The Security Implications of IMSI Catchers

Bryan Harmat, Jared Stroud, Daryl Johnson, Bill Stackpole,
Sylvia Perez-Hardy, Rick Mislan, PhD, Tae Oh, PhD
Department of Computing Security
Rochester Institute of Technology
Rochester, NY 14623

Abstract

According to various news sources, rogue cellular towers referred to as "IMSI catchers" have been deployed across the nation. An academic interest has been taken in determining what information can be acquired when a mobile device associates with one of these towers. These towers focus on manipulating authentication methods to pose as a legitimate GSM tower. Through the use of software defined radios, and open source software an inexpensive GSM protocol-based cell tower was deployed to determine what, if any, security vulnerabilities exist in the current mobile network infrastructure.

1 Introduction

IMSI (International Mobile Subscriber Identity) catchers are devices constructed to execute a man in the middle attack of mobile phone network traffic. These towers can be used to intercept voice calls, texts, and data (such as web browsing)[8]. Federrath notes, "IMSI Catcher(s) [are] capable of signaling to the mobile phone that it should discontinue using encryption on the radio link." [7]. Due to this security flaw in the Global System for Mobile communication (GSM), phones that associate with an IMSI catcher may not be using encryption to secure data in transit if the tower did not tell the device to use an encryption method. This vulnerability results in the attacker possessing the capability to see all data to and from the device. This information allows for an attacker to associate an individual based on their unique individual mobile subscriber identity (IMSI) stored on the mobile device's SIM (Subscriber Identity Module) with a mobile device at a specific location (if telecommunication providers were subpoenaed for such information). A SIM is used to uniquely identify a user for subscription purposes and includes the user's IMSI [9].

2 GSM

GSM is a standard developed to describe cellular network protocols that a large market share of cell phones. The original specifications were developed by the European Telecommunication Standards Institute (ETSI)[23]. As of February 2015, there are approximately 3.6 billion mobile subscribers [11]. Historically, parts of the GSM protocol have been kept proprietary [24]. These "secret items" include encryption and authentication methods. Welte notes, "The specifications of the GSM proprietary On-air encryption A5/1 and A5/2 are only made available to GSM baseband chip makers who declare their confidentiality."[24]. In an effort to make GSM obtainable for academia, open source movements such as OpenBTS[17] have been developing freely available tools to deploy a personal GSM tower. OpenBTS is a solution that allows for a low cost GSM tower deployment. This implementation involved Software Defined Radios (SDRs) as well as OpenBTS.

2.1 GSM Architecture

Bettstetter et al. explain that, "GSM networks are structured hierarchically. They consist of at least one administrative region, which is assigned to a MSC."[2]. GSM architecture can be broken up into two large parts: the Base Station Subsystem (BSS) which consists of a base transceiver station (BTS), and a base station controller (BSC). The other critical section is the Networking Switching Subsystem (NSS).

The BSS consists of a base transceiver station, and the base station controller. These two elements of GSM architecture are responsible for controlling which radio frequency bands and channels are transmitted on, as well as functions that affect data in transport. The NSS is responsible for all information related to the user such as activity status, location information, and the handover process (the process by which devices are able to move

through coverage areas of various base transceiver stations).

There are four types of handover processes that may occur[18]:

- Intra-tower handover - when the mobile must change frequencies due to some type of interference. The device still remains connected to the same tower.
- Inter-BTS Intra BSC Handover - when the device moves out of the coverage of one BTS but into the coverage area of another BTS controlled by the same BSC.
- Inter-BSC Handover - when the mobile device moves out of the range of base station transceivers controlled by a single BSC. This handover is controlled by the MSC.
- Inter-MSC handover - the two MSCs involved between the handover negotiate in order to complete the successful handover.

Base transceiver stations are a core component to radio communication in all wireless communication (for example, GSM, CDMA, 802.11). The BTS portion of the GSM architecture is responsible for handling all radio activities to and from the tower. Each BTS is additionally responsible for encoding, decoding, encrypting, decrypting, and a plethora of other functions that occur during data communication from the mobile equipment to the physical tower.

The base transceiver station lies under the base station controller. The BSC defines which channel and spectrum radio frequency signals are broadcasted on. It is important to note the GSM standard for broadcast channels varies depending on geographic location. The deployment for this project made use of 850, 900, and 1800 MHz bands.

The Networking Switching Subsystem (NSS) is an integral part of the GSM architecture. Key components include the Home Location Register (HLR), Visitor Location Register (VLR), Mobile Services Switching Center (MSC), Equipment Identity Register (EIR) and Authentication Center (AUC).

