Dominion For Mobile Security

Neha Dubey
M.E. Scholar
E&C Department
SRIT Jabalpur

Prof. Ravi Mohan
HOD M.E./M.Tech.
E&C Department
SRIT Jabalpur

Prof. Sumit Sharma
E&C Department
SRIT Jabalpur

Abstract

At present methods for providing conditional access to restricted resources and applications for permitting personnel, such as military members, government agencies, or first-responders are not available. The conditional access is provided if the user is an authentic user in one of the authorized geographic location and is connected to specific base transceiver stations or base station controllers. In this work we introduce dominions for mobile security, which are designed to provide this conditional access, are adjustable and congenial with mobile cellular systems, and can run even without being connected to a devoted back-end network. The aim of the architecture is to provide users who satisfy specific pre-conditions access to restricted resources and applications to which they otherwise normally would not be granted access. These mobile security dominions not only provide strict security by authenticating the user and the geographic location of the device, but also prevent access to networks or resources outside of authorized areas and restrict unauthorized users.

1. Introduction

The past decade has brought many natural disasters and times of strife requiring the quick response of first responders. The first responders have been tasked with many different jobs, such as flood evacuations, aiding tornado affected areas, and setting up and managing assistance centers in earthquake-ravaged countries, to name just a few examples. The coordination and communication of these great missions are largely complicated and often difficult to manage, yet extremely important. The current generation of wireless networks and services can support the coordination and communication requirements of such missions. There has been an explosion in the mobile device technologies recently and an even greater advancement of the capabilities of these devices. First responders can benefit from the advances by using them within secure wireless networks to aid in their efforts. Security is a necessity in these environments and although many mechanisms are currently available for the security of networks, they are not sufficient enough to secure an application to the native device.

2. Secure Dominions

Valuable services and resources must be available to first responders on-scene. These resources are most often applications, which must be secure enough to not only share sensitive data without compromise but also prevent any unauthorized access. Wireless networks currently do an acceptable job with providing security, but there also needs to be a secure form of access control between the user's mobile device and applications or data. A mobile security dominion is a method of access control between a collection of valuable assets and the mobile device. The dominion contains these assets and only allows access to the user when certain conditions exist. The conditional access must be granted specific to the user and device, such as being connected to particular cell tower or present in a pre-specified geographical area. Users who often operate with decentralized mobile networks fall under this category. These types of networks should also provide additional security and present solutions when the permanent infrastructure has been damaged or inaccessible. There are currently no mobile security dominions in use.

3. Objectives

Our goal is to develop an infrastructure for mobile security dominions. The infrastructure will consist of an application to test appropriate conditions under which access should or should not be granted, a method to provide authentication between the secure application and mobile device, and the framework that allows access from device to sensitive assets (the dominion). The following components of the framework will be presented:

- The testing application is the first instance of allowing secure access to the dominion. It tests whether or not the mobile device is currently connected to a particular mobile base station. If the mobile device clears this test, then the authentication between the security dominion and mobile device may begin.
- A method of authentication between the dominion and mobile device is proposed.
- Once the device and dominion are authenticated, assets within the dominion are available to the user. A method of building the dominion is also proposed to include the Android coding required.

4. Cellular Networks and GSM

The need for a wireless infrastructure to support communications and data interactions is now more important than ever with the increased use of mobile devices. Global System for Mobile Communications (GSM) network is used as a test-bed by this thesis. The back-end of any cellular network is the Public Switched Telephone Network (PSTN), which extends out to the Network Subsystem (NSS) that contains the Mobile Switching Centers (MSC), among many other components. MSCs connect to each other and Base Station Subsystems (BSS) that each contains a Base Station Controller (BSC) attached to at least one Base Transceiver Station (BTS), or cell tower. The towers are the components that reach out and "talk" to the mobile devices through the over-the-air interface.

GSM networks contain two separate channels by which mobile device users connect. These are an administration (control) channel and data transfer channel, which itself is comprised of various sub-channels. GSM networks are allotted a frequency range, which is broken down into these channels, eight in all. To avoid frequency overlap, the BTSs will divide their area of coverage up into sections. This also aids in mobile device handoff as it moves from cell to cell. BTSs in GSM networks continuously transmit RF signals on a control frequency for MCDs to detect while mobile stations are continuously scanning the forward control channel (FCC) for paging signals from base stations.

