6.857 Term Project: Cellular Telephone Security

Debajit Ghosh
Sabra-Anne Kelin
Yunzhen Qu
Elliot Schwartz

December 10, 1997

Abstract

With the increasing popularity and ubiquity of cellular phones, one must start considering the security aspects of this technology. After identifying the security requirements of cellular telephones, this paper examines current systems and describes discovered weaknesses. It then reviews currently exploited holes and cellular crime, as well as legal and technical defenses aimed at combatting this crime. Finally, it summarizes some research efforts into the future of cellular telephone systems and concludes with a set of design guidelines and suggestions for implementing future systems.

Contents

1 Introduction

In today's busy society, portable cellular phones have become commonplace for everyone, from executives to university students. However, security issues relating to cellular phones have only recently surfaced. In particular, traditional analog cellular phones suffer from problems related to the privacy of conversations and the ease with which the system can be used without payment. New digital cellular phones are currently emerging in the marketplace, and while some of these boast increased security features, security problems are still likely to exist. In order to identify current security problems and prevent future ones, a thorough analysis of the security aspects of cellular telephone communication is necessary; this paper will attempt to provide such an analysis.

After identifying the necessary security requirements and issues for cellular telephone communication, we will present overviews of some of the security features present in current systems, as well as known weaknesses in those features. Then, we will discuss cellular phone crime in detail, emphasizing what security-related crimes prevail today, some common-sense and technical defenses against those crimes, and the appropriate legal defenses and efforts in this field. We will then explore some systems that are being researched and proposed for the future of cellular telephone communication. Finally, we will present our own findings and thoughts regarding important design considerations for avoiding the weaknesses and problems discussed in the paper.

2 Security Requirements and Related Issues

Before we can examine the security issues with the current and future cellular phone infrastructure and mechanisms, we need to consider and analyze the security requirements for such a system. Indeed, many efforts recognize the importance of this issue and provide their own collection of requirements [13, 41, 22]. Here, we will provide our own summary and discussion of the issues and requirements related to the security of cellular phone systems.

Authentication. Only authorized users should have access to the cellular phone system. The most significant implication of a breach of the authentication requirement is that unauthorized users can use and abuse the system, resulting in phone fraud and incorrect billing. Additionally, one must consider authentication of the system to the user, which prevents masquerade attacks where malicious parties gain confidential information by pretending to be part of the network. Finally, it is desirable to provide mechanisms by which two mobile users can authenticate themselves to one another, although this is more of a requirement for mobile communication rather than strictly mobile conversation. Authentication systems are usually challenged by active attackers.

Privacy. Only the involved parties should be able to listen to a conversation on the system. Third parties and eavesdroppers should not be able to listen in on conversations for obvious reasons, including privacy and protection of sensitive and personal information. Specifically, one must ensure that the link between the mobile user and the network components (such as the base station) is kept private, so that confidential information is not revealed. In addition, one must ensure that privacy between two mobile users is available, to protect voice and data communication between those users. Privacy is often challenged by passive attackers.

Anonymity. The system should reveal neither the identity nor the location of any given user who wishes to gain access. Revealing this information violates privacy concerns of users, who may not wish others to know their travel habits. Further protection must be provided to keep third parties from being able to trace a user through the network, even if the third party does not know the exact identity of the user. Additionally, selective denial-of-service attacks (where a specific user or group of users are denied service from the system) are not possible if an adequate level of anonymity is achieved. Anonymity can be breached by either passive or active attacks, depending on the security considerations in the system.

Availability. The system should be readily available. Although this is more of a general system design consideration than a security specific one, one must ensure that holes do not exist that enable denial-of-service attacks. Availability is susceptible to active attacks such as jamming the network, congesting it, or somehow causing a denial of service to specific users by various means.

Simplicity and Efficiency. Again, this is more of a system design issue rather than a security-specific issue. However, when one takes human factors into consideration, simplicity of the system must be a top priority. More complex systems often encourage users to forgo or bypass security options, thereby transforming a potentially secure system into an insecure one. Additionally, one must consider the fact that the security mechanisms utilized by the cellular phones and devices should be as efficient as possible because of the reduced power and capabilities of these mobile devices. Lengthy session establishment protocols and key exchanges simply are not reasonable for most of the hardware used in current cellular phone systems.

Other issues. Other issues that must be considered include ensuring that base stations and other centralized databases are kept as secure as possible from outside (and inside) attacks, since they often contain valuable secrets. Additionally, one must consider security in light of roaming issues, where security and authentication information may need to be transferred from one part of the network to another as the mobile user roams around.

3 Cellular Telephone Systems and Weaknesses

Cellular telephony is a method of bringing mobile communication to the telephone system. The mobile telephones communicate via radio with base stations. These base stations are operated by cellular service providers and are physically tied into the regular land-based phone system. Regions are divided up into a number of “cells” which can be served by different base stations. As a mobile telephone moves between cells, it changes the base station with which it is communicating.

There are a number of cellular telephony systems in place. They can be broken down into two main categories: those in which the mobile telephone communicates with the base station using analog transmission, and those that use digital transmission. The analog system operates in a similar manner to voice radio and is currently in widespread use. Digital systems are collectively referred to as PCS, or Personal Communication Services. There are several different digital systems currently in operation or being deployed. In North America, these are colloquially known as GSM, CDMA, and TDMA.

3.1 Analog

3.1.1 How it works

In the analog cellular system, the radio spectrum is divided into a number of different channels at different frequencies. Most of these are used for actual analog voice conversations, while a few are used as low bit rate digital control channels. Adjacent cells use different groups of channels so as not to interfere with each other. Each telephone is assigned an identification number (ID) which is used for billing purposes.

Base station selection. Neighboring base stations transmit different signals to allow a mobile telephone to identify them. A mobile telephone collects information on the strengths of these signals. The cell phone then uses this information (in cooperation with its current base station, if any) to determine if it should switch base stations.

Call origination. The mobile telephone transmits on the control channel its ID as well as the number it wishes to call. The base station verifies the ID number, assigns a voice channel, and completes the call. The mobile telephone tunes into the voice channel it has been assigned.

Call reception. The mobile telephone is paged on the control channels of the cells in the area in which it was last registered. Upon receiving the page, it reselects the strongest base station and responds on the control channel. The base station selects a voice channel, informs the mobile telephone of its selection, and completes the call.

3.1.2 Weaknesses

Since the analog cellular telephone system makes no attempt to be secure in any way, it has weaknesses in all critical areas.

Authentication. The mobile telephone authenticates itself to the system by transmitting its ID number in the clear. Anyone with a standard radio scanner can capture and discover the ID number and subsequently masquerade as the telephone.

Privacy. The voice channel is a simple analog channel so eavesdroppers can listen in on conversations with a radio scanner or modified cellular telephone. While there are some methods of making analog communication more difficult to intercept (such as frequency-hopping), these methods are not frequently performed. Moreover, methods such as frequency-hopping do not provide adequate security. Similarly, the telephone number being dialed and calling card or voice mail PINs can also be captured.

Anonymity. Since the ID number of the mobile telephone is used for authentication, anyone who overhears it being transmitted can track the location of the phone.

3.2 CDMA/TDMA

Technically, CDMA and TDMA are just methods of creating a number of channels for use in cellular telephony. There are a number of possible ways cellular telephone systems can utilize them. However, in North America, the terms have become synonymous with the two leading proposals of each type. These are the IS-95 and IS-136 (formerly IS-54) standards, for CDMA and TDMA, respectively. Though these two systems are incompatible, their security mechanisms are identical, so we treat them together.

3.2.1 Security Related Variables and Algorithms

Variables. Several pieces of information are used in the authentication and encryption procedures:

- MIN_2 and MIN_1 are 8 and 24-bit numbers, respectively. MIN stands for Mobile Identification Number, and it is derived from the 10 digit directory number (i.e. area code and local number). Since the directory number needs to be known by people who want to call the telephone, the MIN is essentially public information.
- ESN (Electronic Serial Number) is a 32-bit number that is set at the factory and associated with the particular phone and manufacturer. While knowledge of it is not needed by anyone but the network and the mobile telephone itself, since it is assigned by the manufacturer it should not be considered private.
- *SSD-A* (Shared Secret Data - A) is a 64-bit number that only the network and the mobile telephone should know. It is used for authentication.
- *SSD-B* (Shared Secret Data - B) is a 64-bit number that only the network and the mobile telephone should know. It is used for encryption.
- *A-key* is a 64-bit number known only by the HLR/AC (Home Location Register / Authentication Center, part of the network) and the mobile station.

The CAVE algorithm. The CAVE algorithm, represented by $\mathcal{C}$, is a mixing function that is used within both the authentication and the encryption algorithms. For authentication, it can be used to generate an 18-bit number $AUTHR$ from a 24-bit number $RAND$, MIN_2, MIN_1, ESN, and *SSD-A*. For encryption it can be used to generate a 520-bit duplex voice privacy mask. The complete algorithm is described in [12].

3.2.2 Authentication

System access. Whenever the mobile telephone performs a registration, call origination, or page response (responding to an outside call), it completes the system access procedure. This involves the base station authenticating the mobile telephone with the IS-41 challenge-response protocol. It relies on the property that given a set of overheard challenge-response pairs $(RAND_i, AUTHR_i)$, an eavesdropper should be unable to use $RAND$ to produce $AUTHR = \mathcal{C}(RAND, MIN_2, MIN_1, ESN, SSD\text{-}A)$ without the other information. The protocol operates as follows:

1. The base station generates a random number $RANDU$, and calculates $AUTHR = \mathcal{C}(RAND, MIN_2, MIN_1, ESN, SSD\text{-}A)$.
2. The base station sends $RAND$ to the mobile telephone.
3. The mobile telephone computes $AUTHR$ from $RAND$ by the same method.
4. The mobile telephone sends $AUTHR$ to the base station.
5. The base station compares the received $AUTHR$ to the computed $AUTHR$.

Messages exchanged:

$$\begin{array}{llll} \text{BS} & \rightarrow \text{MS} & : & RAND \\ \text{MS} & \rightarrow \text{BS} & : & \mathcal{C}(RAND, MIN_2, MIN_1, ESN, SSD\text{-}A) \end{array}$$

An alternative to the $RAND/AUTHR$ challenge/response pair (sometimes referred to as the "global challenge") is a $RANDU/AUTHU$ challenge/response protocol (referred to as the "unique challenge"). This alternative challenge/response is used in systems that do not support $RAND/AUTHR$, when $RAND/AUTHR$ fails, or in flash requests (described below).

Call origination. Authentication on call origination is identical to authentication on system access except that MIN_2 is calculated from the telephone number *being called*. This prevents responses from being reused with other telephone numbers.

Weaknesses. The main weakness with the IS-41 protocol is the lack of two-way authentication. Since the system is not authenticated to the user/handset, fraudsters can gain service without actually breaking the CAVE algorithm [31].