The Mobile Services Switching Center (MSC) is the "brain" of the Networking Switching Subsystem. Authentication, handover, location updating, new user registration, and call routing all occur via actions taken by the MSC.

The HLR is a database used solely for user subscription management. All information stored here is considered permanent. A user's profile that contains location information and activity status is also stored here. Information from a SIM card such as a user's data and calling plan is additionally stored here.

The Visitor Location Register (VLR) is a database that contains temporary information about a subscriber. When users roam into a new GSM cell, the VLR may request data about the mobile equipment from the Mobile Services Switching center so that it will have information required for forwarding calls without querying the HLR. This is a sort of caching mechanism.

The Equipment Identity Register (EIR) contains a information about all currently valid mobile devices allowed on a GSM network. The EIR correlates the unique number provided to each mobile device known as the International Mobile Equipment Identity (IMEI). The FCC also uses the EIR and the IMEI to identify lost or stolen devices.[6]

3 OpenBTS Implementation

In the implementation for this project, OpenBTS was used for the software portion of the base station. A laptop running Ubuntu 12.04.4 LTS was the base operating system for the software. The software defined radios used for building this tower were Ettus N210[20] and B210[19] radios. The deployment was running OpenBTS 5.0, which was when the software was in its alpha stages of development, and had contained a few bugs. Utilizing developers' comments and mailing lists, all initial issues were solved. After resolving these issues, it was possible to observe transmitted traffic via Wireshark, and examine appropriate log files for sent text messages.

3.1 OpenBTS Architecture

OpenBTS aims to replicate a modern GSM tower through software implementations. Asterisk, an open source VoIP service, is used to handle all voice traffic to and from the OpenBTS cell tower [1]. While other documented implementations have also used Asterisk, other VoIP solutions could be substituted in Asterisk's place. Part of the the OpenBTS software stack is sipauthserve. Sipauthserve is used for all authentication in OpenBTS, and was specifically developed to handle cellular authentication by the OpenBTS developers.

3.2 Cost Overview

The implementation discussed in this paper is affordable at a cost of approximately $1,250, not including the price of computer hardware. The implementation discussed in the paper requires a Ettus B210 ($1,100USD at the time of this writing)[19] and four Vert 900 antennas ($35USD each at the time of this writing)[21]. While this implementation does not have direct telecommunication access as industrial deployments would, it can successfully

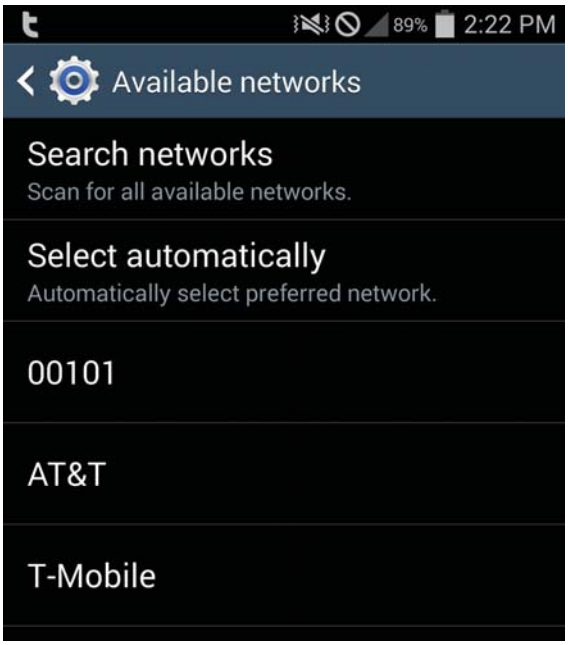

Figure 1: OpenBTS broadcasting as 00101.

act as an IMSI catcher. However, in order to successfully route calls, it would be necessary to configure call routing via a SIP provider. Below is a screenshot of the default network that OpenBTS will advertise (as seen from a Samsung Galaxy S4), 00101.

4 Encryption

As Meyer and Wetzel noted,[14], all encryption and authentication parameters are controlled by the tower. Due to backwards compatibility, GSM phones support a wide band of different cellular technologies. 2G networks originally used A5/1 and A5/2 encryption. A5/2 was developed as "weaker" encryption to conform to US export laws. However, both algorithms have suffered from an onslaught of cryptanalysis, especially with rainbow tables that exist today to crack A5/1 encrypted traffic. Lo and Chen note, "the A5 algorithm, uses a proprietary algorithm for message encryption/decryption."[13]. Kerckhoff's Principle contradicts this paradigm, which as Simmons explains that according to Kerckhoff's Principle, "the opponent knows the system "[22]. The central argument for this principle is that the keys for encryptions should be kept secret, but it should be assumed that the adversary can determine how the cryptosystem works.

