2015

3G UMTS man in the middle attacks and policy reform considerations

Jennifer Lynn Adesso
Iowa State University

3G UMTS man in the middle attacks and policy reform considerations

by

Jennifer Adesso

A thesis submitted to the graduate faculty

in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

Major: Information Assurance

Program of Study Committee:
Alex Tuckness, Major Professor
Doug Jacobson
Dirk Deam
Thomas Daniels

Iowa State University

Ames, Iowa

2016

TABLE OF CONTENTS

LIST OF FIGURES

Page

NOMENCLATURE

AKA Authentication Key Agreement

AMF Authentication Management Field

ARFCN Absolute Radio Frequency Channel Number

AV Authentication Vector

BCCH Broadcast Control Channel

BER Bit Error Rate

BSIC Base Station Identification Code

BTS Base Transceiver Station

CRNC Controlling Radio Network Controller

CS Circuit Switched

ECC IBE Elliptic Curve Identity Based Encryption

EUIC Enhanced User Identity Confidentiality

GMO Genetically Modified

GSM Global System for Mobile Communications

GSMC Gateway Mobile Switching Station

HPLMN Home Public Land Mobile Network

IBE Identity Based Encryption

IMEI International Mobile Equipment Identity

IMSI International Mobile Subscriber Identification Number

ISDN Integrated Service Digital Networks Number

LAC Location Area Code

LAI Location Area Identifier

MCC Mobile Country Code

MM Mobility Management

MME Mobility Management Entity

MNC Mobile Network Code

MSC Mobile Switching Center

MSISDN Mobile Station Integrated Service Digital Networks Number

MSRN Mobile Station Roaming Number

PCN Personal Communications Network

PKG Private Key Generator

PLMN Public Land Mobile Network

PS Packet Switched

PSTN Public Land Mobile Network

RAN Radio Access Network

RAND Random Number

RNC Radio Network Controller

RNS Radio Network Subsystem

RR Radio Resource

SDCCH Stand Alone Dedicated Control Channel

SDR Software Defined Radio

SGSN Serving SPRS Support Node

SRES Signed Response

SRNC Serving Radio Network Controller

TMSI Temporary Mobile Subscriber Identity

TRAU Transcoder Rate Adapter Unit

UE User Equipment

UE User Equipment

UMTS Universal Mobile Telecommunications System

USIM UMTS Service Identity Module

USRP Universal Software Radio Peripheral

UTRAN UMTS Terrestrial Access Network

VLR Visitor Location Register

VPLMN Visited Public Land Mobile Network

ABSTRACT

MAN IN THE MIDDLE ATTACKS ON 3G UMTS HAVE BEEN A KNOWN VULNERABILITY SINCE AT LEAST 2004. MANY EXPERTS HAVE PRESENTED SOLUTIONS TO RESOLVE THIS ISSUE. THE FIRST ATTEMPT TO MITIGATE THE ISSUE IN THE FORM OF MUTUAL AUTHENTICATION FELL SHORT. IT IS NOW PUBLIC KNOWLEDGE THAT LAW ENFORCEMENT AND THE FBI HAVE USED THIS MAN IN THE MIDDLE STYLE ATTACK TO COLLECT INTELLIGENCE WITHIN THE UNITED STATES. IT IS IMPERATIVE WE OPENLY ACKNOWLEDGE THAT WHILE THE MAN IN THE MIDDLE ATTACK HAS IMMEDIATE BENEFITS, THERE ARE ALSO INHERENT RISKS TO MAINTAINING A LOWER STANDARD OF SECURITY.

THERE HAS BEEN NO OFFICIAL DOCUMENTATION FROM THESE AGENCIES ON THE PROTOCOL USED TO CONDUCT THESE COLLECTIONS. THIS PAPER WILL OUTLINE THE DEFICIENCY IN GSM AND UMTS, SHOW HOW A MAN IN THE MIDDLE STYLE ATTACK WOULD WORK AND WHAT IS KEEPING THE ATTACK STILL POSSIBLE AFTER SO MANY YEARS.

FINALLY, THERE WILL BE FOUR POINTS TO CONSIDER FOR PRELIMINARY POLICY REFORM; CONSTITUTIONALITY, OVERSIGHT, VULNERABILITY, AND PROTECTION.

CHAPTER 1

INTRODUCTION: WHO SHOULD CARE?

According to PEW, researchers have found that in January 2014, 90% of American adults own a cell phone. [60] TIME reported in 2013 that more people in the world owned cells phones than had access to toilets. [59] While that statistic might leave us with an ethical concern, the fact that cell phone saturation is global is undeniable.

Much like starting the engine to our car, we just take for granted that our phone just works. There is no need in day to day life to get in to the protocols of how our phones communicate with towers and authenticate, as long as it works when we need it. The following paper will introduce an alternative way of viewing cell phone technology and the information you might be sharing.

Medical facilities and banking establishments have been under the microscope to add information security measures to protect user information. Federal legislation passed by Congress has been instrumental in establishing standards and guidelines to increase technological security measures in these fields. Telecommunication carriers have not been scrutinized in the same manner. While the carriers have added security features to their designs, there has been at least one design flaw that has remained: the Fake Cell Tower Attack. The fake cell tower attack acts as a Man in the Middle who can then compromise any user with in its coverage area. Once a cell phone is connected to a fake cell tower a barrage of attacks can ensue or the attacker can simply wait, watch, and listen. These attacks can come from the good intentions of the law or from foreign entities collecting intelligence. The vulnerability is indiscriminate.

To understand how a Man in the Middle attack would work, a base knowledge of the protocol is essential. Once there is an understanding of how cell towers communicate with a cell phone, then it is easy to see how this protocol allows this style of attack.
Instead of facilitating security measures to be placed to counter this style of attack, regulations have been in favor of continuing the protocol that allows fake cell towers to collect data. Law enforcement and government agencies, such as the FBI, use this weakness in the protocol to collect intelligence to provide security.

It is imperative for experts in technology, security, and legal fields to take a look at policy reform and decide if lowering security standards allows the government to make its citizens more secure. Citizens and civil right organizations need to take an active role in ensuring the establishment of proper policy reform for future cases. Policy reform should not take shape until legal and technological experts weigh in with their sound advice. Therefore, instead of presenting actual policy reform suggestions, I will provide the preliminary consideration for policy reform. This will leave room for the correct legal interpretations and a review of the technological abilities yet still establishing the ground work toward correctly weighing all considerations. There are four points that should be taken into consideration when deciding how to construct policy reform and future regulations: constitutionality, oversight, vulnerability, and protection.

1.1 Research Question and Methodology

We must first be sure that a Man in the Middle attack is possible as believed. Once we establish the protocols it would take to achieve this attack, we then need to discover why this attack is possible. Finally, this vulnerability needs to be viewed from all possible angles to

discover what policy reforms and legislation will lead to maximum security and will minimize foreign and domestic threat.

GSM and 3G UMTS history and protocols will be analyzed from books written on the specifications of the design architecture. The Man in the Middle attack will be constructed using information from documentation obtained from the Institute of Electrical and Electronics Engineers (IEEE).

An analysis of the regulations will include literature from legislation and policies from the Department of Justice, Federal Communications Commission guidance, documents released to the public from the FBI and local law enforcement, and media coverage.

Legal and ethical issues will also take into consideration the local law enforcement and FBI documents as well as heavily rely on research from civil rights organizations.

Ideology will play an important role in discussion of preliminary considerations due to the differences in how citizens prioritize security, surveillance, and privacy. Conclusions should not be made based solely on ideology but rather encompass established laws, policies, and technical accuracy.

These combined areas of research will provide an informed base to begin preliminary consideration to guide a comprehensive reform process.

CHAPTER 2

ORIGINS OF THE MAN IN THE MIDDLE ATTACK

When Global System for Mobile Communications (GSM) became an international standard for many countries, it also became one of the largest targets for attacks. A Man in the Middle (MIM) attack is an intrusive and potentially dangerous attack. A surprising fact is that since the inception of GSM, the MIM attack was a known point of failure. [1] [3] One focus of this paper is to define GSM architecture in such a way that we can see how a Man in the Middle (MIM) attack is technically possible. Once the technical aspects of the vulnerability has been established, there will be evidence provided that will show that while it may not have started as a government introduced security flaw, this vulnerability is exploited by the government to conduct surveillance. While acknowledging the necessity for intelligence collection to aid in national security there is controversy with the regulations, constitutionality, and effectiveness with this style of attack. This analysis will include reasonable preliminary policy reform considerations to include a technical alternative.

*****

1992, Motorola introduced the first commercial global communications system. Ten years prior, in 1982, Group Special Mobile a subgroup existing inside European Post Offices and Telecommunications (CEPT) formed in part to discuss the future of standardizing global telecommunications. [1] Tremendous amounts of research and thus money would be needed to complete a project of this size. Group Special Mobile would need the support and currency of many countries to make this idea a reality. As the concept of an international based standard for telecommunications whispered across oceans, many countries became interested

in joining the movement. In 1985 France and Germany agreed to support a global communications standard. Field trials began in 1987 which resulted in a decision to use digital, narrowband Time Division Multiple Access (TDMA). [1] Just months following the outcome of the field trials in 1987, 17 network operators in CEPT countries signed a Memorandum of Understanding (MOU) showing alliance to complete standardizing the global communications system and begin implementation by 1991. The CEPT countries held true to their cause, in 1990 the standards were complete and implementation began in 1991. [1]

1993, not long after Motorola introduced the first global communications system, the Group Special Mobile received its new name "Global System for Mobile Communications" better known as GSM. [1]

1994, phase 2 of GSM was already beginning. This is a trend we will see continue. Research of the next phase of GSM will begin at the implementation of the previous phase. This puts GSM stepping into a new phase approximately every decade.

The structures that were built to implement GSM in the 1990's were voluntary and a significant financial investment for their prospective countries; both private and governmental. It is in the interest of the system to continue to improve GSM without making costly changes to the physical structures or to create significant changes that cannot be easily adopted by all GSM countries.

Understanding the original design of GSM is important for several reasons. The physical structures were costly so any pending improvements made need to weigh heavily on the existing structures so they can be fully utilized to reduce cost. The concept of GSM is that each country maintains the same standards in architecture and design so that all users will be

able to benefit from the global system. With this being said, consideration must be given to see that each country will be able to meet new standards. This may include financial, expertise, or with physical work on structures.

The following sections will contain a brief overview of the GSM architecture's functions and controls. More detailed information can be found about the GSM architecture in [1] *Mehrotra, A. (1997). GSM system engineering.*

2.1 GSM Construction

GSM is structured in to 5 different levels. The term levels here indicate the amount of coverage area and action that each level is responsible for. The first level, and in a top down approach, is the all-encompassing GSM service area. The GSM service area is viewed as the parts of the world that utilize GSM as a communication standard. Public Land Mobile Network (PLMN) is the next level down, several of these areas can exist in one country. [1] This area is defined as the ability for international calling. At this level the mobile device will be directed to a Gateway Mobile Switching Center (GMSC) which has the ability to send a signal across country boundaries. [1] The third level is the Mobile Switching Center (MSC) level. There will be several MSCs in a PLMN. MSCs know where each mobile device is in its area and will route calls within its area. Location Area (LA) is the fourth level. [1] At this level the mobile device does not need to update its location, but the LA can page the device to make sure it is within its area of operations. [1] There are many LAs in a MSC. Finally, there are many cells within a LA. The cells are the smallest structural level and are serviced by a single base station. [1]

The components of the original GSM architecture are broken into 3 subsystems; network, radio, and Operation and Maintenance Center (OMC).

The network subsystem can be viewed as the overall mobility manager that maintains the connection of a mobile device. A main focus of the network subsystem is the Mobile Switching Center (MSC), which is the physical equipment necessary to carry out the functions that are required to keep the mobile devices connected to the network. [1]
The radio subsystem is typically viewed as the physical towers that a mobile device utilizes to complete the connection to the network, as well as the functions and controls that make that possible. Various functions of the MSC are considered to fall in this subsystem as well as the network. [1]

The operations and maintenance center supports the overall blueprint, billing, and software upgrades to the entire system. This subsystem is connected to all parts of the MSC and parts of the base stations. [1]

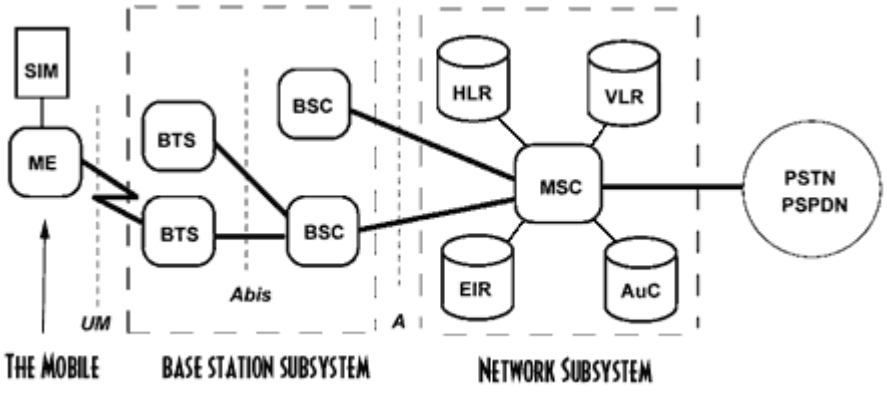

Figure 1 GSM Architecture [32]

2.2 Mobile Stations

The earliest cell phones were referred to as Mobile Stations (MS) and included car phones along with hand held devices. The MS sends and receives voice and data messages to

the GSM network. [1] It is important to the MS to keep time synchronization and will automatically update to a signal sent from a Base Station Controller (BSC) if out of synchronization. Even when the MS is not active it will update its location to the GSM network so if needed it can send and receive signals. Distance from the Base Transceiver Station (BTS) is important because the MS and BTS will need to calculate its time advance since the signal will arrive at different times as the MS moves closer to or further away from the BTS. There are several features of the MS that exist to provide the GSM network the ability to track usage and location of the MS. These features are used for billing and security purposes.