To understand the basic concept behind attacks which exploit this weakness, imagine that there is a team of two fraudsters: an unregistered handset and a network impersonator. Together, the two fraudsters commit a man-in-the-middle attack. Let us call the unregistered handset HI. HI wants to gain access/obtain service from his network, so he listens for the challenge and passes it off to his partner, whom we will refer to as NI. NI searches for legitimately registered handsets and queries them with the challenge in which HI is interested. He relays the response received from the victim handset to HI. HI can then proceed to use this information to gain service at the expense of the legitimate victim handset.

Flaws in system access. Figure 1 illustrates an attack to gain system access. When an HI hears the RAND value broadcast by the network, he relays it to the NI. By this time, the NI has already located a handset whose MIN/ESN it has overheard. The NI then pretends to be the network and queries this handset with the RAND. The handset responds with its MIN/ESN/COUNT/AUTHR, which the NI passes on to the HI. The HI can now use this information to help him get service from his own network.

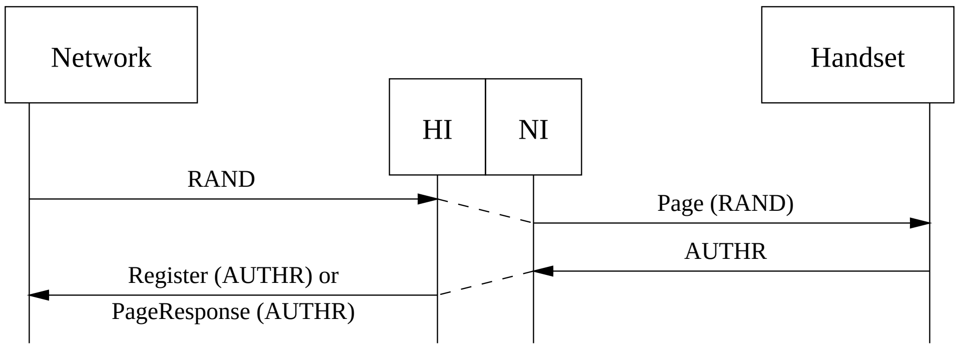

Figure 1: Flaws in system access

The design does prohibit fraudulent call origination, because the AUTHR response in call origination is a function of the dialed digits. It is not possible to make the handset respond with AUTHR for specific digits.

The HI can falsely register in a different location. The only parameter which changes from one system access to another is the RAND value, and the HI can pass the correct RAND value to the NI to use in obtaining the AUTHR. Thus, in court, a criminal can use false phone records to show that he was registered somewhere other than where he actually was. The same method can be applied to allow the fraudster to receive phone calls under an assumed identity, because a page response requires the same information as a registration in generating the AUTHR.

It is very important for the network to use a cryptographically safe random number generator during the periodic update of the RAND value. Something like a noisy diode or network traffic would be ideal. A typical pseudorandom (i.e. linear congruential) number generator can be broken if the sequence is long enough. In that case, the HI will have knowledge of the future RAND values. It can then ask the NI to solicit corresponding responses for use at its leisure.

System access with unique challenge. Some networks do not require or support authentication upon system access. They support authentication only on the voice or traffic channel by performing an unique challenge. The network first verifies the handset's MIN/ESN, then generates the RANDU and sends the it to the handset. It then waits to verify the response.

Figure 2 shows how the fraudsters can get around the unique challenge during system access. To obtain free service, the NI locates a handset and gives the MIN/ESN values to the HI. The HI then relays the unique challenge RANDU value to the NI, who passes it on to the victim handset. The handset's AUTHU response is passed from the NI to the HI, who successfully answers the unique challenge from his network. This scheme would allow the HI to receive free service, including call originations.

System access with unique challenge backup. In addition, when the AUTHR response from the handset fails to match the one generated by the network, a unique challenge can be sent as a backup. This is another vulnerability to the NI/HI

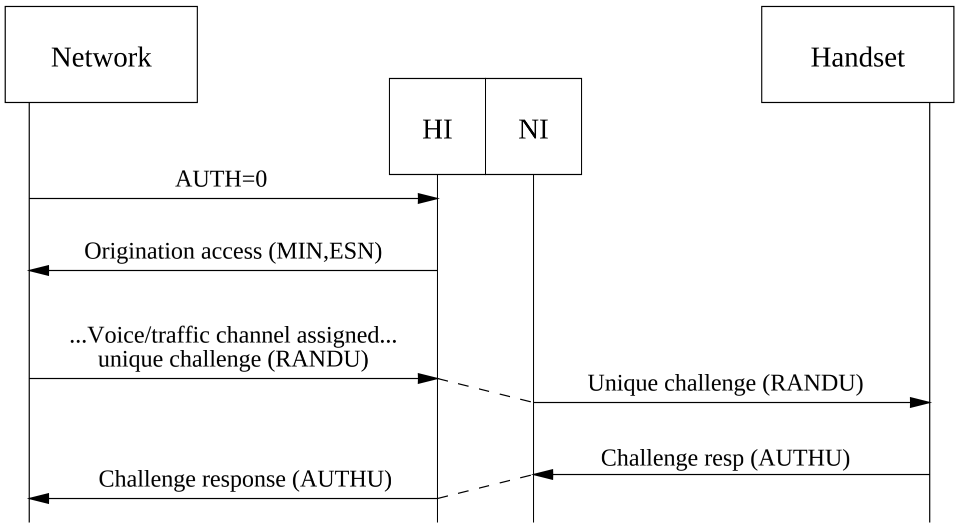

Figure 2: System access with unique challenge

pair. The NI first locates a victim handset, then relays the MIN/ESN information to the HI. The HI uses the MIN/ESN for system access but then intentionally fails the global challenge RAND with an invalid AUTHR. Now the network sends an unique challenge RANDU, which is relayed from the HI to the NI to the victim handset. The AUTHU is then used by HI to get access to the system. Figure 3 illustrates how this attack is done.

Flash request with unique challenge. The flash request can be used to establish a third-party call. Figure 4 shows an attack which begins with the NI finding a victim handset and querying it with the global challenge RAND from the HI's network. The NI gets the AUTHR and relays all the information (MIN/ESN/COUNT/AUTHR) to the HI to register as a clone of the victim. The HI then uses a second handset to place a call to the clone. Upon receiving the page query, the HI listens for and passes the global challenge RAND to the NI. The NI queries the victim with RAND and obtains AUTHR to relay to HI, who then successfully completes the page response system access. Now, in order to establish a third-party call, HI initiates a flash request on the clone. The network will generate a unique challenge RANDU to the clone, and the HI asks the NI to send RANDU to the victim handset to get AUTHU. When the HI answers the unique challenge generated by the flash request, the third party is on the line and the second handset(which the HI used to call the clone) can be hung up. The fraudster has successfully made a free call to this third party.

Mail distribution flaw/compromising the ESN Unlike GSM, which has a SIM to store keys, IS-54 allows the user to enter the A-key and some verification digits into the handset. Incredibly, this secret information may be distributed via postal mail. The idea behind this practice is to have direct contact between the user and the service provider. Obviously, this is a huge breach of security, and the fraudster can

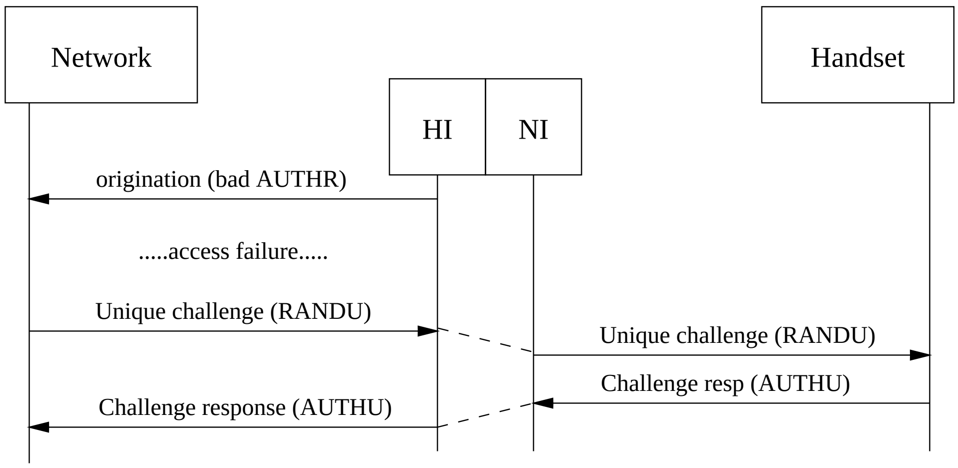

Figure 3: System access with unique challenge backup

therefore easily obtain the key and the verification digits.

The verification procedures require the user to enter the A-key and the verification digits into the handset. The handset then performs rounds of CAVE with the entered A-key and the ESN stored in its memory. If the result matches the verification digits then the A-key is accepted; otherwise, it prompts the user to re-enter the information.

A fraudster who has knowledge of the A-key and the check digits can run the algorithm on all 32-bit values of ESN to find the ones which generate the acceptable check digits. The ESN has a format such that it is possible for the fraudster to rule out most of the values. The eight most significant bits make up the manufacturer code and the eighteen least significant bits are assigned by each manufacturer. The middle six bits are initially set to zero; they are only allocated by the FCC to the manufacturer when all other possible combinations have been exhausted. It is not too difficult to discover the fourteen bits for a manufacturer, especially since the top four manufacturers sell over seventy-five percent of the handsets in North America. By sampling from the air or inquiring at service shops, the fraudster can narrow the choices down to just a few. He can run CAVE on all possible valid ESNs along with the A-key [31].

This is a protocol flaw because there is no need to used the ESN to run CAVE. A simple cyclic redundancy check would suffice to verify whether the user has entered the correct digits.

3.2.3 Audio Encryption

The CAVE algorithm and $RAND$ are also used to produce a 520-bit key for encrypting the audio channel. In TDMA, the key is essentially used as a one-time pad (that is, an XOR mask) that is applied *repeatedly* to the audio data. This means that if the key is discovered, the entire conversation can be decrypted. Moreover, knowing even a short bit of plaintext (for example, the representation of silence) reveals the key. CDMA uses a different scheme which relies on keyed spread spectrum techniques [44].