4.1 Encryption Attacks

Due to this flaw in the logic behind keeping the algorithm secure for the A5 encryption, there have been successful attacks against the A5 cryptosystem that have been developed [3][14]. The cellular base station can depict which encryption algorithm to use for data communication as long as both the phone and the tower support it. Similarly to TLS downgrade attacks, base stations can lower the level of encryption used in an effort to capture weakened encrypted traffic that will later be cracked via brute force or rainbow tables. Additionally the tower could just attempt to use A5/0 (absence of encryption) and collect all free flowing plain text data. Meyer and Wetzel explain that the tower can send false information regarding its encryption capabilities to the mobile device and due to this, encryption can be completely disabled [14]. Since the initial creation of the algorithms, some have been made public, and patented [16].

5 Authentication

Mobile devices must authenticate with the network before being able to utilize the network resources. There are some differences between GSM authentication versus CDMA authentication, however both are still vulnerable to the IMSI Catcher threat. The following sections discuss the authentication methods for the respective architectures.

5.1 GSM Authentication

In order for a cellular phone to perform any normal mobile function such as SMS, MMS, calling, it must first authenticate to a mobile cell. GSM authentication occurs through the A3 authentication algorithm. A high level overview of the algorithm is as follows, the GSM tower will send a random number that has been incorporated with a shared key (Ki) as well the A8 ciphering algorithm to the mobile equipment. The mobile device will then process the random number, and return a signed response known as SRES to the tower [25] .This response will have been signed via the mobile equipments shared private key known as "Ki." Once the tower receives the signed response it will compare the mobile devices signed response to the towers signed response with the users Ki. If they match, authentication was successful. It is important to note that Ki itself is never sent over the network.

5.2 CDMA Authentication

CDMA utilizes a similar challenge response authentication mechanism. The difference lies in the encryption

algorithms in place by CDMA. The Cellular Authentication and Voice Encryption (CAVE) algorithm utilizes a 128-bit key referred to as the "Shared Secret Data" (SSD), an "A-Key", and the electronic serial number (ESN) of the mobile device.

The Shared Secret Data (SSD) is composed of two parts, SSD_A and SSD_B. SSD_A is utilized for creating an authentication signature by the mobile device to return to the tower. This signature proves to the tower that the mobile device is whom it claims to be. SSD_B is used to generate keys for voice and messaging encryption.

The A-Key is programmed into the mobile device (similar to an IMSI on a SIM) and is also stored in a CDMA tower's authentication center. This A key is utilized to generate separate sub-keys for voice and message encryption. A major difference that lies between CDMA and GSM is that the A-Key can be re-programmed where the IMSI cannot. However, after reprogramming the A-Key, the authentication center must be updated with the new number as well.

Upon receiving a random number challenge (RAND) from a tower, the mobile device will use the SSD along with the RAND number as parameters for the CAVE algorithm. The return value of the CAVE algorithm is an 18 bit authentication signature. The authentication signature is then sent to the base station, which compares the authentication signature for validity.

5.3 OpenBTS Authentication

OpenBTS supports the standard mechanisms of GSM encryption as discussed previously in this paper. However, failing to have a copy of Ki also on an OpenBTS deployment will prevent a phone from ever successfully authenticating. If an attacker is attempting to have a mobile device join their GSM tower they will most likely not know the Ki of the mobile device's SIM either. However, successful authentication can be achieved through OpenBTS' open authentication method.

Open authentication does not require prerequisite knowledge of Ki at the GSM tower level. OpenBTS open authentication automatically accepts the the signed response from the mobile equipment. This allows any device to successfully authenticate and then associate with the base station.

During normal authentication when the mobile device returns the signed response a tower would compare the signed response to the output of the tower's Ki and the original RAND challenge for validity. Open authentication accepts any response from the mobile device. This feature allows an attacker to circumvent any prior knowledge of Ki.

Ki is a shared private key stored on all SIMs, as well as stored in the home location registry portion of a GSM base station. This key is used for initial authentication between mobile equipment and tower. Ki never leaves the phone and is only used in authentication for signing the initial random data sent to the mobile device from the tower. Additional encryption measures on a SIM protect the Ki from being accessed. However, manufacturers that implement weak encryption are vulnerable to having the SIM card compromised.