The MCD, BSS and MSC are the components that primarily handle phone calls and text messaging. When a request for a connection to a mobile station in its area is received at MSC, a broadcast message containing the number of the mobile station that is being called is send to all base stations under the control of the specific MSC. The base stations then broadcast the message on all forward control channels. The correct mobile station acknowledges the page by identifying itself over the reverse control channel (RCC). The MSC receives the acknowledgement via the base station and instructs the base station and mobile station to switch to an unused voice channel. A control message is then transmitted over the forward voice channel that instructs the mobile phone to ring [1]. The mobile device measures signal strength of all detected signals and relays this information to the MSC which will calculates whether or not to hand the MCD over to another BTS or BSC. The method is very similar when the mobile device initiates the call instead of from the other side of the MSC. In this case MCD sends a request to its BTS, which is relayed through to the BSC which in turn routes the request to the MSC. The MSC decides if it is needed to forward the request to a connected BSS, a different MSC, or to the PSTN.

The inherent design of cellular networks leads to security problems since tower to mobile device communications are transmitted in the wireless medium. In a GSM network security is achieved by encrypting this link with special ciphers. The ciphers that are used for the purpose of encryption are incorporated into the MCD as a committed die. The cipher key is generated by the SIM during the authentication process. For a SIM to be authenticated by a network, it's identity should be known to the network. As this has to be sent over the air interface, temporary identities are used to countervail the threat of tracing the user's whereabouts [2].It is important to note here the potential weaknesses in the over-the-air interface of data transfer between the MCD and BTS. This is one logical concern which has led to the development of a mobile security dominion for first responders. This interface provides some security, but our proposed dominion would provide a more sufficient means of securing access and data transfer.

4.1 Core Network Communication

Configuring the core network at the MSC can be a difficult task depending on what equipment the first responders are using. This cannot be done on a permanent GSM network without the approval of the system, but other ways are available for testing

and implementation. Mobile base stations having same functionality as the BSC and MSC, and allowing back-end connection to the permanent infrastructures are available. These mobile base stations can be used by the first responders to set up their own networks on the fly, similar to mobile ad-hoc networks (MANETs), but are different in protocol. Mobile networks referenced here should not to be mistaken with MANETs. Users are allowed to communicate and transfer data via GSM devices as though they are present within the same permanent network using mobile networks. The benefit to the mobile BSC/MSC combination is that they can easily be configured and sufficient security methods can be employed. Some open source softwares are also available that allow for the configuration of components of a GSM network if the equipment is not capable.

One such example of open source software is OpenBSC. The OpenBSC project is a software program that benefits researchers in three ways [3]:

- provides for an economical test-bed for experimentation and security research with GSM
- the project documents and points out any security related issues that are found
- researchers learn more about GSM networks on a basic level, particularly the practical issues with real-world equipment

The only requirements for OpenBSC are the software program, a Linux kernel with mISDN support and a GSM BTS. The software program has to be written in C99 portable code.

There are different modes within this program that implement and act as the BSC, MSC and HLR. With the required equipment, one is able to setup up a configurable GSM network for testing and researching purposes. The project also provides functionality for use of AuCs, VLRs and EIRs. The HLR is instantiated from SQLite database that stores entries of the subscribers to the network. OpenBTS is a similar program to that of OpenBSC, but has NSS replaced from the BTS up. The purpose is to provide a software based GSM access point for GSM compatible devices. In addition to software, there are whole components that can be used in manually configuring GSM network components.

Some of the focus in this thesis centers on interaction between the MS and BSS. There exists a possibility to manage this interaction from the MSC. The MSC's purpose is linking groups of BSSs and to control call signaling and processing, among other things. The important aspect is the data transfer through the BSS, destined for HLR, VLR and EIR, necessary for location management.

