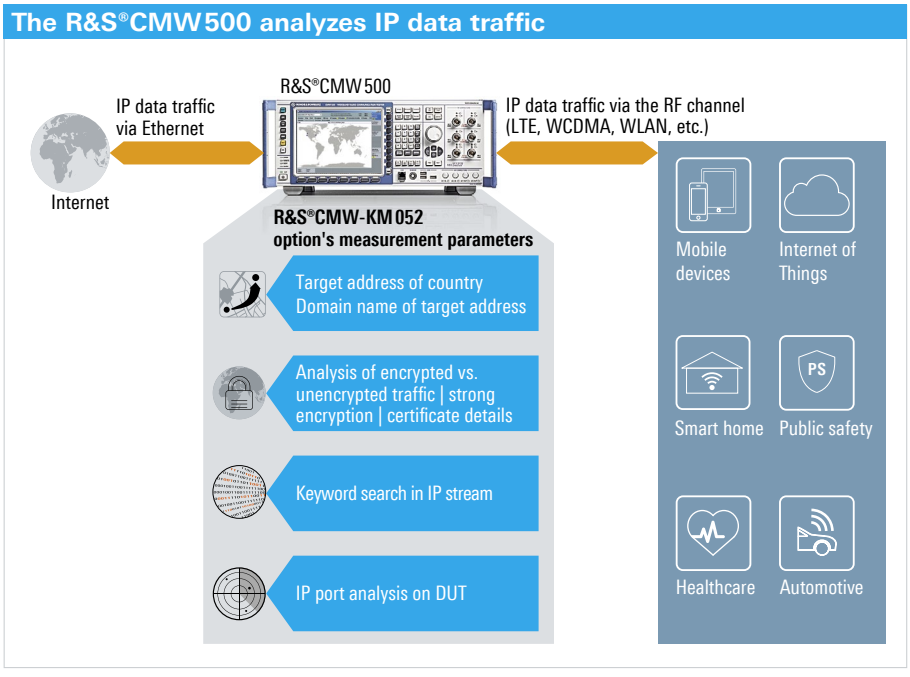
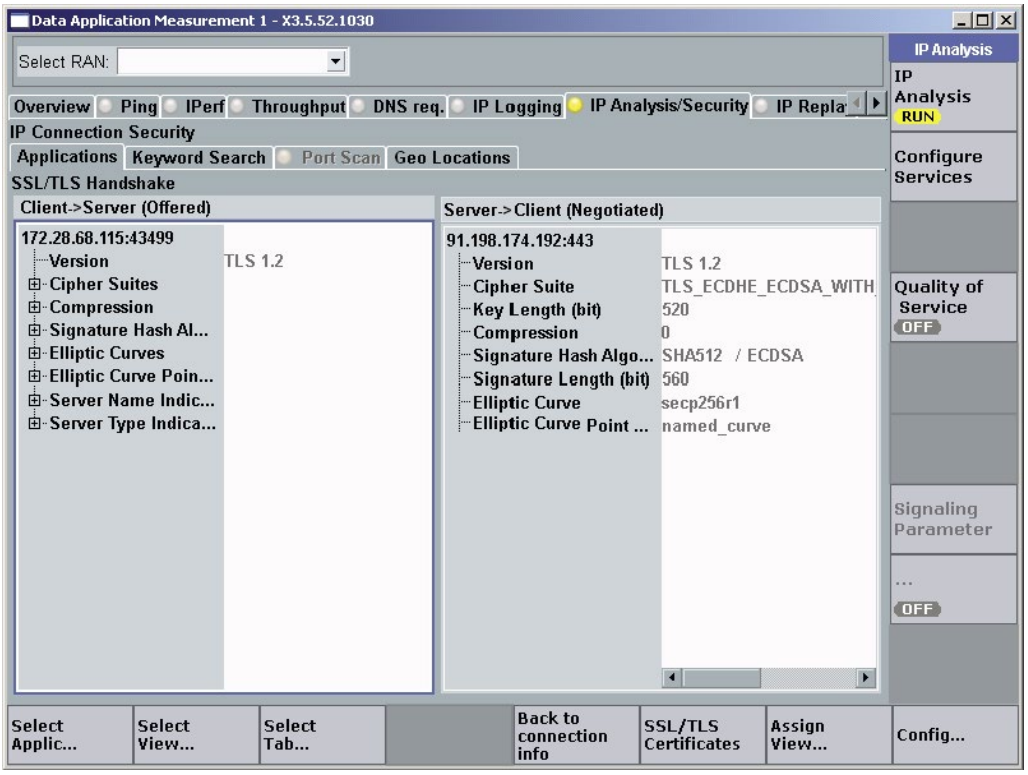


Fig 3: The "path" taken by the data transmitted and received by a connected mobile or IoT device. The R&S®CMW500 manages the data traffic between the wireless product under test and the Internet. Similar to a firewall, it checks for security-relevant content, e.g. whether passwords are transmitted unencrypted.

Fig. 4: The SSL/TLS handshake determines the security of a connection and is comprehensively analyzed.



devices used for business purposes comply with internal security policies.

