SECR3T: Secure End-to-End Communication over 3G Telecommunication Networks

Giuseppe Cattaneo, Giancarlo De Maio, Fabio Petagna
Universitá di Salerno
Dipartimento di Informatica e Applicazioni
cattaneo@dia.unisa.it, g.demaio@gmail.com, fabpet@dia.unisa.it

***Abstract*—Nowadays the use of video conference tools from mobile devices is becoming more widespread. Unfortunately, solutions based only on the security features inherited from the operator infrastructure cannot be blindly trusted. Therefore, the need for secure communication tools is rapidly increasing. Currently, voice and video communication tools are considered unreliable when used in either a mobile context or under poor signal strength conditions. This is particularly true for IP connections routed on the Packet-Switched Domain (PSD) over 3G mobile networks.**

This paper presents the design and the implementation of SECR3T (Secure End-to-End Communication over 3G Telecommunication Networks), a fully-fledged secure communication system for mobile devices based on the native Circuit-Switched Domain (CSD) of 3G networks. To the authors knowledge, this is the first solution for secure communication over the CSD of 3G networks.

The security schemes implemented by SECR3T include mutual end-to-end authentication as well as data encryption. The adopted end-to-end security mechanisms have been embedded within the native 3G-324M protocol and do not require any form of interaction with the mobile network operator.

Relying on the CSD, SECR3T provides a better QoS with respect to the PSD based solutions for 3G networks. It also requires less power consumption as the user is registered once on the Base Station (BS), with the handset not having to implement any heavy keep-alive protocols. In order to prove the effectiveness of the adopted strategy, a prototype was implemented to compare its performance with the well-known PSD solutions. Subsequently, the authors experimentally evaluated the security strengths and the impacts produced on the user experience with respect to traditional tools using CSD.

***Keywords*-UMTS; 3G-324M; X.509; mobile; CSD; audio/video; encryption; power consumption.**

I. Introduction

The services provided by modern 3G telecommunication technology can be divided into two classes, each in charge of two different network domains: Circuit-Switched (CS) and Packet-Switched (PS) domain. Different domains provide different services, for example, videotelephony is routed to the CS domain while IP networking takes place in the PS domain.

Unlike IP networks, terminals in 3G networks are not affected by addressing problems. Every device equipped with an USIM is automatically connected to the mobile network and made available through its telephone number to other mobile devices. Moreover, UMTS networks provide an adequate QoS for real-time communications, including minimum cell rate (64Kb/sec for video-calls) and low latency. The CS connection between terminals is carried out and managed by the network.

Telecommunication companies have put a great deal of effort into the diffusing, global coverage and amount of different services provided to the users, such as videotelephony, text messaging and data communication. However, less effort has been put into providing suitable end-to-end security mechanisms for these services. In fact, voice, text and video communications carried out using 3G networks have been proven to be vulnerable to eavesdropping and unauthorized access. Both wireless data links as well as wired parts of the network are susceptible to several security threats.

Considering that videotelephony is essentially “data communication”, both CS and PS domains on the 3G networks are suitable for this service. The adoption of the PS has many advantages but also several relevant drawbacks with respect to the CS. The most significant advantage of the PSD is the use of the IP protocol, which ensures interoperability with almost all network applications for both mobile and desktop devices. IP security protocols such as TLS, IPSEC and VPN, along with already existing systems for end-to-end security at application level, can be reused without any modifications. Even if efficient and easy-to-use solutions have been presented for voice/video communications over IP networks, an effective and reliable videotelephony service needs both reachability as well as availability which cannot be always satisfied by an IP-based mobile network. Given that mobile networks do not have global coverage, handover processes and high Bit Error Rate (BER) on the wireless link tend to make the channel unstable. On the contrary, the CS network connections are more stable in high-mobility and high-BER conditions, thus granting reachability and availability to the users.

In this work, a metric to evaluate the communication service, based on the following key performance indicators, has been defined: voice and video quality, user data privacy and application impact on the battery life. These metrics are often related to the domain that provides the service. Generally, videotelephony over the CS domain results in a better quality and greater battery saving with respect to the PS domain. In fact, the CS connections between the endpoints are provided by the telecommunication network with a higher QoS value, with it being managed by the BSs rather than by the IP connections which are managed by the peers. On the contrary, applications running over the CS domain must comply with inflexible network protocols through which it is hard to provide the same security level of the applications running over IP. The aim of this work is to improve the security of videotelephony over the CSD, in order to achieve an optimal trade-off for the key performance indicators discussed above.

