

Security Model Evaluation of 3G Wireless Networks

Alexander Kazeka, CSU

Abstract

Second generation mobile phone networks (2G) are currently the most widely used wireless telephone networks in the world. While being an improvement over earlier analog systems, 2G security standards have serious flaws: designed to provide strong authentication and over-the-air encryption, the algorithms used in 2G have been compromised, and means of circumventing the security model altogether have been discovered. Third generation mobile phone standards (3G) have been designed to address those issues and provide a better security model. However, they too have certain limitations. To provide background, this paper presents an overview of security in 1G and 2G networks along with pointing out the known problems. Then, security features of 3G systems are presented and compared to those in earlier systems. Finally, 3G security model is evaluated according to availability-confidentiality-integrity framework.

Keywords – 3G security, mobile phone networks, UMTS, CDMA2000, GSM, cdmaOne

1. Introduction

A recent (Q1 2007) market research by GSMA – a global trade organization of 700 mobile phone operators and 200 manufacturers and vendors from 218 countries – reported 2.8 billion worldwide subscribers. Wireless telephony is part of daily life for almost every third human, and the security of information exchanged through it has a direct impact on our personal security as well as the security of society as a whole – mobile phone security is an important issue.

This paper presents the results of research on security in mobile telephone networks with focus on the newest technologies/standards in use today: GSM, cdmaOne, UMTS, and CDMA2000, together amounting to over 90% of worldwide mobile phone coverage (GSMA data). Most recent of them – UMTS and CDMA2000 – belong to a set of wireless network standards known as 3G, third generation mobile telecommunication standards, which replaced or are replacing the older 2G networks. These two generations of systems can be distinguished by their throughput capabilities: 2G networks provide throughput between 9.6 and 144 kb/s, while 3G networks provide between 384 kb/s and 20 Mb/s [9]. 3G are more than just phone networks – the standards reflect the need for ubiquitous computing and link telephony, multimedia, high-speed wide area networking, Internet, and hardware and software to support it. The technologies involved evolved over past two decades and while maintaining the required compatibility had to assimilate the systems which were designed without strong security considerations, vulnerable to many types of attacks. How vulnerable are 3G systems? This is the main question of this research.

To answer this main question, the first three generations of mobile phone networks are surveyed with focus on security. Corresponding security-related

protocols and their known weaknesses are reviewed and discussed.

The merit of this paper is two-fold: first, it presents a survey of modern mobile phone technology from a security perspective; second, it evaluates 3G systems' security within the view of availability-confidentiality-integrity framework.

This paper is organized as follows: first, related work is described; then the background section gives an overview of earlier generations of mobile phone technologies; after that, the section on 3G systems looks at UMTS and CDMA2000 standards. The paper concludes with the discussion of security model of 3G systems. Due to the complexity of 3G *internetworking* the following is a brief survey of 3G security – comprehensive analysis of the subject is beyond the scope of this paper.

2. Related Work

A significant amount of research was and continues to be devoted to mobile phone systems' security: integral components as well as complete systems are described and analyzed. In addition to component specifications, very relevant to this paper are the cryptanalyses of various algorithms used in mobile phone systems and the overviews of different mobile phone systems.

This work takes a systems overview approach; along the same line, perhaps the best security overview of a mobile phone system is "GSM Interception" by Lauri Personen; another useful sources are sections on security in such books as "3G networks as GSM, cdmaOne and 3G Systems" by Steele, Lee, and Gould, and "W-CDMA and cdma2000 for 3G Mobile Networks" by Karim and Sarraff. A work similar to this, but with focus on CDMA2000 standard is "State-of-the-art on CDMA2000 Security Support" by Luuk Weltevreden; another works that touch on the same topic of 3G security are "UMTS Security" by Boman, Horn, Howard, and Niemi focusing on UMTS, "Evaluation of UMTS security architecture and services" by Bais, Penzhorn, Palensky giving an overview along with a look on how some of the potential threats are addressed, and "Access Security in CDMA2000, Including a Comparison with UMTS Access Security" by Koien and Rose which concentrates on authentication, encryption and integrity-checking in 3G systems.

3. Background

This section provides an overview of the architecture and security aspects of mobile phone systems that preceded 3G.

3.1 Mobile Phone Network Architecture

Despite existence of many different types of mobile phone networks, they all share some basic components necessary to provide elementary functionality. This subsection describes these components and introduces the associated terminology.

The first mobile phone network component that a user comes in contact with is a mobile phone typically referred to as *mobile station (MS)*. MS communicates with the rest of the network via a radio link to the nearest *base station (BS)*, essentially an antenna with electronics and power equipment to support it; area covered by a single BS is referred to as *cell*. The link between MS and BS consists of one or more

traffic channels and one or more *signaling channels*. Traffic channels carry subscriber-generated data, while signaling channels are used to transmit communication control data such as the MS location information, paging data to the MS in case of incoming call, network access-related data in case of call origination, and other network and operator-dependent information. BSs in turn are connected to *mobile switching centers (MSCs)*, usually via dedicated non-radio links. MSCs, similarly to switches in land-line telephone networks, are mainly concerned with routing data. MSs, BSs, and MSCs are essentially all that is necessary to provide elementary mobile phone network functionality, however a few additional elements are normally used to support more than just basic features [26].