2.3 Subscriber Identity Module

A key feature of the MS, in the original GSM, is the Subscriber Identity Module (SIM) card. This was a smart card that could be inserted into an owned or rented MS and would fuse that MS to the identity of whom owned the SIM. [3] This provided certain security features and enabled accurate billing procedures. The SIM contains a unique mobile subscriber identity through a function of an International Mobile Subscriber Identity (IMSI) and an Integrated Service Digital Network (ISDN) number. Originally, a pin was associated with the SIM card so that once put into a MS the user would authenticate himself to the MS and SIM card. Each SIM contains a unique key, $K_{i,}$ that is known by the GSM architecture, specifically the Authentication Center (AUC). [1] Algorithms A3, A5, and A8 are implemented to provide unique authentication parameters. A SIM contains both Random Access Memory (RAM) and Read Only Memory (ROM) to further identify a user without

them being able to change their own identity. [3] This protects both the consumer and the billing companies. Details will follow on specific encryptions and authentication protocols.

2.4 International Mobile Subscriber Identity / Temporary Mobile Subscriber Identification Number

The International Mobile Subscriber Identity (IMSI) is a number that can be no more than 15 digits and held by the SIM card. The first 3 digits represent the Mobile Country Code (MCC). The second 3 digits represent the Mobile Network Code (MNC). The final digits cannot exceed 9 digits and are the Mobile Subscriber Identification Number (MSIN). [1] The IMSI is considered to be the one and only true and absolute identity of the mobile subscriber. This number is permanently stored in the Home Location Register (HLR) and exists in the Visitor Location Register (VLR) so as long as the MS is in the area controlled by that VLR. A Temporary Mobile Subscriber Identification Number (TMSI) attempts to add privacy to a user when traveling outside of the HLR and into a VLR. The number is only assigned when in the VLR and is assigned only after successful subscriber authentication. [1] The TMSI number consists of a country code, a Public Land Mobile Network (PLMN) code, the HLR identification, a serial number in the data base of the HLR, and potentially can have a time stamp to avoid multiple TMSIs delivered. [1]

2.5 Base Station System

The Base Station System (BSS) is the entire system of base stations to include to equipment, controls, and functions. It is broken in to 2 separate parts; the Base Transceiver Station (BTS) and the Base Station Controller (BSC). Between the BSS and the MSC exists

the SS7 interface (A- interface). [1] This standardized interface allows for the purchase of equipment from several retailers whom meet the standard specification, but also has its own list of vulnerabilities. Between the BSC and a remote BTS exists the A-bis interface. [1]

2.6 Base Transceiver Station

A Base Transceiver Station (BTS) is the physical transmission equipment and functions. BTS coverage area is called a cell and is seen as a hexagonal design but in reality its shape cannot be accurately determined due to uneven propagation and terrain. Each BTS serves one cell. [1] BTS has the responsibility of receiving and transmitting radio signals. The signal will go through a transcoder which is located either at the BTS or near the MSC or BSC. This device would take 13-Kbps speech or 3.6/6/12 Kbps data multiplexes and combine and convert them to standard 64-Kbps data, depending on its location. [1] The BTS has responsibility to encrypt, modulate, synchronize time and frequency, control frequency hopping, time advancement, and random access detection. [1]

2.7 Base Station Controller

The Base Station Controller (BSC) sits between the BST and the Mobile Switching Center (MSC) and its main responsibility is to act as the Radio Resource (RR) manager. [1] The BSC monitors the time so that correct synchronization can take place. If it sees that the MSC is not in synchronization then it can have the BST send the MSC the corrected time. [1] The BSC is responsible to assign frequencies to the mobile equipment in its area. It has the control to switch mobile equipment from one BTS in its area to another BTS in its area either

due to movement or heavy use in one cell. [1] The BSC also establishes the hopping sequence that the BTSs and the mobile devices use to communicate. [1]

2.8 Mobile Switching Station

The Mobile Switching Center (MSC) has the responsibility to provide an interface for the mobile device to connect to the BSS. A MSC must know the location of all mobile devices in its area.[1] Depending on the structure level, a gateway MSC may need to route a mobile device to another country. The MSC controls the switching of the higher level, BSS, when a mobile device moves from one area into another area. It is possible that two MSCs will be connected to a mobile device if the device is moving out of the area of one MSC and into an area controlled by another MSC. [1] The MSC collects data from the mobile device for billing and authentication purposes. Encryption standards are passed from the Visitor Location Register (VLR) through the MSC to the BSS. [1] Synchronizing the handoff of BSS is a main focus for the MSC. Three main components exist alongside the MSC to assist in authentication of a MS to the GSM network: Home Location Register (HLR), Visitor Location Register (VLR), and Authentication Center (AUC).

2.9 Home Location Register

Home Location Register (HLR) permanently stores specific identifying numbers and information that are used to authenticate the MS's SIM to the GSM network. Encryption functions are enacted in the HLR to protect this data base of information. Some important numbers stored here are the International Mobile Subscriber Identity **(**IMSI) and the international Mobile Station Integrated Service Digital Network (MS ISDN), both which are

located on the SIM card of the MS. [1] This database also stores the key, k_i, and any information that would restrict access or contain add-ons for a user. [1] HLR informs the Visited Location Register (VLR) of necessary data that is needed to connect the MS to the GSM network. Subsequently, the VLR informs the HLR of the use in its area. [1]

2.10 Visited Location Register

When a MS enters into a Visited Location Register (VLR), it requests information from the HLR. Most of the information in the VLR and the HLR are the same and have the same purpose of assisting in the establishment of authentication to the GSM network. The main difference is that the information in the VLR is only stored as long as the MS is in the VLR coverage area. The VLR assigns and stores the Temporary Mobile Subscriber Identification Number (TMSI). As stated earlier, the IMSI is only stored so as long as the MS is in the area controlled by the VLR. [1] The VLR obtains encryption information from the HLR and passes this to the BSS in the area of operations. [1] Communication between the HLR and the VLR is important to the continuation of information flow and the MSC is utilized for this information flow. This will also become important later during discussion of how the MIM attack works.

2.11 Authentication Center

The Authentication Center (AUC) can be viewed as the database, for both the VLR and the HLR, which contains the sent and received information that authenticates a MS to the GSM network. It also computes certain numbers to verify authenticity. AUC computes and sends a Random Number (RAND) and waits for the reply from the MS called the Signed

Response (SRES). The secret key K_i and the ciphered key K_c are also stored in the AUC to compute encryption values. K_c is transmitted from AUC to the visited MSC across the SS7 interface link. Although, the HLR requires information from the AUC they are two distinct pieces in the GSM architecture.

CHAPTER 3

GSM SECURITY DEFINITIONS

At the time of the original design of GSM, working groups were established to have field professionals address different issues. MOU-SG was the name given to the security working group, since it was established at the time of the Memorandum of Understanding (MOU). [1] There were 2 main concerns of the MOU-SG. The group believed that users needed some privacy so that their communications could not be easily eavesdropped on with radio equipment. [1] Also, authentication of users to GSM networks would be a priority for billing purposes. They established 3 solutions for their security concerns. [1] Using the TMSI would give the user anonymity. IMSI would be used to authenticate a subscriber identity for billing purposes. Finally, encryption would protect both the anonymity and the authentication methods.

3.1 Anonymity

Assigning a TMSI was intended to protect the one real true identity, the IMSI, from being sent over the air. A VLR will decide to authenticate a MS for a few different reasons. The VLR can be set up to authenticate at every new service request or only when the MS enters the VLR owned area. [1] When a MS enters a VLR the MS will automatically send a previous TMSI, if one has already been assigned. If the TMSI cannot be located the IMSI will then be requested by the VLR and sent by the device. [1] Then the VLR will query the MSC in conjunction with the HLR/ AUC. This query is called the MAP/D Update Location and the response is called the MAP/D Update Location Result followed by MAP/D Insert

Subscriber Data. [1] From that point on if an IMSI is requested the TMSI is sent by the MS. Yet, with every rule there is an exception: when there is a failure by the MS to find the newly assigned TMSI or failed location updating then the device will be required to send the IMSI. This request is called the RIL3-MM Identity Request and is sent by the MSC. [1] Once requested the MS is forced to respond with the IMSI. [1] This feature was most likely due to preventing users from hiding their user identities for billing purposes. This idea will become a key feature in how the MIM attack is implemented.

3.2 Authentication

Telecommunication operators in each area are given a lot of latitude to decide when and how often an authentication process will take place. The design of this authentication allows a valid MS to automatically update to a new VLR and BSS without any user input. A special note here is that authentication did *not* intend to authenticate a valid VLR or BSS to the MS, just the MS to the GSM network. [3] This is one-way authentication. The one-way authentication is initially what made the MIM attack possible.

Authentication takes place prior to encryption and the goal is to send a challenge and response that only the true MS could produce all while not sending identifying information over clear air.

As stated earlier, there are a few scenarios that would allow the IMSI to be sent over clear air. The very first time a MS is turned on, the MS sends the IMSI prior to encryption. If the GSM network has any issues validating the identity of a MS, then it can request the IMSI be sent and it is forced to reply with the IMSI. [1] Finally, if the MS is turned off and moved into another VLR then the VLR may not be able to validate the TMSI and thus will request

the IMSI from the MS. [1] [3] The idea that a cell tower can force the MS to respond with the IMSI is going to be a key element to the Fake Cell tower attack.

The authentication process begins when a MS sends a location update to the MSC in the area of the new VLR, which will include the TMSI. The VLR will send a message to the HLR that authentication is needed and include the TMSI. [1] The HLR/ AUC database has the TMSI, IMSI, and K_i information. [1] The AUC will calculate RAND, SRES, and K_c, also referred to as the triplet. [1] The triplet starts with the AUC choosing RAND and then applying algorithms A3 and A8 which creates the SRES and the K_c. The triplet values are transmitted back to the VLR. The MSC associated with the VLR sends the message for the MS to authenticate. [1] This message will contain the RAND. The MS uses the RAND to calculate the $SRES_c$ using algorithm A3 and K_i. K_i and A3 are values that are located in the SIM and are not shared with the MS. $SRES_c$ is then sent back to the MSC which knows the SRES from the earlier VLR message. [1] If the SRES from the MSC and $SRES_c$ from the MS match then a successful authentication has occurred. If these values do not match the MSC will reject the service. If the authentication was successful then the K_c is transmitted from the MSC to the BTS. [1] The BTS and MS will use this value for encrypting and decrypting transmitted information. The triplet is only stored in the VLR so as long the MS is in the area of the VLR. The VLR sends the triplet to the HLR and it is permanently stored and can be automatically retrieved for future requests for authentication without having to require involvement from the AUC. [1] Again, AUC will store K_i and IMSI. RAND is the generation of random numbers by the AUC using values $0 – 2^{128} -1$ and is a 128 bit value. K_c is a 64 bit value and SRES is a 32 bit value. [1] K_i length and format is left up to the discretion of the Public Land Mobile Network Operators (PLMN). [1] Algorithms A3 and A8 are not

completely standardized in the GSM network, which allows the PLMN operators room to choose different versions made by different companies. [1] [3] It is up to the PLMN operators to comply with any nation-state regulations that may exist in their area. At the time of GSM in the U.S. there was strict regulations on encryption methods and may have played a role in how the authentication measures were chosen. These regulations will be addressed in later chapters.