A. Trusting

When an end-user signs a cell-phone contract, he implicitly trusts the mobile network operator, which is supposed to preserve communication privacy. Therefore, the mobile network operator must guarantee adequate security measures to accomplish this task. While on 3G mobile networks, channel encryption has been adopted for wireless links, user data on wired links is transmitted in clear, thus introducing several potential threats. Moreover, 3G networks extensively rely on roaming, following agreements signed between two or more operators. This means that end-users should also trust the roaming operator, given that the physical telecommunication channel is managed by another company.

Encryption at network level may raise several issues. Assuming that end-to-end user communication passes through a lot of network elements, interoperability between different mobile network operators may be harder to reach because cryptographic keys and security protocols should be deployed among network elements managed by different providers. Moreover, there are authorities that must be able to implement phone tapping. In many countries, there are laws against terrorism which enforce the ability of the network operators to intercept the communications related to a suspected user. Encryption at network level may also interfere with these tasks.

The solution proposed in this paper is an end-to-end security mechanism for 3G videotelephony. Such a solution may also include fair mechanisms for key-escrow.

B. Security background

In 1999, with the standardization process of 3G mobile networks, the 3GPP[1] Consortium, which is in charge of producing the technical specifications for the 3G mobile networks, proposed improved security mechanisms for wireless channels with respect to the GSM ones, which have been proven to be vulnerable. The 3GPP introduced a stronger authentication and key-agreement protocol performed by mobile devices and networks, as well as a stronger cryptosystem for wireless data encryption (A5/3 based on the KASUMI [1] algorithm). However, effective attacks which can lead to the decryption of the communication channel have been discovered. Keller and Shamir presented an attack on KASUMI which makes it possible to recover a full A5/3 key using a related-key attack [2]. Karsten et al. [3] showed how to perform a semi-active attack by jamming UMTS frequencies and forcing the mobile device to switch to GSM mode.

There are several projects addressing application-level end-to-end security of voice communications over mobile networks, such as SPEECH [4]. To the authors knowledge, there are currently no tools addressing the security of the videotelephony communication routed by the CSD of the 3G mobile networks.

C. Outline

The rest of the paper is organized as follows. Section II presents the requirements of the project. In Section III, the 3G-324M communication protocol is described, while in Section IV the integrations aimed at enhancing the security of the protocol are discussed. In Section V, the impact on the overall system performance is briefly evaluated. The paper ends with a discussion on future studies in Section VI and the authors conclusions in Section VII.

II. Requirements

The main aim of this work is to present a system that realizes a secure video-call over 3G mobile networks with the following requirements:

- *Strong end-to-end user authentication through digital certificates.* In order to achieve the strong end-to-end user authentication requirement, it is supposed that the user adopts a X.509 digital certificate issued by a trusted Certification Authority (CA), with it being securely stored on the mobile equipment.
- *End-to-end user communication encryption.* The audio, video and data channel encryption requirements can be achieved by using robust and well-known encryption algorithms. The authentication protocols must also implement key-agreement mechanisms in order to properly initialize the channel encryption.
- *Compliance with videotelephony protocols.* The proposed solution must be compliant with existing applications and not require any modifications to the native videotelephony protocol.
- *Infrastructure-side transparency.* It is required that no extra effort should be made by the network elements to support the described end-to-end security mechanisms, therefore the encrypted data must be transmitted between users as normal network traffic.
- *Limited impact on system performance.* The introduction of security mechanisms should not considerably affect the system performance and the user experience. For example, the initial handshake should not delay the communication longer than a few seconds. Analogously, during the conversation, communication delays due to data encryption should not be longer than 300 milliseconds.

[1] The 3rd Generation Partnership Project (3GPP), http://www.3gpp.org/

- *Device constraints.* In order to cope with the low processing power as well as save battery life, local computations and end-to-end communications must be minimized. The secure video-call system should implement public-key encryption schemes based on the Elliptic Curve Cryptography[2] (ECC) instead of traditional public-key cryptosystems.

