Evaluation of UMTS security architecture and services

Abdul Bais
Institute of Computer Technology
Vienna University of Technology
A-1040 Vienna
Austria
bais@ict.tuwien.ac.at

Walter T. Penzhorn
Department of Electrical, Electronic and Computer Engineering
University of Pretoria
0002 PRETORIA
South Africa
w.penzhorn@eng.up.ac.za

Peter Palensky
Institute of Computer Technology
Vienna University of Technology
A-1040 Vienna
Austria
palensky@ict.tuwien.ac.at

***Abstract*—This paper presents an in-depth analysis and evaluation of the security of UMTS. Four classes of attacks and threats are discussed in detail. Thereafter, the available security mechanism and services of UMTS are reviewed and evaluated. It is found that most of the potential attacks and threats can be thwarted by the available security services and mechanisms of UMTS.**

I. INTRODUCTION

First Generation (1G) mobile telephone systems provided essentially no security features. The 2nd Generation (2G) GSM mobile system was designed such that it provides security similar to that of eavesdropping in fixed phones, and to protect against cloning of mobile identities [1]. GSM allows network operator to verify the identity of a user such that it is essentially impossible for someone to masquerade as a genuine user. Encryption of user data and signaling information over the radio interface protects against eavesdropping. Users are assigned temporary identities. These features are referred to as authentication, confidentiality and anonymity [2]. The novel feature of GSM security is the use of the Subscriber Identity Module (SIM), which contains all the identification and security-related data that the subscriber needs to make or receive a call.

UMTS security builds on the success of GSM by retaining (and to some extent improving) its important and robust security features [1].

Although GSM security has been very successful, an objective of the UMTS security design was to address its real and perceived weaknesses [3]. Some of these weaknesses are the following [1, 4, 5]:

- active attacks using a "false base station";
- cipher keys and authentication data are transmitted in clear between and within networks;
- encryption does not extend far enough towards the core network and data is transmitted in clear on the microwave links;
- data integrity is not provided;
- user authentication on a previously generated cipher key and channel hijack depends on the use of encryption;
- fraud and legal interception were not considered in the design phase but came only as after-thoughts;
- 2G systems do not have the flexibility to upgrade and improve security functionality over time.

In addition to the removal of above observed deficiencies, 3G security offers new security features and services. It should be noted that the main objective of 3G security architecture is not to provide a completely secure system, but to build a system that is flexible to adapt to new challenges [3].

This paper is organized as follows: In Section II we present and discuss the security threats of mobile communication systems. Section III outlines the UMTS security architecture. Section IV shows how available UMTS services thwart most attacks and threats. Section V concludes the paper.

II. POSSIBLE ATTACKS ON UMTS PROTOCOLS

In this section we will give a description of attacks or threats that have been identified in [6]. These attacks exploit a weakness of the system. In the next section we will show how each of these possible attacks is counteracted by a specific feature of the 3G security architecture.

To be able to carry out these attacks the intruder has to posses the following capabilities [6]:

Eavesdropping: The intruder is able to listen in to the signaling associated with other users or their data connections.

Impersonation of a user: Enables the intruder to interact with the network as the actual user.

Impersonation of the network: Enables the intruder to interact with the user as if he is receiving signals from a genuine network.

Man-in-the-middle attack: An ability of the intruder to put himself between two communicating parties, a user and the network, enabling him for various actions including eavesdropping, modifying, deleting, re-ordering, replaying, and spoof signaling and user data.

Compromising authentication vectors in the network: The intruder takes control of a compromised authentication vector by compromising network nodes or links.

For his attacks the intruder requires a modified Mobile Station (MS) and/or a modified Base Station (BS).

In the forthcoming sections we will discuss various attacks that an attacker with the above capabilities can carry out against 3G systems [6].

1-4244-9701-0/06/$20.00 ©2006 IEEE

A. Denial of service

The following will result in complete or partial denial of services to the target user.

1) User de-registration request spoofing: If the network cannot authenticate messages then an attacker with a modified MS can send a de-registration request to the network, which is complied by the network and simultaneously sends instructions to the Home Location Register (HLR) to do the same.