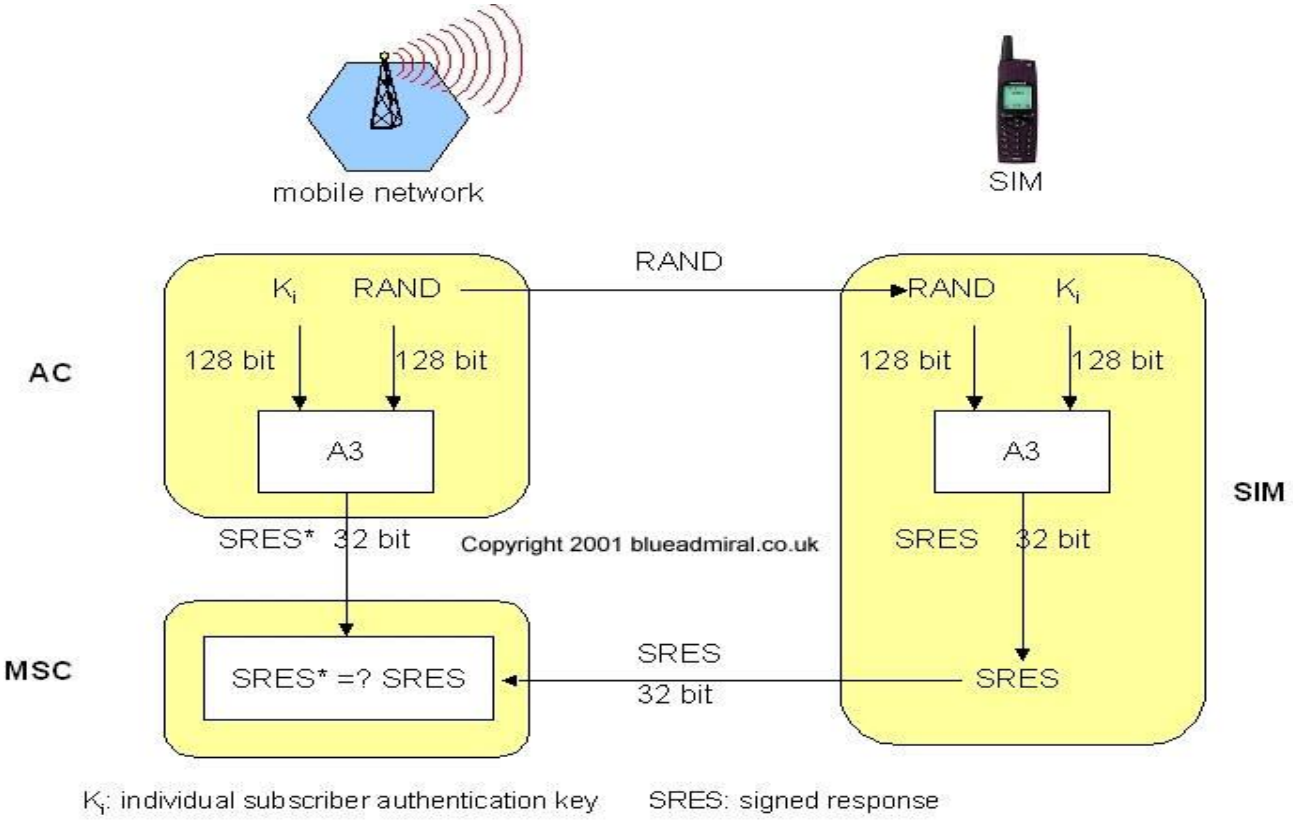

Figure 2 GSM Authentication [33]

3.3 Encryption

After authentication all voice and data transmitted are encrypted. The ciphering algorithm used is called A5. A5 uses K_c as the ciphering key, which as we know, is computed from RAND by A8 using K_i. [1] A8 will always produce a 64 bit value K_c because

if it is less than 64 bits then zeros will be added. K_c is known by the AUC, HLR, VLR, MS, and BSS, but is temporarily stored in the MS and the MSC/VLR. [1] The MSC/VLR sends the message to start ciphering. 22 frame number bits are appended to the 64 bit value of K_c and this value is computed with algorithm 5 which produces modulo 2. [1] Modulo 2 is used to either encrypt plaintext or decrypt cipher text. Just like authentication, this process of obtaining K_c can be initiated at different times according to the direction of the PLMN. A typical implementation seen at its inception was to authenticate at the beginning of each call so that a new K_c is produced and thus each call would use a separate cipher key. [1]

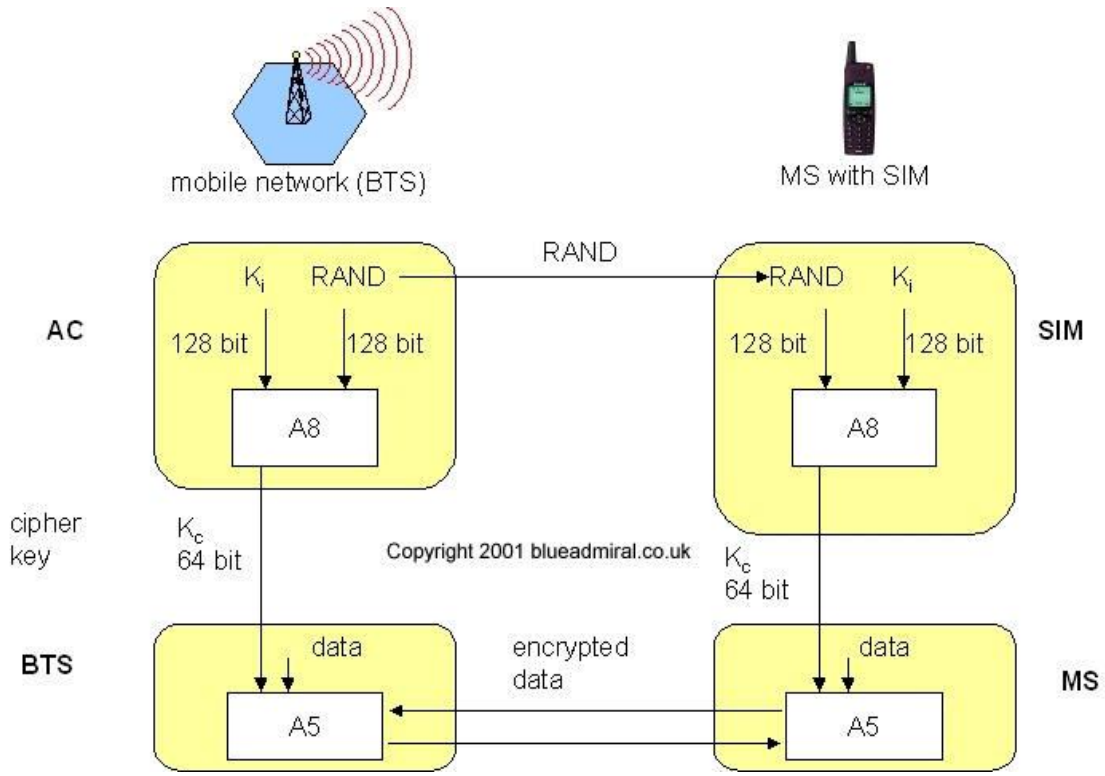

Figure 3 GSM Encryption [33]

Again it is important to note that the encryption process takes place *after* the authentication. Again, at the time of implementation encryption standards were heavily regulated in the U.S.

CHAPTER 4

3G UMTS

4.1 Naming and evolution

We refer to the GSM architecture as 2G, since it was the second generation of mobile communications. 1G was an analog communication that was available in limited areas in 1980. 1G did not have to ability of handovers between towers and did not include any security functions. [3] Most countries were developing different networks in their respective areas. It was the initiative of the Group Special Mobile that really emphasized the need for a collective collaboration of global networking. Even now, GSM is not the standard for all countries but it is the largest and it is the telecommunications network implemented here in the United States. The GSM security work group MOU-SG was fully aware of the security flaw for a Man in the Middle (MIM) attack from a fake BSS being able to connect to a MS but this was considered a very low threat. At the time of implementation the ability to obtain the capital and technology to pose such an attack was considered to be nearly impossible. [1] [3]

UMTS or 3G came out in 2000 and had considerable improvements most notably in end user speed and the allocation of more space available for new users. [3] We have not discussed the protocols associated with speed of service or allocation of space as our focus is with the authentication aspect. By the time 3G was introduced to the market, the technology to imitate a fake cell tower was readily available and a mitigation technique was presented. Mutual authentication during handover was this technique and will be discussed in detail in later sections.

LTE or 4G came out around 2010. Although, 4G is gaining coverage it is still not implemented in all areas of the United States. Even so, the authentication protocol in 4G has not prevented a Man in the Middle attack. The remainder of this document will heavily focus on 3G and reference legacy 2G.

4.2 Mutual authentication in 3G UMTS

There have been changes to the GSM architecture due to the evolution to 3G UMTS. Again, since our focus is the MIM attack only those changes that affect the authentication protocols will be discussed. The backbone of 2G GSM is clearly still in place. The VLR and AUC together are now referred to as the Serving Network (SN) even though they still maintain physical autonomy from each other. The BSS is now considered the Radio Network Controller (RNC). The Mobile Station (MS) is now referred to as User Equipment (UE). The SIM card can still exist in its previous form but it is now called the Universal Subscriber Identity Module (USIM) and may or may not be removable. In many instances it is not removable but is still considered to be a separate logical device from the mobile device. The USIM still permanently stores the key and the IMSI and TMSI. Finally the key is notated now as K and is a standard 128 bit value. [3] Details of why these changes were made are categorized as increasing data speeds, adding macro diversity, and all while adjusting for millions of new users.[3] We will turn our focus to the mutual authentication and encryption methods.

4.3 Authentication

To begin, the USIM will request a location update to the VLR. If this is the first time the UE is turned on, then it will always send the IMSI. If a USIM has already been registered then the TMSI will be sent. For authentication purposes the VLR will send the TMSI or IMSI and look to the HLR/AUC to request the computations take place.
The HLR/AUC conducts the authentication computations and sends these back to the VLR. The VLR forwards the computations labeled RAND and AUTN to the USIM, while keeping other computational data in its temporary storage. [3] The USIM then uses the RAND and AUTN to conduct similar computations. A product of the USIM computation is the RES. RES is sent back to the VLR to compare with the XRES that was stored in the VLR from the AUC. [3] If the RES from the USIM and the XRES from the VLR match then a positive authentication was made and the connection will then continue on an encrypted channel. [3]

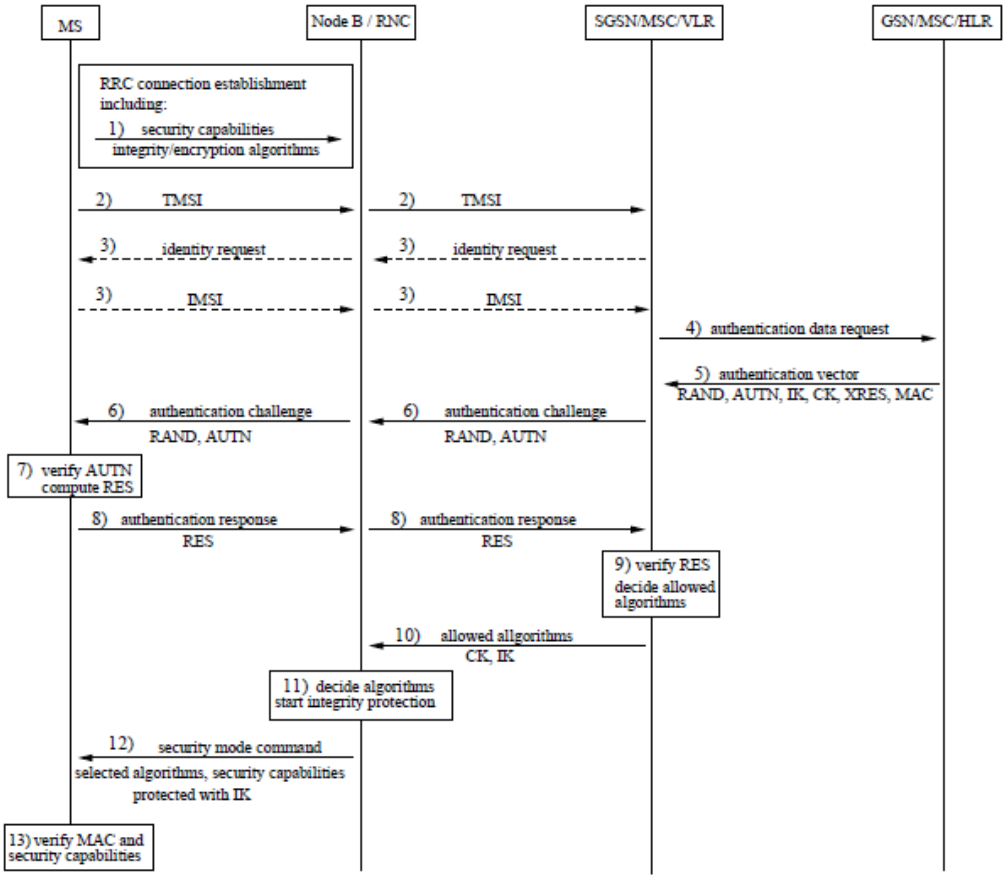

Figure 4 UMTS Authentication [4]