One such data transfer occurs in mobility management. BTSs are periodically broadcasting cell identities to their areas of coverage. Any MCDs within that area of coverage receive that information and relay it to the VLR that is attached to the local MSC, where it calculates signal strengths for other uses, such as handoff. This new location data is sent from the VLR to the mobile device's own HLR via the MSC to update it. The HLR will then send data to the old VLR instructing it to delete the old location info (typically a different MSC) as well as sending the user's service profile to the new VLR, again through the MSC of focus. The data stored in the VLR consists of the International Mobile Subscriber's Identity (IMSI), authentication data, Mobile Subscriber Integrated Services Digital Network (ISDN/MSIDSN) number, GSM services that the subscriber is allowed access to and the HLR address of the subscriber.

4.2 Base Station Subsystem

The BSS's overall responsibilities include: handling traffic and signaling between the MSC and MCD speech channel encoding, radio channel allocation to MCDs, paging, and transmission and reception of signals. These tasks can be handed out, respectively, to the BSC and BTS combination. As with the MSC, it is important to focus on the data transfer between the MCD and BSS to determine possible authentication or access control schemes. There is a significant amount of data that travels through the BSC to other BTSs and the MSC. The focus here is how to manipulate that information to develop a befitting scheme. Other mobile communication traffic, such as telephone calls and SMS, is ignored for this work. Instead, information that is inherent to the BSC or MCD is the focus and is primarily identification and location related. One important example of this is the identification of BSC. The identification, known as the Cell ID, is continuously broadcasted on the broadcast control channel (BCCH) of each BTS [4]. The Cell ID, received by each MCD that is within range, corresponds to the BTS/BSC pair and can be used for updating location and other functions. Many other types of identifications are broadcasted, such as the Location Area Identity (LAI), neighboring cell information, beacon frequencies, and minimum received signal strengths.

The LAI involves location updating and identification of the MCD. This is a combination of the Mobile Country Code (MCC), the Mobile Network Code (MNC), and the Location Area Code (LAC). Each of these numbers represents a specific location in the network. The first time the MCD is powered up it compares the stored LAI in the SIM to the LAI being broadcast by the BTS. If a match is not found, the MCD will update its location through the BSC to the VLR, and to the MSC if the MCD is being served by a different VLR [5]. The LAI is part of the International

Mobile Subscriber Identity (IMSI)/Temporary Mobile Subscriber Identity (TMSI). Another responsibility of the BSS in GSM networks is that of security. There is the potential for compromise of data traffic between the MCD and BTS because of the over-the-air interface. A secret listener with the know-how can intercept a call and listen in on the conversation – among many different types of attacks. There are two approaches to addressing this problem:

1) Authentication for communication between the MCD and MSC and

2) Data encryption between the MCD and BSS [6].

Security within GSM is discussed in the next section, but it is important to know that the BSS does play a minor role in this area.

4.3 GSM Security

The weakest link in GSM security is the over-the-air interface between the MCD and the BTS. The security model for GSM was created to battle this deficiency by offering a method that grants the network and users the ability to avoid sending sensitive identification information over this interface, such as IMSI [7]. There are two primary methods of securing the air interface – authentication and traffic encryption. The first step in the security mechanism is to authenticate the user. The purpose behind authentication is not only for security reasons, but it also plays a role in identifying and locating a user in the network. The moment a MCD attempts to connect to the network, there is back and forth data transmission to identify the device, the user and their network permissions. This depends on proper identification, which is possible only with proper authentication. Authentication for the purpose of properly identifying a user is also a part of architectural design considered here.

An integral component in GSM for providing authentication is the Subscriber Identity Module (SIM). The SIM is an integrated circuit chip fixed to a card (standard terminology, thus—"SIM card") and contains subscriber information, cipher keys and algorithms used in encryption and authentication. The information and secret keys are embedded into the chip during the personalization process with the service provider, and the same information and keys are distributed to the HLR/AuC. The subscriber information contained within it is the IMSI, which is seldom used for security reasons; instead TMSI is mostly used. The keys are shared cipher keys between it and the HLR; they are used for authentication with the MSC. The A3 and A8 algorithm contained within the SIM are used for authenticating the MCD to the MSC and for specific sessions, respectively. The encryption process uses the A5 algorithm. Authentication is possible through the use of shared keys between the MCD and HLR. Ki, the shared key, is a 128-bit key used to generate a 32-bit signed response, SRES, to a random challenge, RAND, and Kc which is a 64-bit session key, . This is all done by the MSC using the A3 and A8 algorithm, respectively [8]. The process starts with the MCD attempting to connect to the network. A set of five triples is created by the associated HLR, each of those containing a RAND, SRES to that particular RAND based on the Ki and a Kc which is based on the same Ki. The HLR will send these triples to the MSC to be used in authentication with the MCD. The MSC in turn sends the RAND of the first triple to the MCD. The MCD will calculate the SRES with the RAND it just received from the MSC and its Ki and send it back to the MSC. The MSC then compares the SRES it just received from the MCD to the one it received from the HLR. If they are the same, the MCD is authenticated.

