SECURE MOBILE VOICE COMMUNICATION ON AN OPEN PLATFORM

Alexander Höftmann *
Christine Mummert **
Christian Paschke ***
Mario Stemmler ****
Günter-Ulrich Tolkiehn *****

An open source project for secure mobile voice communication over IP using strong end-to-end encryption was launched. In its first stage, a solution using Android on two different standard PDA platforms, a central Linux system with Asterisk, and OpenVPN with OpenSSL encryption was realized. SIP-based Voice communication over WLAN with end-to-end security was successfully implemented. Concept, approach, first results and outlook on further work are presented.

INTRODUCTION

Mobile voice communication is ubiquitous today on a global scale. It is increasingly being used even for the most confidential issues. In contrast to older, analogue mobile telephony systems, the digital systems, especially those based on ETSI's GSM-standard, were for some time regarded to be secure, because details of their security mechanisms were not publicly known. A first successful hack on a GSM security feature was reported by the CCC already in 2001[1], and at the latest since 2009[2], this certainly does not hold any longer.

In addition VoIP, and also VoIP over WLAN are increasingly used. In particular VoIP over WLAN, which was not anticipated in the conception of WLAN technology, has never been regarded to be secure.

As a consequence, different approaches have been made to achieve secure mobile voice communication. A few examples: On the CeBIT fair 2010 German Telekom announced their SiMKo2[3] solution. It features secure mobile voice and data communication over IP on the basis of technology from Ethon. TAS on the same event introduced their *Mobikrypt* Solution[4] for secure mobile conferencing, on the basis of Rohde & Schwarz technology. Recently, on the same technology basis, there was a project for secure voice communication for ca. 5000 members of the German government[5] delivered by Secusmart. In both cases, the standardized 9,6kbit/s resp. 14.4 kbit/s CSD-service (circuit switched data) of GSM on standard mobile phones is utilized for voice. The cost of this solution, however, was reportedly exclusive, namely around 2.000 • per user. AT&T

*, **, ***, ****, ***** TFH Wilden, Germany

has in 2009 applied for a patent[6] for the use of SSL for the link between a wireless client system and an SSL enabled wireless access point. A first solution for secure VoIP with open-source technology was reported by Ryu and Nam[7] already in 2008. They did however neither use standard PDAs nor the Android platform.

Approach, Implementations, and Experiences

In the course of our discussions with a German specialist for secure communication, the ATMedia GmbH, the idea formed, to look for an easy solution for licence-free secure mobile voice communication on the basis of standard mobile platforms and open source software.

We had some experience with the Openmoko[8] platform, which is a completely (meaning hardware as well as software) open platform. This openness is very desirable, but some technical restrictions and reported problems of the Openmoko initiative just before the beginning of our project made us start with the Android[9] platform, developed by the Open Handset Alliance[10]. Some experiences with Android on HTC's *Dream* and *Hero* hardware were already present.

Our idea was, not to use the CSD or HSCSD service, but the packet-based services and to implement strong IP-based end-to-end encryption for the VoIP communication as well as potentially any other IP based communication over WLAN and alternatively over the packet-based GSM/UMTS services. Of course, for both options, unauthorised monitoring of the conversation shall be made difficult, in the air as well as on the fixed networks. In our project's first phase, about which we report here, we worked with VoIP over WLAN using the SIP technology (IETF RFC 3261 and related specifications).

As mobile system platforms two standard mobile devices of HTC with Android were chosen, the *Dream* , *Hero*, and the *Tattoo*.

To create secure connections, we used OpenVPN 2.1.1, which is available in a version specially precompiled for the Android platform. OpenVPN uses OpenSSL for encryption. OpenSSL contains different encryption groups, namely AES, Base64, Blowfish, CAST, DES, and RC. Security level and the computing resources required vary for the different standards. For voice over WLAN, we typically use small IP packets of 160 byte payload. Modern mobile devices, however, generally have sufficient CPU performance and memory.

The operating systems of the mobile devices had to be replaced, as the delivered versions contain restrictions, which prevent the installation of OpenVPN. For Linux-based platforms his process is called *rooting*. In the internet, various runtime versions of the operating system (called ROM) including installation instructions are available, differing on the one hand in the Android version (1.6, 2.0, 2.1, and 2.2) and on the other in the repertory of different functions and applications contained. We tried different versions.