Home location registers (HLRs) store information about subscribers – at the very least the type of service supported and current location of each user. When a user enters a cell this information is copied to the respective *visitor location register (VLR)* for efficiency purposes. Each VLR may control one or more cells. When a subscriber leaves the area controlled by a VLR their information is moved to the new VLR. When a cellular network supports security features, the necessary information is stored in *authentication center (AuC)*. Additionally, *equipment identity register (EIR)* may be used to track MSs [26].

Using the terminology presented above it is possible to look at early mobile phone systems' security.

3.2 1G Analog Networks

First cellular telephone systems available on the market were deployed in early 1980s. Before then radio telephony was used for communication by governments and militaries since 1940s, however the invention of efficient *handover* mechanisms, which allowed moving from one cell to another, enabled mobile phone technology to be introduced to consumers. The MSs in 1G systems transmitted radio signals in clear using FM over UHF [16]. The only security feature was authentication of an MS when initiating *roaming* – using a network of a given provider – by checking the MS identification number and the subscriber identification number against HLR. The security belief was that the price and complexity of equipment needed to receive and create such transmissions was prohibitive for an intruder. This assumption was wrong, and resulted in extensive exploits of 1G systems. Two major issues were eavesdropping on conversations and phone cloning. Eavesdropping could be accomplished by simply picking up the FM signals using a radio scanner tuned to UHF; phone cloning involved eavesdropping on authentication exchange between MS and the network and then reproducing that exchange from another MS to gain fraudulent access to the network [25].

3.3 2G Digital Networks - GSM

By mid-1980s the deployed disparate 1G networks in Europe began approaching their capacity limits and an international coordinating body – Groupe Special Mobile (GSM) – was created to develop a new unified mobile phone system specification. It was required to support greater number of users, similar or lower operating costs, similar or better speech quality, and be able to coexist with older analog systems. To achieve these goals GSM committee selected TDMA over UHF, a digital multiplexing

technique which allowed a more economic and efficient use of UHF frequencies [26].

Based on previous experience with 1G networks, security-related design goals of GSM were prevention of phone cloning and making mobile phone conversations no more vulnerable to eavesdropping than fixed phones. The standard addressed these stipulations by providing authentication, confidentiality, and anonymity features [22].

Next subsection describes the network elements that were added in GSM* system to support the above security features, and the section following next describes these features and their security in detail.

3.3.1 GSM Network Architecture

Perhaps the single most important GSM innovation is *subscriber identity module (SIM)* – a removable smart card which contains the identification and security-related information the subscriber needs to use the network. Typically users are identified by their phone number, and use of SIMs enables decoupling of subscriber identities from the MSs and allows switching MSs while keeping the number. On the network side, AuC provides authentication and encryption functions. AuC and SIMs are complimentary units in security sense - their authentication and encryption algorithms and associated keys ultimately have to match for successful communication.

3.3.2 GSM Security Features

GSM networks provide a security enhancement over 1G by authenticating users and supporting confidentiality and anonymity features. However, the related algorithms initially weren't open for community review, which caused some serious flaws to be overlooked. Eventually GSM security algorithms leaked and their flaws were discovered [13].

GSM security model is based on a 128-bit shared secret K_i between the subscriber's SIM and the network – if that key is compromised, the entire account is compromised. When a MS first enters the area of coverage of the network, HLR and AuC provide the appropriate MSC with five triplets each containing 128-bit RAND, 32-bit SRES, and 64-bit K_c . RAND is a random challenge used for authentication, SRES (signed response) is the expected response to that challenge based on RAND and subscriber's K_i , K_c is the session key also based on RAND and K_i . Each triplet is used for one authentication, and after all the triplets have been used up, the MSC is provided with another set of five [13].

Authentication is the first line of defense in GSM: it allows subscribers to use the network and establishes the encryption, if any. Authentication in GSM proceeds as follows: MS receives the RAND from MSC, calculates the SRES with A3 algorithm using RAND and K_i , and sends it back to MSC. If SRES matches the one stored at

* After the standard was developed, Groupe Special Mobile was merged into European Telecommunications Standards Institute (ETSI) and GSM has been renamed 'Global System for Mobile Communications' [26].

MSC, the authentication succeeds and the corresponding Kc is used to encrypt further over-the-air communications between MS and BS/MSC [13].