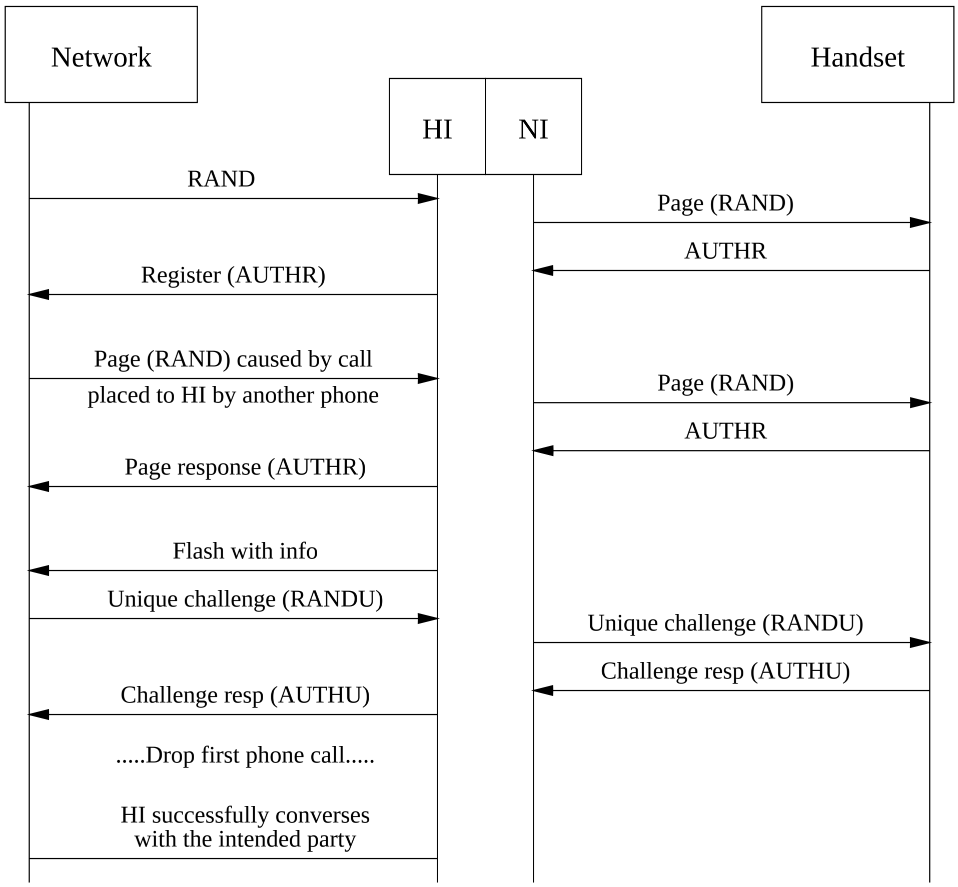

Figure 4: Flash request with unique challenge

3.2.4 Control Encryption

The Cellular Message Encryption Algorithm (CMEA) is a Telecommunications Industry Association (TIA) standard that is used to encrypt a control channel between the cellular telephone and the base station.

A main use of the control channel is for sending data such as digits dialed on the keypad. These might include the telephone number called, a PIN for a voicemail system, a calling card number, or a credit card number. It is also used for alphanumeric paging.

The algorithm. CMEA is a simple block cipher with a 64-bit key. It supports variable block sizes, but two to six byte blocks are typically used in the United States. The algorithm operates in three passes, each of which help to propagate changes using linear and non-linear techniques, as well as lookup tables. Full specifications for CMEA are given in [12, 39].

Weaknesses. Counterpane Systems and UC Berkeley recently announced flaws in CMEA. Bruce Schneier and John Kelsey of Counterpane, along with graduate student David Wagner of Berkeley, published their analysis, discussing some fundamental weaknesses of CMEA, as well as chosen- and known-plaintext attacks [44].

Fundamental weaknesses in CMEA include the following:

- CMEA is its own inverse. Thus double encryption of the plaintext yields the plaintext itself.
- As block cipher, CMEA does not use random initial vectors or block chaining. Since the key is rederived for each call, codebook attacks are theoretically impossible. However, in practice it has been found that when each digit dialed is encrypted in a separate CMEA blocks, codebook attacks are indeed still possible.
- The least significant bit of the ciphertext is the complement of the least significant bit of the plaintext, which results in a one-bit "leak."
- The T-box algorithm is such that changing certain combinations of the key bits does not affect the output value. This effectively reduces key space.
- The attacker does not have to know the key in order to break CMEA. By recovering values of the T-box entries, he can learn the plaintext.
- The value of T(0) is relatively easy to compute. This value enables the attacker to learn the input to the T table for the second byte of the plaintext.
- The CaveTable distribution is not well suited for CMEA. Its distribution is skewed such that 92 of the 256 possible 8-bit values never appear. This causes the T-box values to be skewed as well. T(i)-i is known to be in the CaveTable, so for any input to the T-box, 92 possibilities for the corresponding output can be eliminated instantly.

The chosen-plaintext attack discussed in the paper required 338 chosen plaintexts on average. It proceeds by recovering T(0) first, then the remainder of the T-box entries. In practice, the chosen-plaintexts may be obtained by persuading the targeted cellular telephone user to call a number under the attacker's control. Upon connection, the user is prompted to enter digits chosen by the attacker.

The known-plaintext attacks are even more disastrous. For 3-byte blocks, 40-80 known texts are required. The cryptanalysis begins by gathering information about the T-box from known CMEA encryptions. Then, using pruned search and meet-in-the-middle techniques, the attacker can exploit the skew in the CaveTable to recover the CMEA key. The known plaintext is collected by convincing the user to dial a number under adversarial control, using their calling card. The attacker will then have knowledge of the DTMF tones and user-dialed digits.

Although most cellular standards use 3-byte block widths, a few, such as CDMA(IS-95), use CMEA with a 2-byte block. This makes things worse still – a known-plaintext attack on 2-byte blocks needs just four plaintexts.

3.2.5 Data Encryption

ORYX is a very simple LFSR-based (Linear Feedback Shift Register) stream cipher used for encryption for wireless data services that has a 96-bit key space [44, 23, 25].

Weaknesses. The same team which successfully broke CMEA also published a paper on the cryptanalysis of ORYX [25]. Schneier, Kelsey, and Wagner devised an attack which employs a divide-and-conquer technique: start by guessing the higher order bits of the registers to find part of the generator state, then check the possibilities against the next byte of key stream. The entire state can be recovered using about 24 bytes of known-plaintext and 2^{16} time. Once again, the authors showed that a widely used cipher was not as secure as it was thought to be.

3.3 GSM

3.3.1 How it works

GSM, a "Global System for Mobile communications" (but originally named after Groupe Spéciale Mobile), is a digital system that is widely deployed in Europe. It encompasses not only the interface between the user and the base station, but also provides standards for the internal operation of the system and interfaces that support roaming across different carriers. The mobile telephones and the base stations communicate using a time-division scheme (i.e. GSM is TDMA-based). GSM service is offered in a few parts of North America.

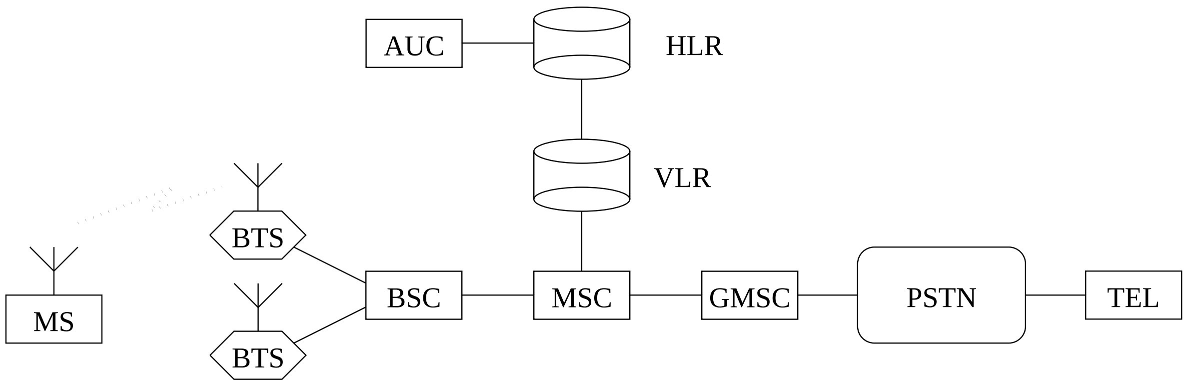

Figure 5: Overview of GSM Architecture

Network architecture. The network architecture of GSM is described in [30]. There are several components of the architecture which participate in security-related transactions. *MS* is the Mobile Station i.e. the mobile telephone itself. *BTS* or *BS* is Base Transceiver Station Controller or Base Station, which performs encryption, decryption, and other security features with the mobile telephone. *HLR* and *VLR* are the Home and Visitor Location Registers, respectively. These store information required for authentication which is obtained from the Authentication Center *AUC* (or *AC*). Other components which do not participate in security-related transactions are the *BSC* (Base Station Controller), the *MSC* (Mobile Switching Center), the *GMSC* (Gateway Mobile Switching Center), the *PSTN* (Public Switched Telephone Network), and the *TEL* (the remote telephone).

Identification. For identification, GSM mobile telephones have a smart card more commonly referred to as the "subscriber identity module" (SIM). A SIM can be used with any GSM phone to allow users to make calls on their personal accounts. A GSM phone without a SIM is useless. The SIM contains the circuitry that implements security-related algorithms such as A3, A5, and A8 (described below), as well as identification information. In particular, the SIM stores an IMSI (International Mobile Subscriber Identity), a TMSI (Temporary Mobile Subscriber Identity) and a shared key K_i with the system. The IMSI is a permanent identification number that is kept private (i.e. it is not related to the telephone number and is never transmitted in the air). The TMSI is a temporary identification number that is assigned during location update to protect the true identity of the caller. The shared key is permanent and is used to produce challenge-responses and session encryption keys.

Authentication. The following protocol is used to authenticate the mobile telephone to the base station during initial registration, at call set-up, and during a location update (handoff). $\mathcal{A}3$ is the A3 algorithm, which runs on the SIM. The authentication protocol relies on the property that given a set of overheard challenge-response pairs $(RAND_i, SRES_i)$, an eavesdropper should be unable to use $RAND$ to produce $SRES = \mathcal{A}3(RAND, K_i)$ without K_i.

1. User enters PIN. The mobile telephone sends an access request to the network.
2. Network generates random number $RAND$ and sends it to the mobile telephone.
3. The mobile telephone calculates $SRES = \mathcal{A}3(RAND, K_i)$, and transmits it to the network.
4. The network compares the received $SRES$ with one it has calculated in the same manner.
5. Both parties use $RAND$ and K_i to generate a Communications Key K_c for encryption.

The following diagram shows the messages exchanged. The source and destination of the messages are listed on the right, with an arrow indicating the direction of transmission. The contents of the message are given after the colon.

						MSC/VLR	$\leftarrow$	HLR	$\leftarrow$	AUC	:	$(RAND, SRES)$
User	$\rightarrow$	MS									:	PIN
		MS	$\rightarrow$	BS	$\rightarrow$	MSC/VLR					:	Access requested
		MS	$\leftarrow$	BS	$\leftarrow$	MSC/VLR					:	$RAND$
		MS	$\rightarrow$	BS	$\rightarrow$	MSC/VLR					:	$SRES = \mathcal{A}3(RAND, K_i)$

Encryption. GSM uses encryption to protect the privacy of audio data. Encryption is set up just after the authentication takes place. In fact, the random number $RAND$ that is transmitted as a challenge to the mobile telephone is also the basis for the encryption key K_c. While the A3 algorithm produced the challenge response, the A8 algorithm produces the encryption key:

$$K_c = \mathcal{A}8(RAND, K_i)$$

Messages are then encrypted as follows:

$$E = \mathcal{A}5(M, K_c, frame)$$

Where E is the ciphertext, M is the plaintext, K_c is the encryption key for the session, $frame$ is the TDMA frame number, and $\mathcal{A}5$ is the encryption algorithm used.