4.4 Computations in authentication vector

The computations in the HLR/AUC and the USIM are used for authentication and the by products are used for cryptography. When the VLR sends HLR/AUC the TMSI or ISMI, the AUC will be able to use the key associated with the IMSI to assist in creating the Authentication Vector (AV). [3] The TMSI is stored as a pointer to the IMSI so sending the TMSI to the database can retrieve the IMSI. The calculations are possible because when the UE, with the IMSI, is purchased; a 128 bit secret key is assigned to it. [3] The IMSI points to this key. Subsequently, a pseudo random generator will create a 128 bit random value called RAND. [3] A sequential value called SQN is chosen as an increasing value to verify the

Authentication Vector is fresh. [3] An Administrative Management Function (AMF) value is chosen and added for billing purposes. Finally, the RAND, the key (k), SQN, and AMF are computed through a cryptographic function 1 (f1) which creates a 64 bit Message Authentication Code (MAC). [3] Concurrently, the RAND and K are sent through 4 separate functions: f2, f3, f4, and f5. F2 creates a 32-128 bit value called the XRES. [3] F3 creates a 128 bit value called the CK. F4 creates a 128 bit value called IK. F5 creates a 64 bit value called the AK. Finally, SQN is added bit by bit to AK, AMF, and MAC to create AUTN. The HLR/AUC then sends RAND, XRES, CK, IK, and AUTN to the VLR. [3] The VLR will store these values in its database. Then the VLR sends RAND and AUTN to the USIM. [3]

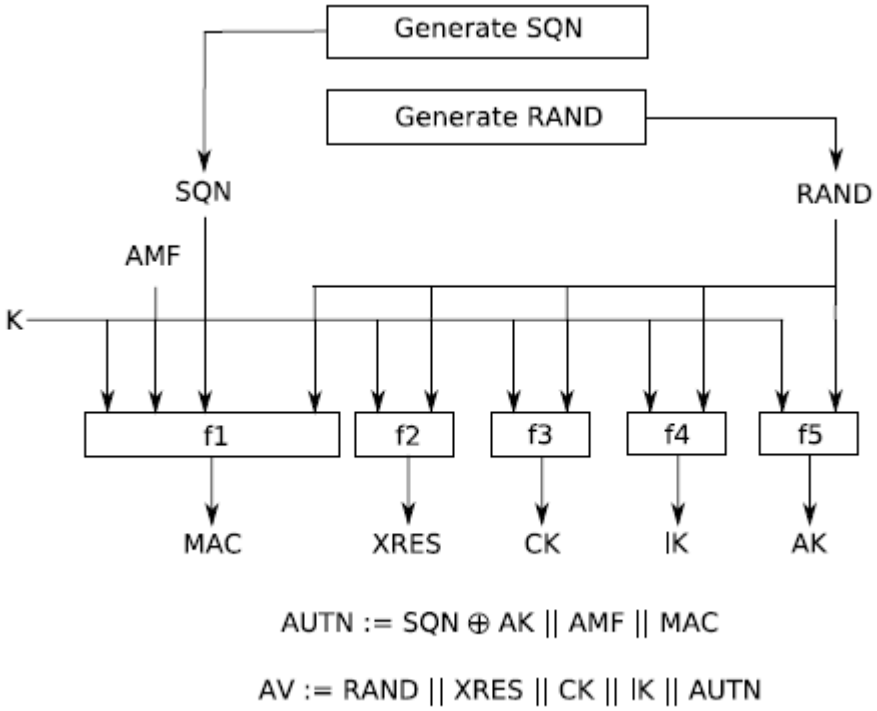

Figure 5 UMTS Authentication Computations [13]

Now the USIM conducts its verification. First, RAND and K are sent through f5 to get AK. Concurrently, RAND and K are put through functions f2, f3, and f4. F2 produces RES. [3]

F3 produces CK and f4 produces IK. After these processes are complete then f1 is used in conjunction with AUTN. Using the information from inside the AUTN, AK from f5 is processed with the concatenated SQN and AK to produce the original SQN. Then, SQN and AMF is sent through f1 to produce XMAC. This is the value that must match the MAC on the network side. [3]

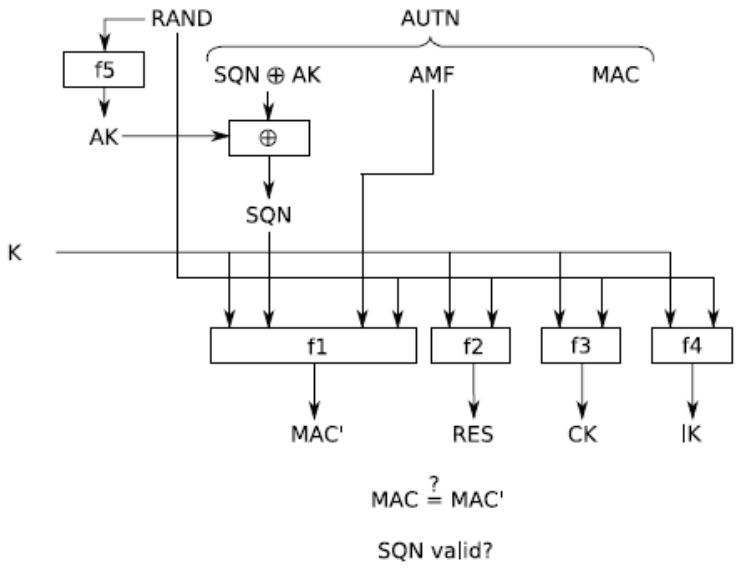

Figure 6 UMTS MS Authentication Computations [13]

4.5 3G encryption

Encryption protocols are developed and deployed based on location. Local authorities, retain the control to set regulations and requirements for cryptographic methods. In UMTS 3GPP R99 an algorithm is defined. [3]

Encryption is initiated after the Serving Network (SN) has calculated the CK and the command to begin encryption has been sent. [3] A stream cipher begins which implements function f8. In this stream, the CK value from authentication is introduced along with a

counter COUNT-C, an identity of the radio called BEARER, a value for DIRECTION, and length are concatenated. [3] These values are sent through f8 and produce a key stream block that is used as a MASK. COUNT-C is used to make sure no plaintext will ever be the same as another plaintext. [3] This key stream also referred to as MASK, can then be added to the plaintext bit by bit to encrypt. This implementation method requires low computational effort. [3] F8 encryption, outlined in 3GPP 35.201. F8, is based on KASUMI which is an older encryption algorithm. [3] Basically, this block cipher takes a 64 bit input and produces a 64 bit output. CK value is the main function for f8. Again, ciphering is regulated at a local level by governments. Ciphering is not mandatory. [3] Ciphering in a government decision. This will play in to issues that arise with constitutionality. Specific issues with the Fourth Amendment will be discussed in chapter 7.

4.6 Review

To review, the HLR/ AUC and the USIM store the IMSI, K, and the SQN after the initial register. SQN, as stated earlier, is needed for the FRESH of the signal, so it is vital this number stays in synchronization. If synchronization fails then the USIM takes priority to update the network to its current SQN. [3]

So we can now see that the mutual authentication is actually verifying that two entities are able to access K and calculate the needed responses. This will become important in the next chapter when the MIM attack is described.

The only static identity that is being used to authenticate is K. [3] The AUC stores the K and is able to retrieve K when the USIM sends ISMI. This means that the K and IMSI are stored in pairs in the AUC database, along with TMSI in case that is sent in place of the

IMSI. The USIM stores K in memory that cannot be accessed by the user but is used in the background calculations.

This is a very important point. Having the ability to access K and complete the functions is the mutual authentication that is actually taking place. In the intended protocol design for 3G UMTS this means that the USIM and the AUC have authenticated each other. When a Man in the Middle (MIM) attack occurs it violates the assumption of these principles.

CHAPTER 5

MAN IN THE MIDDLE

UMTS 3G mutual authentication protocol was thought to have mitigated the threat of a Man in the Middle (MIM) attack. This procedure allowed a mobile device to authenticate the network and be able to disconnect if the correct methods could not be established. [3] Furthermore, even if an entity could impersonate the network it was thought that no useful information could be obtained due to the encryption that followed. [2] These ideas did not hold true. There have been many papers written about the flaw of GSM that continued into UMTS to make a MIM attack not only possible but easy. A majority of the reliable documents that describe MIM attacks in UMTS are printed in publications from the Institute of Electronics and Engineers (IEEE). A document from 2004 describes in detail how an attack on UMTS would work when relying on the authentication protocol. [4] In 2011 a document that addressed many aspects of security with telecommunications and mobile devices had laid out the procedures for a MIM attack with in UMTS [7]. A publication that addresses how mutual authentication can still allow room for a MIM attack was written in 2013 [6]. In 2014 an extremely thorough document was published that described in precise detail how Commercial Off the Shelf (COTS) equipment could be used to conduct a MIM attack on the current state of UMTS [8]. This document included exact names of equipment and how it would need to be set up. There are many more references that are used to show that extensive research has been conducted on the MIM attacks that occur with GSM and UMTS. [12] [13] [5] One of the known commercial producers of this type of equipment is Harris Corporation, which has the Stingray. Harris Corporation does not provide any

information of specific protocols of their equipment and often times require users to sign non-disclosure agreements to protect their protocols. [9] [10] Therefore, next will be a brief explanation of how a fake cell tower Man in the Middle attack can easily take place based on the publications from combined experts who have published with IEEE and other sources.

5.1 Man in the middle protocol

There are many different scenarios to show a MIM attack. Since UMTS was designed to be backward compatible to GSM there exists situations in which you may have a combination of UMTS and GSM equipment. The attack will have a different protocol depending on if the network is GSM or UMTS and if the mobile device is GSM or UMTS. Meyer and Wetzel describe a situation in which the mobile device is UMTS and the attacker is playing the role of a GSM network. [4] This would be a rollback MIM attack and seems to be one of the most effective and intrusive.

To begin, the attacker will impersonate a BS. In both 2G and 3G, mobile devices are programmed to continuously scan for base stations with the strongest signal. They will automatically transfer to a stronger signal if one is found. An attacker will take advantage of this standard by impersonating a tower that is transmitting with very high power to seem as though it is the best signal. For the attack, the fake base station pretends to be a base station to the mobile device and a mobile device to the real base station. [4] The attack then happens in two phases. The mobile device will attempt to connect and will send the TMSI. [4] The fake BS will send the TMSI to the real VLR. If the real VLR cannot locate the TMSI then the request for IMSI will be sent and the fake BS will pass this to the MS. [4] The real VLR does what it is supposed to do and send the IMSI to the HLR/AUC. Once the correct calculations

take place the real VLR sends RAND and AUTN to the fake BS. At this point the fake BS then can disconnect from the real VLR. [4]

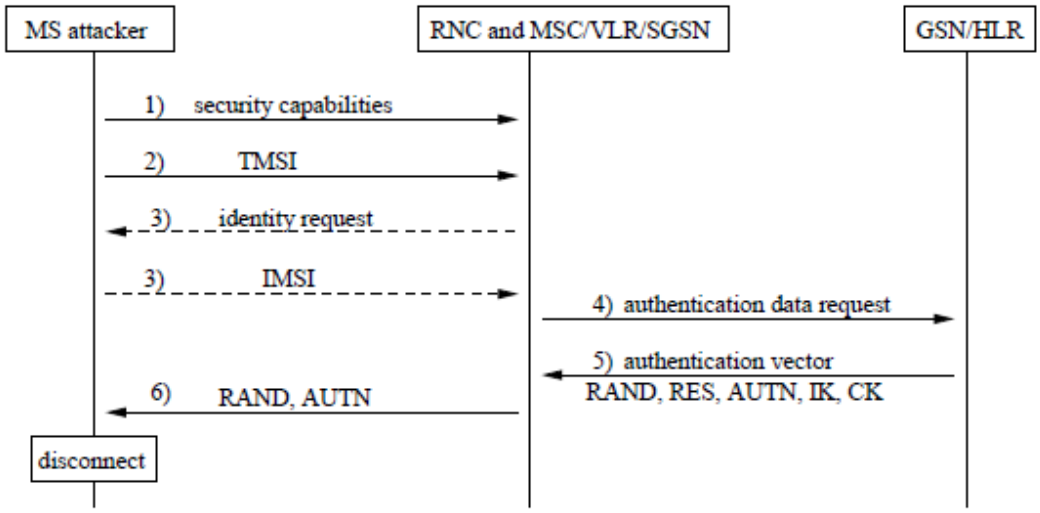

Figure 7 MIM Attack Protocol to Network [4]

Phase two now begins. The fake BS will then send RAND and AUTN to the mobile station. This will only work if done very quickly so as not to expire SQN. [4] The MS then conducts the correct calculations and sends back a valid XRES. The fake BS will then accept the XRES and request the MS use no or weak encryption. [4]

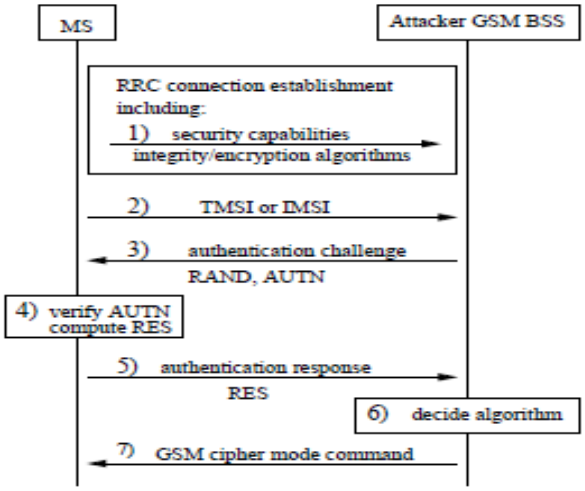

Figure 8 MIM Attack Protocol to MS [4]

As you can see with this protocol, there is no real network that the MS can use. To rectify this if the fake BS has a valid IMSI it could stay connected to the real network and use this to provide service to the MS. [4] This set up would allow for real service but cost the attacker real money since the charges of the MS would be billed to the fake BS IMSI. [4] This would allow the fake BS to continue to be in the middle when the MS placed calls, sent messages and much more. [4] [13] [8] Essentially, once the MIM attack has occurred other attacks are much easier to deploy. The government is not just taking advantage of this flaw, they are creating the flaw through the regulations and then exploiting it. This could backfire since as technology has advanced, it has become much easier and cheaper to reproduce this equipment.