2) Location update request spoofing: Instead of sending requests for de-registration, the attacker sends a location update request from a different area from the one in which the user is presently located. As a result the user is paged in the new area.

3) Camping on a false BS/MS: The attacker with a modified BS/MS puts himself in-between the Serving Network (SN) and the target user.

B. Identity catching

Mobile users are identified by temporary identities, but there are cases where the network requests the user to send its permanent identity in clear text.

1) Passive identity catching: The attacker with a modified MS waits passively for a new registration or a database crash as in such cases the user is requested to send its identity in clear text.

2) Active identity catching: In this case, the attacker with a modified BS entices the user to camp on his BS and then asks him to send his International Mobile Subscriber Identity (IMSI).

C. Impersonation of the network and thereby eavesdropping

In this sub-section we cover attacks where the intruder masquerades as a genuine network towards the user.

1) By suppressing encryption between the target user and the intruder: An attacker with a modified BS entices the user to camp on his false BS and when the service is initiated, the intruder does not enable encryption.

2) By suppressing encryption between the target user and the true network: In this case, during call setup the ciphering capabilities of the MS are modified by the intruder and it appears to the network that there is genuine mismatch of the ciphering and authentication algorithms. After this the network may decide to establish an un-enciphered connection: The intruder cuts the connection and impersonates the network to the target user.

3) By forcing the use of a compromised cipher key: The attacker with a modified BS/MS and a compromised authentication vector entices the user to setup a call while camped on his false BS/MS. The attacker then forces the use of a compromised cipher key.

D. Impersonation of the user

1) By the use of a compromised authentication vector: The attacker with a modified MS and a compromised authentication vector impersonates the target user towards the network and the other party.

2) By the use of an eavesdropped authentication response: The intruder with a modified MS uses an eavesdropped authentication response if the same challenge is used again.

3) Hijacking outgoing calls in networks with encryption disabled: The intruder with a modified BS/MS pages the target user for an incoming call, who then sets up a call which it allows to occur. The intruder modifies the signaling elements and it appears to the serving network that the user wants to set-up a mobile originated call. The intruder then cuts the connection with the target user, and makes fraudulent calls on the user's subscription.

4) Hijacking outgoing calls in networks with encryption enabled: In this case the intruder also modify the ciphering capabilities of the MS to suppress encryption.

5) Hijacking incoming calls in networks with encryption disabled: An associate of the intruder makes a call to the target user, which is relayed by the intruder until authentication and call setup has been done. If the network does not enable encryption the intruder releases the target user, and uses the connection to answer the call.

6) Hijacking incoming calls in networks with encryption enabled: In such instances, apart from the method used in subsection 5, the intruder suppresses the encryption as well.

III. Overview of the UMTS security architecture

The 3G security architecture defines five distinct security features, intended to meet certain threats [7] and to establish required security services [8]:

1) Network access security: provides confidentiality of user identity and that of the user and signaling data, integrity protection of critical signaling data, authentication of user and network, and identification of Mobile Equipment (ME).

2) Network domain security: enables different nodes in the provider domain to securely exchange signaling data, and protects against attacks on the wire line network.

3) User domain security: ensures only authorized access to Universal Subscriber Identity Module (USIM).

4) Application domain security: enables applications in the user and provider domains to securely exchange messages.

5) Visibility and configurability of security: informs the user whether a security feature is in operation and if the use and provision of services should depend on the security feature.

A. Network access security mechanisms

Network access security is a key component in the 3G-security architecture. Security features in this class are a superset of those provided in GSM [1, 4, 8].

1) User identity confidentiality: The main objectives of user identity confidentiality feature are to prevent intruders from eavesdropping the IMSI and the location of the user.

To achieve these objectives the user is identified by means of a Temporary Mobile Subscriber Identity (TMSI/P-TMSI) on the radio interface which has local significance and is combined with Location Area Identifier (LAI) or Routing Area Identifier (RAI), for the Circuit Switched (CS) and Packet Switched (PS) domain respectively. Whenever a user tries to access 3G services, it identifies itself by means of the TMSI/LAI or P-TMSI/RAI.

