Security in mobile phone systems

Alexandre Lung-Yut-Fong and Boris Granovskiy

October 23, 2006

Abstract

In this paper, we discuss security issues associated with mobile telephone networks and focus on the unique issues that appear due to the mobility of the user. We provide an overview of how some of these issues are addressed in the second-generation mobile network GSM and consider some of the possible shortcomings of that network. We then compare security features in GSM with those implemented in UMTS, a third-generation mobile telephone network, whose security measures aimed to build on the success of GSM and provide protection against actual and perceived vulnerabilities of GSM, as well as against new attacks that have appeared in more recent years.

Introduction and history

When the so-called first generation of mobile telephone systems became popular starting in the mid 1980's, mobile fraud and abuse followed very shortly after. The most common abuses of the early mobile systems included eavesdropping on the analogue radio signal, thus listening to other people's calls, as well as cloning, an example of identity theft where the attacker reprogrammed the identity of a mobile phone so that the calls made on it were charged to another customer. It was mainly with an eye on these flaws that research began into creating a mobile network that provided a certain level of security. The second generation mobile network GSM (Global System for Mobile communications) was designed and released in the early 1990's and was the first widely used mobile system to provide security features ensuring some levels of authentication, confidentiality, and anonymity. GMS proved to be very successful and has become widespread throughout the world in the 1990's. Over the course of that decade, work began on the third generation of mobile phone systems, the best known of which is the Universal Mobile Telecommunications System, or UMTS. The first UMTS specifications were released in 1999, and showed that UMTS security built on the success of GSM and provided new security features to protect against new types of attack or to address certain weaknesses of GSM, specifically its lack of protection against so-called "false base station attacks", where an attacked pretends to be a GSM network. In this paper, we will talk about various security features implemented in GSM and then compare them with the new and improved security provided by UMTS.

1 Security requirements in mobile telephony systems

Unlike the first generation, analog, mobile cell phone system, second, and later, third generation mobile telephony had to be designed by taking into account security principles. Let's review the main security properties that had to be implemented in the user part of the network infrastructure, which are authenticity, confidentiality and anonymity.

Authentication features allow the network operator to make sure that a given user is who she claims to be, thus denying fraudulent calls. For example, a user must not be able to have a phone call and have this call reported on another customer's bill. Confidentiality is used to protect users' data or phone calls, as well as signaling or dialed phone numbers. That security feature protects communications and data from eavesdropping. As the mobile equipment is (indeed) mobile, the location of the terminal may be sensitive information. So the anonymity features of the mobile phone systems need to protect the user's location from being tracked or her communications from being identified just by knowing the unique identifier associated with the mobile phone.

These three security properties were used as design principles for digital cell phone systems. But unlike with security in a computer system, network designers had to take into consideration radio constraints as well as law enforcement rules that may exist in some countries. For example, the radio channel use for communications is likely to be subject to noise, so a likely error bit may affect a whole transmitted frame. Alternatively, a government may want the ability to "wiretap" a communication for judiciary cases.

2 Security in GSM network

2.1 Architecture

See figure 1. The network operator deploys a set of base stations (BTS) that enable the mobile phone to be within the range of one of the base stations. Each BTS is physically linked to a Base Station Controler (BSC) that takes care of many BTS. BSCs are themselves linked to Mobile Switching Centers (MSC) which are assoicated with a Visitor Location Register, a "database" dealing with the communications of a geographical zone (about a hundred of radio cells). VLR records the subscriber's location and manages call routing. The mobile phone, or Mobile Station (MS) can be viewed as the association of a Mobile Equipment (ME) (which is the cellphone itself) and a Subscriber Identity Mobile (SIM) which is a smart card chip that computes cryptographic operations, and that may also contain the user's personal data.

2.2 TMSI

One important security issue that GSM attempted to deal with is the conflict between untraceability and authentication for mobile users outside of their "home domain." If a user travels outside of her region and appears in another domain, she has to somehow identify herself to the service provider in the foreign domain in order to receive service. However, providing such information about her location can