According to GSM recommendation, most network operators use COMP128 algorithm for A3 implementation. COMP128 produces 128-bit output given two 128-bit inputs (in case of A3 those are Ki and RAND); SRES is the first 32 bits of that output [13]. In 1998 ISAAC researchers demonstrated that COMP128 can be broken with chosen-challenge attack: repeatedly querying SIM about 150,000 times with specially-chosen RANDs and analyzing the resulting SRES outputs reveals Ki. Querying SIM can be accomplished using an off-the-shelf smart card reader in about 8 hours as well as over the air in a longer, but not prohibitively long period of time (up to 13 hours due to radio communication latency). Gaining knowledge of Ki effectively means cloning a SIM and allows the attacker to eavesdrop on conversations as well as make calls billed to the SIM's owner. Although GSM has a mechanism that detects duplicate active SIMs thus alleviating the fraudulent billing problem, eavesdropping is still an open issue. After flaws in COMP128 have been revealed, a patched version of the algorithm was developed, but due to the expense of replacing SIMs in such a widely distributed system it is unclear if and when the compromised version of COMP128 will be completely updated [7].

Session key Kc, used for over-the-air encryption after a MS has been authenticated, is generated with the A8 algorithm. The GSM recommended A8 implementation, again, is COMP128, and most network operators follow that suggestion. While the first 32 bits of COMP128 output are used for SRES, the last 54 bits are padded with zeros to produce 64-bit Kc. As mentioned previously, COMP128 has been cryptanalyzed. Therefore it is possible to recover Ki from Kc, RAND, and SRES: RAND and SRES are sent in clear and Kc can be deduced from encrypted communications using some of the attack techniques described below [13].

Over-the-air encryption in GSM employs different variations of A5 algorithm. A5 is a stream cipher that is re-initialized for every frame sent (every 4.6 milliseconds [21]) using 64-bit session key Kc and 22-bit frame number. Given that input, A5 outputs unique 228 bits of key-stream for each frame. The first block of 114 bits encrypts the radio link from the network to the subscriber, while the second block of 114 bits encrypts data sent in the opposing direction. Encryption is done by a simple XOR of the frame to be sent with the key-stream [10, 13].

Due to export restrictions the strongest version of A5 called A5/1 is only used in Europe and US, while a weaker version of the algorithm called A5/2 has no export limitations and is used elsewhere in the world. Network operators are also free to use an algorithm of their choice or no over-the-air encryption at all, however those approaches aren't widespread [10].

The A5 stream ciphers work by clocking *linear feedback shift registers (LFSRs)*: A5/1 uses three LFSRs 19, 22, and 23 bits long, while A5/2 uses an additional 17-bit long fourth register. Each register has taps and a feedback function. When a register is clocked, the bits at tap positions are XORed and the result is stored in

rightmost bit of the left shifted register; the output bit is a non-linear function of the internal state of the registers. A5/1 and A5/2 share the same basic mode of operation because they were designed to run on the same hardware, their differences lie in register initialization and feedback functions, which allows for weakening of cryptographic strength of A5/2 as compared to A5/1 [10, 21].

The brute-force attack on A5 algorithms is infeasible in real-time – searching a keyspace of 2^{54} (10 bits of the 64-bit session key Kc are zeroed out) bits takes too long. However, it is still possible to record the encrypted conversation and do a brute-force attack off-line [13]. Other, and perhaps more viable, alternatives involve using the more sophisticated attack techniques summarized below.

In 2000 Biryukov, Shamir, and Wagner described two real-time attacks on A5/1 that exploited the fact that its LFSR register sizes are small enough to have all their states pre-computed and stored in RAM on a PC. After additional lookup tables that describe all the possible interactions of the registers have been generated, the attacks requiring at most 2 minutes of A5/1 encrypted data for analysis can be carried out in mere seconds [RT-Cryptanalysis].

In 2003 Barkan, Biham, and Keller described an instant ciphertext only attack on A5/2 which exploited the fact that error-correcting codes employed in GSM reveal information about the plaintext. This attack, requiring several hours of pre-computation, needed only 8 GSM frames and recovered the key within seconds. The authors also described how a similar attack carried out as part of the man-in-the-middle attack could be used to uncover session key Kc regardless of the actual algorithm used by the network, as long as the victim's SIM supported A5/2 (which most SIMs do) [10]. Such man-in-the-middle attack on mobile phone systems is an instance of *rogue base station* attack in which an adversary impersonates a BS and requests information from a mobile. This type of attack presents a challenge not expected by the 2G system designers – again, it was mistakenly believed that launching such an attack would be too expensive [22].

To sum up, the standard GSM cryptographic algorithms have been compromised. However, an attacker may not even need to break any algorithms to eavesdrop on a conversation: since only the radio link between MS and BS is encrypted, a wiretap on the operator's network past the BS gives instant access to all data going through [13].