2) Authentication and key agreement: The AKA mechanism accomplishes mutual authentication of the user and the network using a symmetric key (K) and derives the new cipher and integrity keys [9]. The USIM AKA (Fig. 1) is chosen in such a way as to achieve maximum compatibility with the current GSM/GPRS security architecture. [1,8]. USIM AKA is a one-pass challenge response protocol [10].

The UMTS authentication mechanism has been thoroughly studied [11, 12, 13, 14, 15], resulting in suggestions for some improvements.

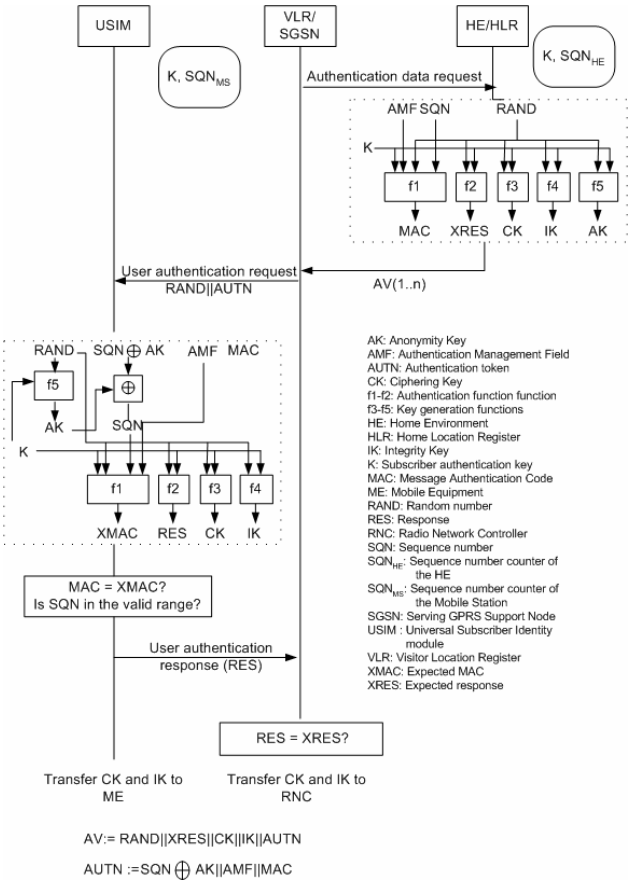

Figure 1. UMTS Authentication and key agreement[8]

3) Security mode set-up procedure: The sequence of message flow that is followed for both ciphering and integrity protection set-up is shown in Fig. 2 [1, 8].

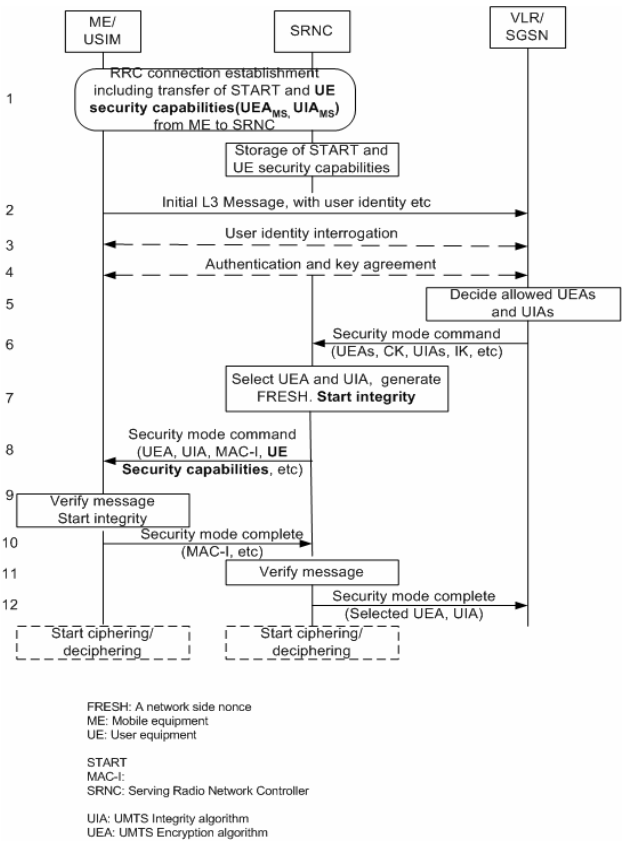

Figure 2. Security mode set-up procedure[8]