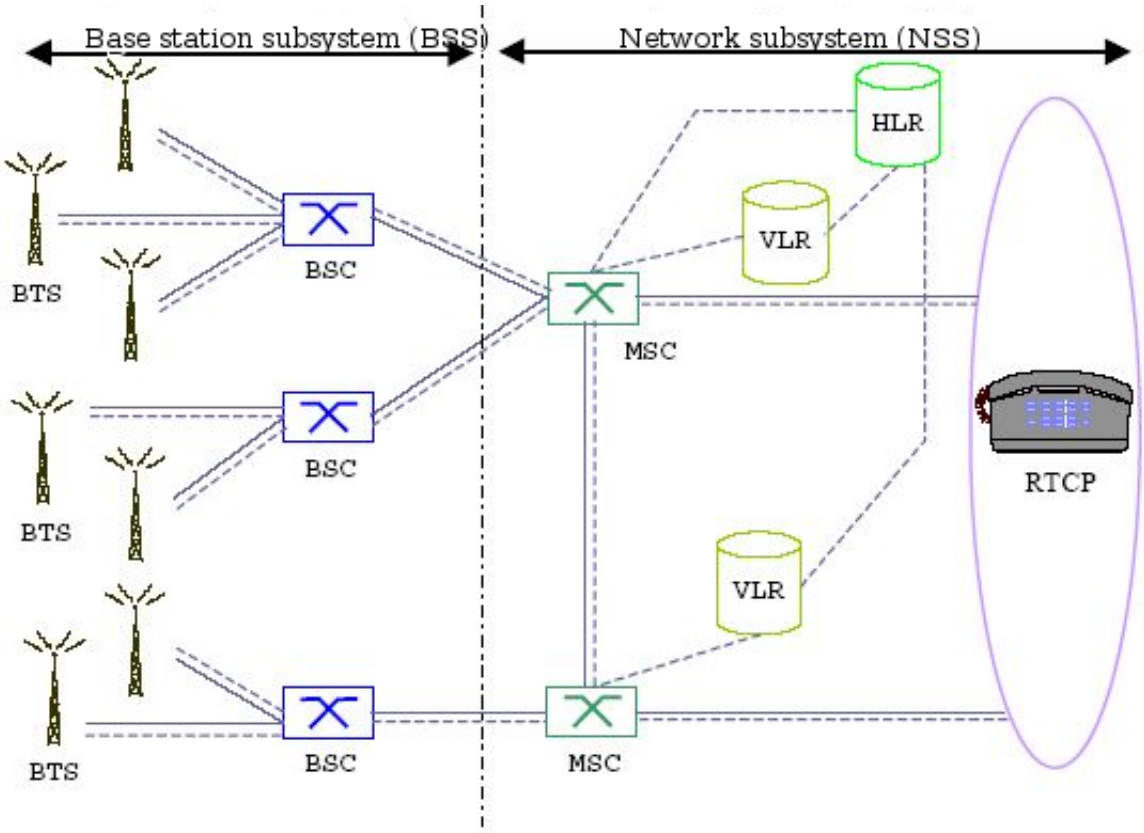

Figure 1: GSM architecture

be seen as a violation of privacy, as unauthorized third parties can now track the whereabouts of the mobile user. Therefore, a conflict is created between the need to keep the user's location information private and the need for the user's identity to be authenticated in order for her to receive service. GSM solves this problem by using aliases, or temporary user IDs. When the user first appears in the foreign region, she identifies herself that one time by her (usually encrypted) International Mobile Subscriber Identity (IMSI), a unique way to identify her as a GSM user. Once the initial authentication is made, the user is assigned a Temporary Mobile Subscriber Identity (TMSI), which she is identified by for the duration of her stay in the foreign domain. Even though this is an improvement over referring to the user by her real identity the entire time, it is still an imperfect solution. An attacker continuously tracking the user can still monitor her location by the initial use of the IMSI each time she appears in a new domain. Furthermore, some information about the user's identity can be inferred from the relationship between the user and the home domain, which needs to authenticate her each time she enters a new domain. A good example of this problem is provided in [3] Samfat, Molva, and Asokan: "if an aliased user x visiting a remote domain in France wants to authenticate to his home domain WhiteHouse.gov and an intruder happens to know that the only users from WhiteHouse.gov currently in France are President@WhiteHouse.gov and VicePresident@WhiteHouse.gov, the intruder can conclude that the user x corresponds to one of those two real identities." (p.3). So, GSM provides a good, but not perfect solution to this issue by using different aliases each time the user enters a new domain, only transmitting the user's IMSI once in each domain, and, whenever

possible, encrypting information that can identify the user.

2.3 GSM encryption

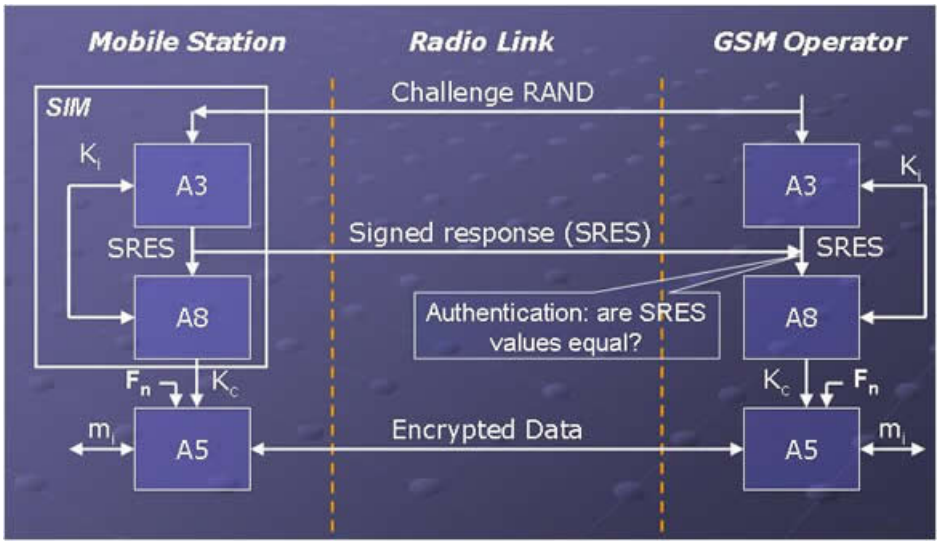

Figure 2: GSM user authentication, from http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group7/index.html