One last point to make about GSM security is the fact that its anonymity feature is somewhat inadequate. In an effort to prevent anyone knowing the subscriber's identity (essentially their phone number) from eavesdropping on that subscriber and determining their location, temporary identities are used during communication between a MS and the network. A temporary identity is assigned to each MS when it is authenticated. However, the network can request the MS to send the real identity of its user at any time and that information is then transferred in the clear over the operator's network [11, 26]. Additionally, a rogue base station can exploit that part of the protocol to retrieve the real identity of a user [25]. A more adequate anonymity provision would be never to send the true identity of a

subscriber over an unencrypted or unauthenticated channel [20].

This section provided an overview of GSM, the system currently used by 80% of worldwide mobile phone users (Q1 2007 GSMA data), and pointed out some of its known security problems. The next section surveys another widely deployed 2G system – cdmaOne.

3.4 2G Digital Networks - cdmaOne

Another prominent 2G standard is cdmaOne, commonly referred to as IS-95 (Interim Standard number 95) in the US. It was developed by Qualcomm Incorporated in 1990s [26]. Historically used for secure military communication, CDMA stands for *code division multiple access*, a spread spectrum modulation technique. In CDMA each user's message is modulated according to their assigned spreading sequence. The spreading process increases the message's bandwidth while reducing its power spectrum, which allows CDMA messages to achieve high tolerance to interference and low power requirements [19]. Qualcomm engineers saw potential for mobile communication using CDMA and developed cdmaOne standard that was first deployed in Hong Kong in 1995 and has since been launched in many countries around the world including the US [26].

cdmaOne networks are composed of the same basic components as GSM [5, 25]; their most significant security-related distinctive features are CDMA radio link and authentication and encryption algorithms.

3.4.1 cdmaOne Physical Layer

As compared to TDMA over UHF in GSM systems, cdmaOne also uses UHF, but employs a more sophisticated multiplexing technique in which a signal is first spread over a range of frequencies using a so-called channelization code and then scrambled using a pseudo-random sequence. Such scrambling makes the signal difficult to intercept. While the GSM signal can be picked up by simply using a radio scanner tuned to appropriate frequencies, cdmaOne signal is impossible to recover without also knowing both the channelization and scrambling codes – this is known as CDMA built-in physical layer security [19].

Since channelization in cdmaOne is done with relatively easy to generate 64-bit Walsh codes, the built-in security mainly relies on pseudo-random scrambling. The scrambling sequence is generated from 42-bit *long-code mask* and 42-bit LFSR: each bit of the sequence is a result of modulo-2 inner product of the mask and current state of LFSR. Although brute-force reconstruction of the scrambling sequence takes prohibitive $O(2^{84})$, knowledge of the published characteristic polynomial of the LFSR makes a ciphertext-only attack feasible in $O(2^{42})$ [19]. Therefore CDMA built-in physical layer security alone does not provide adequate security for cdmaOne mobile phone networks.

3.4.3 cdmaOne Security Features

Similarly to GSM, cdmaOne provides authentication and encryption, but does so with different algorithms.

cdmaOne uses *cellular authentication and voice encryption (CAVE)* algorithm to generate authentication and encryption keys. Essentially, CAVE is a 128-bit hash function which is first supplied authentication key A-key of the subscriber, equipment serial number (ESN) of the mobile, and a random challenge RANDSSD generated at HLR/AuC to produce 128-bit hash value *shared secret data (SSD)*. SSD is then split in two parts: SSD_A are the first 64 bits, then combined with random challenge RAND broadcasted by MSC as inputs to another invocation of CAVE to create 18-bit authentication signature; and SSD_B – the last 64 bits, used for encryption. If the authentication signature matches the one expected by BS, the MS is authenticated by the network [12, 18].

In 2004 Millan and Gauravaram demonstrated an attack on CAVE that can reveal all possible inputs to the algorithm in $O(2^{72})$ with most of those steps susceptible to efficient pre-computation into look-up tables. This attack could be used recover the A-key and ESN to clone the MS and also to reveal encryption key SSD_B [6, 12].

SSD_B has three encryption-related functions: it is used in generating long-code mask for physical layer scrambling, as input to CMEA signaling channel encryption and as input to ORYX data traffic encryption algorithms [18]. Both CMEA and ORYX have been crypt-analyzed [8, 17].

CMEA is a variable-width block cipher used in ECB mode to encrypt the signaling channel in cdmaOne networks. In 1997 Wagner, Schneier, and Kelsey described a chosen plaintext and a known plaintext meet-in-the-middle attacks with time complexity $O(2^{24} \cdot 2^{34})$, which allow them to recover 64-bit key in minutes on a standard workstation [8].

ORYX, a stream cipher based on three 32-bit LFSRs and one *substitution box (S-box)*, is used for encrypting data traffic in cdmaOne. Wagner et al. published a known plaintext attack that could be extended to ciphertext-only attack on ORYX in 1998. The attack exploited dependencies between LFSRs and used divide-and-conquer approach to recover the 96-bit secret key in $O(2^{16})$ [17].