III. Videotelephony over UMTS

In this section a brief introduction to the 3G videotelephony protocol is presented in order to explain how it can be extended to support security mechanisms.

3G-324M [5] is the 3GPP umbrella protocol for videotelephony in 3G mobile networks. The 3G-324M protocol operates over an established CS connection between two communicating peers. It is based on the ITU-T[3] H.324 [6] specification for multimedia conferencing over CS networks.

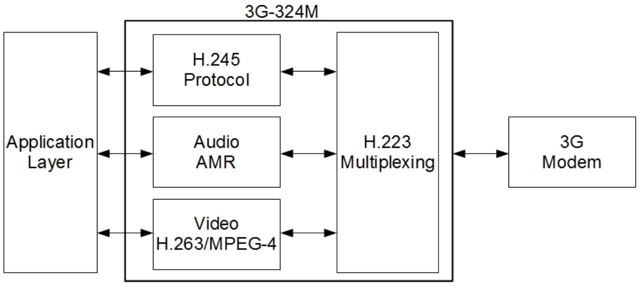

Figure 1. 3G-324M protocol: simplified architecture.

Figure 1 shows the main components of the 3G-324M protocol. The H.245 protocol is designed to provide reliable, acknowledged transmission of session control information. It uses a Numbered Simple Retransmission Protocol (NSRP) as well as a Control Segmentation and Reassembly Layer (CSRL) in order to segment larger control messages and reduce their susceptibility to error. H.223 provides the functions used to multiplex audio, video and text in a single stream processed by a 3G modem. The audio and video modules provide standard procedures to encode the media streams. The mandatory audio codec for 3G-324M is GSM-AMR [7]. H.263 [8] is the mandatory video codec whereas the MPEG4 is optional. The Application Layer (AL) represents the existing videotelephony application and is not part of the 3G-324M protocol stack.

Considerations on the video codecs: The video codecs used in the 3G-324M protocol have some characteristics which are to be considered for the correct design of the SECR3T framework.

On the transmitter side, H.263 and MPEG-4 codecs produce variable-length frames which are divided into Group Of Blocks (GOBs) to be sent to the multiplexing level. Every GOB has a resynchronization marker to reduce the error propagation caused by the nature of Variable Length Code (VLC) into a single frame. On the receiver side, the blocks are received one-by-one from the multiplexing layer, with the reception of a resynchronization marker indicating the start of a new GOB. Due to the resynchronization marker and the VLC, the encryption of a GOB must be performed block-by-block.

IV. A secure video-calling system

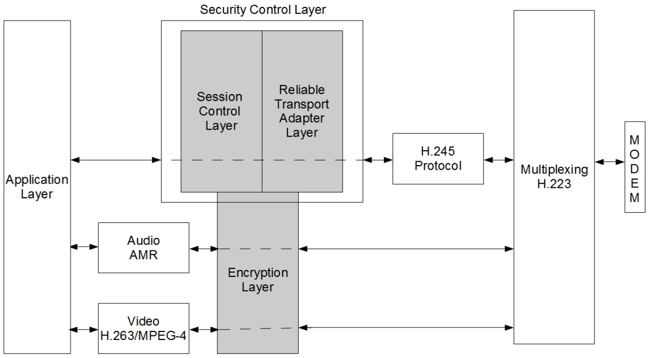

Figure 2. The extended 3G-324M architecture: the white modules compose the original 3G-324M architecture. The gray modules represent the proposed extensions for secure end-to-end communication.

A. High-level design

The SECR3T project consists of a framework which extends the 3G-324M specification and makes it possible to integrate security mechanisms within the existing videotelephony protocol. The high-level architecture of SECR3T is shown in Figure 2. The Security Control Layer (SCL), which includes the Session Control Layer (SESCL) and the Reliable Transport Adapter Layer (RTAL), is a middleware added to provide the AL with the procedures to initialize and manage the security protocols. It uses the reliable H.245 protocol to interact with the peer. The AL also sends to and receives data from the Audio/Video (A/V) modules, which control the communication of the multimedial streams. A/V data can pass through the Encryption Layer (EL) which provides the encryption functions for the outgoing streams as well as the decryption functions for the incoming streams.

The SCL implements the configuration module, the key-agreement and authentication protocols. The EL includes the audio, video and text encryption mechanisms.