During these works it appeared that for rooting the use of microSD modules of manufacturer Kingston is recommended. Rooting of the HTC Tattoo turned out to be relatively easy. After installation of the HTC Sync Software and activation of the USB debugging mode it could be done with a previously downloaded *rootTattoo.batch* script. Subsequently the installation of a ROM with root-rights could be done. Choosing a suitable ROM is not very easy as very many different versions are available from the Android community. From Android 2.0 upwards, applications may be stored on the microSD-module, which is very helpful. On the other hand, for the HTC Tattoo, Android 1.6 is the only version supported by the manufacturer. Custom ROMs for higher Android versions are available, but e.g. none of these contains camera support.

The custom ROMs are delivered as packed archives with signature. This signature is stored in different files of the Custom ROM. If you want to do changes, you have to produce new signatures, which are checked by the bootloader during the update.

An Asterisk[11] switch and an OpenVPN server were installed on a standard Ubuntu 9.10 Linux system on a standard desktop PC hardware connected to the WLAN.

As a first step, we implemented a connection between a mobile client and the Asterisk switch. The second step was then a SIP controlled VoIP connection between two mobile devices over (non-QOS) WLAN via the local server.

First results and further work

In the first stage of the two-semester-project, which was finished by July, 2010, we managed to find and implement a solution for secure SIP-based voice-over WLAN. Voice over WLAN is the most vulnerable type of digital mobile communication. Our solution uses Android, sipdroid[12] beta 1.5.4 and the OpenSSL encryption of OpenVPN. Our first test result with different encryption groups unexpectedly showed, that AES in 128bit cipher chaining mode yielded the highest data throughput.

The solution is completely free of licence fees. The prototypes are running on two standard HTC hardware's so far.

Voice conversation was clearly understandable. The additional latency imposed by the encryption/decryption is small, as was expected. Extension of connections outside the LAN over the "public" internet, more detailed QOS-measurements, as well as codec's with better voice quality are on the agenda. Consumption of system resources seems to be uncritical, but will also be further investigated in more detail.

Our next goal is to implement voice over IP using the IP data services of the mobile operators as well. Here we face the situation, that as long as we do not use EDGE (Enhanced Data Rates for GSM Evolution) or UMTS, for plain GPRS (56 kbit/s) we have to restrict ourselves to licence-free low bitrate IP codecs (i.e. not ITU-T G.729 or G.723.1). Another expected advantage besides better connectivity is lower power consumption compared to WLAN.

To make such solutions usable for end-users, an important issue is to prepare easy-to-use update make-files. Others are the key-management and the user-interface. Here one goal is the integration of the OpenVPN into the sipdroid GUI. Implementation on other hardware platforms as well as the support of non-voice services will be further issues.

These issues will be addressed in our next project-phase (autumn term 2010).

References

„CCC clont D2 Kundenkarte", 26. Nov. 2001,
http://dasalte.ccc.de/gsm/?language=de

S. Krempl, "GSM-hacking made easy", Heise Online, 28. Dec. 2009
http://www.h-online.com/open/news/item/26C3-GSM-hacking-made-easy-893245.html

SiMKo2 announcement
http://www.telekom.com/dtag/cms/content/dt/en/813118

Press information about Mobikrypt
http://www.tas.de/fileadmin/user upload/ temp / PM Security2010.pdf

F. Gathmann and M. Kremp, „Merkel wird abhörsicher", Spiegel-Online, 18. Nov. 2009
http://www.spiegel.de/netzwelt/gadgets/0,1518,661812,00.html

AT&T patent application "Communication via a wireless gateway device and SSL", Pub. No.: US 2010/0177896 A1, Jul. 15, 2010
DH Ryu and SG Nam "
Implementation of Wireless VoIP System based on VPN .
" in 7th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications, Cambridge, UK, February 20-22, 2008

Openmoko Project
http://wiki.openmoko.org

Android
http://www.android.com

Open Handset Alliance
http://www.openhandsetalliance.com

Asterisk, the open source telephony project
http://www.asterisk.org/

Sipdroid
http://sipdroid.org/