Encryption occurs in a similar fashion. MCD will create a session key Kc, once it is granted access after successful authentication with the MSC. This key is created with the A8 algorithm using the same RAND challenge it received from the MSC and the Ki stored in the SIM [9]. The BTS has the same Kc from the group of triples it received from the MSC. Encryption between the MCD and BTS occurs on each frame with a different keystream between the two. This keystream is generated using the A5 algorithm initialized by the Kc and the number of the frame to be encrypted.

4.4 MCD Application

Applications are computer software programs developed for the end-user. These software programs can be built with as little as a few dozen lines of code or are as large as millions of lines in different programming languages, such as Java, C++ and Python. Applications are not limited to personal computers. They have appeared in personal data assistants (PDAs), cell phones, portable game consoles, and Smartphones. Essentially anything with the ability to store and execute code can run an application. Smartphone applications have taken over the digital world with the advent of their "pocket-sized" computers.

5. Location Based Application

The global positioning system (GPS) is being put to use in many different dimensions of technology. It is embedded in various means of transport and dashboard-mounted navigation units. GPS

receivers have been incorporated in wristwatches for runners and bikers. Many Smartphone applications depend upon getting a MCD's GPS coordinates for use in gaming, shopping, social networking, geo-locating, and so on. Numerous applications (also known as Location Based Services—LBSs) for mobile devices rely on or utilize the location of the device, which can be found through a few different methods. It is relatively easy to track a MCD using the MSC and VLR. Both MSC and VLR contain the information about the BSS that the device is connected to. Knowing the BSS, it is easy to find the cell in which the device is located. Thus the search is narrowed down and the precision is limited by the cell size.Localization or triangulation of BTSs and signal strengths are other methods that can be used. Another method is the use of a GPS receiver embedded in the phone. The LBSs are implemented by applications written for the device. Another example of an application that queries for location information is one that checks for the Cell ID. Every BTS has coverage area, called a cell, and an identity. The area of coverage is the extent of the geographic range within which a MCD can make a reliable connection to the BTS.A unique number assigned to each BTS or sector (cell) of that BTS is called a Cell ID. This data is used when the MCD periodically sends signal strength and connection quality data to the MSC where it is calculated for handoff determination [10]. Similar to the location based Java classes mentioned above, there are classes that allow a developer to utilize the Cell ID of a BTS that the device is connected too.

6. Architecture and Design

The architecture incorporates a test application for location-verification, an authentication mechanism and the secure dominion. The goal is to develop a working solution based off of the described infrastructure. This development consists of a test application that allows authentication to occur between the application and mobile communications devices (MCDs), which further allows the access to the dominion.

6.1 Location Verification Application

The purpose of this initial test is to verify the user is in a particular location that is authorized to have access to an dominion. This test is the first part of the connection between the user and secure or restricted-access resources. This section discusses two methods of verifying that the user is at a particular location, which will in-turn authorize them access. These locations can be geographic or conditional on connections to base stations since each BTS has a limited range for its transmissions.

The proposed test application is designed for the Android operating system and GSM network. The Android software development toolkit (SDK) allows for applications to be built by using its application programming interfaces (APIs) and the Java programming language [11]. The Java is an object-orientated language that makes use of objects and classes, which are used in development of this test application. The important point here is that the Android OS contains classes within its SDK that allows for an application to obtain the Cell ID of a base station that the MCD is connected to. The Android SDK also allows for access to GPS coordinates.

