GSM Risks and Countermeasures

STI Group Discussion and Written Project

Authors: Greg Farnham, Kevin Fuller
Advisor: Johannes Ullrich

Accepted: February 1, 2010

Abstract

Recent research has shown that GSM encryption can be cracked with relatively modest resources. This is an important issue as 80% of cell phones use GSM and these users are potentially at risk. These risks can be mitigated with various countermeasures. This paper reviews the risks and possible countermeasures. Recommendations are included for a fictitious small high tech company, "GIAC Enterprises".

1. Executive Summary

Recently, cell phone eavesdropping has been in the news. These news stories resulted from research published in late 2009 showing the ability to crack GSM cell phone encryption. GSM is the most commonly deployed cell phone technology today. The GSM association states that 80% of all cell phone users are on GSM. The GIAC Enterprise corporate cell phones use GSM. GSM phones can use one of four different standards for encryption: A5/1, A5/2 and A5/3. A5/1 is the most commonly used standard and is used by GIAC Enterprises' cell phone carrier. This is also the standard that has gotten the most attention of researchers trying to crack the encryption. The A5/3 standard is newer and stronger, but it has also been shown vulnerable to attacks.

The latest attack on the A5/1 standard relies on pre-computed rainbow tables to reduce the time to crack encryption for a given call. In his presentation of the attack, Karsten Nohl outlined the requirements for building an interceptor using open source components. This research has shown that the attack that used to require hundreds of thousands of dollars now only requires thousands of dollars. The time to crack encryption is estimated at 30 minutes or as little as 30 seconds with a multi node cluster.

This weakness in GSM cell phone encryption represents a moderate risk to GIAC Enterprises. An organization with sufficient resources motivated to snoop on GIAC Enterprises' calls has a good chance of success. Given that our cell phones are used at manufacturing locations there are a number of static targets available. Due to the competitive nature of GIAC Enterprises' business the loss of confidential data would be financially catastrophic.

Due to the risk to GIAC Enterprises there are a number of recommendations to reduce the risk. There are short term recommendations which should be implemented as soon as possible. First, create a cell phone usage policy which prohibits discussion of confidential information. Second, conduct awareness training on the policy and secure cell phone usage as described in the countermeasures section. Third, use the secure email solution for confidential information exchange on the cell phone.

There is also a long term recommendation. The long term solution is to execute a project for secure cell phone implementation. This project will investigate technology used by available providers including encryption technologies. It will also evaluate third party solutions for end to end encryption. After evaluation a solution will be selected and implemented.

By implementing the recommendations, the risk to GIAC Enterprises will be reduced to an acceptable level.

2. Introduction

GIAC Enterprises is a small high technology company which produces sub components for human implantable communication devices. GIAC has had success within this market. Their Bio Organic Repeater Group has consistently led the market for human implantable communication components. There have been rumors that GIAC is on the brink of a technological breakthrough, but the company has not made any public statements on the rumors. Consumers, the Press and competitors are all highly motivated to find out the details of GIAC's product development.

The GIAC CEO is concerned about recent reports of GSM phones being vulnerable to call interception. She has assigned the Information Security Group the task of researching and reporting on the topic. There are two key factors to consider for the research. First, if a third party gains access to GIAC development plans, it would be financially catastrophic. GIAC would likely lose a major contract to develop a brain implantable phone product. Second, the CEO discusses confidential information on her GSM phone. The CEO regularly travels the country to visit factories. While on travel she uses her GSM phone exclusively. GIAC is currently using smart phones on a 3G network. The cell phone carrier is configured to use the GSM A5/1 standard. GIAC has deployed VPN client software for secure email access from the smart phone.

The new product will be released in 3 months. Any countermeasures will need to be inexpensive as GIAC has not been paid yet for development of the new product.

3. Detailed Analysis

3.1. GSM Overview

GSM is short for Global System for Mobile Communication. It is the most popular cellular standard with over 80% of the Global market of cell phone users. (GSM World, 2009) GSM is considered a 2nd Generation (2G) mobile phone system. It was one of the first mobile technologies to utilize a digital format for signaling and speech. Other features include a low cost Short Messaging Service (SMS), commonly called text messaging, worldwide emergency telephone service and the ability to use the same GSM phone with several GSM networks through roaming agreements with those providers.