It is mandatory to start integrity protection of signaling messages by use of this procedure at each new signaling connection establishment between MS and VLR/SGSN. The User Equipment (UE) security capabilities i.e. the USIM Encryption Algorithms (UEAs) and the USIM Integrity Algorithms (UIAs) are transferred from ME to Serving Radio Network Controller (SRNC) during the Radio Resource Controller (RRC) connection establishment.

After the initial connection establishment there may be an optional user identity request and AKA. The SRNC decides which algorithms to use by selecting the highest preference algorithm from the list of allowed algorithms that matches any of the algorithms supported by the MS. The SRNC generates (an integrity protected) RRC message, security mode command (Fig. 2, Message 8), which includes the UE security capabilities. This provides protection against "bidding-down attack" [1].

4) Access link data integrity: As discussed in the previous section the integrity protection of signaling messages, between ME and Radio Network Controller (RNC) starts during the security mode set-up as soon as the integrity key and integrity protection algorithm is known. A Message Authentication Code (MAC) function is applied to each individual signaling message at the RRC layer of UMTS Terrestrial Radio Access Network (UTRAN) protocol stack [16].

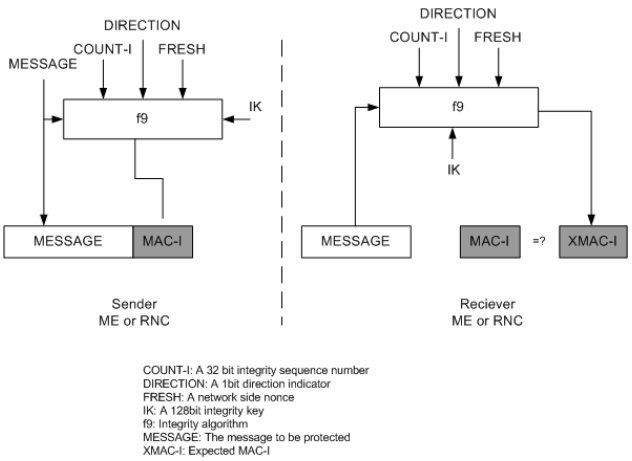

Figure 3. Derivation of MAC-I (or XMAC-I) on a signaling message[17]

Fig.3 illustrates the use of integrity algorithm f9 to authenticate the data integrity of an RRC signaling message [4]. Currently only one algorithm called KASUMI [17, 18] is standardized. Integrity protection of critical signaling messages provides protection against active man-in-the-attacks on UMTS [19].

5) Access link data confidentiality: In the 3G Security, user data and some signaling information elements are considered sensitive and may be confidentiality protected [7]. The need for a protected mode of transmission is fulfilled by a confidentiality function f8 as shown in Fig.4[17, 18]. The encryption function is applied on dedicated channels between the ME and the RNC [8]. In current specifications the function f8 is based on KASUMI.

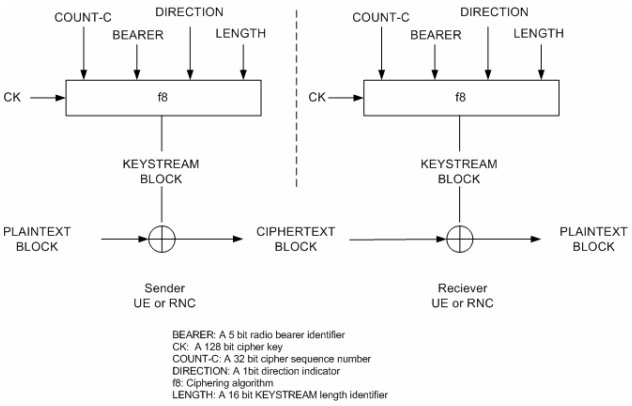

Figure 4. Ciphering of user and signaling data over the radio access link[17].

