Smart and secure: tap-proof voice calls on smartphones

Protecting call confidentiality on smartphones is a problem that etches deep worry lines into the brows of IT managers. Mobile phones are open to numerous avenues of attack by eavesdroppers. The TopSec Mobile, a handy little encryption device from Rohde&Schwarz SIT GmbH puts an end to all those worries. Connected to mobile phones over Bluetooth®, it encrypts calls using an approach that leaves no room for attack. It is also the world's first hardware encryption solution that works with unmodified iPhones.

Maximum security does not compromise convenience

Smartphones are now an integral part of our lives. It is hardly surprising that people sometimes unthinkingly use them to make calls that should be kept confidential. Users are often unaware of just how susceptible today's mobile phones and transmission paths are to attack by resourceful hackers (see box on page 45). In fact, the need for effective means of securing communications on mobile phones is huge: The armed forces, policymakers, government authorities and businesses all need solutions that let them use mobile phones without the permanent risk that the confidentiality of their calls is being compromised.

This challenge was taken on by Rohde&Schwarz SIT GmbH, a Rohde&Schwarz subsidiary whose information and communications technology security solutions are certified by the German Federal Office for Information Security (BSI) and NATO/SECAN. One requirement was clear from the outset: The solution would have to be one that a broad user base would willingly embrace. Users want to be able to make and receive secure business calls on mobile phones with the same ease and convenience as regular calls. And these users tend to upgrade regularly to new, more advanced models. This meant that an integrated cryptographic solution for smartphones was out of the question.

Rohde&Schwarz SIT has succeeded in creating a product that reconciles high security requirements with users' ease-of-use expectations. The TopSec Mobile (Fig. 1) is a handy encryption device that allows users to quickly and conveniently set up secure VoIP calls from a smartphone or laptop to other users anywhere in the world.

The TopSec Mobile is a crypto headset that connects to a smartphone over Bluetooth®. Calls are transmitted over an Internet connection using secure voice over IP (sVoIP) technology. VoIP is a global standard that offers smartphones universal and inexpensive access to the Internet over mobile networks and WLAN.

Fig. 1 The TopSec Mobile provides tap-proof, end-to-end encryption for mobile voice calls and works with laptops and almost all commercially available iOS and Android smartphones.

End-to-end security

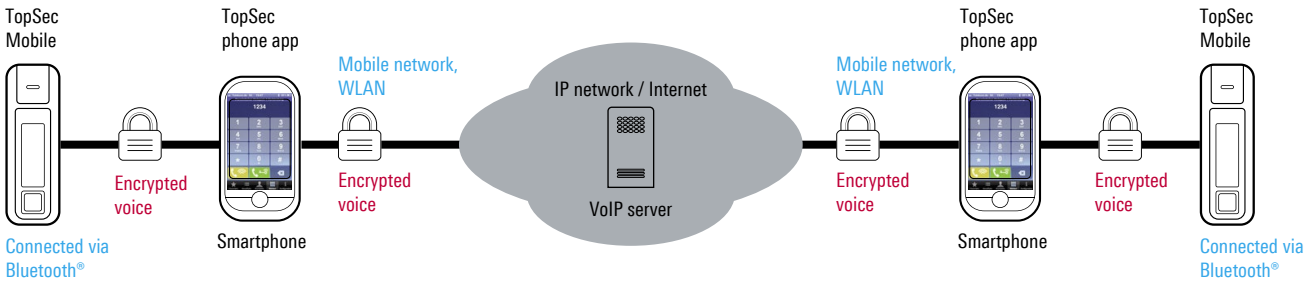

Fig. 2 End-to-end encryption with the TopSec Mobile.

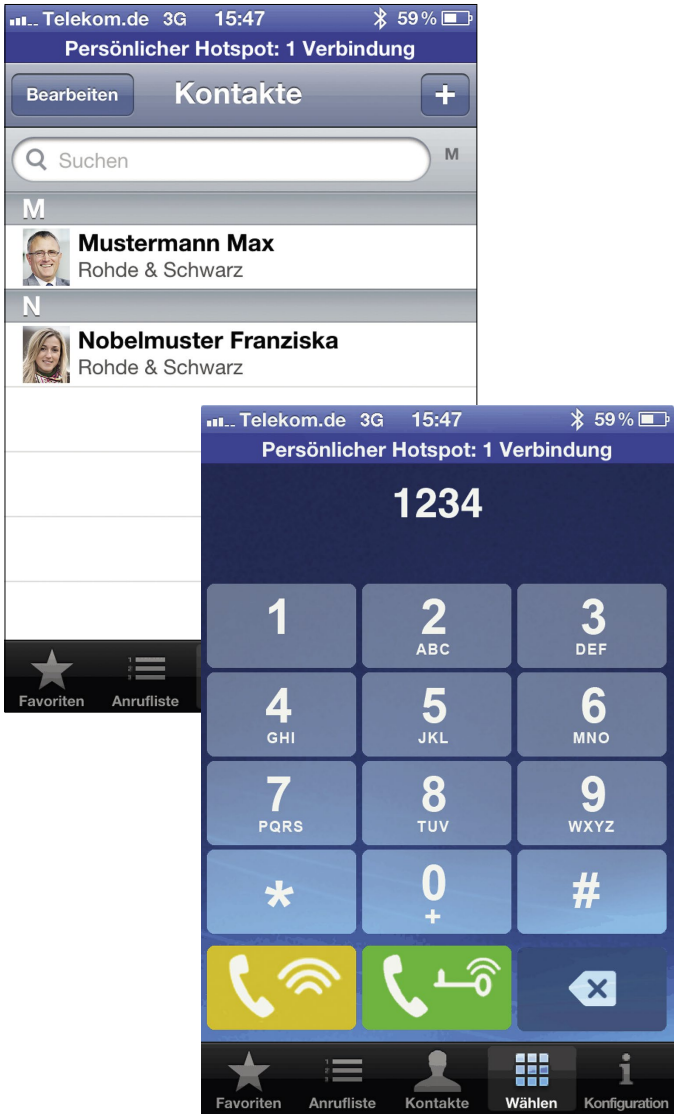

Fig. 3 The TopSec phone app: contact management and keypad for Internet telephony. The green call button sets up an encrypted connection over the TopSec Mobile; the yellow call button is for unencrypted VoIP calls.