Additionally, cdmaOne provides a similar anonymity feature to GSM with TMSI [18]. Overall, however, the security of cdmaOne networks, similarly to GSM, has a lot of holes and, as GSM, does not provide significant protection against phone cloning or eavesdropping – the two original 2G security design goals. Despite great market success of 2G systems, their security is mediocre. The next section looks at how security is addressed in 3G networks.

4. 3G Networks

The development of 3G standards started right after GSM launch. Due to complex nature of the vision for 3G networks that incorporates mobile telephony, multimedia, high-speed wide area networking, and the Internet, standardization is a coordinated effort by a number of organizations. International Telecommunication Union (ITU) defines the overall view for 3G wireless networks under International

Mobile Telecommunications 2000 (IMT-2000)* family of standards.

IMT-2000 family is composed of the following six technologies operating in UHF band:

- IMT DS (Direct Sequence): UMTS Terrestrial Radio Access (UTRA) and W-CDMA (wideband CDMA);
- IMT MC (Multicarrier): CDMA2000, 3G version of cdmaOne;
- IMT TC (Time Code): UTRA mode that uses time division duplexing;
- IMT SC (Single Carrier): accommodation of Enhanced Data Rates for GSM Evolution (EDGE) technology to 3G;
- IMT FT (Frequency Time): Digitally Enhanced Cordless Telecommunications (DECT) system;
- IMT OFDMA: WiMAX;

[26, [27](#)]

ITU defines a set of security requirements for IMT-2000 systems within the structure of Open Systems Security Architecture (ITU Recommendation X.800). The requirements are: “

- only authorized users should be able to access and use telecommunication networks;
- authorized users should be able to access and operate on assets they are authorized to access;
- telecommunication networks should provide privacy at the level set by the security policies of the network;
- all users should be held accountable for their own but only their own actions in telecommunication networks;
- in order to ensure availability, telecommunication networks should be protected against unsolicited access or operations;
- it should be possible to retrieve security-related information from telecommunication networks (but only authorized users should be able to retrieve such information);
- if security violations are detected, they should be handled in a controlled way in accordance with a pre-defined plan to minimize potential damage;
- after a security breach is detected, it should be possible to restore normal security levels;
- the security architecture of telecommunication networks should provide a certain flexibility in order to support different security policies, e.g., different strength of security mechanisms; ” [15]

The first five of the above goals are to be achieved by implementing confidentiality, data integrity, accountability – including authentication, non-repudiation, and access control, – and availability mechanisms [15].

A major design consideration for 3G is interoperability among networks – due to a large number of deployed systems of different generations any viable new

* 2000 signifies the year of initial deployment; although IMT-2000 networks have been deployed since October 2000, they still serve only a little over 15% of mobile phone networks' subscribers [5, 29].

standard has to work with the older systems. Another major factor is having a clear transition path for the operators to upgrade to the latest standards – the upgraded networks have to be able to continue serving existing subscribers who may be using older technologies. The next subsection looks at security aspects of two 3G technologies which are the next evolutionary steps for GSM and cdmaOne, currently two of the most prevalent 2G systems, – UMTS and CDMA2000 which are the most widely deployed 3G systems today [18, GSMA].

4.1 3G Mobile Telecommunication Networks – UMTS, CDMA2000

UMTS and CDMA2000 specifications are developed by separate, but collaborating organizations - Third Generation Partnership Project (3GPP) and Third Generation Partnership Project 2 (3GPP2) respectively. The standards developed by 3GPP and 3GPP2 share a lot in common – that is not surprising given the fact that the systems have to coexist and cooperate to provide roaming services. A major shift from 2G is the use of CDMA multiplexing across both systems. That means that the two systems share similar CDMA built-in physical layer security properties.

UMTS, as CDMA2000, uses varied size Walsh codes for generation of channeling codes to allow for adjusting throughput on channels depending on network traffic; the size of Walsh codes varies from 4 to 256 bits. A more significant security impact, as in cdmaOne, has the scrambling key which can be also varied in length to change bandwidth on the link between MS and the network based on network congestion. Maximum length of the scrambling key on both UMTS and CDMA2000 is 42-bits. The attack by Li, Ling, and Ren described in subsection on physical layer security of cdmaOne networks is applicable to UMTS and CDMA2000; it has the same time complexity on CDMA2000 since the same characteristic polynomials are used as in cdmaOne, and on UMTS it actually has lower complexity due to dependencies among LFSRs used to generate the scrambling key. Li, Ling, and Ren suggest using AES for secure scrambling; this however has not been implemented [19, 24, 27]. Overall, however, the transmission over air is reasonably secured to protect from casual eavesdropping.

4.1.1 Authentication, Encryption and Integrity Features

To achieve secure authentication of subscribers on heterogeneous networks while providing enhancement and interoperability with GSM, standardized *authentication and key agreement (AKA)* algorithm is used. AKA is a mutual authentication algorithm that involves *universal SIM (USIM)* – a smart card similar in function with GSM's SIM, which uniquely identifies each subscriber and contains security-related information; MS, BS, VLR/MSC – which may belong to a roaming partner of home network; and HLR/AuC – the home network with which the user has a service agreement. AKA proceeds in three stages: initiation, transfer of credentials, and challenge-response exchange [14, 23].