The application's operation is straightforward for the user. The user opens the application on the MCD and executes a "Connect" function, which is a simple command that instructs the application to perform its test. The application pulls the necessary information from either the base station or the GPS receiver in the MCD to determine authorization. The authorization is coded into the application during the programming phase, and can be only changed by making changes in the code. If the test passes, then the application will advance to the next portion in the architecture – authentication of the application to the MCD in order to connect to the dominion in a secure session. Otherwise, if the test fails, then the application will just notify the user that the conditions have not been met. The two methods to test the application are described in the following two sections:

6.1.1 Cell ID. In this test, the application is checking to see if the MCD is connected to the appropriate base station. Each base station is assigned a unique identification number by the telecommunication services provider, which distinguishes it from other base stations. The unique identification number is broadcast on the broadcast control channel (BCCH) of each BTS. The MCD receives this data from the BSC to which it is connected, so the application simply reads that unique ID from the MCD. The application contains a function that directs further action if the Cell ID read is one of the listed "authorized IDs". These authorized Cell IDs will be coded into a list within the application for cross referencing. It is also possible to change the configurations, including the Cell IDs, of some mobile base stations from the network management level. Thus, this Cell ID check is not limited to just permanent GSM infrastructures.

6.1.2 GPS Coordinates. This test application obtains the GPS coordinates from the receiver in the device. A small method is written to get the coordinates; the application will perform a calculation. An example of this would entail limiting access to specific city blocks. The

coordinates that outline the collection of authorized city blocks are written into the application. When called upon to test a location, the application performs a simple calculation on the users current GPS coordinates, to determine if the users are within the authorized blocks.
This method has the advantage in that GPS coordinates cannot be spoofed, unlike Cell IDs, but has a drawback of potentially being in a location that does not receive GPS signals. This method is implemented statically and would be useful in situations where the authorized locations are known in advance and do not change.

6.2 Authentication of Application to MCD

The purpose of the overall framework is to provide a secure method of granting access of vital resources and applications, contained within a dominion, to first responders and emergency personnel. Architecture needed to provide the first form of security by checking location of the device was discussed in the previous section. This section discusses the second form of security – authentication of an application and the MCD. Both methods of location verification and authentication occur in the same application. Once the application verifies that the MCD is in the proper location, either by GPS coordinates or connection to a specific BSS, then it must authenticate with the MCD. This authentication provides another layer of security for access to the dominion, ensuring that the individual and device attempting to access the dominion is authorized. The authorized individuals and devices are pre-programmed into the application, can be pre-loaded onto a removal storage device or via another means such as accessing the network. This architecture only focuses on the application containing the authorizations. The primary authentication mechanism is challenge-and-response. The application must challenge the user and dependent on the user response, grants access to the dominion. The first component in this process must be a valid piece of identification. There are a few different forms of identification available to test against on a GSM connected MCD, some of them are the shared keys on the SIM cards, ICCID, IMSI and IMEI, . Each of these IDs can be retrieved with the proper coding in Android, but the most secure is to use the shared keys contained within the SIM card. In order to use this method of authentication, the application authenticates the user by sending a challenge to the SIM invoking a response. The challenge is a 128-bit random number (RAND) and is generated by the application. The SIM contains algorithms that combine the RAND and a shared key, Ki, to form a session key, Kc and response key. The application contains similar algorithms and with a copy of the same shared key, generates its own response and Kc. Additionally, shared key and IMSI (or some other form of identification) matched pairings need to be stored within the device so that the application will know which shared key to use for the present SIM. Authentication is successful when a match is found between both the responses match. Following authentication, the application will send a request to open the security dominion. This request contains the challenge, the IMSI and the generated Kc. This is the only way to open up the dominion.

6.3 Dominion Structuring

The third component to the architecture is the security dominion. The important aspects of this element are strict security features that must be in place for it to be accessed and the fact that it contains vital resources for the users, such as applications or data. The dominion is application-based as well, which offers a few different security methods that prevent unauthorized access. Another benefit of being application-based is that updates can be sent to the devices that contain the dominion similar to that of other applications on the network.
The primary aspect of the dominion is the means of opening it. There are alternate means of structuring the dominion such as building it into a separate partition of the hard drive, developing a separation kernel for it or embedding it within an application. This work focuses on the application method. The application will be written such that the only way it can be started is by a request from the authentication application above.
Sending an intent, or coded message, from the authentication application to the dominion to open it, does this. The intent contains user information, a session key and a specific request to start the dominion application. The dominion will first run the A3/A8 algorithm to produce the Kc, similar to that generated during authentication, as described above. It will compare both session keys, and if they are equivalent, will grant the dominion access for the user.
Another form of security for this method that is included in the application is the use of developer certificates. Restrictions can be applied within the code that forces the application to verify both applications (location-verification/authentication & dominion) contain the same developer certificate before allowing access. This method prevents other applications from being granted access by sending their own requests for access to the dominion.
Once the dominion is successfully opened, the user will gain access to the contents contained inside. The application is written such that the user will be presented with a list or separate desktop on the device that contains the resources. The coding for