5.2 Proposed solutions to MIM attack

The earliest published document found that addressed the MIM attack on UMTS was in 2004. [4] At the time of this writing, 11 years has passed and no solution has been implemented. Nearly the entire world either uses GSM, or communicates through GSM architecture. It is difficult to believe that preventing a MIM attack has stumped experts for 11 years. As we dig deeper, it seems there have been more papers published that address fixing the authentication vulnerability than there are explaining how the insecurity works. Some experts suggest that the IMSI / TMSI number that is sent over the clear be replaced with a non-relevant number. [6] [15] [13] [18] These options rely on the preexisting structure and therefore no expensive changes would be required. Some experts offer a new system that implements Public Key Infrastructure (PKI). [19] [16] [17] [18] PKI is a method that is already implemented in some internet exchanges. PKI relies heavily on a network of trust since the issuing authority of the keys comes from a third party. [20]

There are known problems with PKI, mostly due to the requirement of trusting a third party. With that being said, this method has been generally successful in the internet arena. When a new security concern presents itself, in internet PKI, experts in the field implement fixes and small scale restructuring.

Changing the IMSI / TMSI number that is sent over clear air will undoubtedly mitigate a MIM attack. There have been many practical examples of this working for the current MIM attack. [6] [15] [13] The problem with changing the IMSI number to a non-relevant number is that at some point attacks will be able to break this. All the methods presented were practical and well thought out but with protocols that happen prior to encryption, only time is needed for a determined attacker to find a way through. [20]

Since this MIM attack in the authentication vector has been known the fixes started rolling in from experts in the field. Yet, only a mitigation technique, mutual authentication, was implemented and did not prevent a MIM attack. So why have no other solutions been implemented? We can be assured it is not due to lack of solutions being available.

Once we analyze U.S. regulations, we will see that this security flaw is used to collect intelligence by the FBI and law enforcement. This type of surveillance is called Lawful Interception and has been an important piece of operations for some time. These regulations utilize the security flaw to further Lawful Interception.

CHAPTER 6

GOVERNMENT INVOLVEMENT

6.1 Standardization of 3G UMTS

3G UMTS was built first and foremost to comply with known and anticipated Lawful Interception regulations: not security, speed, or reliability. [3] Standardizing telecommunications for the movement from 2G to 3G fell to an organization called 3GPP, or 3rd Generation Partnership Project. [37] This organization brought together seven standardization entities from many different countries to develop the next evolution. America's representative was an organization named ATIS. The other countries that developed these new standards are: ARIB from Japan, CCSA from China, ETSI from Europe, TTA from Korea, and TSDSI from India. [37] This evolution consisted of many working groups and security was a concern. 3GPP representatives took into account Lawful Interception as a backbone element and a high level of consideration was given when creating the new design. Exactly what decisions came out of the consideration for Lawful Interception is unknown. [37] Encryption was also developed but the method is only a suggestion not mandatory. [37] As stated in previous sections the mutual authentication standard was added as part of the 3G UMTS evolution. We can see that the mutual authentication protocol in the authentication vector added a mitigation technique while leaving room for a roll back attack at the very least. With experts from seven different countries all evaluating and developing new standards it is hard to believe that this type of attack was simply overlooked but rather it was intentional to assist in Lawful Interception. It is not baseless to make that claim since we know the governments use this as a technique for

Lawful Interception. Also, we know that the vulnerability has been widely publicized since 2004 and no further modifications have been made to deny access to the roll back MIM attack. Since Lawful Interception is specific to each country's government, the answer to why this attack is still possible might be found in an analysis of the United States' regulations.

6.2 History of regulations

Government agencies such as the FBI, NSA, U.S. military, and local and federal law enforcement have long realized the importance of collecting intelligence. Collecting intelligence, in this sense, can be viewed as obtaining any information that would lead a person of authority to make a more informed decision. [41]

As many civil rights organizations remind us, the 4th amendment of the United States Constitution has highlighted the distinction between government agencies collecting intelligence on domestic and foreign interests. [20] [21] It has long been established that government agencies need a warrant prior to any invasive intelligence collection on U.S. people.

Lawful Interception is one method that the FBI and law enforcement use to collect intelligence on U.S. people. The idea behind Lawful Interception is lawfully obtaining communications data for analysis that can prevent a crime from occurring or act as evidence. [35] To fulfill the lawfulness of intercepting communications a warrant is the means. There are four different courts that may issue this type of warrant: federal, state, local, and FISC. Federal, state, and local courts have been in the public eye for many years. The Foreign Intelligence Surveillance Court (FISC) was established with the Foreign Intelligence

Surveillance Act in 1978 as a secret court. [35] The court has the ability to govern the intelligence collection of U.S. people that may lead to intelligence of foreign powers. [35] If served a warrant from a FISC, you would be mandated by law to keep this secret. [35] Although heavily redacted, an example of an order from a FISC can be found at [36].
The idea of Lawful Interception is a theme throughout many countries although its implementation will differ. For the United States these regulations are embedded in the Communications Assistance for Law Enforcement Act (CALEA) and title 47 of the Code of Federal Regulations. CALEA was passed so that telecommunication carriers could not implement designs in architecture that would prevent Lawful Interception but also not impede free market telecommunication evolution [21] [22]. So as natural evolution occurred in telecommunication architectures, carriers would then be responsible for development of complimenting designs that would allow wiretapping and assist in the collection of Meta data information. The regulations that assist in collection of data for the government actually hinder experts in the field from implementing security designs that would prevent MIM attacks. This idea will raise possible issues with the Fourth Amendment and will be addressed in chapter 7.

A brief history of how these regulations came about will help define their broad nature. GSM is a company based out of Europe and set the initial standards. To make GSM more appealing to countries with various political structures the intent was to leave a majority of the security decisions up to the telecommunication carriers and governments.[1] [3] From there, democratic governments have typically taken the lead with not for profit organizations conducting research and implementing designs in conjunction with telecommunication carriers.

A good starting point is with the European Telecommunication Standard Institute (ETSI) which was founded in 1988 by CEPT. [26] Remember, ETSI partners with 3GPP to develop standards for current and future telecommunications. Though ETSI is located in France and under French law, their 800 members are from 64 countries. Their main focus is to facilitate trade through interoperability. [26] ETSI has numerous working groups that specialize in various fields which require a very high working expertise. For example, Security Algorithms Group of Experts (SAGE) focuses on development and implementation of a variety of encryption methods. [26]

American National Standards Institute (ANSI) controls many of the same aspects for the United States. ANSI is also a not for profit organization and boasts that they have several government agencies as well as 125,000 companies as members. [25] They have several subcommittees and working groups that deal specifically with telecommunications. Some high profile groups that ANSI is a part of include: International Telecommunications Union (ITU), International Organization for Standardization (IOS), and the International Electrotechnical Commission (IEC). [25] Some independent outside agencies such as IEEE are also utilized to advise ANSI. In 1955 ANSI produced a technical manual T1.413 and then in 1998 they updated the version of this manual. [23] The technical manual further defined how the telecommunications systems would be implemented in the United States to include Lawful Interception yet did not define the details behind a MIM style collection method.
In 1994 U.S. Congress passed the CALEA legislation. [21] [22] This law is now the leading point of authority specific to Lawful Interception. So now we view CALEA as the legislation that must be obeyed and ANSI as the specification standards on how to implement those standards. As with many specialized laws, a regulatory agency was appointed to oversee and

define specific applications of this law. [21] This regulatory agency is the Federal Communication Commission (FCC). It would benefit us first to further define CALEA and then analyze the role the FCC plays.

CALEA was designed to assist law enforcement to intercept the content of a user's communication. This meant that telecommunication carriers would need to comply with this law and implement designs to assist law enforcement to be successful with interception. Under CALEA, telecommunication carriers can be punished for not providing assistance to an agency's interception capability. [35] The carriers must also provide any encryption keys that they implement but are not fined if a user is in possession of encryption that is not provided by the company. [35] No single law could anticipate the evolution of telecommunications therefore the law was written with broad language to encompass these changes. So when when a new technology comes out to assist law enforcement with interception, the FCC, not the judicial branch, evaluates this technique. All techniques are subject to a judicial review if contested. [21] [22] Any method that is deemed compliant with CALEA is subject to the law. One becomes CALEA compliant by regulations established by the FCC, specifically title 47 of the Code of Federal Regulations. [24] Title 47 of the Code of Federal Regulations is document with hundreds of pages of limits, requirements, and attempts to set goals for CALEA among other standards. [21] [22] The FCC is the final authority of what provisions are set. The important note here is that the FCC decides what techniques are used in lawful interception which is used by local police and the FBI. The FCC maintains the right and responsibility to continuously update regulations to keep up with technology specific to Lawful Interception.

The steps that must occur for the FCC to update the requirements for Lawful Interception is fairly straight forward yet the process has been investigated for flaws. [21] The FCC will post a Notice of Proposed Rulemaking (NPRM) in the Federal Register. [21] This will then go through an analysis period. During the analysis period experts can evaluate and comment on the proposed rule change. [21] The FCC then issues a final rule that is updated in the Code of Federal Regulations. [21] [22] In the past, the FBI has filed NPRMs and this has been hotly contested as a conflict of interest. [22] This controversial move by the FBI has been debated in the public spotlight with civil rights unions but there has been no official judgment on the legality. [21] [22]

6.3 How we know the government uses MIM attacks

We can be positive that the FBI and local law enforcement use the MIM attack as a CALEA compliant method, due to some recent revelations. In 2012 the Electronic Frontier Foundation published a document reporting on a legal action they were pursuing against the FBI for allegedly not releasing proper information about the use of a Stingray, which is a name brand of an IMSI catcher used in a MIM attack. [9] This document and the legal action created an interest into what actions and abilities the FBI and local police have to intercept communications, which eventually lead to a response from the Department of Justice.
In 2015 the Department of Justice released policy guidance titled ‘Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology’. [28] This policy guidance was one of the first official documents that acknowledged the use and criteria for the MIM attack.
The Electronic Frontier Foundation (EFF), a civil rights organization, has closely followed CALEA and its controversies. With our focus solely on the MIM attack, their work has shed

light on how the FBI and local governments use CALEA and Title 47 of the Code of Federal Regulations to conduct a MIM attack. The EFF filed an amicus brief, in 2012, to suppress evidence collected in the criminal case: United States of America v Daniel Rigmaiden. In this situation the federal government used a fake cell tower to collect the location of the suspect. They also used the fake tower to collect intelligence that lead to his arrest. The argument was that the judge who issued the warrant had no knowledge of how intrusive the means to obtain the information was, since the specific details were not given. The judge was not told that the law enforcement even had the capability to conduct a MIM attack. Therefore, the judge did not have all the information necessary to make the decision to issue the warrant. Also, the EFF focused on the fact that while collecting information on Mr. Rigmaiden, they subsequently collected information on numerous other devices in the area.