6) Evaluation of confidentiality and integrity algorithms: The block cipher KASUMI is a modification of MISTY1 [20]. KASUMI has been tested by the design team and independent evaluation teams using cryptanalytical methods [21]. The extensive analysis on MISTY1 [22, 23, 24] and KASUMI itself [25, 26] has strengthened the position of KASUMI as a secure cryptographic primitive. The MISTY1 and KASUMI constructions have also been proven to provide pseudo randomness [27].

The best known attack on f9 requires approximately 248 chosen input messages [28], which is still considerably more than for the regular CBC-MAC mode [29]. The provable security of f8 and f9 construction is reported in [30].

B. Network Domain Security

The term 'network domain security' in the 3GPP specifications covers security of the communication between network elements which may be in the same or two different [1, 31, 32].

The mobile specific part of Signaling System No. 7 (SS7) signaling is called the Mobile Application Part (MAP) [33]. 3GPP has developed security mechanisms that are specific to MAP. The complete collection of protocols and procedures needed to protect MAP messages is called MAPsec [31] and is briefly discuss in the next section.

The Internet Engineering Task Force (IETF) has standard security mechanisms for IP-based networks. For the 3GPP, the main emphasis is on how to use IETF protocols to protect IP-based communication in 3GPP networks [1].

1) MAPsec: The plaintext MAP message is encrypted and the result is put into a 'container' in another MAP message. At the same time a message authentication code covering the original message is included in the new MAP message. MAPsec has borrowed the notion of a security association (SA) from IPsec [34]. The SA contains cryptographic keys and other relevant information. For signaling protection at the application layer the necessary SAs will be network-wide and they are negotiated by key administration centre (KAC) [5]. The KACs also distribute the SAs to the network elements.

2) IPsec-based mechanisms: The UMTS network domain control plane is sectioned into security domains, which typically coincides with the operator borders. Security gateways (SEGs) are entities at the borders of the IP security domains used for securing native IP-based protocols [32] are responsible for enforcing the security policy of a security domain towards other SEGs in the destination security domain.

In IPsec-based solution all control plane IP communication towards external networks go via SEG. 3GPP defines the minimum set of features of IPsec that must be supported for internetworking purposes. These simplifications are: only Encapsulating Security Payload (ESP) [34] is used for protection of packets; ESP is always used in tunnel mode; Advance Encryption Standard (AES) is used as the encryption algorithm.

IV. THWARTING FORESEEN ATTACKS ON UMTS

In this section we discuss in slightly more detail the measures that have been taken to protect UMTS from attacks discussed in Section II [6].

A. Denial of service

1) User de-registration request spoofing: Integrity protection of critical signaling messages is mandatory. The serving network verifies the de-registration request for integrity and replay.

2) Location update request spoofing: The location update request is always protected against replay and modification.

3) Camping on a false BS/MS: The integrity protection of critical signaling messages protects against the denial of service to some degree, as the intruder can't modify signaling messages. However, the system does not prevent the intruder from relaying of messages between the network and the target user or ignoring some of them.

B. Identity catching

1) Passive identity catching: The use of temporary identities inhibits passive identity catching since the intruder has to wait for a new registration or a mismatch in the serving network database in order to capture the user's permanent identity in clear text.

2) Active identity catching: 3G does not provide protection against this type of attack. However, the user identity is not a security feature.

C. Impersonation of the network

1) By suppressing encryption between the target user and the intruder: Data authentication and replay protection of a mandatory cipher mode command (Section III.A.3) allows the mobile to verify that security has not been suppressed. Further more, the visibility and configurability of security features prevents such an attack to go unobserved.