Efficiency requirements are obtained employing robust and well-known implementations of the encryption protocols as well as techniques to reduce the communication overload. Cryptographic algorithms have been chosen according to these requirements. For example, ECC based algorithms

[2] With respect to RSA, ECC offers equivalent security with smaller key sizes, which results in faster computations, lower power consumption as well as memory and bandwidth savings.

[3] International Telecommunication Union - Telecommunication Standardization Sector, http://www.itu.int/ITU-T/

have been adopted, given that they guarantee the same security level of traditional encryption algorithms but more efficiently.

SECR3T is compliant with the UMTS network protocols, in other words, the execution of the cryptographic protocols and the algorithms are carried out transparently to the network. The system also performs an auto-discovery procedure to determine if the peer is able or not to run the security extensions.

1) Authentication and Key-Agreement: Whenever two video-calling applications establish a communication channel through the 3G-324M protocol, the users can initiate a secure conversation running a key-agreement protocol through the SECR3T extensions. The purpose of these protocols is to generate a common session key to be used for encrypting voice, video and text data streams and, optionally, to verify the identity of the parties in the conversation.
SECR3T supports three different forms of user authentication and key-agreement schemes, each with a different level of security.

- *Elliptic Curve Diffie-Hellman Key-Agreement.* Whenever two users initiate a new conversation, SECR3T permits to run the 521-bit prime Elliptic Curve Diffie-Hellman (ECDH) key-exchange protocol [9] to agree upon a common secret key. This form of agreement does not guarantee the user the identity of the other endpoint of the conversation but it is enough if one is merely interested in guaranteeing the confidentiality of a conversation.
- *Passphrase based Key-Agreement.* Two users interested in having a secure conversation choose a pre-shared passphrase. Whenever a new secure conversation has to be initiated, each one will generate a secret using the pre-shared passphrase. The reuse of the same passphrase is always possible. In fact, the generated common secret (and consequently the session keys) will be never the same because the key-exchange algorithm is based on the exchange of encrypted random values. This approach gives a basic form of authentication since it is expected that the passphrases are only known by their legitimate owners.
- *Certificate based Key-Agreement.* Two users initiating a new secure conversation own a legitimate X.509 digital certificate which has been previously loaded onto their device. Moreover, the certificates of the root CAs must be available on the devices in order to verify the validity of the peer certificate. If these conditions are met, the two parties use the standard TLS 1.0 protocol [10] to carry out the mutual authentication and key-agreement. The call originator plays the role of client in the TLS protocol, while the receiver plays the server role. According to the TLS specification, each client submits to the peer its X.509 certificate and provides it with the possibility to verify its identity.

2) Encryption: The key-agreement scheme produces a random shared secret which is processed by the PBKDF2 algorithm (Password-Based Key Derivation Function)[4] to generate the cryptographic keys for the symmetric ciphers currently in use. It generates six 256-bit cryptographic keys, each used for a single unidirectional data stream:

- Output *audio* encryption key
- Input *audio* decryption key
- Output *video* encryption key
- Input *video* decryption key
- Output *text* encryption key
- Input *text* decryption key

AES with 256-bit key in Output Feedback mode (OFB) provides the encryption of the communication channels. The AES algorithm is one of the most commonly used encryption standards, with it being chosen due to its proven robustness and efficiency. The OFB mode avoids bit error propagation and does not affect the error resilience mechanism of underlying communication levels.

3) Secure Instant Messaging: A textual Instant Messaging protocol with Security extensions (SecIM) was implemented exploiting the H.245 control channel. The SecIM protocol is a proof-of-concept utility which demonstrates that arbitrary data can be exchanged between the video-call participants. The data integrity of the messages exchanged by the peers using SecIM is provided by the HMAC-MD5 algorithm. This result opens the way to a large number of promising applications. For example, it could replace the current SMS technology used for device-to-device alerting systems. Unlike SMS, the designed messaging protocol can guarantee reliability and real-time delivery.