This case, along with the Patriot Act being put in the spot light, prompted the Department of Justice to take action. The Department of Justice exercised their power of oversight and set a policy to reign in use of the MIM attack with a policy entitled 'Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology'. [29] This landmark announcement was made on September 3, 2015. Initial analysis of the guidance has been conducted but the true implementation of the policy will certainly unfold in the months and years to come. This policy restricts the fake towers to be set in 'pen register' mode only and not collect contents of communications. [29] The policy also states that the GPS function is not to be used. The policy adopts the idea that the location GPS function has never been authorized for use. [29] If this is the case, one can only assume that triangulation or a well-known vulnerability in the SS7 network is used to identify the location, since location identification was used in the case of the United States of America v Daniel Rigmaiden . [61]

[9] [10] Finally, this policy allows for ‘Exceptional Circumstances Where the Law Does Not Require a Warrant’. [29] It is unclear at this time how that will be interpreted and enforced. Another reason that we can be sure the MIM attack specifically is being conducted is that the technology costs a great deal. To offset the cost to the telecommunication carriers Congress has approved a method to compensate carriers for their expenses. Therefore the government uses tax dollars to pay for carriers to provide interception services. In most cases we can track the tax dollars that are spent on IMSI catchers. You can review some of these charges in the yearly report to Congress from the Administrative Office of the United States Courts. [22] A wire tap report is also posted yearly on the United States Courts website. [27] This report consists of the names of the judges that are authorizing wire taps, locations, days of operation, and many other details. The earliest report published was dated for 1997. Although, wiretaps may include MIM style attacks, the methods are not released here and do not include PEN trap wiretaps. A PEN trap wiretap is the collection of just the numbers dialed on devices but no communication data. [39] It is unclear if any of these reports include any MIM style attacks since they are now required to operate under PEN register mode only. Opponents of the MIM attack seem to reiterate some key points. Even though there are no published specifications on how a fake tower works in an official manner with the law enforcement, we can use the knowledge from IEEE and other experts to determine: there is no feasible way to only trick one USIM into connecting to a fake tower, while leaving other devices connected to the real tower. The fake tower *must* act like a real tower to all USIMs in the coverage area. Therefore, every phone that sees this fake tower as the best signal will undoubtedly connect. This brings concern to constitutionality. Secondly, this type of MIM attack is not well known due to classification labels of the FBI and the non-disclosure

agreements made with local law enforcement. [10] [9] [31] Therefore, obtaining a warrant from a knowledgeable judge would be difficult. A judge would need an extensive explanation of the data actually being collected and the methods that allow that data to be obtained to understand the full ramifications of issuing a warrant. There is also the idea that an act conducted for National Security reasons may not need a warrant at all. This idea may delve into the Patriot Act, or more recently the Freedom Act, and is beyond the scope of this paper. There have been several news stories on major news networks about the FBI possibly having fake cell towers in place to conduct MIM attacks. [10] [11] [12] [29] [30] [31] [35] [36] It has also been reported that the FBI uses airplanes that fly around with an IMSI catcher to assist in MIM attacks, referred to as DRTboxes. [34]

So the conflict we see in the use of fake cell towers that lawfully collect intelligence of U.S. people is broad. There is an understated tone that people expect to be protected by their government, at the same time, they do not wish to give up certain rights for that protection.

To summarize the conflicts of the use of the MIM attack we can first begin with knowledge of its use. Very little is known about how the FBI and law enforcement utilize this technology. With that being said, it would be difficult to find a judge with the proper information to make an informed decision on what the warrant being issued will actually be capable of allowing.

Second, when a fake cell tower is used to intercept communications, there is no discrimination on what phones are initially collected on. This is a drag net style collection on communication which has been a hotly debated conversation since the revisions of the Patriot Act / Freedom Act. The point being is that the IMSIs that are not included in the warrant may

not have a legal basis to be collected on. It has been a topic of conversation that once an IMSI has been identified as a target, it is possible to initially collect all IMSIs from an area and then release any unwarranted IMSIs. [34] Although with this method it is assumed that a positive identification is already made on the IMSI and the targeted user. If this connection is unknown, the only way to find the connection would be to sift through all users until the desired target is found. This will again bring forward questions of the constitutionality of the collection method.

Finally, the vulnerability alone, which is established in the authentication vector, does not stipulate when and who can collect information. It is possible that only the FBI and law enforcement collect intelligence information on U.S. persons and only after they get an appropriate warrant. Yet, the vulnerability is always there so anyone at anytime can collect intelligence on anyone in the coverage area. There is a push by civil rights organizations to change the legislation on how government agencies are allowed to operate when it come to intelligence collection on U.S. people. While regulation may reign in U.S. government agencies, the vulnerability will be need to addressed specifically.

From the current state of regulations, legal actions, media coverage, and civil right organizations research, we can be assured the government is using the MIM style attack. The vulnerability in the authentication vector gives the technical ability to conduct the attack. The regulations give the legal authority to do so.

When looking to the future in the realm of securing information we must not be short sighted and only focus on the regulations or vulnerability. I will propose we take in to consideration a four point approach to policy reform of the MIM attack. This approach will be able to address all aspects of concern. Once each of these points are addressed then

recommendations can be made to reform CALEA, Title 47 of the Code of Federal Regulations, warrant procedures, the vulnerability, and privacy law. At this point we can also have an understanding of base guidelines for future security procedures.

CHAPTER 7

POLICY CONSIDERATIONS

Up to this point we have established the fact that a MIM attack is technically possible. Regulations have clearly established the atmosphere for a MIM attack to fit into a category of Lawful Interception. Now it is time to take a closer look at the issues that arise with these two established points.

We can fit the concerns of these established points into four policy considerations: Constitutionality, Oversight, Vulnerability, and Protection.

7.1 Constitutionality

Constitutionality in this sense has several meanings. First and foremost amendment 4 is traditionally quoted for the mechanism of protection.

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."
[46]

This right guaranteed to U.S. citizens of unreasonable searches seems to contradict the process in which the MIM attack works. When an IMSI catcher, such as a stingray, is activated there is no way to selectively search for only the information related to the USIM in which the warrant was obtained. The seizure of the information obtained has recently been addressed. In the Policy issued in September 2015 it was stated that any user data collected outside of the warranted data must be deleted once the intended user is found or at minimum

once daily. [28] [29] Although, there is no guarantee of recourse or suppression for a user whose data may have had their rights violated. [30]

Constitutionality also involves interpretation of past cases which is difficult to apply in areas of technology. Today cell phones have the same and often times more capabilities than that of computers, containing bank information, years of emails, medical records, password files, legal accounts, and movement tracking information. Only recently in June 2014 was the issue of unwarranted searches and seizures of cell phone data been addressed by the high court. [58] The Supreme Court officially voted 9-0 in the case Riley v California in favor of making warrants mandatory prior to searching a cell phone that has been seized by a person who has been arrested. [58] There is exclusion to emergency circumstances in such cases as a kidnapping or immediate bomb threat. [58] Yet, when a fake cell tower is operational there is no ability to only choose to collect information on the user that the warrant was issued for. It is possible to sift through this information and release certain devices but the initial collection would from all devices in the coverage area. It is also not apparent when the initial collection happens what information is exactly being viewed to make the determination of the user. Is it legal to collect the IMSI and view billing records, email, or user data? How is the determination of the user made?

Therefore the legal interpretation of capabilities will need to be further defined prior to regulation reform to prevent assumptions. A team of legal experts with a technical back ground would be needed for a comprehensive analysis. This definition will need to be a living breathing definition and constantly change with new technology and terms.
There are many legal arguments that will take place as to how to interpret the fourth amendment in application. It is clear from the regulations implemented by CALEA and

lawful interception that the U.S. government plays an active role in maintaining insufficient communication standards in an effort to exploit them. Many interpretations of CALEA state that if an advancement in technology is made, that a concurrent ability to allow interception of communications must also be achieved prior to its implementation. Therefore a security measure to disallow a MIM attack must be followed up by another method to allow interception. So in this sense the insecurity of the authentication vector is not a ‘problem’, it is doing achieving what it was intended to achieve.

We have established that the government is not just exploiting a vulnerability in a third party system but actually setting the blue print through regulations, policies, and law. This idea is important for several reasons. It is possible for a defense to be made by the government that the telecommunication carriers are a private third part and therefore have given third party consent. This would not be an appropriate defense because the design of the system is not entirely controlled by the private third part telecommunications. They are bound to reduce security standards if they impede the ability of lawful interception.

Judges in state, local, and federal court have been known to not receive all the information about the MIM style attack prior to issuing a warrant. It is vital that a judge be aware that specifically the MIM style attack will be used because during the attack it is impossible to collect Meta data only on the individual a warrant is being issued for. Only at that point can a judge make an informed decision on if any issues with the Fourth Amendment are raised. If the information is not presented to a judge any Fourth Amendment issues cannot be addressed.

Even if the warrant was issued with full disclosure there is always the concept of the plain view doctrine. If a check point is set up on a road and everyone who passes is stopped

for a brief moment and law enforcement find drugs in plain view then this would tend to be permissible in court. I would argue that this does not hold the same value in the sense of the MIM attack. The policy released by the DOJ states that only Meta data will be collected and that any person's information outside of the warrant that was collected on should be released within 24 hours. This policy would make it difficult to use any information in plain view for a subsequent case. It would take some work beyond plain view to interpret the type of data being collected. This work would be beyond the scope of plain view. The work may consist of relating phone numbers from the device in question to other devices, searching billing records that are located using the IMSI, time and duration of calls describing who was on the other end of the line, and tracking the location. This type of work would extend well beyond plain view. There should be a specific policy to state exactly how plain view should be dealt with if the situation does arise with the advancement of technology. Of course, this policy can also change as the evolution occurs in telecommunications. It would be my argument that because of the work needed to make sense of the Meta data and the reasonable expectation of privacy, no criminal activities in plain view are applicable in the MIM attack.

It would be a mistake not to address the idea of reasonable expectation of privacy. This idea is one of the cornerstones for the Fourth amendment. It could be argued that there is no reasonable expectation of privacy since the telecommunication infrastructures offer up this style of attack through design. I will again emphasize that this design is not solely constructed by the telecommunications carriers due to CALEA and the FCC. Therefore, it should not be accepted that this design flaw is intentional by the carriers or that a security solution would not be implemented if not for government involvement. Actually, through

IEEE we know that the contrary is true. There are designs that claim there is a technical solution. [6] [13] [15] [16] [17] [18] [19]

Secondly, an expectation of privacy can be seen to evolve through G1, G2, and G3. In G1 no security measures were put into place whatsoever and the signal was more broadcast based. There was little to no expectation of privacy with this type of implementation. With G2 the concern for privacy was addressed and authentication and encryption methods were established. At this point regardless of the flaws an expectation of privacy was established. To further the case for expectation of privacy, a mitigation technique was implemented to the design with 3G. This mitigation technique attempted to authenticate both the tower and the mobile device to mitigate attacks. We know that this mitigation attempt was not fully successful but a flaw in the system does not necessarily reduce the expectation of privacy. It is actually more important at this point to add further security measures so that we can protect the expectation of privacy. There is no benefit to the government or users to allow cell phones to be attacked due to a lack of expectation of privacy. This idea has the potential to risk national and state security.

Laws on the implementation of MIM attacks can happen at the local, state, and federal level. National security is not the only reason the MIM attack takes place. States and local government use the MIM attack in criminal cases. It would easier to have federal legislation regulate the use of fake cell towers with a federal law but that is not necessarily how we can implement change. Each state will have their own set of laws that will govern how the MIM attack will be applied in criminal investigations. Each state has the opportunity to set the standard and attempt to mitigate the improper use of the MIM attack. While the states cannot change CALEA, which will ultimately allow the security vulnerability to be

fixed, they can implement laws that will reduce the dependency on the fake cell tower. More importantly the states could potentially have cases that question whether or not a violation of the Fourth Amendment occurred. This could end up in the Supreme Court and end up setting a precedence for future fake cell towers. States may also make their own determination of the law and restrict their state and local use. This is potentially the vehicle in which we will see the first step towards policy and legal change.

Overall the constitutionality of specifically the MIM attack has not been completely reviewed by a high court. [22] [30] Thus we should reject the temptation to label the attack or the collection unconstitutional but rather work toward policy reform. Policy reform will give guidance on how to conduct future operations. This will allow the experts in that field to make informed educated decisions that will create the ground work for future cases.

7.2 Oversight

In Baltimore, Maryland a judge threatened an officer with contempt for refusing to testify about the phone collection device that was used in a case involving robbery. The officer believed the department had signed a non-disclosure agreement with the FBI for the phone collection device. [47] In the end, the officer did not testify, and the prosecution removed the evidence that the phone collection device presented.

This police officer was threatened with contempt if he did not reveal information that many believe should have been included in a warrant request regardless of the existence of a non disclosure agreement. It is also a testament to how difficult it can be for a judge to gain the knowledge needed to make informed decisions about what is being authorized. This is also one example that highlights the lack of oversight this type of attack can encounter. To be

able to protect constitutional rights you must be able to provide some type of oversight with a review process to investigate cases where an injustice may have occurred. The police have a duty to request a warrant and be beholden to the judicial branch when it references the collection of the intelligence listed in the fourth amendment and this concept has long been established.