2) By suppressing encryption between the target user and the network: During the initial RRC connection establishment the MS sends its security capabilities to the SRNC. These security capabilities are sent in clear and can be modified by the man-in-the-middle. But, at a later stage, the SRNC includes the security capabilities of the MS in a mandatory security mode command. This information lets the MS know that the security capabilities are intact. The MS tells the serving network about the unbroken security capabilities in a security mode complete message, leaving the intruder in trouble.

3) By forcing the use of a compromised cipher key: The presence of a sequence number in the challenge helps guard against forced re-use of a compromised authentication vector.

D. Impersonation of the user

1) By the use of a compromised authentication vector: The same mechanism as discussed in Sub-section IV.C.3 protects against this type of attacks.

2) By the use of an eavesdropped authentication response: The presence of a sequence number in the challenge protects against multiple use of an authentication vector.

3) Hijacking outgoing calls in networks with encryption disabled/enabled: The intruder cannot turn off the encryption. However, integrity protection of signaling messages by the use of procedure discussed in Section III at each new RRC connection establishment between MS and VLR/SGSN is mandatory which allows the serving network to verify that the request is legitimate.

4) Hijacking incoming calls in networks with encryption disabled: Connections accept message is integrity protected which allows the serving network to verify its legitimacy. This means that the intruder cannot accept a connection on behalf of the target user. After the initial connection establishment, periodic integrity protected messages are exchanged during the connection which protects against hijacking of un-ciphered connections.

V. CONCLUSION

The access security mechanisms in UMTS now protects against the false base station attacks. An example authentication algorithm set has been provided for those who prefer not to design their own. The confidentiality algorithm is stronger than its GSM predecessor. The integrity mechanism works independent of confidentiality protection and provides protection against active attacks. The design of cryptographic algorithms is open and they are extensively crypto analyzed. Moreover, the architecture is flexible and more algorithms can be added easily.

Although 3G Security marks a large step forward however there are some short comings. The user data over the air is not integrity protected and the network domain security does not extend to the user domain. IMSI is sent in clear text when allocating TMSI to the user. Hijacking of channel between periodic integrity protection messages is still possible.

REFERENCES

[1] C. J. Mitchell, "*Security for Mobility*", Institute of Electrical Engineers, December, 2004.

[2] 3GPP TS 03.20 (9.0.0), "Security related network functions" *Release 2000,* January, 2001.

[3] 3GPP TS 33.120 (4.0.0), "3G Security; Security principles and objectives", *Release 4*, March, 2001.

[4] G. M. Køien, "An introduction to access security in UMTS", *IEEE Wireless Communications*, Volume 11, Pages: 19-25, 2004.

[5] C. Xenakis, L. Merakos, "Security in third Generation Mobile Networks", *Computer Communications,* Vol.27, pp. 638-650, 2004.

[6] 3GPP TR 33.900 (1.2.0), "A Guide to 3G Security" January, 2000.

[7] 3GPP TS 21.133 (4.1.0), "3G Security; Security threats and requirements", *Release 4*, December, 2001.

[8] 3GPP TS 33.102 (5.2.0), "3G Security; Security Architecture", *Release 5*, June, 2003.

[9] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", *Internet Draft, IETF*, December 2004. draft-arkko-pppext-eap-aka-15.txt

[10] ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function"

[11] G. Rose and G.M. Køien, "Access security in CDMA2000, including a comparison with UMTS access security" *IEEE Wireless Communications*, Volume 11 Issue 1, Pages: 19-25, 2004.

[12] P. S. Pagliusi and C. J. Mitchell, "Heterogeneous Internet access via PANA/UMTS", Proceedings of the 3rd WSEAS International Conference on Information Security, Hardware/Software Co-design and Computer Networks (ISCOCO 2004)

[13] H. Kim, H. Afifi, "Improving mobile authentication with new AAA protocols", *IEEE International Conference on Communications*, *(ICC '03)* Page(s): 497- 501 Volume: 1, May 2003

[14] G. Kambourakis, A Rouskas, S. Gritzalis, "Performance Evaluation of Public Key-Based Authentication in Future Mobile Communication Systems", *EURASIP Journal on Wireless Communications and Networking* Volume 1, Pages 184–197, 2004.