Enhanced Data Rates for GSM Evolutions (Edge) is the current standard for 3rd Generation GSM. It features improved speed for the transfer of data and the ability to operate over data networks like the Internet.

Encryption for GSM is provided primarily by the A5/1 encryption cipher, a 64 bit stream based cipher.

This type of cipher takes each bit of data and encrypts it with each successive key bit in the cipher key. When the last cipher key bit has been used the process is repeated with the next bit of data encrypted with first key bit in the encryption key. The process repeats itself until the entire data stream is encrypted.

The A5/2 cipher is similar to the A5/1 cipher but was deliberately designed to be less secure in order to meet export requirements to certain regions of the world.

The A5/3 cipher, also known as Kasumi, is a 64 bit block cipher with 128 bit keys (Dunkelman, 2010) for use with 3rd generation (3G) GSM, General Packet Radio Service (GPRS) and Universal Mobile Telecommunications System (UTMS) networks.

With a block cipher, the data is broken up into blocks and then each block is encrypted with the same key. It relies on the likelihood that no two blocks will have the exact same data in them. Block sizes and key lengths can vary.

It is important to note that both ciphers are over twenty years old. In their day, they were robust encryption solutions. With the computing power available today, they are very vulnerable to attacks designed to crack their encryption.

3.2. Recent Research, Attack Description

Security researchers have previously shown that GSM encryption has weaknesses. Attacks can be categorized into active and passive.

Active scanning involves using an “IMSI Catcher” or virtual base transmission station (VBTS) (Frick, 2000). This is a hardware device designed to emulate a cell phone base station. It exploits the requirement that the cell phone authenticate to the network and not the other way around. This device acts like a man in the middle and intercepts the cell phone communication listening in on it as it passes the communication to the real cell phone network.

Passive scanning involves not much more than a programmable antenna and laptop. Much like standard wired and wireless network sniffing the attacker simply listens and captures all the traffic to a data file. Once the data has been saved it can be taken off line where the encryption if used can be cracked and the conversations can be viewed.

Recent research has significantly lowered the bar for passive attacks on GSM encryption. The most recent research was presented in December 2009 at the 26C3 conference (Nohl, 2009). The attack reduced the time to break the encryption by using a rainbow table based pre-computed code book.

Researchers have shown weaknesses in GSM encryption before, but attacks were generally considered impractical. In 2008 and 2009, research was presented which showed practical methods for cracking GSM A5/1 encryption. Hulton presented information at Schmoo con that claimed to be able to crack GSM encryption (Hulton, 2008). In this research, Field Programmable Gate Arrays (FBGA) are used to greatly reduce computation time. Hulton predicted that GSM encryption could be cracked within 30 minutes with typical computing resources and as quickly as 30 seconds if a multi node cluster is used. This research was followed up in 2009 with practical intercept system outline using open source components (Nohl, 2009). Previous attacks have required the use of sophisticated hardware to setup a rogue base station. The latest technique is passive. The attack on the A5/1 algorithm is enabled by the pre-computed rainbow tables. For the Nohl research, these tables were calculated by using optimized algorithms on Graphical Processing Units (GPUs) and Playstations. The total storage required for the pre-computed values is 2 Terabytes.

Researchers have also shown that practical attacks against the GSM A5/3 standard are also possible. Nohl proposed a semi-active attack using A5/1 and A5/3 traffic (Nohl, 2009). Dunkelman has published research that uses a "sandwich attack" to attack the Kasumi block cipher in A5/3 (Dunkelman, 2010).

While we are primarily interested in the local connection from the cell phone to the tower, other infrastructure components also could be attacked.