B. Low-level design

SECR3T was designed using a bottom-up approach, with the lower-level modules being designed first. A preliminary experiment was carried out in order to confirm that the 3G networks can deal with encrypted payloads. In other words, the SECR3T protocol expects that non-standard data can be transmitted between the video-call users, with audio/video encrypted packets being routed through the telecommunication network and the network entities treating them as common packets. To confirm this hypothesis, a XOR-module was integrated into the existing 3G-324M protocol stack in order to encrypt voice, video and text just before the radio transmission. This module performs a one-time-pad XOR encryption and decryption,

[4] PBKDF2 is part of the Public-Key Cryptography Standards (PKCS) by RSA Laboratories, specifically PKCS #5 v2.0 [11]

respectively, of the outgoing and incoming audio data. To encrypt the video packet, the most difficult task was to deal with the characteristics of the video codec, as explained in Section III. The audio and video XOR experiments were carried out with success and confirmed that the network-level protocols were completely unaware of the application-level traffic. The XOR module was replaced by the EL in the release version of SECR3T, as shown in Figure 2.

1) Encryption Layer: The EL is composed of two sub-modules which deal with the audio and the video streams. It implements AES to encrypt/decrypt the audio/video streams. On the transmitter, the audio sub-module takes the AMR audio as input and encrypts it using AES. The video sub-module runs a similar procedure encrypting the single blocks instead of the entire video frame, as discussed in Section III. On the receiver, the EL takes the encrypted packets coming from the multiplexing module as input and uses the appropriate key to decrypt them. The plain-text data is subsequently passed to the higher protocol layers.

2) Session Control Layer: The SESCL is introduced in order to provide procedures to configure and manage the security mechanisms. As shown in Figure 2, it directly interacts with the AL and the EL. The SESCL encapsulates the cryptographic protocols and performs all the session-specific operations as cryptographic keys management, EL initialization and virtual streams initialization. Simultaneously, it abstracts the AL from the underlying security protocols. It contains procedures to generate the cryptographic material used by the PBKDF2 function. Moreover, it provides a function to enable/disable on-the-fly the security extensions. This runtime activation function can be useful, for example, in order to avoid cryptographic overhead if encryption is not necessary.

The SESCL includes robust well-known authentication and key-exchange protocols such as TLS and ECDH (see Section IV-A1 for details). It also provides primitives to integrate new communication protocols within the SECR3T system. In order to register a new protocol implementation, an adapter it is necessary which makes use of the RTAL functions (discussed below) to implement the communication between the peers. As a proof-of-concept, the SecIM protocol was implemented demonstrating the flexibility of the SCL managing general-purpose communication protocols.

3) Reliable Transport Adapter Layer: Reliable data delivery is crucial for the proper functioning of the authentication and key-agreement protocols, because an error on a single bit during the data-exchange will cause the entire re-execution of the protocol. The extremely high BER of the wireless links ($10^{-3} \leq BER \leq 10^{-2}$) is worked around by implementing a reliable transport layer over the H.245 protocol. As explained in Section III, H.245 provides reliable, acknowledged transmission of control information and segmentation of larger messages. Moreover, it provides support for user-defined communication through the *UserInputIndication* message, originally introduced to simulate the transmission of DTMF tones over digital networks. In particular, the *UserInputIndication* message is defined in the H.245 standard using the ASN.1 encoding and makes it possible to exchange arbitrary alphanumeric strings between the peers. The RTAL uses the *UserInputIndication* mechanism to provide procedures in order to open virtual streams between the peers and transmit general-purpose data structures. The RTAL interface exposes a basic symmetric non-blocking primitive *put()*, which sends data on an opened virtual stream, and a symmetric blocking primitive *get()*, which receives data from an opened virtual stream.

C. Implemented protocol stack

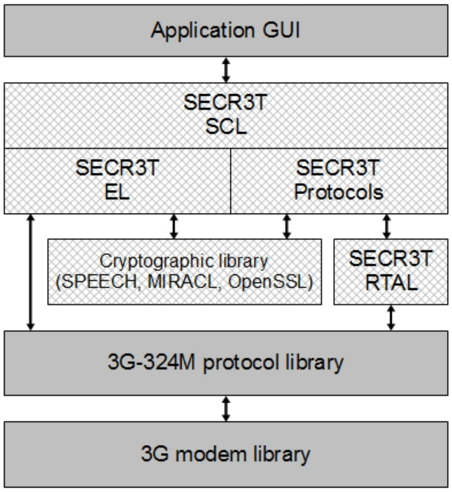

Figure 3. SECR3T implementation stack.