this will be similar to that of the intent transfer between the authentication and dominion applications.

7. Conclusion

This paper proposes architecture to allow personnel, such as first responders and military members, to securely access and manage valuable resources and applications conditionally. Also, unauthorized, access to the same resources and applications is prevented. The proposed architecture lays out the blueprints for three major components of a security dominion: the location-verification application, user authentication mechanism and the security dominion construct that contains the valuable resources and applications.

The first component is the location-verification application. This is an Android application that can either check GPS coordinates or the Cell ID of the BTS to which the MCD is connected, or both. The application crosschecks this with a list containing authorized coordinates or Cell IDs before allowing the user to attempt the second form of authentication.

The second component is the authentication mechanism. This component can only be accessed after being properly validated by the location verification application. This mechanism uses a challenge and response method similar to that of the GSM authentication process. The challenge is created using an algorithm (COMP128) that is compatible to the A3 algorithm used in the GSM network. This challenge is sent to the SIM card of the device where a response will be generated in similar fashion. Only authorized SIM cards will generate an appropriate response that confirms authentication. Upon location verification and user authentication, the mobile security dominion is accessible to the user. The dominion can take many forms, but this thesis describes the framework necessary to make it application based. The dominion securely contains any resources or applications to which the user is allowed access. The protected assets are readily accessible and transitioning from one to another is similar to that of changing activities in an Android application.

8. Future Work

Besides the architecture described in this thesis, there are a few general areas that require further study. The first area focuses on back-end network integration, specifically pursuing other services or databases that aren't local to the device, encryption, and establishment of an update mechanism. Another area of interest is component integration to include use of removable storage devices. Finally, there are a few recommended software areas to research such as continued location verification and a method to avoid hard coding the application with authorizations. Each of these areas is described in greater detail in the following sub-sections. Addressing these concerns will ensure a product that is more robust, more flexible, and more appropriate for deployment.

10. References

[1] L. O. Walters and P. S. Kritzinger, "Cellular Networks: Past, Present, and Future," *Crossroads*, Vol. 7, Issue 2, pp. 5, 2000.

[2] K. Vedder, "GSM: Security, Services, and the SIM," *Computer Science*, 1528, pp.227, 1998.

[3] Osmocom, "OpenBSC," April 12, 2011. http://openbsc.osmocom.org/trac/wiki/OpenBSC

[4] A. Mehrotra and L. S. Golding, "Mobility and Security Management in the GSM System and Some Proposed Future Improvements," *Proceedings of the IEEE*, Vol. 86, Issue 7, pp. 1483, 1998.

[5] Y. J. Choi and S. J. Kim, "An Improvement on Privacy and Authentication in GSM," *Computer Science*, 3325, pp. 17, 2005.

[6] Y. J. Choi and S. J. Kim, "An Improvement on Privacy and Authentication in GSM," *Computer Science*, 3325, pp. 15, 2005.

[7] L. Pesonen, "GSM Interception," *White Paper*, University of Technology, Helsinki, pp. 2, 1999.

[8] A. Schoffl and M. Irger, "Communication Infrastructure: GSM Communication," Johannes Kepler Universitat Linz, 2001.

[9] A. Mehrotra and L. S. Golding, "Mobility and Security Management in the GSM System and Some Proposed Future Improvements," *Proceedings of the IEEE*, Vol. 86, Issue 7, pp. 1489–1491, 1998.

[10] Android. "What is Android?" August 5, 2011. http://developer.android.com/guide/basics/what-is-android.html

[11] Android. "What is Android?" August 5, 2011. http://developer.android.com/guide/basics/what-is-android.html