The analysis software produces real-time statistics of the IP connections and communications protocols used. The software module makes it possible to search for sensitive information in data streams, including for user-specified input such as passwords and device IMSIs. If this information is transmitted unencrypted, the software lists the target address, domain name and, if possible, the source app. The module also analyzes SSL/TLS handshake parameters as well as certificates and country/domain names of the server location.

The SSL/TLS handshake that the client and server use to agree on the cryptographic method is essential for a secure connection and is therefore closely examined (see box on page 22). The R&S®CMW-KM052 displays the cryptographic methods (cipher suites) offered by the client during call setup as well as the cipher suite chosen by the server, including key lengths and other parameters (Fig. 4). The CMW KM052 can even analyze the certificate transmitted by the server.

When analyzing communications behavior, one of the most important things users want to know is where the involved servers are located (country). Geolocation (IP address assignment according to geographic location) makes it possible to determine this information. Since IP domains are unique and registered, localization is successful 95 to 99 percent of the time. Domain names provide additional security-related information. The new analysis option enables users to easily detect suspicious domains and unwanted countries that might present a security problem (Fig. 5).

The port scan function is another important security feature of the software. The client and server of an application talk to one another via ports. Via the operating system, an application offering a service in a network (server) opens a port (an address) that the client can access. This port waits for inquiries in the "listen" state. A port in "listen" state that is unintentionally open to the Internet is a potential gateway for attackers. Malware such as Trojans often open "backdoors" via freely accessible ports (some ports are reserved for certain applications). This is why it is highly recommended to review the open ports in a system from time to time – an easy to implement measure with the R&S®CMW-KM052 option.

No additional software is required on the DUT to use the analysis tool. The tests are independent of its operating system. DUTs with an antenna connector can be connected to the R&S®CMW500 via a cable. DUTs without a connector can be accommodated in an RF shielded box from Rohde&Schwarz and connected to the R&S®CMW500 via an air interface (Fig. 6).

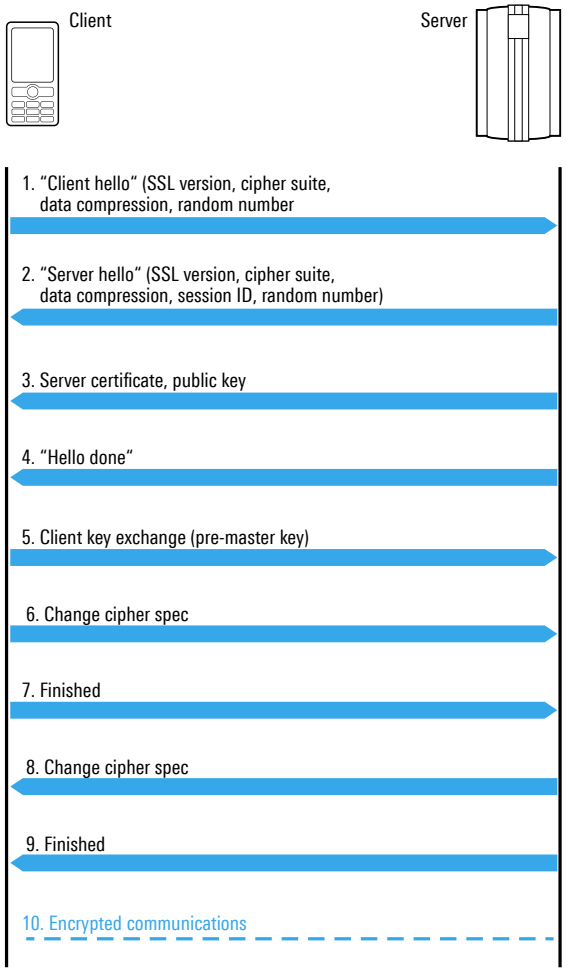
IP connection security

Transport layer security (TLS) – more commonly known as secure sockets layer (SSL) – plays a key role in secure online communications. The last version of the SSL protocol was 3.0. After that, development and standardization continued under the new name TLS, starting with version 1.0.

SSL/TLS defines security levels for communications between clients and servers, verifies the authenticity of the certificates and negotiates session keys. All of this takes place during the SSL handshake at the outset of each connection.

Due to the central importance of strong encryption for secure IP communications (key length recommendations available at www.keylength.com), the R&S®CMW-KM052 software thoroughly examines the SSL handshake. The clearly structured parameter list makes it easy to determine if connections meet security requirements (Fig. 4).

SSL/TLS handshake process



Source: https://publib.boulder.ibm.com/tividd/td/TRM/GC32-1323-00/en_US/HTML/admin231.htm

1. The client sends a "client hello" message that lists the cryptographic capabilities of the client (sorted in client preference order), such as the version of SSL, the cipher suites supported by the client, and the data compression methods supported by the client. The message also contains a 28-byte random number.
2. The server responds with a "server hello" message that contains the cryptographic method (cipher suite) and the data compression method selected by the server, the session ID, and another random number.
   Note: The handshake will fail if the client and server do not support at least one common cipher suite. The server generally chooses the strongest common cipher suite.
3. The server sends its digital certificate, which contains its public key. The client uses other certificates (TrustStore) to authenticate this certificate.
4. The server sends a "server hello done" message and waits for a client response.
5. The client sends a "client key exchange" message containing the pre-master secret that enables the server to generate the master secret for a symmetric cipher suite. The pre-master secret is encrypted using the server's public key and can only be decrypted with this key.
6. The client also generates the master key and sends a "change cipher spec" message to inform the server that the key was changed.
7. The client sends a "finished" message that is encrypted using the master key.
8. The server responds with a "change cipher spec" message …
9. … and also sends a "finished" message.
10. End of the SSL handshake and transmission of encrypted data.