A SECR3T prototype working in a real environment was developed by the authors. The prototype runs on PCs equipped with UMTS USB tokens and was implemented for Windows XP/7 platforms.

The overall implementation is in standard ANSI C++ and the adopted IDE was Visual Studio 2008. The project consists of more than three thousand source files and headers. OpenSSL was used to implement the TLS handshake. Implementations of ECDH, passphrase authentication and AES was imported from the SPEECH project, which uses the MIRACL[5] library for high-precision operations on elliptic curves.

[5] Multiprecision Integer and Rational Arithmetic C/C++ Library at http://www.shamus.ie/

Figure 3 shows the SECR3T implementation stack. The users interact with the SECR3T GUI module, which sends commands to the SECR3T core modules. The SCL module manages the authentication and key-agreement procedures, and interacts with the EL, which creates the encrypted data channel. The data delivery is demanded to the 3G-324M protocol library, which directly interacts with the hardware.

V. System performance

In order to gain a more detailed understanding of the impact produced by the proposed extension on the original 3G-324M protocol, an experimental analysis on the implemented prototype is required. Performance evaluation in this context is known to be difficult. This is mainly due to the unpredictable side-effects introduced by the network elements used to connect the endpoints. In fact, depending on the BS load and distance, the interconnection links can increase the system entropy. Consequently, the testing methodology is only aimed at measuring the effect introduced by the security modules/protocols on the overall system performances compared to the performances obtained using the standard (unencrypted) protocols.

Although an exhaustive performance analysis is not part of this study, the early experiments in a real environment have shown that the prototype is robust and flexible enough to be adopted under several network conditions. The key-agreement and authentication protocols were tested with success and the network never rejected the encrypted packets.

A. Experimental setup

In order to obtain factual results, SECR3T was tested using USIMs belonging to all the Italian UMTS network operators (TIM, Wind, Vodafone, H3G). The experiments were carried out using the 3G network as if regular customers. In other words, the operators were not aware of the tests being carried out.

The prototype was tested using the following hardware platforms:

- PC1: Notebook with CPU Intel Core Duo T2300 at 1.66GHz, SDRAM DDR2 1GB;
- PC2: PC with CPU Intel Core Duo 2 E6400 at 2.13GHz, SDRAM DDR3 2GB.

The following devices were used for the 3G connectivity:

- UMTS USB Token - Onda MSA523HS;
- UMTS USB Token - Onda MDC502HS.

The prototype was tested on Windows XP SP3 and Windows 7 Professional.

The execution time of the prototype procedures was measured using the high-resolution performance counter library, included in the Windows API, called *QueryPerformanceCounter()*.

B. Results

The privacy provided by SECR3T to the user relies on the security strength of the cryptographic protocols that have been used. The battery consumption strongly depends on the implementation of the adopted protocols. It was measured that a secure video-call, performing a TLS handshake and lasting 5 minutes, do not discharge the device battery more than 1/10 of the original video-call application. The service quality was evaluated empirically, with the SECR3T implementation not showing to cause any detectable degradation of the user experience with respect to the ordinary video-call. The early experimental results were confirmed by an analysis of the delays introduced by the protocols and encryption procedures, respectively reported in Table I and Table II.

Table I
Delay introduced by the protocol execution

Protocol	**Minimum**	**Maximum**
Passphrase	1678,73 msec	2100,03 msec
ECDH	1171,92 msec	1363,27 msec
TLS	6325,2 msec	9227,11 msec

Table II
Delay introduced by the local encryption procedures

	Data Type	
Avg	**Audio**	**Video**
- per-packet delay	0.00821606 ms	0.0112831 ms
- packets sent every 60sec	3000	900
- delay every 60sec	24,65 ms	10,15 ms

VI. Future works

The experimental results of the SECR3T framework appear promising and encourage further research. In particular, the SECR3T project is a starting point to design mechanisms for the authenticity, integrity and non-repudiation of the conversation, in order to provide a multimedial communication service which has legal validity and can be used, for example, in a Court of Law for remote interrogations, in contracts signing, in remote purchases, etc.

With this aim, the authors are working on the following improvements.

User certificate in the USIM card: The achieved implementation of the TLS protocol over 3G-324M for user-authentication and key-agreement is an important result and can motivate the introduction of digital certificates within USIMs, both simplifying and reinforcing the realized security infrastructure. However, this task should be implemented by the mobile telephone companies.