[15] C. F. GRECAS, S. I. MANIATIS and I. S. VENIERIS, "Introduction of the Asymmetric Cryptography in GSM, GPRS, UMTS, and Its Public Key Infrastructure Integration", *Mobile Networks and Applications*, Volume 8, 145–150, 2003.

[16] 3GPP TS 25.331 (6.4.0), "Radio resource controller, Protocol specification", *Release 6*, December, 2004.

[17] 3GPP TS 35.201 (5.0.0), "3G Security; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specification", *Release 5*, June, 2002.

[18] 3GPP TS 35.202 (5.0.0), "3G Security; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: KASUMI specification", *Release 5*, June, 2002.

[19] U. Meyer, S. Wetyel, "A Man-in-the-Middle Attack on UMTS", *Proc. of 5th International Conference on Web Information System Engineering,* Brisbane, 2004.

[20] M. Matsui, "Block encryption algorithm MISTY" in Proceedings of Fast Software Encryption (FSE'97), Lecture Notes in Computer Science, Volume 1267, Pages: 54–68, Springer-Verlag, 1997.

[21] 3GPP TR 33.909 V1.0.0 (2000-12) Technical Report; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Report on the Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms (Release 1999)

[22] S. Babbage and L. Frisch, "On MISTY1 higher order differential cryptanalysis", *in Proceeding of International Conference on Information Security and Cryptology (ICISC 2000), Lecture Notes in Computer Science* Volume. 2015, Pages: 22–36, Springer-Verlag, 2001.

[23] U. Kühn, "Cryptanalysis of reduced-round MISTY", *in Proceedings of Eurocrypt'01, Lecture Notes in Computer Science*, Volume 2045, Pages: 325–339, Springer-Verlag, 2001.

[24] U. Kühn, "Improved cryptanalysis of MISTY1", *in Proceedings of Fast Software Encryption (FSE'02), Lecture Notes in Computer Science*, Volume 2365, Pages: 61–75, Springer-Verlag, 2002.

[25] M. Blunden and A. Escott, "Related key attacks on reduced round KASUMI", *in Proceedings of Fast Software Encryption (FSE'01), Lecture Notes in Computer Science*, Pages: 277–285, Springer-Verlag, 2001.

[26] H. Tanaka, C. Ishii, and T. Kaneko, "On the strength of KASUMI without FL functions against higher order differential attack", *in Proceedings of the Third International Conference on Information Security and Cryptology (ICISC'00), Lecture Notes in Computer Science*, Volume 2015, Pages: 14–21, Springer-Verlag, 2000.

[27] H. Gilbert and M. Minier, "New results on the pseudorandomness of some block cipher constructions", *in Proceedings of Fast Software Encryption (FSE 2001), Lecture Notes in Computer Science*, Volume 2355, Pages: 248-266, Springer-Verlag, 2002.

[28] L.R. Knudsen and C.J. Mitchell, "An analysis of the 3GPP-MAC scheme", *Workshop on Coding and Cryptography (WCC 2001)*, Pages: 319-328, 2001.

[29] K. Nyberg. "Cryptographic Algorithms for UMTS", *European Congress on Computational Methods in Applied Sciences and Engineering (ECCOMAS '04)*, July 2004

[30] T. Iwata and T. Kohno, "New Security Proofs for the 3GPP Confidentiality and Integrity Algorithms", *in Proceedings of Fast Software Encryption (FSE 2004), Lecture Notes in Computer Science*, Volume 3017, Pages: 427-445, Springer-Verlag, 2004.

[31] 3GPP TS 33.200 (6.0.0), "3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security", *Release 6*, December, 2004.

[32] 3GPP TS 33.210 (6.5.0), "3G Security; Network Domain Security (NDS); IP network layer security", *Release 6*, June, 2004.

[33] 3GPP TS 29.002 (6.8.0), "Mobile Application Part (MAP) specification", *Release 6*, December, 2004.

[34] IETF RFC 2401-2412, "IPsec protocol suite", 1998.