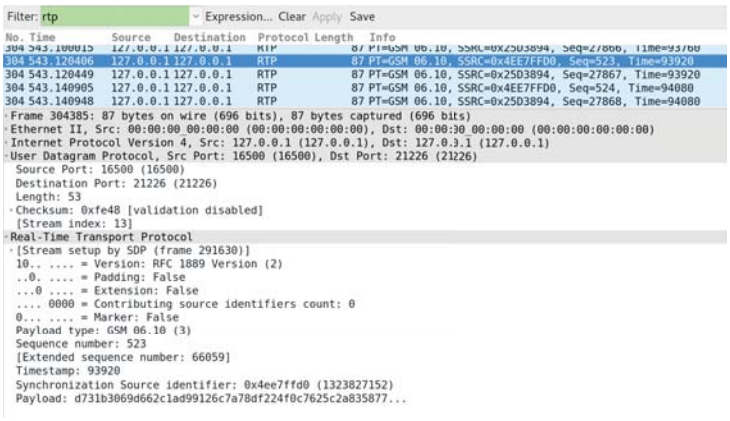

Figure 2: Wireshark RTP traffic.

It is important to note that according to *Getting Started with OpenBTS*, "OpenBTS has an alternative authentication method for this situation known as 'Cache Based Auth.' It performs an initial authentication exchange with the handset and records the results. It uses this same request and expects the same answer in the future. The method is not as secure as unique exchanges for each request but is still better than completely disabling authentication."[10].

6 Proof of Concept

The OpenBTS implementation, allows for packets to be captured on the interface connected to the software defined radio. By utilizing Wireshark, an open source packet capturing application, phone calls between mobile devices were captured. Wireshark provides the ability to examine the RTP streams containing GSM payloads. The figure below shows a screenshot of a packet capture using Wireshark [26].

The figure below displays output from a log file with decoded text messages containing "ICMP_REQUEST" and "ICMP_REPLY."

The figure below is also a screenshot on one of the devices that sent a text that was logged in the figure above.

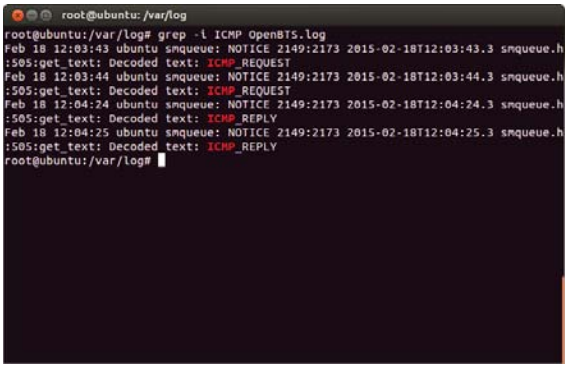

Figure 3: OpenBTS log of text messages sent.

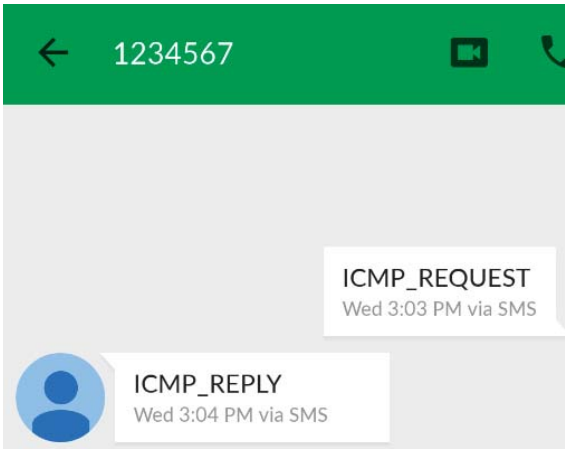

Figure 4: Text message application displaying a conversation.

7 Results

The experiment with open authentication on the OpenBTS tower resulted in several phones associating and authentication without any indication of foul play. Due to the GSM protocol allowing the tower to define which authentication and encryption methods to implement, it is trivial to configure a tower to use encryption methods with known attacks. However, utilizing A5/0 encryption and open authentication allows for plain text communication to occur with data in transit and the mobile device to associate without knowing the private key, Ki.

Additionally, modifying the mobile network code through the OpenBTS configuration command line interface can force the tower to appear as a major mobile carrier to all mobile devices. This code is represented as a two to three integer value accompanied with a mobile country code, also a two to three integer value. The mobile country code represents a geographic location numerically. By modifying these values, the tower can appear as any major network carrier from any geographic location.