The TopSec Mobile is a self-contained, independent security product that protects smartphones more reliably than integrated encryption solutions and avoids known vulnerabilities of WLAN and Internet interfaces or infected apps that can leave smartphones open to attack. All it needs is a Bluetooth® connection to the smartphone. The TopSec Mobile itself is a tiny headset with headphones, so the smartphone can stay in one`s pocket, handbag or drawer. Since the user's voice is encrypted by the TopSec Mobile prior to transmission and is decrypted by a TopSec Mobile at the other end, the call cannot be tapped, even if a phone has been compromised by malware (Fig. 2).

Mobile phones may come and go, but TopSec Mobile remains

The TopSec Mobile is a smart solution that accommodates the popular habit of frequently upgrading to the very latest phone models. By using Bluetooth® to connect to smartphones, the device can encrypt and decrypt calls. Since practically all smartphones today offer Bluetooth®, the TopSec Mobile can work with all leading Android mobile phones and the iPhone, which together account for around 85 % of the global smartphone market.

The device is also unique in that it is currently the only solution of its kind to work with the iPhone. Prior to the advent of the TopSec Mobile, specialized encryption apps were the only means of making tap-proof calls on the iPhone, and they cannot generally be classed as secure. Even the encryption solutions available on microSD cards, which typically afford greater protection than software-only encryption apps, are not completely secure since they do not connect directly to the phone's microphone.

One transmission path, multiple points of attack

Tapping calls on the smartphone itself is the easiest method, but not the only one. Mobile VoIP calls can also be attacked over the air interface, on WLAN routers, on the Internet and on VoIP servers (Fig. 4). Calls are also vulnerable to attack on UMTS or LTE connections, particularly when smartphones are forced to fall back to GSM mode.

Tapping is easiest to carry out on the smartphone itself due to the complexity, configurability and vulnerabilities of smartphone operating systems. Moreover, operating system updates can introduce new loopholes that may take software makers a long time to close. The sheer number of apps available for today's smartphones also aggravates the problem because it is nearly impossible to guarantee that they are all virus-free. And not all operating systems show users the access rights to local resources granted to the apps they download, or allow users to change them.

Security risks

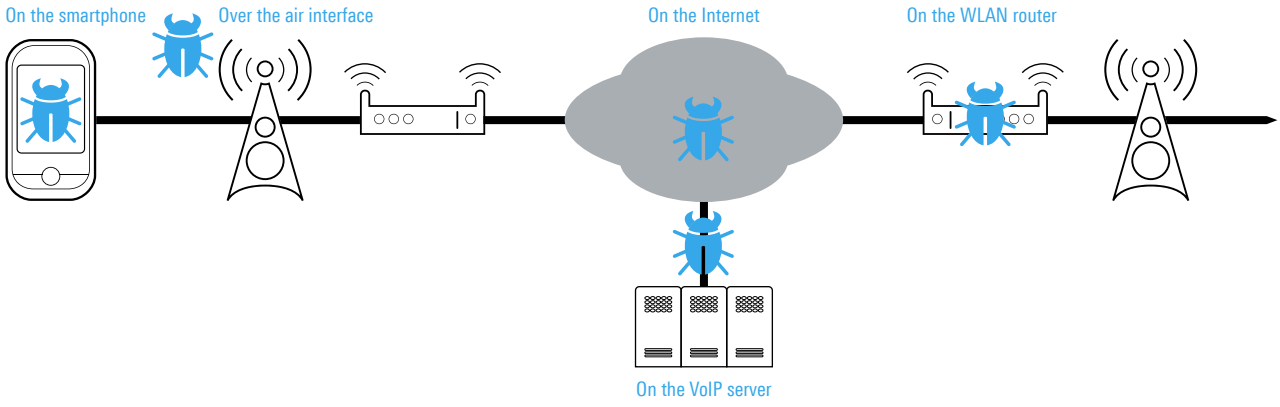

Fig. 4 Points of attack on mobile calls (example: VoIP calls).

Just how simple it is

All it takes to fully protect confidential calls are the following components:

- A smartphone or laptop with WLAN or mobile network access
- The TopSec Mobile
- The TopSec phone app

To place an encrypted call, the caller opens the TopSec phone app and chooses a contact from their personal contact list (Fig. 3). The caller then presses the encryption call button to call the contact's TopSec Mobile. If the contact accepts the call, the caller's TopSec Mobile rings. After the caller has confirmed the secret connection, the devices set up a secure link – a process that takes just a few seconds.

The TopSec phone app supports both encrypted and unencrypted VoIP calls. Encrypted calls take place directly on the TopSec Mobile. The device encrypts and decrypts calls independently, without involving the smartphone or laptop. When making secure calls, users talk and listen through the TopSec Mobile's own microphone and speaker, effectively eliminating any manipulation by malware.

VoIP calls have to be set up through a server, and users must be registered on the server in order to make and receive calls. The TopSec Mobile sets up encrypted connections using SIP and IAX2, two common signaling protocols. It works with both public SIP servers and with the R&S®VoIP-SERVER S110. The R&S®VoIP-SERVER S110 is ideal for user groups with special security requirements who prefer to operate their own VoIP server.

Erika Friesen