At some point most cell phone calls move from wireless cell towers to the provider's wired network. At this point the security provisions for protecting the conversation data reverts to many of the same controls used on data networks. Once on the network the call may traverse several different provider networks. While cell phone providers have been more responsive about providing security controls for their cellular networks, there is no way to ensure that all provider's security postures are equal. This is particularly true of encryption. While most all providers use or support the A5 series of encryption some overseas providers utilize the weaker algorithms or no encryption at all. In this case when the cell phone may be configured to use the A5/3 encryption but actually drop to the A5/1 or no encryption at all if that is what the provider's network supports.

As a final note, cell phone provider networks are obligated by government regulations to provide the ability for government agencies to connect into the provider network for the purpose of court ordered eavesdropping of cell phone conversations. So no matter how secure a cell phone provider network is there is a built in security hole that they must maintain.

3.3. Risk

GSM phone snooping is a moderate risk to GIAC Enterprises. The risk is evaluated by looking at requirements for attackers, the likelihood of an attack and the impact of a successful attack. For the attacker, the latest attack is passive. Previous active attacks with a rogue base station would be easily detectable. The passive attack essentially allows the attacker to conduct the attack un-detected. They are therefore able to do the attack with very little risk. The availability of a pre-computed code book significantly lowers the resources required for the attack. However, the author does indicate that a "Non-trivial RF setup" (Nohl, 2009) is required.

It is difficult to comprehensively identify all possible threats. We can identify the profile of an attacker. They would need to be willing to spend thousands of dollars on hardware. They would need to assign personnel to build and operate the interceptor system. They would also need to be willing to break the law. Given these characteristics, we believe this puts the threat above a hobbyist or target of opportunity threat. It would have to be an organization specifically targeting GIAC Enterprises. Simon Bransfield-Garth from CellCrypt stated, "the publication opens call interception to any reasonable well-funded criminal organization" (O'brien, 2009).

How likely is a successful attack? An important scenario we are concerned about is executives traveling to factories and using their GSM phones. Information discussed by executives is often confidential. The factories are in known locations, so this is a static target for attackers. The other information the attackers would need is executive phone numbers. The phone numbers could be acquired from public sources or social engineering.

To summarize the risk components, an outline for an interceptor system is publicly available although non-trivial. Organizations that fit an attacker profile could exist today. If an organization were to commit resources to the attack, they would likely be able to listen in on GSM phone traffic.

Stan Schatt from ABI Research believes that, "Organizations must now take this threat seriously and assume that within six months their organizations will be at risk unless they have adequate measures in place to secure their mobile phone calls." (O'brien, 2009). Overall, we rate this risk as moderate.

3.4. Countermeasures

With regard to the individual end user and corporations such as GIAC Enterprises the greatest risk remains the capturing and decrypting of the wireless cell phone signal and the risk associated with the content of the cell phone call data. Mitigating this risk involves several non-technical and a couple technical strategies.

> Formulate a cell phone usage policy and include prohibiting the use of GSM phones for confidential information.
>
> Include cell phone security in user Security Awareness training include such things as:
>
> > Always assume that cell phone conversations, like email, are insecure and susceptible to eavesdropping or interception.
> >
> > Treat text messaging exactly like email. After all that is almost exactly what it is: real time email using a different transmission medium.
> >
> > Always use a complex password (PIN) to secure access to the cell phone and to secure the cell phone conversations and text messages when possible.
> >
> > Never leave your cell phone unintended. An attacker only needs a few minutes to steal the phone or install a malicious software or hardware (battery, SIM card, memory card).
> >
> > Do not open or respond to unsolicited or unknown texts. Do not click on embedded links in texts.
>
> Turn off Bluetooth wireless when not in use.
>
> Do not use bluetooth headsets when discussing information of a sensitive nature. Security researcher Josh Wright amongst others has shown that bluetooth wireless can be sniffed. An attacker can listen in on cell phone conversations transmitted over a Bluetooth headset without ever needing to address bypassing encryption.
>
> If there is a need to discuss confidential information over a cell phone use the following techniques
>
> > Choose a location where you cannot be overheard
> > Use code words when discussing confidential projects
> > Try engaging multiple channels (email, text messaging and voice) to break up the information.
>
> Use secure email from smart phones for secure conversations.
>
> Check with Cell phone vendors to use A5/3 standard instead of A5/1.