Audio/Video integrity: A possible extension of SECR3T is the support for data integrity at the EL. This task may be difficult due to the inflexibility of the communication protocols. Audio and video packets have a fixed size, with it being possible to append information about data integrity (for example a HMAC code) only reducing the payload size. This solution led to audio/video quality loss and is not compliant with the 3G-324M specifications. A possible solution is to exploit the H.245 control channel to send the integrity information separately. However, it is important to note that audio/video packets are not numbered and packet loss is highly probable due to the BER, which increases the difficulty when implementing this solution.

Non-repudiation: Non-repudiation mechanisms can be designed over the SECR3T framework. It would be useful for both parties to have, at the end of the communication, an identical copy of the conversation. Such a task is not easy as it seems because both the underlying communication channel and the transport protocol may be unreliable, with audio/video packets possibly being damaged or lost. The out-of-band H.245 channel could be used to implement this feature, for example, sending the digital signature and the integrity information of the packets.

VII. Conclusions

This work demonstrates that it is possible to integrate cryptographic mechanisms within the 3G-324M protocol (and most generally in H.324) in a totally transparent way for the mobile operators, preserving compatibility with the 3G network specifications, resulting only in a minimal delay of the communication. The QoS provided by the telecommunication network for the underlying CS channel connecting the 3G-324M endpoints is generally better that the one provided for the IP channel in high mobility environments. The proposed solution is a valid alternative to the existing IP-based protocols for secure video-calling, providing reachability and availability features.

The SECR3T framework is an extended 3G-324M protocol which includes several security features. Authentication and key-agreement protocols were designed using the reliable H.245 control channel. The TLS handshake protocol provides strong user authentication using X.509 digital certificates. The SECR3T framework provides encryption for voice, video and textual communication. It supports the installation of new cryptographic protocols through its extensibility interface.

A SECR3T prototype was realized and tested in a real environment. Early experiments have confirmed the robustness of the SECR3T protocol. The TLS handshake takes between 8 and 13 seconds. The audio/video delay introduced by the encryption process is undetectable. Assuming that the user authentication only happens once at the beginning of the conversation, it is possible to conclude that the overall system performance seems to be suitable for real-case use. The authors are currently carrying out a detailed experimental analysis in order to minimize the impact of S3CRET on the overall system performance.

References

[1] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects, "3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification," 2000, http://www.3gpp.org/ftp/Specs/html-info/35202.htm.

[2] O. Dunkelman, N. Keller, and A. Shamir, "A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony," Cryptology ePrint Archive, Report 2010/013, 2010, http://eprint.iacr.org/2010/013.

[3] N. Karsten and C. Paget, "GSM: SRSLY?" in *26th Chaos Communication Congress*, 2009. [Online]. Available: http://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html

[4] A. Castiglione, G. Cattaneo, A. D. Santis, F. Petagna, and U. F. Petrillo, "SPEECH: Secure Personal End-to-End Communication with Handheld," in *ISSE*, 2006, pp. 287–297.

[5] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects, "Codec for circuit switched multimedia telephony service; Modifications to H.324 (Release 9)," 2009, http://www.3gpp.org/ftp/Specs/html-info/26111.htm.

[6] ITU-T Standardization Sector, "Recommendation H.324: Terminal for low bit-rate multimedia communication," 2009, http://www.itu.int/rec/T-REC-H.324/recommendation.asp?lang=en&parent=T-REC-H.324-200904-I.

[7] 3rd Generation Partnership Project, Technical Specification, "3GPP TS 26.190; Transcoding functions," 2009, http://www.3gpp.org/ftp/Specs/html-info/26190.htm.

[8] ITU-T Standardization Sector, "Recommendation H.263," 2007, http://www.itu.int/rec/T-REC-H.263/en.

[9] E. Barker, D. Johnson, and M. Smid, "NIST Special Publication 800-56A; Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography," 2007, http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf.

[10] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2," 2008, http://tools.ietf.org/html/rfc5246.

[11] RSA Laboratories, "PKCS #5: Password-Based Cryptography Specification Version 2.0," 2000, http://tools.ietf.org/html/rfc2898#section-5.2.