During the initiation stage of AKA, MS based on data contained in USIM provides the VLR/MSC of the respective BS with either IMSI or TMSI of a subscriber – if the subscriber hasn't been authenticated by the network and TMSI is not available then IMSI has to be sent on the clear. In the transfer of credentials stage, HLR/AuC transfers one or more *authentication vectors (AVs)* to VLR, each AV

containing RAND, XRES, CK, IK, and AUTN values, where RAND is the random challenge, XRES is the expected response corresponding to RAND, CK is 128-bit session cipher key used for encryption, IK is 128-bit session integrity key, and AUTN is the authentication token. These values are generated using subscriber-specific 128-bit secret key K as follows:

$$\text{RAND} = f_0()$$

$$\text{XRES} = f_2(K, \text{RAND})$$

$$\text{CK} = f_3(K, \text{RAND})$$

$$\text{IK} = f_4(K, \text{RAND})$$

$$\text{AUTN} = \text{SQN} \oplus \text{AK} \parallel \text{AMF} \parallel \text{MAC}$$

$$\text{MAC} = f_1(K, \text{SQN} \parallel \text{RAND} \parallel \text{AMF})$$

$$\text{AK} = f_5(K, \text{RAND})$$

where SQN is a sequence number to protect against replay attacks, AK is an anonymity key to thwart identity tracking by observing SQNs, AMF is authentication management field, and $f_0..f_5$ are security functions discussed later in this section. Secure transmission of AVs across providers' networks is addressed after security functions [3, 14, 23].

In the final stage of AKA, MS/USIM and VLR authenticate each other. First, VLR sends one of the received $\langle \text{RAND}, \text{AUTH} \rangle$ combinations to MS/USIM, MS/USIM then calculate SQN as follows to detect replay attacks:

$$\text{SQN} = (\text{SQN} \oplus \text{AK}) \oplus f_5(K, \text{RAND})$$

after that MAC is checked, once it is confirmed, MS/USIM computes

$$\text{RES} = f_4(K, \text{RAND})$$

which is checked by VLR against XRES. If it they are the same, MS/USIM and VLR are mutually authenticated and proceed to set up a secure channel using CK and IK [14].

UMTS and CDMA2000 standards define security functions $f_0..f_5$ for use in AKA. The function descriptions are as follows:

- f_0 : random challenge generation function;
- f_1 : network authentication function;
- f_1^* : re-sync message authentication function;
- f_2 : user challenge-response authentication function;
- f_3 : cipher key derivation function;
- f_4 : integrity key derivation function;
- f_5 : anonymity key derivation function;
- f_5^* : re-sync anonymity key derivation function [3, 25].

Implementation of random challenge function f_0 is left to UMTS network operators, the only requirement being that its output doesn't repeat during USIM lifetime since that would allow the replay attacks [UMTS-Intro]. CDMA2000, on the other hand, specifies 128-bit SHA-1 for pseudo-random RAND generation [3]. Although a number of attacks has been devised to find collisions in SHA-1 better than brute-force attack, no practical implementation exists.

UMTS also leaves the $f_1..f_5$ security function implementation choice to

operators since there isn't an explicit need to standardize that across networks as long as the algorithms used are cryptographically secure 128-bit block ciphers; instead, UMTS provides a sample implementation called Milenage [2]. This implementation is based on Rijndael block cipher and according to independent analysis is sufficiently secure [4]; no known realistic attacks have yet been demonstrated. Alternately, CDMA2000 fully defines the implementations for security functions f1..f5; the implementations, however, are too based on 128-bit Rijndael algorithm.

For encryption and integrity protection UMTS standard defines two additional functions f8 and f9 respectively which are implemented using KASUMI Feistel-based 8 round block cipher [1]. Despite some known weaknesses, no practical attack on KASUMI has yet been demonstrated. In turn, CDMA2000 uses 128-bit Rijndael for encryption and 128-bit SHA-1 for integrity protection [3]. In both UMTS and CDMA2000 user data is only encrypted while signaling data is only integrity protected [3, UMTS-Intro].

It is worth noting that CDMA2000 standard defines and fully specifies *USIM authentication key derivation (UAK)* function f11 along with an algorithm to verify the presence of USIM - *UMAC*. USIM authentication is necessary to counter the so-called *rogue station* attacks in which a phone does not delete keys CK and IK when USIM is removed or even sends them to another mobile. To authenticate USIM f11 generates a UAK which is used by UMAC, essentially a SHA-1 based hash function, to transform authentication tag on signaling messages. UAK is never passed out of USIM, therefore the above transformation ensures USIM is present [3].