Use an end to end voice encryption solution (e.g. Rohde & Schwartz or CellCrypt)

Switch to different cell phone provider:

Currently both Sprint and Verizon are developing 3G cell phone networks based on Universal Mobile Telephone Systems (UMTS). This digital technology is being developed by European Technology Standards Institute (ETSI) within the International Telecommunication Union's (ITU) IMT-2000 Mobile phone standards framework. It is similar to and builds upon GSM. Two important caveats for UMTS is that most UMTS handsets support GSM in a dual channel operation. Additionally, and most importantly, UMTS utilizes Universal Subscriber Identity Module.

This is an application embedded on the Universal integrated Circuit Card (UICC), similar to the SIM card used on GSM phones it can store user information, authentication information contacts phone book entries, etc. More importantly, as part of the authentication process, it stores a more robust authentication and encryption methodology

The first part is a long term pre-shared secret key. This is shared with an Authentication Center located on the provider network The USIM also verifies a sequence number used to prevent replay attacks and to generate session keys to be used with the Kasumi block cipher that is used to encrypt the cell phone traffic (Wikipedia, 2010).

Furthermore, USIM technology not only requires the cell phone to authenticate to the network it also requires the network to authenticate to the cell phone. This mitigates the risk of man in the middles attacks and passive sniffing of cell phone data traffic.

Another important benefit of phone networks based on this technology is an established upgrade path. There is already development being done on a 4G network based on UMTS technology.

3.5. Recommendations

The recommendations are divided into two categories, short term and long term. Short term recommendations have little or no cost and can be implemented within 30 days. Long term recommendations require further investigation and a longer time frame.

There are three short term recommendations. First, create a cell phone usage policy which prohibits discussion of confidential information. Second, conduct awareness training on the policy and secure cell phone usage as described in the countermeasures section. Third, use the secure email solution for confidential information exchange on the cell phone.

The long term solution is to execute a project for secure cell phone implementation. This project will investigate technology used by available providers including encryption technologies. It will also evaluate third party solutions for end to end encryption. After evaluation a solution will be selected and implemented.

4. Summary

With recent news stories about cell phone calls being vulnerable to snooping, the Information Security Group was asked to research and report on the issue. This report has summarized the results of the research. There is published research that significantly reduces the level of effort to sniff on GSM cell calls. The attack is still non-trivial and does require some knowledge and resources. This attack represents a moderate risk to GIAC Enterprises. Given the importance of GIAC Enterprises' confidential data several short term recommendations have been provided to reduce the risk. A long term recommendation was also made to implement a solution for secure voice traffic on cell phones.

5. References

Dunkelman, Orr. (2010, January). A Practical-time attack on the a5/3. Retrieved from http://eprint.iacr.org/2010/013.pdf

Frick, J. (2000, November 8). Method for identifying a mobile phone user or for eavesdropping on outgoing calls. Retrieved from http://v3.espacenet.com/publicationDetails/biblio?CC=EP&NR=1051053&KC=&FT=E

GSM World, Initials. (2009, June). Market data summary. Retrieved from http://www.gsmworld.com/newsroom/market-data/market_data_summary.htm

Hulton, D. (2008, February). Intercepting gsm traffic. Retrieved from http://blog.washingtonpost.com/securityfix/shmoocon-Feb08-gsm.pdf

Nohl, K. (2009, August). Subverting the security base of gsm. Retrieved from https://har2009.org/program/attachments/119_GSM.A51.Cracking

Nohl, K. (2009, December 27). Gsm srsly?. Retrieved from http://events.ccc.de/congress/2009/Fahrplan/attachments/1519_26C3.Karsten.Nohl.GSM.pdf

O'Brien, K. (2009, December 28). Cellphone encryption code is divulged. Retrieved from http://www.nytimes.com/2009/12/29/technology/29hack.html?_r=3&pagewanted=1

Wikipedia, Initials. (2010). Subscriber identity module. Retrieved from http://en.wikipedia.org/wiki/Subscriber_Identity_Modulehttp://en.wikipedia.org/wiki/Subscriber_Identity_Module