Fig. 5: Certain IP addresses and countries can be unwanted in the data stream. The R&S®CMW-KM052 option shows whether the DUT contacts them.

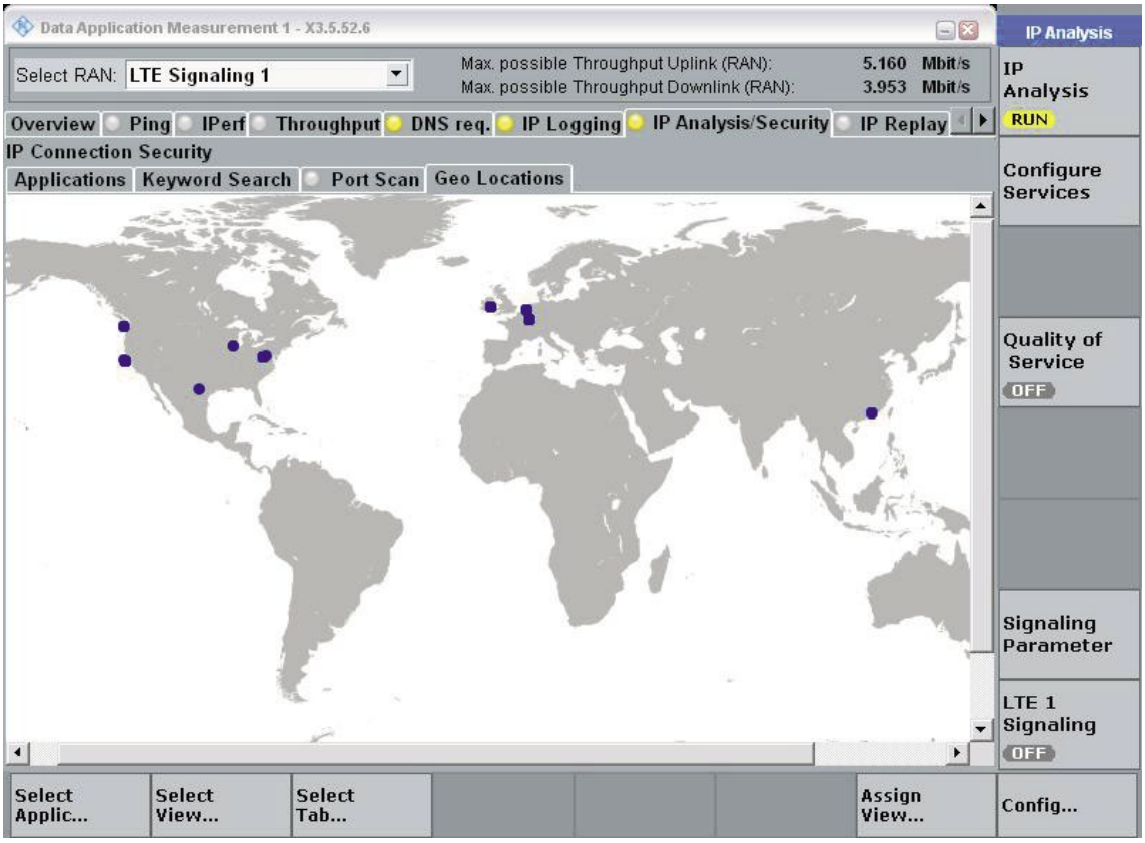


Fig. 6: DUTs without an antenna connector can be placed in an R&S®CMW-Z10 RF shielded box and connected to the R&S®CMW500 over the air.

Summary

Up until now, it was very difficult to analyze data traffic from mobile and IoT devices. Security weak points could go undiscovered for long periods of time. The R&S®CMW500 wideband radio communication tester with the R&S®CMW-KM052 analysis option solves this problem. Users can obtain a detailed overview of security-relevant communications parameters in a freely configurable controlled wireless environment and also determine whether a device behaves differently in WLAN and cellular networks.

Developers can detect security gaps early in the design process. IT teams can analyze the communications behavior of smartphones, tablets and apps used in the corporate environment. Automotive OEMs and network operators can verify that connected car and IoT devices comply with the specified connection security standards.

The test sequence is very simple since the DUT requires no preparation. The R&S®CMW-KM052 option integrates seamlessly into the powerful R&S®CMW500 test suite. A single T&M instrument now enables RF analysis in cellular and non-cellular networks, protocol tests and IP application tests as well as analysis of security-relevant parameters for IP data communications. A truly unique solution.

Christian Hof