When decisions about encryption algorithms for GSM were made, public-key cryptography was not as widespread as it is today, and so GSM uses symmetric cryptography for encryption and subscriber authentication. Because of certain restrictions on the publishing of cryptographic information in the 1980's, the specific algorithms used by GSM were never published, but have been either leaked or deduced over the years. These algorithms are commonly known as A3 (the authentication algorithm), A5 (the encryption algorithm), and A8 (the key generation algorithm). A3 and A8 are shared between the user and her network, and thus can be independently selected by each network, while A5 has to be standardized. The subscriber identity authentication in GSM takes place using a challenge-and-response protocol. The user initiates the process by sending her identity, either TMSI or IMSI to the local domain's visitor location register (VLR). The VLR maps the user's TMSI to IMSI if needed, and forwards it to the authentication center via a secure channel. The authentication center generates a random 128-bit challenge and computes the correct response by using the algorithm A3, the challenge, and the user's individual subscriber authentication key (Ki), which is known to the authentication center. It also uses Ki and the challenge to create a 64-bit encryption key Kc, which is generated by the algorithm A8. The challenge, response, and Kc are all sent back to the VLR, which stores response and Kc and forwards the challenge to the user's phone. In the user's SIM card, the response is calculated by using A3, Ki, and the challenge and sent back to the VLR. If the responses sent by the authentication center and the user match. Then the user is successfully authenticated.

3 UMTS

UMTS (Universal Mobile Telecommunications System) is a third generation (3G) mobile telecommunication network system, standardised by the 3GPP consortium. It is nowadays deployed in Europe and in some countries in Asia and features the W-CDMA modulation standard, enabling a theoretical throughput of up to 11Mbps (against 56 kbps in GPRS/2G mobile systems). The network subsystem is very similar to the one used in GSM/GPRS networks, since its main features were widely reused by 3GPP network designers.

Differences between UMTS and GSM security

When it was designed, UMTS was aimed to build on the success of GSM, rather than provide a complete overhaul of the system that worked well as it was. Thus, many of the security features in the two systems are similar, but there are also improvements that were made in UMTS. The basic principle, though, is the same: the subscriber has a smart card (the Universal Subscriber Identity Module, or USIM) and shares a secret key with the authentication center in her home network. The first differences in security between the two systems is that UMTS was created at a time of more openness about cryptography, and thus its encryption algorithms were published along with its other standards. Since some of the algorithms do not need to be standardized, just like in GSM, UMTS specifications provide sample algorithms that can be used for encryption, such as MILENAGE. Additionally, the encryption algorithms used by UMTS are more modern and more effective and user a longer cipher key length, up to 128 bits from the 64-bit keys used by GSM. The major type of attack to which GSM networks remained vulnerable is the so-called "false base station attack", where an attacker poses as a fake GSM network and requests the user to provide her IMSI or turn off encryption. The logical solution to this is the introduction of mutual authentication, where both the user and the network need authenticate each other. In practice, this has been shown unfeasible, since the individual phone only has a pre-established relationship with its home network, making direct authentication of each visited network impossible. Additionally, extended use of authentication protocols runs the risk of failure if a single bit is transmitted incorrectly, which is highly likely on the noisy mobile channels. In view of this, the UMTS Authentication and Key Agreement (AKA) protocol was created. It provides mutual authentication in that the subscriber's identity is corroborated by the serving network, and the subscriber verifies that she is connected to a serving network that is authorized provide her with services. Additionally, the challenge used in the AKA protocol is protected against replay attacks by a sequence number and is also signed, meaning that old authentication data cannot be used to mount a false base station attack. Finally, the AKA generates an integrity key to protect integrity of the data sent between the mobile phone and the base station. A more detailed description of AKA can be found in Boman, Horn, Howard, and Niemi, page 195. The conflict between authentication and untraceability in UMTS is resolved the same way as it is in GSM, by using aliases (TMSI's) and only transmitting the IMSI in an encrypted version.

Conclusion

In this paper, we have provided a brief overview of the security issues unique to mobile telephony and have considered several ways of dealing with some of these issues. We took a look at the attempts by second-generation mobile systems to implement security and then considered the improvements and additions made to these systems in the third generation of mobile phones. We have also seen that the currently existing solutions are still imperfect and that more effective solutions to some major security issues still remain to be found.

References

[1] "Boman, K., Horn, G., Howard, P., and V.Niemi. UMTS Security. *Electronics & Communication Engineering Journal*, October 2002:191-204"

[2] "Gollmann, D. Computer Security. John Wiley & Sons, West Sussex, England, 2006"

[3] "Samfat, D., Molva, R., and N.Asokan. Untraceability in Mobile Networks. *Mobile Computing and Networking, 1995:26-36"*