To comply with export regulations CK, IK, and UAK key lengths may have to be reduced. This is done using full length key, some publicly known but varying value (time for example) as *salt*, and a hashing function SHA-1. The algorithm is as follows:

- an intermediate key K is generated using SHA-1(CK, salt);
- all but the desired number of bits of K are set to zero;
- a new CK is formed by SHA-1(K, salt);

which effectively reduces the entropy for CK but keeps the number of possible keys large [3].

In addition to authentication, encryption and integrity, 3G networks provide anonymity features by using TMSIs, but, as in GSM, IMSI of the subscriber may still be transmitted in clear on request from VLR [14].

4.1.2 Network Domain Security

Network domain security in UMTS and CDMA2000 networks relates to communication on and among operators' networks. A serious vulnerability of 2G networks is the absence of network domain security mechanisms – at the time of their design it was believed that limited access to core switching networks would provide sufficient protection. This situation is changing with the advent of 3G systems as more and more operators enter market. Additionally, operators turn to IP-based communication on networks instead of Signaling System 7 (SS7) -based

Mobile Application Part (MAP) protocol or IS41-based protocols of earlier mobile telecommunication systems. The network domain standardization is necessary in order to achieve interoperability among different operators' networks. Two models address network domain security: MAPsec and IPsec [22, 23].

MAPsec provides a security wrapper for earlier-generation MAP messages. It can operate in three modes: no protection, integrity protection only, and encryption with integrity protection. MAPsec uses 128-bit Rijndael algorithm: in counter mode for encryption and in cipher block chaining message authentication code mode for integrity protection [22].

IPsec is a security protocol suite for secure communication over IP networks; it can be used to secure communication over an IP-based 3G operator network. Standards specify the use of Rijndael algorithm for encryption, which is, as mentioned before, considered to be cryptographically secure [22].

IPsec and MAPsec use Internet Key Exchange protocol for key distribution [22].

To sum up, 3G standards enable network operators to use MAPsec or IPsec to provide network domain protection – the use of those protocols, however, isn't mandatory.

4.2 3G Telecommunications Security Evaluation

Previous section gave a brief overview of 3G security features. Despite a somewhat blurry security requirements set out by ITU for 3G, the security of the system is a definite improvement over 2G: phone cloning and eavesdropping are much harder to carry out due to the use of longer keys and more secure algorithms; rogue base station attacks are countered with the mutual authentication; rogue shell attacks are handled by USIM authentication in CDMA2000. Despite addressing all ITUs requirements, not all the expected security mechanisms are in place: there is no support for non-repudiation and no clear access control model.

So how secure are 3G systems? Availability-integrity-confidentiality framework may provide a useful tool in answering that question, which can be restated as how well the key security objectives of availability, integrity, and confidentiality are met by 3G telecommunications networks.

Availability is critical for 3G: aside from the fact that an increasing number of emergency calls is placed from mobile phones [GSMA], availability underpins the other two security objectives. 3G addresses the availability concerns by authenticating users and securing operators' networks. AKA is considered to be secure with the algorithms used by UMTS and CDMA2000. IP-based operator network, on the other hand, is not and IPsec use isn't mandatory. This can be a potential vulnerability and IP-based DDoS attacks on 3G operator networks may prove to be real threats.

Confidentiality, perhaps the best achieved objective of the three, is,

nonetheless, not completely realized – it is possible to gain improper access to information on 3G networks by exploiting AKA compatibility with GSM authentication. As mentioned in subsection on GSM security features, Barkan, Biham, and Keller showed how an instant ciphertext only attack can be used to recover the session key on GSM networks and consequently on 3G. Another possible attack may involve eavesdropping on IMSI transmission when TMSI is unavailable and MSC requests IMSI to be sent in the clear. IMSI can also be retrieved by an attacker who gained access to the operators' network. In other words, despite the use of strong encryption provided by 128-bit keys and Rijndael, confidentiality objective isn't fully reached on 3G networks.

Integrity option in 3G is only provided for signaling channels - this objective is perhaps the least achieved in availability-confidentiality-integrity framework.

To sum up, from the point of view of availability-confidentiality-integrity framework, 3G systems aren't secure. Having said that, 3G systems are also very open and perhaps do not require high levels of security – sensitive applications may be better off implementing necessary security features themselves according to the end-to-end principle; additionally, due to severe hardware constraints of the least common denominator on the 3G network – a basic cell phone – the more advanced security features – for example longer keys, digital signatures, public keys, key escrow for legitimate eavesdropping, or RBAC – aren't yet practical. Overall, 3G development is a step in the right direction: only collaborative, evolving, open standards can provide adequate security for such a large and diverse system.

5. Conclusion

This paper presented a survey of three generations of mobile phone systems from a security perspective. 3G networks' standards were evaluated within availability-confidentiality-integrity framework and found to not be secure. This fact, however, should be considered with realization that mobile phone systems first and foremost need to provide telecommunication service to their subscribers and have certain limitations that prevent them from achieving higher levels of security.