3.3.2 Weaknesses.

Two major problems have been identified with the GSM system. One is an operational blunder which allows for attacks on authentication. The other is a protocol weakness that compromises anonymity.

Authentication. Although the GSM specification calls for encryption of traffic between the base station and the authentication center, in practice, many operators actually leave transmissions in the clear. Therefore, if an attacker can discover the identity (the IMSI) of the target phone, then he can transmit this information to the authentication center and intercept the responses as they come back to the base station. He will then have the correct response to the authentication challenge and be able to encrypt the traffic with the correct key. Thus, he can charge his calls to the target phone. It is relatively easy to find the IMSI of a particular phone; commercial scanners are available for passive or active eavesdropping.

This is precisely the attack Cambridge University devised, in response to a challenge announced by German TeleKom [14]. There was a reward of 100,000 DM to a telephone hacker who is able to communicate at the expense of the (national) number. The related smartcard was said to be safely stored in lawyer's office. Some security hackers at the Cambridge University Computer discovered the lack of encryption of traffic between the GSM base stations and decided to exploit this weakness. Their plan was to do the transmission and interception online with a smartcard emulator hooked up through a PC to a microwave protocol analyzer. Unfortunately, the financial reward eventually fell through and the actual attack was not deployed. However, their principle was sound.

Privacy. The original A5 encryption algorithm, A5/1, was thought to be too strong so it could not be exported to many nations under the COCOM (Coordinating Committee for Export to Communist Area) agreement [21, 33]. (While COCOM is now defunct, the export rules still exist.) Because of this, a weaker algorithm called A5X or A5/2 was developed by the European Telecommunications Standards Institute (ETSI) which is exportable and is currently being used outside the former COCOM countries. In [33], there are claims that the algorithm is just as secure as the old one, but it "does not use as much mathematics as the old one." On the other hand, [21] claims that it is a weaker algorithm and is easier to crack, and there are "hints that several European police forces and security organizations would be happier if the A5X standard would be adopted in the old continent also."

Anonymity. GSM uses an alias scheme which allows a user to be referenced without revealing his real identity. However, once a mobile user is disconnected in mid-conversation, he is required to transmit his real identity in the clear to the base station upon reconnection [13]. Then a new alias is issued and transmitted back to the user for use in future communications. This provides an easy target for eavesdroppers and possibly active attackers who might cause such disconnections.

4 Crime and Related Legislation

4.1 Introduction to Cellular Phone Crime

4.1.1 Overview

People who want to take advantage of a large system will invariably attack its weakest point. The cellular telephone network is no exception. Although some insecurities exist in digital systems, exploiting them requires computational power and knowledge of encryption. Today's crooks instead tend to exploit the cellular phone network in less sophisticated ways.

We will first examine why people would want to commit cellular phone crime. Then we will describe how people take advantage of the cellular phone network. Lastly, we will note which laws govern cell phone crime.

4.1.2 Benefits of Making Illegal Calls

Two major types of cell phone crime are prevalent today. The first type of crime involves making illegal cell phone calls (also called stealing air time). These illegal phone calls are attractive for two reasons: the calls are free, and they cannot be traced back to the caller. Criminals have developed various attacks for stealing air time. Of course, the criminals do not always use the free air time themselves. They can sell it to other people, thereby making money selling something they do not own and possibly providing others with a cheaper rate.

The other benefit of making phone calls illegally is that they cannot be traced back to the caller. Consider this situation: the police have obtained a warrant to tap a criminal's home phone. The criminal, however, makes all of his business calls illegally via a cell phone, so the illegal phone calls are billed to a legitimate user's account. Police would then encounter difficulty in tracing the crook's calls. First of all, the police must determine which account the calls are being made from, since the account is not in the criminal's name. Then, even if the correct account were found, the police could not obtain a warrant to listen to calls billed to that account because that would invade the legitimate user's privacy.

4.1.3 Eavesdropping

The second type of cell phone crime is eavesdropping. Eavesdropping is illegal because of the obvious invasion of privacy. Just as wiretaps of land phones are illegal without a warrant, it is also illegal to eavesdrop on others' cellular phone conversations. The law in this area has recently been clarified with passage of the Electronic Communications Privacy Act (ECPA) in 1986.

4.2 Illegal Calls - Making Them, Preventing Them

The methods of making illegal calls range from low-tech to high-tech. We will concentrate here on the high-tech methods, which are used to commit access fraud. Although access fraud is committed using high-tech tools such as software and hardware programming, the crook seldom has to invent these tools himself. They are easy to come by if one knows where to look [32, 37, 38]. Thus, even though access fraud is high-tech, it is still much easier to commit access fraud than to try to eavesdrop by exploiting a weak encryption system.

Before discussing access fraud, we will briefly discuss stealing phones and subscription fraud, since these low-tech methods cause service providers and legitimate customers to lose a noticeable sum of money every year. The Cellular Telecommunications Industry Association (CTIA), a lobbying group in Washington, has spent many years investigating cellular phone fraud in general. Many parts of this section are based on their work [17].

4.2.1 Stealing Phones

The ultimate "brute force" method to make an illegal phone call is simply to steal the phone of a legitimate user. Once a criminal has stolen someone's phone, he can make as many free calls as possible until the owner reports the phone being stolen. As soon as the theft is reported, the service provider deactivates the missing phone, thereby preventing further abuse.

The first step in preventing theft of cellular phones is to educate users on how to protect their phones. In [16], cell phone owners are told not to lend their phones to strangers or leave their phones unattended. It is also suggested that an owner remove the speaker and antenna from his phone if it will be in his car for a long time. Finally, users can also request long-distance call restrictions for their cell phones.

The second way of preventing unauthorized phone calls is to equip the phone with a security feature such as a PIN number or a smart card. Phones with these safety features prevent phone calls from being made without first dialing the PIN or swiping the smartcard (only the owner should know the PIN number or possess the smartcard). Unfortunately, these methods do not always work in practice because of inconvenience to the user and laziness on his part. Some users choose not to use the PIN feature because they do not want to memorize the PIN, while other users leave the smartcard in the phone so they do not have to find it the next time they want to make a call. Thus, it would seem that user error and laziness is one of the most vulnerable parts of the cell phone system.

4.2.2 Subscription Fraud

Another way of making illegitimate phone calls is to sign up with a service provider using a false identity. Criminals can give a false name and address so that when the bill finally arrives (after they have made a month of free phone calls), it is sent to a non-existent individual. By the time the service provider cancels the account for nonpayment, the damage has already been done.

This type of fraud is decreasing for many reasons. First of all, service providers now check all applications for unusual features, such as home addresses which differ from the city postmark. Service providers can also check that the person listed on the application really does exist. But the most effective move by service providers to decrease subscription fraud is charging a fee up-front before the cell phone can be activated.

4.2.3 Access Fraud (Tampering With the Phone)

Introduction to access fraud - how cell phones work. Before we can discuss the details of how phones can be modified to make illegal calls, we should review how legitimate phones work. Each cellular phone has a unique 13-digit number which is assigned to it by its manufacturer. This number is called the Electronic Serial Number (ESN). The ESN is similar to an automobile's Vehicle Identification Number, or VIN. It is against FCC Rules to alter or copy the ESN of a cellular telephone (see Related Legislation, 47 CFR 22.919). This means that one ESN is used for the entire life of the phone.

Each cellular phone also has a 10-digit number which is composed of the phone's 3-digit area code and 7-digit local phone number. This number is called the Mobile Identification Number (MIN). The MIN is assigned by the wireless carrier to a customer's phone. Unlike the ESN, the MIN is designed to be changed. For example, when a customer moves to another city, he may want to change his phone number for local billing purposes.

Lastly, each cellular phone has programmable system parameters which are set by the phone dealer [36]. Collectively, these parameters are called the Number Assignment Module (NAM). For example, the MIN is part of the NAM.

A scenario for the commission of access fraud. According to [17], access fraud is "any unauthorized use of a wireless service through the intentional or unintentional tampering, manipulation, or programming of a wireless phone's Electronic Serial Number (ESN) and/or Mobile Identification Number (MIN)." The steps involved in committing access fraud are well known [20].

The main step in committing access fraud is programming a new ESN and/or MIN into a cellular phone (Depending on which type of fraud one wants to commit, either the ESN, the MIN, or both must be reprogrammed). To accomplish this, the crook first removes the chip holding the ESN/MIN information from the cell phone. In its place he installs a socket that takes an EPROM chip. He programs the ESN/MIN into an EPROM, which he then installs in the phone. Software also exists to reprogram some cell phone chips by connecting a laptop computer to the phone's data port [36]. This software is currently available legally, although legislation has been proposed to make this software illegal (see Wireless Telephone Protection Act).

The modified phone can now be used to commit many types of access fraud, such as call selling, extension phones, tumbling ESN phones, and cloning and emulation phones, as discussed below.

Call selling. Call selling combines a modified cell phone with a stolen long-distance calling card number [17]. The call seller, masquerading as a licensed reseller, offers international calls to customers at a low price. Depending on how the phone is actually modified, this type of fraud can be prevented.

Extension phones. An extension phone, which is used to commit "two phones, one number" fraud, is one of two different phones which are programmed with the same MIN and ESN. The process starts with one legitimate phone. This phone is brought to an illegal business where a second phone is altered to have the same ESN and MIN as the first phone. This way, incoming calls will be answerable on either phone. Of course, calls made on the second phone will be charged to the owner of the first phone.

The idea of having an extension phone for a cellular phone is not inherently dishonest (although it is easy to see the enormous potential for abuse). Many legitimate cellular customers desire this service so that they can have two phones with the same number. For example, one phone could be left in the car and one could be left at home. Or, the extension phone could be given to another family member. The problem with extension phones is that ESNs are factory set and are not supposed to be changed by anyone. A few years ago, anyone who wanted an extension phone had to have it made illegally. In response to this, wireless carriers have developed a software solution for extension phones. These phones are programmed with the same MIN, but they have distinct ESNs (Since the ESNs are distinct, this type of extension phone is not illegal).

Tumbling ESN phones. Tumbling ESN phones were first created in late 1990. Normal cellular phones were altered so that they used a different ESN each time the caller made a new phone call. This made the caller appear to be a new customer for each call. Installing a special NAM in a phone granted the tumbler caller the ability to generate 48,000 possible ESNs.

When a cell phone wants to initiate a call, it sends its ESN and MIN to the nearest switching station. If the ESN and MIN match a that of a current subscriber, then the call is allowed to go through. If the ESN and MIN fail to match a subscriber, then either the phone is "roaming" (i.e. it is out of its local service area), or the phone is a tumbling ESN phone. Back when tumbling ESN phones were popular, service providers naively assumed that if the phone was not in their system, then the caller was a legitimate out-of-town roamer. When the existence of tumbling ESN phones was discovered, the first solution was for the service providers to ban all customers from initiating calls outside their home area. This brute force method was later replaced by pre-call validation: If the phone trying to initiate a call does not belong to a subscriber from the local system, then the local system checks the phone's ESN and MIN with the phone's home system. This test must be completed successfully before the call is allowed to go through. Pre-call validation has decreased the existence of tumbling ESN fraud significantly.