It is possible, in the case above, that a secret warrant existed. This warrant would have been issued by a FISA court. The FISA court, at its inception, was intended to be the oversight for surveillance conducted by government agencies. The FISA court was created to hold government agencies accountable to request warrants prior to surveillance, which would prevent unlawful interception. [48] This court deals with classified information and the warrants requested can deal with electronic interception of U.S. people whom may have information on foreign powers. [35] Because of the nature of the requests its legacy has been secretive. Most court opinions are redacted and details on decisions can be completely hidden. Many civil right organizations have shed light on this secret court as being one sided. [49] For example in 2011 government agencies applied for 1,676 warrants to the FISA court. [48] All the warrants were approved. In 2012 government agencies applied for 1,789 warrants. [48] All the warrants were approved. As we dig a little deeper, the FISA court has only rejected 11 total requests for warrants from 1979 to 2013. [50] During that same time period over 34,000 warrant requests were made. [50] This is a 99.97 chance for approval. The Supreme Court is able to hear certain cases that may arise with a complaint against the FISA court. The Supreme Court receives approximately 10,000 total requests for review per year and only hears 75-80 of those. [52] As of 2013, no FISA court case has ever been heard in the Supreme Court. [50] Since the decisions of the FISA court are classified there is no

way to review the requests. These warrants directly impact the ability of the FBI to conduct a MIM attack by granting the legal authority to do so.

Do to the approval rate of the FISA court to issue warrants over the last three decades and the atmosphere of secrecy, policy reform will need to include a restructure of oversight that takes into consideration the classified nature of these cases. This restructure must include a viable review process that is readily available and must contain technically and legally savvy individuals who can maintain to utmost impartiality.

7.3 Vulnerability

As stated previously the technical aspect of the vulnerability has been addressed by several experts in the field. Our focus to this point has been on the network being updated to include security protection measures.

In the spirit of private business, companies have responded to the concern for privacy by looking beyond the core network for a solution. There now is in existence a cellular device that attempts to prevent the vulnerability in authentication vector. Two of these phones are the GMSK Cryptophone and the Black Phone 2. [39] [40] These devices boast that they will send an alert or outright disallow a fake cell tower connection when it is attempting to turn off your encryption or lower the standard of the encryption, which we know is part of the rollback attack. [39] [40] Also, upon purchase and set up of your device, encryption is established at the very beginning and is not allowed to be removed in the communications process. [40] The entire connection to the cell tower is encrypted. These companies do not follow the same rules that fall under CALEA because they are not telecommunication carriers, they only provide the device and do not promote any carriers.

[39] [40] There are no telecommunication carriers, which I am aware of, that offer these style of crypto phones. We can assume this is due to the CALEA regulation. A drawback of these phones is the price. These phones can range from $799 to $1300 and higher per device. Another technique that is effective to defeat the fake cell towers is to use what are called burner phones. This method is simply buying several disposable prepaid cell phones at cheap prices and throwing them away so they cannot link the user and the IMSI. This method has been stated in the media to have been used in several terrorist attacks in recent years. With these two methods we can see that with little to no technical knowledge and a few hundred dollars, someone who is cognizant to the vulnerability and has the desire can arrange work arounds.

An aspect of the technical vulnerability that has made headlines is the inability to prevent unwarranted MIM attacks. If the vulnerability continues to exist in the network, there will be millions of phones that will be able to be collected on at any given time regardless of the work arounds, since the majority of people do not own a Cryptophone or employ the use of burner phones. With this vulnerability in place inside the core network, there is no way to prevent who will be doing the collection.

A proposed technical solution would be to allow PKI to be implemented in the authentication vector. In this method it would fall on the telecommunication carriers to provide the private key. By providing the private key they may also store this key and provide it to the FBI or law enforcement in a Lawful Interception event. This would allow the telecommunication carriers the ability to implement a security design that would secure the authentication vector while still allowing lawful interception to occur.

Another proposed solution would be to replace the IMSI number with a non-relevant number. This solution would make it harder for fake cell towers to conduct a MIM attack. Specific information would need to be obtained from telecommunication carriers about the IMSI for a MIM attack to work. The FBI and law enforcement would no longer have immediate access to cell phone information in this scenario. A warrant would need to be issued and orders given to the telecommunication carriers on what information would be needed to make this attack possible.

If our government can conduct a MIM attack on phones to collect intelligence then so can enemies of the state. Fake cell towers can be the size of a real tower and collect hundreds of users or can be as small as a suitcase or vest and collect on the few that might be in the coverage area. [21] [22] [9] [10] With that being said, when policy reform takes place a special consideration should be placed on whether or not this vulnerability is actually making us more secure or leaving Americans open to foreign and domestic attacks.

If we allow the vulnerability to continue to exist in the authentication vector, we can no longer claim ignorance that it leaves millions of phones open for interception by unknown agents.

7.4 Protection

Protection is the most controversial topic of the four. Finding the social equilibrium of security and privacy protection might be considered a bridge too far. Yet, the real problem comes when we become dispirited and stop chasing the idea that a common ground cannot be achieved. Perfection may never be obtained but when we decide to settle for one side or another then we will inevitably stand further from the goal. So in the spirit of finding a

common ground we will aim high and make an extreme case for both sides so we can venture closer to a middle ground.

From 2000 to 2014 there have been 392 reports of terrorist attacks on North America. [54] On 9/11/2001 in just one of those attacks; 2,759 people were killed and 8,700 people were injured. [55] The government is looked upon to provide the protection to their citizens and prevent this type of attack from happening again. To date, since 9/11, there have been several more attacks. From 1865 to December 3, 2015 there have been approximately 5,105 people killed in attacks labeled as terrorist attacks and 22,197 people injured in these attacks. [54] (Values of 0 were replaced for unknown.) The United States went to war in October 2001 and will be entering year 15 shortly with no successful end in sight. Intelligence collection is used to anticipate the moves of attacks on not only war mobility but to prevent attacks on U.S. soil. Intelligence collection is a strategic necessity. Some people who have no terrorist ties will have their information compromised by the government just simply by mistake while in the process of trying to locate the threats.

An important point brought up by the director of the NSA about programs that are similar to the MIM attack, is that these collection methods don't just protect the U.S. from terrorist attacks. Intelligence collection can be used to locate and prevent human trafficking, drug rings, nuclear weapons advancement, and other nation states that are posturing for war. [56] There are some nefarious people, nation states, and world changing events that are occurring all the time and governments need to be able to stay abreast of this to protect its citizens. Intelligence collection is not a full proof method but it gives people of authority a

better battle field view of how to implement protection. No number can be given to estimate the amount of people protected from information gathered by this collection method. Bradley Morrison of the FBI stressed the importance of the secrecy of these types of attacks as well. Mr. Morrison is a Supervisory Special Agent and worked as the Chief in Tracking Technology in the Operational Technology Division in Quantico Virginia. [57] He was deposed and in a statement confirms the use of non disclosure agreements with local law enforcement. [57] The argument he makes is that if criminals become aware of the technical specifics of the fake cell tower attack then they will begin to find ways to circumvent the attack. This will lead to less successful intelligence collection and possibly put lives in danger. [57]

Yet many critics of the U.S. surveillance program use the term ‘surveillance state’ to describe what could or is happening to the U.S. when these types of programs are in place. Dr. Hubertus Knabe the Director of Berlin-Hohenschonhausen Memorial spoke on a Ted Talk about the Stasi secret police. The Stasi used intelligence collection to the effect of being considered a surveillance state. [53] The Stasi also collected intelligence on Dr. Knabe for transporting books, which was a crime at this time. If we analyze the Stasi, a known surveillance ‘state’, we can have a better understanding of how intelligence collection can go awry.

A few highlights from his speech emphasize information gained from wiretaps and how the Stasi used that information. Dr. Knabe went on to explain that he, as well as many historians, have studied the actual documents that came directly from the Stasi, which was a secret police state in full affect by 1953. [53] At this time cell phones and the internet did not

exist but the collection was impressive. Telephones were wire-tapped, even the German Chancellor's telephone. [53] 90,000 letters were opened daily by machines. [53] The smells of people were even collected and held in closed jars. [53] Once the Stasi gained information about people through their telephones and mail, they then sent in investigators to report on the actions of people. Many times instead of introducing new people, the Stasi would convince friends and relatives to report on the people of interest. [53] At one point Dr. Hubertus Knabe stated:

The main purpose was to control the society. In nearly every speech, the Stasi minister gave the order to find out "Who is who?" – what meant: who thinks what? He didn't want to wait until somebody tried to act against the regime. He wanted to know in advance what people were thinking and planning. [53]

He goes on to state that the Stasi did not arrest people of interest, "they preferred to paralyze them." [53] Fear was a motivating factor for people to get in line with the Stasi. They did not torture people they had the ability to destroy their lives with the information they had about their personal affairs.

Some critics of programs like the MIM attack argue that if our governments start collecting intelligence on its own people we no longer live in a democracy but more of a surveillance state. This would be a state where the government can control its citizens through fear because they know who thinks what.

The MIM attack has the ability to collect very personal information about people that could be used to persuade action. The collection of information also has the affect of predicting action which can be used to influence ideas.

Protection will be evolutionary; a never ending document that lives and breathes with the changes that consume its future. Each and every technological advancement should be looked upon to verify the security features. This should not be strictly dominated by governments; private companies need to be held to a high standard of compliance. Private companies should also challenge government standards. Governments, citizens, and private companies can, in essence, be a check and balance for each other at every turn. The goal will be to allow the government the tools necessary to keep its citizens safe while protecting the massive amounts of information that can be used to anticipate actions and control society. For policy reform; standards, regulations, and operations need the systematic evaluations of private think tanks, companies, citizens, and government agencies.

CHAPTER 8

SUMMARY AND CONCLUSION

What we can be assured of is that MIM attacks are possible and there are possible solutions from experts to fix this deficiency in the core of the network. Federal laws and regulations are in place that anticipates the continued the use of the MIM attack. [21] [22] [27] [24] [29] [30] [31]

Once a carrier becomes CALEA compliant with a method such as a MIM attack, it is difficult for carriers to prevent this style of Lawful Interception unless the carrier provides another means to authorities. [21] [22] Implementing a design solution for the MIM attack could result in large fines or being shut down. [21] [22] So for carriers to be able to fix security vulnerabilities, regulations need to reflect that telecommunication carriers must be able to make independent decisions on security measures. Fourth Amendment concerns have been addressed in earlier sections and are the driving force for civil rights organizations to seek change.

Arguments that it is imperative to keep the MIM attack a secret for national security are invalid. The vulnerability has been known since 2004 and the regulations that allow fake cell towers can be and have been defeated by crypto phones and burner phones.

It is time to begin work on how we want policy reform to take place to address the MIM attack. There are four areas that hold the preliminary concerns for the debate: constitutionality, oversight, vulnerability, and protection. In this process; private companies, government agencies, citizens, civil right organizations, experts in the specific fields, and legislators need to take an active role.

Envisioning the process of policy reform will be undoubtedly easier than implementation. Future research for the constitutionality of this attack will need to come in the form of legal analysts who have a technical background. The government should be responsible for setting up a committee of experts who are chosen based on previous experience. These individuals should come from a mixture of private companies and government work. It might be necessary to include people who have been members of the FBI and local law enforcement who have worked on the equipment. This team can develop a standard operating procedure that can be referenced when the legality of interception is in question. This team should also begin to pursue legislation that interprets how certain technological abilities impact constitutional law. I have no doubt that the interpretation of laws and their implications to constitutionality will result in a massive restructure of policy. This team will not only be looking at the MIM attack but also the storage of data obtained, the individuals with access to the information collected, the security of the stored data, and the responsibility of the FBI or law enforcement to maintain confidentiality of information collected. After these issues have been reviewed then it would be appropriate to establish similar laws that have applied in the medical and financial realms. Legislation that introduces a minimum level of security to citizens should be presented. This level of security will address the inability of the private market, such as telecommunication carriers, to produce secure products with the MIM attack built into the core of the system.

Future oversight goals should include a reform of the FISA court. The high percentage of warrants issued is concerning. Although, it is possible that each case followed legitimate procedures, it is impossible for anyone outside the court to verify the results. This could be remedied with an appellate court. This court would be one step of oversight that

could exist in the classified realm that would be able to hear more cases than the Supreme Court. Companies and individuals who wish to pursue a review of the case would not have to rely on the Supreme Court level alone.