8 Conclusion

Several methods have been proposed that attempt to change how mobile devices authenticate with networks. These changes have been proposed in order to prevent man in the middle attacks such as the IMSI Catcher method described in this paper. For example, Lee et. al propose that the HLR can give a VLR a temporary key that it may use to authenticate the mobile station without knowing its Ki[12]. The paper also discusses how this method can be used for "bilateral authentication" because the mobile station will be able to authenticate that the VLR is an imposter since it will have to get a secret from the mobile station's HLR. Chang et. al also propose a method to share a secret key between the mobile station and the visitor location registry in order for the device to be authenticated with the home location registry [4]. If implemented, these methods would be able to ensure that simple man in the middle attacks such as the IMSI Catcher detailed in this paper would not be possible to implement.

9 Future Work

Public awareness of GSM interception attacks is increasing, along with applications that aim to detect IMS catchers and rogue towers. Analysis of Android application IMSI detection techniques will be investigated for effectiveness and possible mitigations.

Future work will focus on deploying a multi-tower network to analyze network traffic overhead, and inter tower communication and how to intercept the handoff.

10 Acknowledgements

This research would not be possible without a grant from the Office of the Provost and the Rochester Institute of Technology [15]. This implementation supports the Rochester Institute of Technologys mobile security and forensic curriculum [5].

References

[1] ASTERISK.ORG. Asterisk, 2015.

[2] BETTSTETTER, C., VOGEL, H.-J., AND EBERSPACHER, J. Gsm phase 2+ general packet radio service gprs: Architecture, protocols, and air interface. *Communications Surveys & Tutorials, IEEE 2*, 3 (1999), 2–14.

[3] BIRYUKOV, A., SHAMIR, A., AND WAGNER, D. Real time cryptanalysis of a5/1 on a pc. In *Fast Software Encryption* (2001), Springer, pp. 1–18.

[4] CHANG, C.-C., LEE, J.-S., AND CHANG, Y.-F. Efficient authentication protocols of gsm. *Computer Communications 28*, 8 (2005), 921–928.

[5] EMBLING, E., GILBERT, S., AND MISLAN, R. Designing and implementing a wireless carrier topology in a lab environment. In *Global Wireless Summit* (2013).

[6] FCC.GOV. Protect your smart device, 2015.

[7] FEDERRATH, H. Protection in mobile communications.

[8] GOLDE, N., REDON, K., AND BORGAONKAR, R. Weaponizing femtocells: The effect of rogue devices on mobile telecommunications. In *NDSS* (2012).

[9] HERMANSSON, J., MANSSON, C., JACOBSSON, A., NYSTROM, Z., KARLSSON, B., PALMGREN, C., LEUHUSAN, G., AND ORNEHOLM, F. Digital mobile telephone system in which each subscriber is assigned a telephone number and several subscriber identity module (sim) cards, Aug. 12 1997. US Patent 5,657,373.

[10] IEDEMA, M. *Getting Started with OpenBTS*. O'Reilly Media, 2014.

[11] INTELLIGENCE, G. Definitive data and analysis for the mobile industry, 2015.

[12] LEE, C.-C., HWANG, M.-S., AND YANG, W.-P. Extension of authentication protocol for gsm. *IEE Proceedings-Communications 150*, 2 (2003), 91–95.

[13] LO, C.-C., AND CHEN, Y.-J. Secure communication mechanisms for gsm networks. *Consumer Electronics, IEEE Transactions on 45*, 4 (1999), 1074–1080.

[14] MEYER, U., AND WETZEL, S. On the impact of gsm encryption and man-in-the-middle attacks on the security of interoperating gsm/umts networks. In *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on* (2004), vol. 4, IEEE, pp. 2876–2883.

[15] MISLAN, R. Mobisploit provost implementation grant, 2014.

[16] MURTO, J. Subscriber authentication in a mobile communications system, Nov. 23 1999. US Patent 5,991,407.

[17] OPENBTS.ORG. A platform for innovation. Online.

[18] RADIO-ELECTRONICS.COM. Gsm handover or handoff, 2015.

[19] RESEARCH, E. Usrp b210. Online.

[20] RESEARCH, E. Usrp n210. Online.

[21] RESEARCH, E. Vert900 antenna. Online.

[22] SIMMONS, G. J. Authentication theory/coding theory. In *Advances in Cryptology* (1985), Springer, pp. 411–431.

[23] SPECIFICATION, G. 11.10. *ETSI TC-SMG: Digital cellular telecommunications system (Phase 2+)* (2000).

[24] WELTE, H. Anatomy of contemporary gsm cellphone hardware. [Online. Accessed 15-February-2015].

[25] WILLASSEN, S. Forensics and the gsm mobile telephone system. *International Journal of Digital Evidence 2*, 1 (2003).

[26] WIRESHARK.ORG. Wireshark, 2015.