Cloning/emulation phones. Cloning/emulation phones represent the state-of-the-art in cellular service fraud. In this attack, a cell phone is modified to look like a legitimate phone. This is accomplished by installing in the phone an EPROM (as described above) which is programmed with the ESN and MIN of a legitimate user. Calls are then billed to the legitimate user.

The hardest part of making a cloned phone is obtaining valid ESN/MIN pairs. Luckily for the crooks, any cellular phone which is turned on broadcasts its ESN and MIN every couple of minutes to tell the mobile switching station its location. A phone also broadcasts its ESN and MIN when a call is made or received [35]. The crook then uses a monitoring device, such as a scanner, to intercept the phone's ESN and

MIN [45]. These devices are currently being sold on the open market, but legislation has been proposed to make these devices illegal (see Wireless Telephone Protection Act). The ESN/MIN combination can also be obtained through contacts who work for a cell phone retail agent or service carrier.

One sophisticated variation on cloning/emulation phones is the lifetime phone. The lifetime phone contains a chip that is programmed with many different valid ESN/MIN pairs. The idea here is to use one ESN/MIN pair until the fraud is discovered and the pair is canceled by the service provider. At that time, the phone's ESN and MIN can by reprogrammed by merely pressing buttons on the keypad. The key benefit with a lifetime phone rather than a simple cloned phone is that you can reprogram the phone using software rather than having to replace the chips themselves. Depending on how many valid pairs are stored in the phone, the phone could indeed last a "lifetime."

Preventing access fraud. Until recently, with the invention of RF fingerprinting (described below), it was difficult for service carriers to determine whether a call was being made from a legitimate phone or an illegitimate phone just by analyzing the phone's signal. After all, the illegitimate phone and the legitimate phone were broadcasting the same ESN and MIN. Service providers *were* able to decrease access fraud somewhat by using computers to analyze calling patterns of each user's account. When an unusual pattern was detected, such as more than 60 minutes of calls being made in one hour or two calls that took place near each other in time but originated in two different states, the service provider called the customer to investigate. This method of detecting fraud is similar to that used by credit card companies to detect when a person's credit card number has been stolen.

Use of digital cellular phones can also help prevent fraud. Unlike analog phones, digital phones make it easy to encrypt ESNs and MINs before they are transmitted to the switching stations. This makes it much more difficult for crooks to obtain unencrypted ESN/MIN pairs.

Indeed, some explicit mechanisms to prevent fraud are emerging in modern systems, especially in new digital protocols. Specifically, AT&T Wireless Services recently introduced a new security service called **Authentication** [2], already included in their Digital PCS phones. It is supposed to prevent fraud by using a "complex security feature that contains a secret code and special number." The code and number are based on a cryptographic algorithm known only to the cellular telephone and the wireless network. When a call is placed, the system and the phone go through an authentication protocol that occurs without delaying a legitimate connection. Unfortunately, we were not able to find a disclosure of the authentication protocol, but this sounds like a simple authentication protocol based around proof of knowledge of some shared secret via the digital network.

The newest and most effective way of preventing fraud is the use of radio frequency (RF) fingerprinting [19]. RF fingerprinting works for both analog and digital phones. Cellular phones broadcast information at radio frequencies. Due to the nature of electronic components, no two phones are exactly alike. This means that the exact pattern of signals a phone emits varies from one phone to another. The RF fingerprint of a particular phone is the value of a particular function computed on that phone's signals.

RF fingerprinting makes detecting illegitimate phones easy. Consider this scenario:

A cellular phone broadcasts its ESN and MIN to a switching station so that it can place a call. That phone's RF fingerprint is calculated. The switching station checks that the fingerprint matches that of a registered phone on the system with the same ESN/MIN pair. If the fingerprints do not match, then the phone in question is deemed to be an illegitimate phone. At this time, the illegitimate phone can be disconnected, thereby preventing the phone's owner from making the illegal call.

One of the most appealing aspects of fingerprinting is that it is transparent to the user. Fingerprinting can be used to prevent fraud without requiring users to memorize PIN numbers or keep track of their smartcards. This is because deploying fingerprinting affects only the software and hardware used by the service providers. Also, since fingerprinting prevents fraud by detecting and disconnecting illegitimate phones (instead of by invalidating a particular ESN/MIN pair that has been stolen), a legitimate user who has had his ESN and MIN stolen will not have to get his phone number changed to prevent fraud in the future.

4.3 Combating Eavesdropping

The best hope for ensuring privacy while talking on a cell phone is to use a digital phone that encrypts all the messages it sends. This behavior is not completely safe, however, as recent holes have been discovered in some digital cellular systems (as previously discussed). Service providers still urge customers not to discuss sensitive matters on their cell phones. It is also customary business practice to announce to the other person on the line that the call is taking place on a cell phone, therefore, the conversation is not completely private.

It seems as if service providers have been spending almost all of their research and development money on finding ways to prevent people from stealing air time; not much has been said about ensuring the privacy of their customers. Of course, this is understandable, since businesses are frequently more worried about losing money than exposing their customers to a possible loss of privacy.

However, some manufacturers and service providers are finally providing several solutions and approaches to ameliorate the eavesdropping problem in analog systems.

The first solution, the Cellular Slice Device (CSD), is compact module (about 5" x 3") designed to be placed between the cellular handset and the battery [7, 6, 5]. With the push of a button, the phone call is digitized and encrypted. Motorola, Lucent Technologies, and TCC have all incorporated this security device into their recent products. Thanks to Bell Lab's "advanced encryption algorithm," the voice transmission supposedly rivals that of unencrypted conversations.

Another new analog product is the CryptoPhone from Transcrypt [3]. Activating the keypad produces rapid shift of frequencies and the codes. We were not able to find any discussion on the quality of the transmission. However, the fact remains that there are simply not very many frequency channels available, so once the attacker figures out the range, he may still be able to unscramble the conversation [40].

In order for the hardware devices to be effective, both (or all) parties of the conversation must be using secure phones. To complicate things, although some CSD phones from different manufacturers – such as those made by Lucent and Motorola – are interoperable, others are not. Therefore, a user must make sure that the other end of the line has a compatible phone before starting a private conversation.

Therefore, again, digital phones seem to provide the best solution. Since cell phone calls are broadcast over radio frequencies, it is relatively easy to listen in on someone's conversation – all one needs is a programmable cell phone, an expensive radio, or a scanner. If the conversation itself is broadcast directly on radio frequencies (as in analog phones), then there is a chance that it will be overheard by someone. If, on the other hand, the call was made from a digital phone, then the conversation will be converted into bits (and hopefully encrypted) before it is broadcast. Anyone overhearing this conversation would need to go to greater lengths to know what is being said.

4.4 Related Legislation

The cellular industry is moving rapidly, and the U.S. Government is attempting to keep pace. There are some important laws regarding cell phone fraud which have been passed.

One important item of note is that modifying ESNs (as per 47 CFR 22.919) is only a civil offense, while modifying ESNs with the intent to defraud (as per 18 USC 1029) is a criminal offense. It is sometimes difficult to prove that people trafficking in modified cell phones are intending to defraud the service carriers or the legitimate cell phone owners. For this reason, service providers are lobbying to make modification of ESNs a criminal offense in itself (see Wireless Telephone Protection Act below).

4.4.1 In Effect

18 USC 1029. Section 1029 of the US Code was last updated on January 3, 1995. The law states that a person is committing a criminal offense if he "knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services." Likewise, a person is committing a criminal offense if he "knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver or hardware or software used for altering or modifying telecommunications instruments to obtain unauthorized access to telecommunications services."

47 CFR 22.919. 47 CFR 22.919 (part of the FCC Rules and Regulations) became effective on February 2, 1995, and expressly forbids tampering with ESNs of cellular phones. "The ESN must be isolated from fraudulent contact and tampering." The FCC continues, urging cell phone manufacturers to surround the ESN modules with safety precautions:

> If the ESN host component does not contain other information, that component must not be removable, and its electrical connections must not be accessible. If the ESN host component contains other information, the ESN must be encoded using one or more of the following techniques:
>
> 1. Multiplication or division by a polynomial;
> 2. Cyclic coding;
> 3. The spreading of ESN bits over various nonsequential memory locations.

Electronic Communications Privacy Act of 1986. The Electronic Communications Privacy Act of 1986 (ECPA) addresses, among other things, the legality of eavesdropping on cellular telephone conversations [24]. According to the ECPA, a protected "wire communication" includes "communications utilizing wires, cables, or other line connections within a switching office...regardless of whether the communications are between two cellular telephones or between a cellular telephone and a 'landline' telephone."

The ECPA also decreased the penalty for eavesdropping on unencrypted cellular phone calls from a felony to a $500 fine. This was to encourage cell phone users to encrypt their conversations.

4.4.2 Proposed

Wireless Telephone Protection Act. The most promising legislation that has been proposed for updating cell fraud laws is the Wireless Telephone Protection Act (WTPA). The WTPA was just passed by the Senate on November 10, 1997 as bill S. 493. The WTPA is currently being debated in the House of Representatives as bill H.R. 2460.

The WTPA is meant to amend 18 USC 1029 with respect to cellular telephone cloning paraphernalia. If the WTPA becomes a law, then it will be a Federal crime to use, produce, traffic, have control or custody of, or possess hardware or software knowing that it has been configured for altering or modifying a telecommunications instrument so that such instrument may be used to obtain unauthorized access to telecommunications services. The WTPA also defines a "scanner receiver" to include a device or apparatus that can be used to intercept an electronic serial number, mobile identification number, or other identifier of any telecommunications service, equipment, or instrument. Scanner receivers are considered "access devices" with respect to code prohibitions against fraud and related activities (see S. 1148 for more about access devices).

Many forces have come together to write the WTPA and lobby for its passage, including the Cellular Telecommunications Industry Association (CTIA), the US Secret Service, and many cellular phone manufacturers and service providers. The bill has many supporters, so it is likely to be passed.

S. 1148. Another bill that is being discussed is S. 1148, which is meant to amend 49 US Code (Federal transportation law). If S. 1148 passes, it would declare counterfeit access devices and device-making equipment to be contraband. These devices and equipment would then be subject to mandatory seizure and forfeiture when they are discovered. This law would ensure that hardware and software used to program cellular phones and scanners used to intercept ESNs and MINs would be confiscated when found.

4.5 Summary

In summary, crooks have found many ways to exploit flaws in the cellular phone network. The existence of these flaws, along with the lack of legislation to deal harshly with those who take advantage of the network, has contributed to placing criminals one step ahead of the game. Recently, however, service providers and cell phone manufacturers have begun to concentrate on preventing cellular phone crime. Their research has resulted in many technological advances which have tightened the security of the cell phone network. Legislation has also been passed which deals directly with the issues involved in cellular crime. With the new technological advances and the laws passed in Washington, we may finally be able to turn the tables on those who commit cellular fraud.