The future work on the vulnerability will need to come from the experts in the field. Once a decision is made through legislation that this MIM attack is no longer a viable option for use in protection measures, the technology experts need to take over. Experts have been producing solutions for some time now. IEEE has conventions all over the world that bring together experts from all over the world that discuss security measures such as this. Once the approval from the U.S. government shows that a solution will be allowed there will be very little time before a team will take advantage of that opportunity. A security solution will be created to eliminate the MIM attack in short time since many solutions have already been introduced in previous papers.

Again future research on protection versus security will be the toughest topic to tackle. Ideologies will change over time. Certain security measures that the FBI, NSA, and local law enforcement use to protect civilians may need to kept secret so as not to allow workarounds. In the case of the MIM attack, an understanding is imperative that this style of attack is no longer beneficial since it is well known with several work arounds. If there is usable intelligence that is being collected currently, it is only a matter of time before the people who wish to remain anonymous utilize the work arounds. At that point, the attack becomes virtually useless and will only be collecting on innocent people. It is also possible to have the attack turned against the very people who created it to secure people. There is a chance right now to get ahead of the problems that the MIM attack creates and find an

alternative solution before it becomes a useless security vulnerability that creates a threat to the people who use it for legitimate reasons.

Establishment of the legislation would need to be prioritized in front of all other concerns. Once the ground work is done in this area then the other areas are released from the constraints and can begin work on establishing security and forging a way ahead for policies, procedures and documentation.

It is time to establish the working documents and standards on how we plan to secure information for the future generations to build on.

REFERENCES

[1] Mehrotra, A. (1997). *GSM system engineering*. Boston: Artech House.
[2] Korhonen, J. (2014). *Introduction to 4g mobile communications*. Artech House.
[3] Kaaranen, H. (2005). *UMTS networks: Architecture, mobility, and services* (2nd ed.). Chichester, West Sussex, England: J. Wiley & Sons.
[4] Meyer, U., & Wetzel, S. (2004). A man-in-the-middle attack on UMTS. *Proceedings of the 2004 ACM Workshop on Wireless Security - WiSe '04*, 90-97. Retrieved November 2, 2015, from http://ece.wpi.edu/~dchasaki/papers/mitm_umts.pdf
[5] Meyer, U., & Wetzel, S. (2004). On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks. *2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE Cat. No.04TH8754)*, 2876-2883.
[6] Koien, G. (2013). Privacy enhanced mutual authentication in LTE. *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, 614-621.
[7] Becher, M., Freiling, F., Hoffmann, J., Holz, T., Uellenbeck, S., & Wolf, C. (2011). Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. *2011 IEEE Symposium on Security and Privacy*, 96-111.
[8] Hadzialic, M., Skrbic, M., Huseinovic, K., Kocan, I., Musovic, J., Hebibovic, A., & Kasumagic, L. (2014). An approach to analyze security of GSM network. *2014 22nd Telecommunications Forum Telfor (TELFOR)*.
[9] Fakhoury, H., & Trimm, T. (2012, October 22). Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About. Retrieved November 2, 2015, from https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy
[10] Gallagher, R. (2012, October 19). FBI Accused of Dragging Feet on Release of Info About "Stingray" Surveillance Technology. Retrieved November 2, 2015, from http://www.slate.com/blogs/future_tense/2012/10/19/stingray_imsi_fbi_accused_by_epic_of_dragging_feet_on_releasing_documents.html
Threat to Cell Phone Privacy You Don't Know About. Retrieved November 2, 2015
[11] Fakhoury, H., & Trimm, T. (2012, October 22). Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About. Retrieved November 2, 2015, from https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy
[12] Van den Broek, F. (2010). Eavesdropping on GSM: State-of-affairs. Retrieved November 2, 2015, from http://www.cs.ru.nl/~F.vandenBroek/WISSec2010_GSM_Eavesdropping.pdf
[13] Broek, F., Verdult, R., & Ruiter, J. (2015). Defeating IMSI Catchers. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15*, 1-12.
[14] Strobel, D. (2007). IMSI Catcher. Retrieved November 3, 2015, from https://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf

[15] Shafiul Alam Khan, M., & Mitchell, C. (2015). Improving Air Interface User Privacy in Mobile Telephony. Retrieved November 1, 2015, from http://www.chrismitchell.net/Papers/iaiupi2.pdf
[16] Prasad, M., & Manoharan, R. (2014). A Robust Secure DS-AKA with Mutual Authentication for LTE-A. Applied Mathematical Sciences, 9(47), 2337-2349.
[17] Arapinis, M., Mancini, L., Ritter, E., Ryan, M., Golde, N., Redon, K., & Borgaonkar, R. (2012). New privacy issues in mobile telephony: Fix and Verification. *Proceedings of the 2012 ACM Conference on Computer and Communications Security - CCS '12*. Retrieved November 3, 2015, from http://markryan.eu/research/UMTS/UMTSprivacy.pdf
[18] Khan, M., & Mitchell, C. (2014). Another Look at Privacy Threats in 3G Mobile Telephony. Information Security and Privacy Lecture Notes in Computer Science, 386-396. Retrieved November 3, 2015, from http://www.chrismitchell.net/Papers/alapti.pdf
[19] Mobarhan, M., & Mobarhan, M. (2012). Evaluation of Security Attacks on UMTS Authentication Mechanism. International Journal of Network Security & Its Applications IJNSA, 37-52. Retrieved November 3, 2015, from http://airccse.org/journal/nsa/0712nsa03.pdf
[20] Rouse, M., Cobb, M., Brayton, J., Finneman, A., Turajski, N., & Wiltsey, S. (2015). What is PKI (public key infrastructure)? - Definition from WhatIs.com. Retrieved November 3, 2015, from http://searchsecurity.techtarget.com/definition/PKI
[21] CALEA. (2015). Retrieved November 4, 2015, from https://www.eff.org/issues/calea
[22] FAQ on the CALEA Expansion by the FCC. (2007, September 19). Retrieved November 4, 2015, from https://www.eff.org/pages/calea-faq
[23] ANSI T1.413-1998. (1998). Retrieved November 5, 2015, from http://ftp.tiaonline.org/TR-30/TR-30.3/Public/WH-027.pdf
[24] Rules & Regulations for Title 47. (2015). Retrieved November 5, 2015, from https://www.fcc.gov/encyclopedia/rules-regulations-title-47
[25] ANSI: Historical Overview. (2015). Retrieved November 5, 2015, from http://www.ansi.org/about_ansi/introduction/history.aspx?menuid=1
[26] ETSI - What we are, role in Europe, creation, funding, history. (2015). Retrieved November 5, 2015, from http://www.etsi.org/about/what-we-are
[27] Wiretap Reports. (2014). Retrieved November 6, 2015, from http://www.uscourts.gov/statistics-reports/analysis-reports/wiretap-reports
[28] Justice News. (2015, September 3). Retrieved November 6, 2015, from http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators
[29] Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology. (2015, September 3). Retrieved November 2, 2015, from http://www.justice.gov/opa/file/767321/download
[30] Cardozo, N. (2015, September 3). Finally! DOJ Reverses Course and Requires Warrants for Stingrays! Retrieved November 6, 2015, from https://www.eff.org/deeplinks/2015/09/finally-doj-reverses-course-and-will-get-warrants-stingrays
[31] Nakashima, E. (2015, May 14). FBI clarifies rules on secretive cellphone-tracking devices. Retrieved November 6, 2015, from https://www.washingtonpost.com/world/national-security/fbi-clarifies-rules-on-secretive-cellphone-tracking-devices/2015/05/14/655b4696-f914-11e4-a13c-193b1241d51a_story.html

[32] Scourias, J., & Farley, T. (2015). Privateline.Com: GSM/PCS by John Scourias with comments by Tom Farley. Retrieved November 6, 2015, from http://www.privateline.com/PCS/GSM03.html
[33] The future of modern mobile communications. (n.d.). Retrieved November 6, 2015, from http://blueadmiral.com/dev/Test/comms/gsm_016.html
[34] Pagliery, J. (2014, November 14). Federal agents fly planes that spy on American cell phones. Retrieved November 7, 2015, from http://money.cnn.com/2014/11/13/technology/security/federal-planes-spy/
[35] Timeline of NSA Domestic Spying. (2012, November 30). Retrieved November 19, 2015, from https://www.eff.org/nsa-spying/timeline
[36] Crocker, A., & Cohn, C. (2015, March 19). Twenty-four Million Wikipedia Users Can't Be Wrong: Important Allies Join the Fight Against NSA Internet Backbone Surveillance. Retrieved November 20, 2015, from https://www.eff.org/deeplinks/2015/03/twenty-four-million-wikipedia-users-cant-be-wrong-important-allies-join-fight
[37] About 3GPP Home. (n.d.). Retrieved November 19, 2015, from http://www.3gpp.org/about-3gpp/about-3gpp
[38] Dempsey, J. (2000, April 4). Amending the Pen Register and Trap and Trace Statute. Retrieved November 24, 2015, from https://cdt.org/files/security/000404amending.shtml
[39] Background - GSMK. (n.d.). Retrieved November 24, 2015, from http://www.cryptophone.de/en/background/
[40] Silent Circle. (n.d.). Retrieved November 24, 2015, from https://www.silentcircle.com/products-and-solutions/devices/
[41] Intelligence Collection Disciplines (INTs). (2010, May 21). Retrieved November 29, 2015, from https://www.fbi.gov/about-us/intelligence/disciplines
[42] Coursera - Free Online Courses From Top Universities. (2015). Retrieved December 4, 2015, from https://www.coursera.org/course/surveillance
[43] 18 U.S. Code Chapter 119 - WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS
[44] 50 U.S. Code § 1881a - Procedures for targeting certain persons outside the United States other than United States persons. (n.d.). Retrieved December 4, 2015, from https://www.law.cornell.edu/uscode/text/50/1881a
[45] Jarrett, M., Bailie, M., Hagan, E., & Judish, N. (n.d.). Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Retrieved December 4, 2015, from http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf
[46] Friedman, B., & Kerr, O. (n.d.). Amendment IV Search and Seizure. Retrieved December 5, 2015, from http://constitutioncenter.org/interactive-constitution/amendments/amendment-iv
[47] Fakhoury, H. (2015, January 2). Electronic Frontier Foundation. Retrieved December 5, 2015, from https://www.eff.org/deeplinks/2015/01/2014-review-stingrays-go-mainstreamhttps://www.eff.org/deeplinks/2015/01/2014-review-stingrays-go-mainstream
[48] Greenwald, G. (2013, May 3). The bad joke called 'the FISA court' shows how a 'drone court' would work. Retrieved December 7, 2015, from http://www.theguardian.com/commentisfree/2013/may/03/fisa-court-rubber-stamp-drones
[49] EPIC - Foreign Intelligence Surveillance Court (FISC). (2015, November 10). Retrieved December 7, 2015, from https://epic.org/privacy/surveillance/fisa/fisc/

[50] Lichtblau, E. (2013, July 6). In Secret, Court Vastly Broadens Powers of N.S.A. Retrieved December 7, 2015, from http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?_r=0
[51] Lideman, T. (2013, June 7). The Foreign Intelligence Surveillance Court. Retrieved December 7, 2015, from https://www.washingtonpost.com/politics/the-foreign-intelligence-surveillance-court/2013/06/07/4700b382-cfec-11e2-8845-d970ccb04497_graphic.html
[52] Frequently Asked Questions - Supreme Court of the United States. (2015, October 25). Retrieved December 7, 2015, from http://www.supremecourt.gov/faq.aspx
[53] Knabe, H. (2014, June 23). The dark secrets of a surveillance state. Retrieved December 8, 2015, from https://www.ted.com/talks/hubertus_knabe_the_dark_secrets_of_a_surveillance_state?language=en
[54] Johnston, R. (2015, December 3). Terrorist attacks and related incidents in the United States. Retrieved December 8, 2015, from http://www.johnstonsarchive.net/terrorism/wrjp255a.html
[55] SEARCH RESULTS: 141966 INCIDENTS. (2015, June 1). Retrieved December 8, 2015, from http://www.start.umd.edu/gtd/search/Results.aspx?charttype=line&chart=attack&casualties_type=&casualties_max=®ion=1
[56] Transcript of "The NSA responds to Edward Snowden's TED Talk" (2014, March 1). Retrieved December 8, 2015, from https://www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk/transcript?language=en
[57] Deposition of Bradley S. Morrison. (2014, April 11). Retrieved December 9, 2015, from http://www.sandiego.gov/cityattorney/pdf/news/2014/nr141222c.pdf
[58] Riley v. California. (2014, June 24). Retrieved December 10, 2015, from http://www.scotusblog.com/case-files/cases/riley-v-california/
[59] Wang, Y. (2013, March 25). More People Have Cell Phones Than Toilets, U.N. Study Shows | TIME.com. Retrieved December 11, 2015, from http://newsfeed.time.com/2013/03/25/more-people-have-cell-phones-than-toilets-u-n-study-shows/
[60] Mobile Technology Fact Sheet. (2013, December 27). Retrieved December 11, 2015, from http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/