Finally, some limitations of this work are: omission of discussion of currently deployed 2.5G/2.75G systems (for example EDGE, GPRS) – the security aspects of these systems, however, are closely related to their 2G predecessors'; some of the protocols/algorithms/attacks mentioned haven't been analyzed in much depth; finally, there is no experimental data supporting the claim that 3G systems aren't secure. Future work can be geared toward filling those gaps.

6. References

- [1] 3GPP, 2007. TS 35.202 V7 (Specification of KASUMI).
- [2] 3GPP, 2007. TS 35.206 V7 (Specification of MILENAGE).
- [3] Rose, G., Koen, G., 2004. Access Security in CDMA2000, Including a Comparison with UMTS Access Security. IEEE Wireless Communications, February 2004.
- [4] Hawkes, P., Rose, G, 2001. Analysis of the Milenage Algorithm Set. Qualcomm Incorporated.
- [5] CDMA Development Group. www.cdg.org (12-7-2007)
- [6] Millan, W., Gauravaram, P., 2004. Cryptanalysis of the Cellular Authentication and Voice Encryption Algorithm. IEICE Electronics Exprss, Vol.1, No. 15.
- [7] Goldberg, I., Briceno, M., 2001. GSM Cloning.

www.isaac.cs.berkeley.edu/isaac/gsm-faq.html (12-7-2007)

- [8] Wagner, D., Schenier, B., Kelsey, J., 1997. Cryptanalysis of the Cellular Message Encryption Algorithm. Proceedings of Crypto 1997.
- [9] Frodigh, M., Parkvall, S., Roobol, C., Johansson, P., Larsson, P., 2001. Future-Generation Wireless Networks. IEEE Personal Communications. Vol. 8, Issue 5, October 2001.
- [10] Barkan, E., Biham, E., Keller, N., 2003. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. Proceedings of Crypto 2003.
- [11] Gindraux, S., 2002. From 2G to 3G: A Guide to Mobile Security. 3G Mobile Communication Technologies Conference. May 8-10 2002.
- [12] Millan, W., Gauravaram, P., 2004. Improved Attack on the Cellular Authentication and Voice Encryption Algorithm. International Workshop on Cryptographic Algorithms and their Uses. Gold Coast, Australia, July 2004.
- [13] Personen, L., 1999. GSM Interception.
<http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-9900/a5/Netsec/netsec.html> (12-7-2007)
- [14] Shin, M., Ma, J., Mishra, A., Arbaugh, W., 2006. Wireless Network Security and Internetworking. Proceedings of the IEEE. Vol. 94, No. 2.
- [15] ITU-T, 2006. Security in Telecommunications and Information Technology: An overview of issues and the deployment of ITU-T Recommendations for secure telecommunications.
- [16] Nichols, K. R., Panos, C. L., 2002. Wireless Security. McGraw-Hill
- [17] Wagner, D., Simpson, L., Dawson, E., Kelsey, J., Millan, W., Schneier, B., 1998. Cryptanalysis of ORYX. Lecture Notes In Computer Science; Vol. 1556.
- [18] Wingert, C., Naidu, M., 2002. CDMA 1xRTT Security Overview. Qualcomm Incorporated.
- [19] Li, T., Ren, J., Ling, Q., 2007. Physical Layer Built-In Security Analysis and Enhancement Algorithms for CDMA Systems. EURASIP Journal on Wireless Communications and Networking.
- [20] Kim, J., Oh, M., Kim, T., 1998. Security Requirements of Next Generation Wireless Communications. International Conference on Communication Technology. October 22-24, 1998. Beijing, China
- [21] Biryukov, A., Shamir, A., Wagner, A., 2000. Real Time Cryptanalysis of A5/1 on a PC. Fast Software Encryption Workshop. April 10-12 2000.
- [22] Boman, K., Horn, G., Howard, P., Niemi, V., 2002. UMTS Security. Electronics & Communication Engineering Journal. October 2002.
- [23] Bais, A., Penzhorn, W., Palensky, P., 2006. Evaluation of UMTS security architecture and services. 2006 IEEE International Conference on Industrial Informatics.
- [24] Kareem, M. R., Sarraf, M., 2002. W-CDMA and cdma2000 for 3G Mobile Networks. McGraw-Hill.
- [25] Weltevreden, L., 2006. State-of-the-art on CDMA2000 Security Support. 4th Twente Student Conference on IT.
- [26] Steele, R., Lee, C., Gould, P., 2001. GSM, cdmaOne and 3G Systems. John Wiley & Sons, Ltd.
- [27] Korowajczuk et al., 2004. Designing cdma200 Systems. John Wiley & Sons, Ltd.
- [28] International Telecommunication Union. www.itu.int (12-7-2007)
- [29] GSM Association. www.gsmworld.com (12-7-2007)