5 Research Efforts and Future Protocols

With the emerging popularity of cellular communication and mobile systems, there is an enormous amount of research in the field of attempting to improve and advance the capabilities and features of wireless communication, including the security aspects. In order to better understand the problems and issues related to this field, one needs to review current proposals and research areas, as often problems and weaknesses with current systems are exposed and addressed in research. Additionally, because the field is a rapidly changing one, one cannot merely look at the present protocols and problems, but must also seriously consider future ones, in order to keep track of where the field is moving and to prevent mistakes and weaknesses from entering future protocols. Because this paper focuses strictly on cellular telecommunication, our review of current research areas and proposals will focus on this as well.

5.1 Third Generation Mobile Systems

So-called third generation mobile systems (TGMS) attempt to improve first generation (analog) and second generation (digital) systems in use today. Two major world-wide TGMS research efforts are being undertaken in order to advance the state of the art in the cellular communication infrastructure into the next century. The Universal Mobile Telecommunications System (UMTS) and the International Mobile Telecommunications 2000 (IMT-2000, originally called the Future Public Land Mobile Telecommunications Systems) represent these efforts and aim to provide the new European or possibly world-wide cellular and wireless telecommunications systems starting around the year 2000. Both of these efforts recognize the security considerations related to this field and address them in their own individual research areas.

5.1.1 UMTS

UMTS [8, 46] represents the European Union's coordinated research effort at addressing the growing telecommunications needs and the future of cellular communication, beyond the already predominant GSM standard. The project is widely distributed, but it has a clear set of motivations, goals, and sub-projects and seems to be well coordinated and documented.

Motivations. Researchers in UMTS cite the high growth rate in the mobile telephone market (projected to reach roughly half of all telephone calls by the year 2000, with a higher growth rate than that of standard telephones [8]) as their primary motivation. They wish to deal with system issues such as resolving network congestion and allow for the convergence of mobile and fixed telephones. And, of course, because of the continual presence of hackers and organized crime, they recognize and realize that security issues must still be addressed, especially with the newer and more sophisticated applications (and means of attack) being made available.

Goals. UMTS wishes to "provide high-quality services using lightweight headsets," [8], enabling more than just voice, but also broadband and multimedia communication. Another primary goal is to upgrade the security of mobile telephones and their networks until they are at least as secure as fixed networks.

Structure. UMTS plans on making coverage as complete as possible, by moving to a layered cell architecture, with mega, macro, micro, and pico-cells. These cells cover areas as large as those covered by satellites, or as small as those from individual sections of an indoor facility. Because of this and complexities in the proposed infrastructure, UMTS has a completely separate research effort which is entirely devoted to investigating and addressing the relevant security issues, named ASPECT [1]. ASPECT aims to investigate the advanced security features for future personal communication networks and wants to provide many important features. These features include mutual authentication of the user and network, key agreement for encrypting the air interface, confidentiality of the user identity on the air waves, authentication of service providers to the user, non-repudiation on transmitted data, and assurances that certificates are not unjustifiably revoked. Because these goals and features cover such a broad area, ASPECT is further sub-divided into other groups which attempt to attack specific research areas.

Research areas. ASPECT identifies key issues that are current problems in cellular communication that it explicitly wishes to address. These include scanning, eavesdropping, and telephone cloning. While ASPECT acknowledges that GSM has countermeasures against these threats, it states that "it's only a matter of time before organised crime finds a way of hacking into the GSM system." [11]. Thus, ASPECT wishes to investigate more advanced security means to counter eavesdropping and telephone fraud, as well as other important issues such as the migration path [42] between the current system GSM and UMTS, the use of Trusted Third Parties [18] to provide features and services, secure billing, and new research areas such as fraud detection [26]. We will now discuss each of these efforts.

Migration. No new or proposed system can survive unless there is a detailed plan for making the transition from current systems to the new one. Otherwise, because of inertia, the public will continue to use the likely antiquated, highly insecure old system. Thus, ASPECT is planning for a four-stage migration plan from GSM to UMTS [42]. Specifically, this plan will first upgrade just the UIMs (smartcards on the mobile telephone) and the home service provider, increasing their capabilities. Second, the air interface used will be upgraded, to concur with that proposed to be used by UMTS. Third, the full services and features of UMTS will be added, maintaining backwards compatibility with GSM. Finally, in the fourth stage, UMTS will be fully deployed and the transition from GSM to UMTS will be complete.

These plans include provisions for UMTS's "framework for authentication." This modular design feature includes the concept of capability classes, in which a UIM declares its authentication capabilities, and network operators can then negotiate and agree which authentication mechanism to use (and learn unknown mechanisms from trusted parties, if necessary). This allows for a great amount of flexibility and the possibility of easy protocol upgrades, while taking the authentication capabilities of all parties into consideration.

Trusted Third Parties. The chief objectives of using Trusted Third Parties (TTPs) revolves around providing mechanisms for certification, key escrow, and end-to-end security (between two mobile users, perhaps in different domains) [18]. This research effort states that it wishes to make heavy use of new smartcards with public-key cryptography capabilities. In addition, the TTPs will act as key distribution centers, providing end-to-end security between mobile users, while also providing a key-escrow mechanism to satisfy governments (rather than using other explicit back-doors or otherwise weakened cryptography). The TTPs can cooperate and help mobile users generate session keys (via a Diffie-Hellman mechanism); because it helps set up this key, it knows the key and can store it for the escrow purposes. Additionally, the TTPs will act as certificate managers, dealing with generation, maintenance, storage, and revocation issues, allowing for mutual authentication between users and stations, as well as for secure billing purposes. The exact contents of these certificates is specified in [18]; the major fields include version numbers, serial numbers, public-keys, the issuer, and the validity period.

Secure Billing. Because more than simple voice communication is envisioned in these new cellular systems, ASPECT is investigating incorporating secure billing or making several protocols available. These include many micropayment schemes, such as PayWord, for use in paying for so-called "Value Added Services" above and beyond a simple telephone call. These mechanisms use UIMs to perform the computations for authentication and payment purposes. Specifically, the UIMs perform variants on the Diffie-Hellman protocol (with randomization to prevent the same key from being generated repeatedly), based on elliptic curves for authentication. This could actually present a potential problem, because of recent discoveries in weaknesses in certain groups of elliptic curves [34].

Fraud Detection. This emerging research field is similar to intrusion detection techniques, in its underlying objectives and mechanisms. Essentially, because one cannot realistically prevent all instances of fraud, efforts are being made in improving the ability to recognize fraud automatically, so efforts and actions can be taken in a timely manner. This research group in ASPECT emphasizes differential analysis [26], or seeing how spending habits evolve over time, rather than looking at static figures. This analysis attempts to flag large spikes in spending changes for a particular user at a particular time. It utilizes usage, mobility, and so called deductive indicator, where the latter refers to indicators which reflect the effects of several factors and indirect results. The detection systems all use the current and future toll tickets recorded by telephone systems for their input.

These efforts aim to detect fraud using three basic mechanisms. First, the ever popular rule-based systems, prevalent in the field of AI, use the above inputs and indicators and a set of if-then style rules to decide if spending behavior indicates fraud. The second and third efforts revolve around another field of AI, involving neural nets. The second system uses supervised neural nets, which require input data which is pre-tagged as being fraudulent (or not); obtaining enough of this tagged data is obviously quite an undertaking. Accordingly, the third system uses unsupervised neural nets, which uses clustering techniques to divide data automatically into the relevant groups; however, in order for this to work, the must easily be clusterable into the desired groups.

Proposed authentication mechanisms. Several specific protocols are being proposed for the security needs and purposes of UMTS. These needs are specifically identified and documented and in [41]. The proposals primarily revolve around the tricky issue of performing authentication while being careful not to compromise anonymity. Because these proposals are a current and continually evolving work, it is too early to detail the specifics of those protocols. However, the protocols do seem to concentrate on both symmetric key techniques, updating the ones used in GSM, as well as newer public-key and certificate based techniques. The symmetric key proposal is interesting because it specifically addresses the issue of tracking temporary IDs and proposes the aliases and cipher keys periodically. The public-key and certificate based techniques mostly handle anonymity by encryption of sensitive information, by establishing and using session keys. One note of interest is that some of these public-key based techniques also make heavy use of elliptic curves in hopes of gaining efficiency and lowering the computational cost of the authentication mechanisms.

5.1.2 IMT-2000

IMT-2000 is the new name of the international FPLMTS effort at upgrading and advancing cellular telecommunication technology [4]. One of the primary participants in developing IMT-2000's standards is Japan, making up for their less active participation in defining GSM. This effort also has its own security-centered research, including an outline of the specific security issues it wishes to address. Unfortunately, this information is not easily obtainable or publicly available; most of it is restricted to subscribed members of certain organizations. Two documents of particular interest in this effort, however, are the outline of the security principles in FPLMTS/IMT-2000 [10] and an evaluation of the proposed security mechanisms [9].

5.2 Other Research

Many other research efforts are being undertaken to study and propose solutions for current and future security needs in mobile networks. Much work is being done in the field of mobile and wireless data communication, and thus many researchers are investigating improvements and alternatives to one of the current data standards, the Cellular Digital Packet Data (CDPD) protocol. Some have identified specific security weaknesses in CDPD and suggested several improvements to the basic protocol [22]. Others have analyzed another proposed authentication protocol, the Beller-Chang-

Yacobi (BCY), which was the first to combine private-key and public-key authentication, and suggested improvements to discovered weaknesses [47]. In addition, much recent work has been done in suggesting how one can achieve end-to-end security or use certificates in mobile communication systems [43, 29]. All of these works may provide an interesting source of ideas for the overall design for the security portions of future cellular communication systems.

6 Design Guidelines and Suggestions

In attempting to design a system with security in mind, it is useful to review previous, current, and proposed works and their respective weaknesses. One should also study the security issues that are generally accepted as being difficult, before beginning to outline the overall design considerations or investigate specific ideas. We have already reviewed past and existing systems and their weaknesses, as well as proposed systems and research efforts; here we will review the other pertinent considerations. Since the cellular communication system and its security-related aspects is a rather broad and deep field of research, rather than declaring specific algorithms and protocols (which would likely be rather error-prone and not necessarily useful), we will instead make suggestions and outline guidelines for designing secure cellular systems.

6.1 Difficult Issues

Several research efforts have been made into ascertaining what it is, exactly, that makes securing cellular communication systems difficult. Among these, [28] names several issues that make this such a difficult problem. Specifically, it mentions key synchronization as one of the most difficult problems, due to the limited handful (in general) of options for achieving this synchronization. Typically, one can only use broadcasting to share keys, agreement on a pre-specified set of keys, reliance on some secure, "master" key to encrypt session keys, or use public-key cryptography. Another difficult issue in cellular communication is the fact that it mostly relies on broadcasting information on air waves, which makes this information readily available to almost anyone. Other issues which complicate security are the lower performance and capabilities of mobile devices and the often high cost of communication on this medium (which motivates the requirement of fairly compact and efficient security protocols).

6.2 Overall Considerations

When studying existing and proposed cellular communication systems and their security aspects, one can see a common set of issues and guidelines that should be considered and followed when trying to design new systems. We will introduce and explain these considerations and guidelines here.

Define assumptions and requirements explicitly. Before anything else, one must make sure that the desired security requirements and relevant assumptions are explicitly stated. This allows for a more formal verification of the system. Specifically, that the system does indeed satisfy the requirements, given a set of assumptions, and that these assumptions are reasonable and viable.

Also, after defining the exact security requirements one wishes to achieve, one should ensure that the security mechanisms, algorithms, and protocols used are appropriate for the desired goal. Part of the CMEA weakness [44] results from using one security mechanism for another, inappropriate application.

Avoid use of new algorithms. When designing security features for potentially critical applications, one should not attempt to "re-invent" cryptography tools. New cryptography mechanisms take time to be (thoroughly) checked and established, which is reasonable for research, but may not be appropriate for commercial or critical applications. Again, CMEA suffers from this problem. Additionally, some of the proposed algorithms in the ASPECT/UMTS projects suggest using elliptic curves for the basis of cryptography algorithms, which may be problematic given recent discoveries in weaknesses in certain groups of elliptic curves [34]. Thus, one should try to make sure that only "mature" cryptography algorithms are used in these systems.

Avoid closed-door or proprietary designs or standards. Many cryptography algorithms or mechanisms attempt to rely on security through obscurity. This approach is inherently flawed because researchers and hackers often find a way to reverse-engineer systems, or information about proprietary systems leaks out into the public. The danger there consists of malicious people making more of an effort to find the exact specifications of a closed system and hacking it for fraudulent or criminal purposes, than researchers exposing holes for the general good of society. If standards are open and easily available, then researchers and experts are more likely to examine and test the soundness of a system.

Consult experts. Along with keeping standards open, one should explicitly attempt to have "experts" examine and evaluate cryptographic and security systems, especially for commercial or critical applications such as cellular communication. Since hackers will often put their best efforts into bypassing the security mechanisms, an essential defense is to encourage those who are more cooperative and willing to share their findings to attempt to find weaknesses in the system first.

Avoid back-doors. No system should have "back-doors" incorporated into the design. Even if the back-door has an honorable justification, their mere existence weakens the security of the system and can be attacked and exploited by malicious parties. A thorough review by expert consultants should prevent the possibility of any back-doors.

An interesting side-issue and political debate is whether or not incorporating key-escrow into security systems represents a back-door. Indeed, their existence can be justified, but their presence may compromise the security of systems that use them, as they may be exploited or abused. The answer to this question indeed revolves around Robert Morris's query, "do you trust your government?" [27]

Avoid shared secrets. A shared secret key security system is only as secure as the secrets involved. Because shared secrets invite insiders and outsiders to attempt to hack systems, especially base stations and servers which contain these shared secrets, relying too heavily on these secrets may be a problem.

In addition, as mentioned above, key synchronization is one of cellular communication's most difficult problems, so establishing these shared secrets is often non-trivial.

Public-key based systems are attractive because they help solve these problems and minimize the number of secrets that must be maintained, limiting the storage of the secrets to one party, in most cases. Certificate-based authentication systems are especially attractive for this reason, relying on presentation of signed certificates for authentication, rather than potentially revealing some secret information.

Support end-to-end security. Although parties can implement and utilize their own end-to-end security mechanisms at levels above the underlying cellular communication design, providing standard and built-in mechanisms can ensure that this security is readily available and usable. Because end-to-end security is a highly-desirable and essential component of the system, it makes sense to provide some standard mechanism.

Only broadcast the minimum necessary. To protect confidentiality and to prevent possible leaks of critical information useful for attacking the system, one should ensure that every piece of information that is released or broadcast has a *definite and explicit* purpose. Therefore, a good rule of thumb, for authentication and related protocols, is to broadcast only the minimum amount of information necessary to complete the protocol.

Prevent identification or tracing of users on the network. Anonymity is a key issue in mobile communication. Users do not want their identity, location, spending habits, or traffic patterns, revealed merely because they wish to use the network. Therefore, even though anonymity directly conflicts with the authentication requirement, a balance must be found that allows users to feel secure and satisfied with their level of privacy, or they may have reservations about using the system [15]. Thus, the proposed protocols and mechanisms should avoid revealing user identifications to any untrusted parties, and perhaps should even prevent tracing of temporary IDs by changing those (or the used certificates) regularly.

Make using security as easy and simple as possible. When designing a security system, one should consider the user interface issues at least as much as the actual protocols themselves. Otherwise, if the mechanisms are not easy to use, users may not use them, which makes the effort put into securing the protocols less worthwhile.

Additionally, one should not implement inherent weaknesses into protocols and mechanisms, such as allowing PINs to be disabled on cellular telephones, or allowing encryption to be turned off in messages between stations on the network. Because of the principle of using the worst-case scenario when examining security, one must assume that if users have the option of turning off security mechanisms, they will do so.

Consider migration path. Without considering how one can migrate from existing systems to the newer, proposed systems, it is difficult to convince others to accept or use the new system. A clear path of transition between systems is a necessary part of designing new large-scale systems such as a cellular communication infrastructure.

Avoid passwords if possible. Password-based security is often not very secure, since passwords can be compromised (even by social-engineering type methods). Also, if a password is the only obstacle between a hacker and information contained in a telephone, the hacker can tamper with the unit and break into it, extracting the information anyway. Utilizing smartcards in a reasonable manner may be a more sensible option, since smartcards that contain sensitive information can be removed from the telephone, to protect the information in case of theft of the telephone itself.

Trust as few parties as necessary. Because a large-scale system such as the cellular telephone system consists of a large number of parties, it may not be reasonable to trust every party in the system. For this reason, designing protocols which reveal as little information as possible to most parties (except for the few, truly trusted ones) is a safe and logical approach. On the same idea, one should authenticate all parties, if possible, before attempting communication, especially of any sensitive or secure information. Currently, a number of attacks are possible because of implicitly trusting the network and revealing sensitive information to malicious network operators.

Consider faults. A complete system should not only cover how to implement and maintain security, but also how to handle problems and breaches of security. Obviously, protocols should specify what actions to take should a party not pass authentication or other security tests. In addition, a cellular system should consider how to handle breaches in security, when malicious parties manage to break into a system, commit fraud, prevent machine availability, or other related scenarios. ASPECT'S examination of fraud detection is a good example of this type of design consideration. More realistically, one needs to be able to recover from exposures of weaknesses in security mechanisms and algorithms in a sensible and reasonable fashion. Potential solutions include system modularity, such as that incorporated into UMTS's "Capability Classes," and isolating cryptographic mechanisms and protocols in reprogrammable devices to provide a recovery mechanism.

6.3 Specific suggestions

Here, we consider what specific algorithms or protocols may be suitable for cellular telephone security. We will concentrate on the authentication aspects, because almost every security aspect of this communication hinges on being able perform authentication in a reasonable manner. Once authentication is established, parties can establish session keys in one of many methods.

Minimize the computational complexity. Because cellular and mobile devices have lower computational power than desktop computer systems, minimizing the computation complexity is a key issue. One can perhaps achieve this minimization by use of alternative algorithms or schemes, such as MSR for public-key cryptography (as suggested in [29]), or even elliptic curves, once they are more established as being secure.

At the same time, one must also optimize protocols in order to minimize the cost and overhead of unit initialization and transition between networks. This can be done by, again, ensuring that all information that is sent out is absolutely necessary, as well as attempting to handle as much of the authentication off-line or via machines on the network rather than the mobile unit. [29] and others propose mechanisms for this exact issue.

Zero-knowledge authentication. Because authentication and anonymity conflict each other, one needs to consider methods which explicitly allow proving one's identity or authorization without revealing any useful information that could be used or abused by attackers listening on the network.

Zero-knowledge protocols may provide such a solution. By utilizing zero-knowledge protocols, a user can prove his or her identity without sending passwords or other potentially sensitive information on the network. Blobs may especially be suited for this task, as they would allow a user to demonstrate that they are on a list of authorized users, without explicitly specifying which user they are.

Of course, one issue here is that these protocols can require a large number of message exchanges or computation, which contradicts another requirement and suggestion. In addition, if blobs were used, one would need to permute the order of commitments in some reasonable manner to prevent replay attacks. However, despite these issues, authentication mechanisms based on these types of protocols may have great potential.

Use dynamic aliases or certificates. Even if one's identity is hidden by means of aliases or encrypted information in certificates, attackers may still potentially track users as they roam, by their temporary ID rather than their real ID. One can prevent this by attempting to change aliases or certificates dynamically, as in [41, 29].

Anonymously purchased debit-cards. Finally, one can achieve authentication and anonymity by completely separating a user's identity from his or her billing information, even from the billing party. This can probably most easily be achieved by means of using pre-paid debit cards, which would be purchased anonymously. With these cards (which could simply be electronic), less effort needs to be put into protecting the identity of the user, because the user is completely disassociated with the "identification" on the debit card (due to anonymous purchase), but the billing party remains satisfied that bills will be paid. Thus, this rather simplistic solution may have some promise for balancing authentication and anonymity.

7 Summary and Conclusions

The security requirements for cellular telephones are fairly straightforward: they include authentication, privacy, anonymity, and other traditional system requirements. However, in the past, they have rarely been discussed explicitly, which has lead to problems. Security requirements seem to have been entirely overlooked in the ubiquitous analog system. The new digital standards that are just being deployed (GSM, TDMA, and CDMA) do have security features, but they still fall short. Many of the requirements are unfulfilled, while others contain critical weaknesses, as shown below.

	Analog	CDMA/TDMA	GSM
Authentication	ID sent in the clear.	Man-in-the-middle & mail theft attacks possible.	Operators do not encrypt internal traffic.
Privacy	All transmissions sent in the clear.	Problems with voice, data, and control schemes.	Weaker A5X algorithm may be used.
Anonymity	ID sent in the clear.	N/A	Aliasing fails under transmission problems.
Availability	Noise causes unintelligible audio.	N/A	N/A
Simplicity & Efficiency	N/A	PIN used (can be tedious).	Smartcard and PIN used (can be tedious).

However, as far as we know, these cryptographic problems have not yet been exploited in practice. The majority of crimes currently being committed consists of stealing airtime and eavesdropping, both of which are trivial to accomplish. Over time, cellular telephone crime has diminished somewhat due to service providers using new technologies. Laws have also been passed which require harsher penalties for cellular criminals.

Future research efforts may also bring about greater security in many ways. These include using trusted third parties for key establishment and key escrow, new techniques for fraud detection, and new protocols for authentication and anonymity. However, industry and researchers need to keep in mind the general design principles that cryptographers and computer scientists have learned over the years.

Glossary

Access Fraud Tampering with a cellular phone's Electronic Serial Number (ESN) and/or Mobile Identification Number (MIN) to obtain unauthorized usage of a wireless service.

ASPECT Advanced Security for PErsonal Communication Technologies. Subset of UMTS research effort entirely devoted to studying security issues in UMTS.

BS Base Station.

CAVE A mixing function used for key generation and challenge-response authentication protocols.

CDMA Code Division Multiple Access. A method of producing channels for cellular transmission.

Cloning/Emulation Phone A chip is installed in the phone which is programmed with the ESN and MIN of a legitimate user.

CMEA A block cipher used for control data in IS-95 and IS-54 (CDMA/TDMA).

ECPA Electronic Communications Privacy Act of 1986.

ESN Electronic Serial Number. A unique 13-digit number assigned to a wireless phone by the manufacturer.

ETSI European Telecommunications Standards Institute.

FCC Federal Communications Commission. Regulatory body in charge of the phone industry ever since the Wire Communications Act of 1934.

GSM Global System for Mobile communications. A European TDMA cellular standard.

HLR/AC Home Location Register / Authentication Center. A unique location for storing information about a subscriber.

IMSI International Mobile Subscriber Identity. A unique identification number issued to all subscribers. A subscriber is identified in the GSM network by the IMSI.

IMT-2000 International Mobile Communications 2000. Formerly known as FPLMTS (Future Public Land Mobile Telecommunications Systems). An international effort at a proposed TGMS.

IS-136 A North American TDMA cellular standard, formerly known as IS-54.

IS-41 The authentication system used by IS-54 (and IS-95).

IS-54 An old version of IS-136.

IS-95 A North American CDMA cellular standard.

LFSR Linear feedback shift register.

MIN Mobile Identification Number. A 10-digit number that is the cell phone's phone number.

MS Mobile Station. The mobile telephone.

MSR Modular Square Root. A public-key cryptography mechanism which supposedly requires less overhead and computation than RSA; this may be of interest in the cellular community, with its low-powered mobile devices.

NAM Number Assignment Module. A cellular phone's programmable system parameters as set by the phone dealer.

ORYX A stream cipher used for cellular data in IS-95 and IS-54 (CDMA/TDMA).

PCS Personal Communications Service. A general name for digital cellular service.

PIN Personal Identification Number. Typically a short code a user must type into a device to authenticate to it.

Q. Why do cryptographers prefer blinded dates?

A. They're afraid of commitments.

TDMA Time Division Multiple Access. A method of producing channels for cellular transmission.

TMSI Temporary Mobile Subscriber Identity.

TGMS Third Generation Mobile Systems. Future (proposed and researched) protocols for the "next generation" of cellular communication.

TTP Trusted Third Party. Used especially in UMTS (proposals) for session key establishment, secure billing, and providing a mechanism for key escrow for government use.

Tumbling ESN Phone Phones that has been altered such that they use a different ESN each time the caller makes a new phone call.

UMTS Universal Mobile Telecommunication System. Proposed European standard for a TGMS.

WTPA Wireless Telephone Protection Act. Proposed legislation that would make access fraud a Federal crime, whether or not there was intent to defraud.

References

[1] AC095: ASPECT – Advanced Security for Personal Communications Technologies. http://www.esat.kuleuven.ac.be/cosic/aspect/aspect.html.

[2] AT&T Wireless introduces new security technology to reduce cellular fraud. http://www.att.com/press/0397/970305.pcb.html.

[3] Cryptophone. http://www.transcrypt.com/Pages/Telephony/crypto.html.

[4] FPLMTS-IMT2000. http://ktpcx.kotel.co.kr/imt-2000.html.

[5] Motorola's CipherTAC Security Module Provides Portable Cellular Voice Security. http://www.mot.com/GSS/SSTG/PR11_CipherTAC.html.

[6] TCC: Secure Telephone. http://www.tccsecure.com/csd3600.htm.

[7] The Slice Cellular Security Device. http://interop.sbforums.com/ltbdir/company/191770/339104.html.

[8] UMTS – The Universal Mobile Telecommunications System. http://wwwat.infowin.org/ACTS/IENM/Bulletin/11-1996/umts.html, November 1996.

[9] Evaluation of security mechanisms for IMT-2000. http://ties.itu.int/itudoc/itu-r/rec/m/1223_37805.html, July 1997. M.1223.

[10] Security principles for future public land mobile telecommunication systems (FPLMTS). http://ties.itu.int/itudoc/itu-r/rec/m/1078_25005.html, March 1997. M.1078.

[11] UMTS Part 2 – Is the future of UMTS secure? http://wwwat.infowin.org/ACTS/IENM/Bulletin/03-1997/umts2.html, March 1997.

[12] TIA IS-54 Appendix A. Dual-mode Cellular System: Authentication, Message Encryption, Voice Privacy Mask Generation, Shared Secret Data Generation, A-Key Verification, and Test Data, February 1992. Rev. B.

[13] A. Abdul-Rahman and S. Hailes. Security Issues in Mobile Systems. http://www.cs.ucl.ac.uk/staff/ucacfxa/docs/sec-in-mob.html, November 1995.

[14] R. Anderson. GSM hack – operator funks the challenge. e-mail, November 1997.

[15] D. Atkins. Physical Location via Cell Phone. In P. Neumann, editor, *RISKS DIGEST 16.18*. ACM Committee on Computers and Public Policy, June 1994.

[16] Cellular One Puerto Rico. Cellular One - Security and Protection. http://www.cellularonepr.com/english/care_seg.htm, 1997.

[17] Cellular Telecommunications Industry Association. Wireless Telephone Fraud Glossary. http://www.wow-com.com/professional/fraud/, 1997.

[18] L. Chen, H.-J Hitz, G. Horn, K. Howker, V. Kessler, L. Knudsen, C.J. Mitchell, and C. Radu. The Use of Trusted Third Parties and Secure Billing in UMTS. http://www.esat.kuleuven.ac.be/cosic/aspect/summit_all.htm.

[19] Corsair Communications, Inc. What is RF Fingerprinting? http://www.corsair.com/fingerprint.html, 1997.

[20] R. DeMaria. Cellular Counterfeiting/Cloning Fraud. http://www.annonline.com/interviews/961119/how.html, 1996.

[21] E. Eklund. Controlling and securing personal privacy and anonymity in the information society. In *Proceedings of the HUT Network Seminar 1995*, 1995.

[22] Y. Frankel, A. Herzberg, P. Karger, H. Krawczyk, C. Kunzinger, and M. Yung. CDPD Wireless Network Security: fraud-prevention, availability, confidentiality, and anonymity. Technical report, IBM Research Center, Yorktown Heights, NY, May 1995.

[23] Texas Instruments. What's An LFSR. http://www.ti.com/sc/docs/psheets/abstract/apps/scta036a.htm, 1997.

[24] Jones Telecommunications and Multimedia Encyclopedia. Electronic Communications Privacy Act of 1986. http://www.digitalcentury.com/encyclo/update/ecpa.html, 1997.

[25] J. Kelsey, B. Schneier, and D. Wagner. Cryptanalysis of ORYX. http://www.cs.berkeley.edu/ daw/oryx.ps, May 4 1997.

[26] Y. Moreau, B. Preneel, P. Burge, J. Shawe-Taylor, C. Stoermann, and C. Cooke. Novel Techniques for Fraud Detection in Mobile Telecommunication Networks. http://www.esat.kuleuven.ac.be/cosic/aspect/WP22_M06.htm.

[27] R. Morris Sr. Protection of Valuable Information. Quotation from talk, November 20 1997. MIT Lab for Computer Science: Distinguished Lecture Series.

[28] I. Nurkic. Difficulties in Achieving Security in Mobile Communications. In Jose L. Encarnacao and Jan M. Rabaey, editors, *Mobile Communications: Technology, tools, applications, and security*, IFIP World Conference on Mobile Communications, pages 277–284, Canberra, Australia, 2-6 September 1996.

[29] C-S Park. On Certificate-Based Security Protocols for Wireless Mobile Communication Systems. *IEEE Network*, pages 50–55, September/October 1997.

[30] K. I. Park. *Personal and Wireless Communications: Digital Technology and Standards.* Kluwer Academic Publishers, Norwell, MA, 1996.

[31] S. Patel. Weaknesses of North American Wireless Authentication Protocol. *IEEE Personal Communications*, pages 40–44, June 1997.

[32] Spectre Press. Cellular Phone Hackers Bible. http://www.spectre-press.com/, 1997.

[33] S. H. Redl, M. K. Weber, and M. W. Oliphant. *An Introduction to GSM.* Artech House, Inc, Norwood, MA, 1995.

[34] RSA. Flaw Discovered in Elliptic Curve Cryptography. http://www.rsa.com/ecc/, 1997.

[35] R. G. Smith. Preventing Mobile Telephone Crime. http://www.dot.gov.au/programs/btce/forum/papers/premobil.htm, 1996.

[36] Pyro Teknik. Cellular fraud. http://spasm.redcat.org.uk/ pteknik/, 1997.

[37] Telecode. Cellular Hackers Bible, Volume 1. http://www.hackerscatalog.com/cl1index.htm, 1997.

[38] Telecode. Cellular Hackers Bible, Volume 2. http://www.hackerscatalog.com/cl2index.htm, 1997.

[39] TIA TR45.0A. Common Cryptographic Algorithms, June 1995. Rev. B.

[40] A. Vanderploeg. Wireless Communication Security. http://pw1.netcom.com/ vanderpa/wireless.htm.

[41] G. Vanneste and J. Degraeve. Initial report on security requirements. Technical Report AC095, ASPECT, ftp://ftp.cs.rhbnc.ac.uk/pub/aspect/asp_d02.zip, February 1996.

[42] G. Vanneste, J. Degraeve, G. Lyberopoulos, Y. Vithynos, and C. Cooke. Migration/Evolution Towards UMTS – Security Issues. http://www.esat.kuleuven.ac.be/cosic/aspect/A061_E2.htm.

[43] V. Varadharajan and Y. Mu. Design of Secure End-to-End Protocols for Mobile Systems. In Jose L. Encarnacao and Jan M. Rabaey, editors, *Mobile Communications: Technology, tools, applications, and security*, IFIP World Conference on Mobile Communications, pages 258–266, Canberra, Australia, 2-6 September 1996.

[44] D. Wagner, B. Schneier, and J. Kelsey. Cryptanalysis of the Cellular Message Encryption Algorithm. http://www.counterpane.com/cmea.ps, March 1997.

[45] Dave X. How to Build an ESN/MIN Snarfer: The Basic Requirements. http://spasm.redcat.org.uk/ pteknik/, 1997.

[46] D. Youngs. Project Linkages. Technical Report AC095, ASPECT, ftp://ftp.cs.rhbnc.ac.uk/pub/aspect/asp_d01.zip, November 1995.

[47] Y. Zhen. An Authentication and Security Protocol for Mobile Computing. In Jose L. Encarnacao and Jan M. Rabaey, editors, *Mobile Communications: Technology, tools, applications, and security*, IFIP World Conference on Mobile Communications, pages 249–257, Canberra, Australia, 2-6 September 1996.