GSM Sniffing

Ethan Wilder

Introduction

A couple years ago I attended Defcon in Las Vegas. Every year they put up the "wall of sheep". It's a simple list containing e-mail addresses and corresponding passwords that people have successfully gathered while sniffing the WiFi traffic from other people attending the conference. It's a good reminder to ensure your communication over the Defcon Wireless Network is encrypted.

As a result of the "Wall of Sheep", thousands of attendees refused to connect their mobile devices to the wireless network. Defcon had for the first time provided a WPA2 encrypted wireless network for public use as well, but people would still refuse to use it. Instead they would check e-mail or surf the web over their standard GSM data connection. The use was so heavy that the 3g network was unusable between sessions. Every time I tried to connect to my Gmail account over SSL on the 3g network I couldn't help but wonder if someone was sniffing that too. It is just radio waves after all.

This paper aims to explain how an individual can go about sniffing GSM data in transit. It was discovered early on that much of this has been researched in theory already. The first section describes 2 methods to go about sniffing GSM traffic. The second section goes into detail about the implementation build and the challenges encountered. The third section describes the last ditch attempt to overcome the hurdle described in section 2.

Methods

There are several methods for sniffing GSM traffic. This paper discusses 2 of the most logical:

- Basic Intercept
- Fake Base Station

Basic Intercept

This method is about as straightforward as it gets. GSM data is transmitted wirelessly from base station to mobile device. This technique involves simply listening on the GSM frequency band and recording what it hears. There are a few challenges to this:

Frequency Hopping Challenge

GSM transmissions use frequency hopping for reliability. This means that each transmission operates on a different frequency channel chosen “secretly” to an external listener. Therefore to record a complete transaction requires listening on all available frequency channels and piecing together the complete transaction. This is more difficult than impossible.

Encryption

GSM air transmissions are encrypted using the A5/1 algorithm. It was shown in a presentation at the BlackHat convention in 2008 [1] that this encryption method had some flaws. In particular the key selection was weak and could be brute forced ‘quickly’. While this challenge seems overcome in theory the practical implementation of this theory is considered difficult.

The method of intercepting traffic out of thin air is possible but difficult. It requires an air interface antenna that could receive the traffic. It would then have to reassemble the entire transmission from encrypted fragments. Again, while possible this would be relatively difficult. If there were to be multiple devices transmitting in the same area this method would become even more challenging.

Fake Base Station

This method is really an evolution from the previous. Building a device that can listen to GSM traffic off the air is a large piece of the work needed to just create a base station. The addition of having a base station opens up the very appealing opportunity of creating a Man in the Middle situation. The theory is very simple, create a base station and have mobile stations communicate directly with your base station. This quickly alleviates the challenges involved in the first method. It does however present a new challenge.

User Interaction

Base stations that are part of a single network essentially know about each other. While there isn't a significant amount of authentication involved in connecting to a base station within a network like using a network specific secret key, there's enough information to where the mobile device effectively knows it's connecting to something new. Some mobile devices will blindly accept this and continue on as normal. Other mobile devices may prompt the user and ask if they wish to connect.

Ultimately user interaction is not a significant challenge to overcome as most users won't know the difference. It is therefore probably the best method to intercept GSM data traffic. Unfortunately the effectiveness may be reduced at an event like Defcon vs an average coffee shop.

Build

Building a fake base station requires the following components:

- **Antenna** capable of listening to the GSM frequency band
- **Software Radio Interface** to handle processing of incoming traffic.
- **Internet connection** to forward traffic so that the base station acts like a real base station.

The last 2 items are easy. Any computer with an internet connection satisfies the last condition. Open BTS [2] is an open source implementation of a software radio interface. The issue comes from finding a suitable antenna.

There are 2 possible antennas that could connect to OpenBTS that were under $5,000. The first one was OpenBTS's recommended RangeNetwork's Development Kit [3]. The other is a USRP (Universal Software Radio Peripheral) [4]. Both of these options were a large sum of money.

Cell Phone Option

The final option considered was to use the GSM antenna for this project that is used every day. The cell phone. In a world where the concept of the app dominates it seems rather unlikely we couldn't hack an android or iphone into acting as a base station.

I looked closely into the programmer API's of both iPhone and Android. iPhone does not have anything even remotely resembling an interface other than its public socket API. Some extreme hacking would have to be done to reverse engineer where exactly it calls the RLI "Radio Layer Interface".

Android does have a RLI “Radio Layer Interface” library on some android platforms [5]. It’s specifically setup for telephony functionality. It’s intended to “send” more than “receive” which are the requirements of a base station.

Ultimately the cell phone libraries are not quite exhaustive enough to be used in placement of an antenna. At least not economically.

Conclusion

The sniffing of GSM traffic is theoretically possible. Unfortunately it requires a financial an investment that is not within means for everyone. Cellphone API might eventually evolve to where it needs in order to achieve this functionality but with awareness of cellular data security growing it seems unlikely that vendors will be willing to expose such APIs. Perhaps an open source library coming out sometime to accomplish this. Until then it is bitter sweet to know not just anyone can be reading my data over the air unless they’re significantly invested in doing so. In which case there is likely a bigger threat looming than mischievous teenage behavior.

References

[1] Intercepting GSM traffic. Steve D. Hulton.
http://www.blackhat.com/presentations/bh-dc-08/Steve-DHulton/Whitepaper/bh-dc-08-steve-dhulton-WP.pdf

[2] Open BTS
http://openbts.org/

[3] RangeNetwork Development Kit
http://www.rangenetworks.com/store/development-kit

[4] USRP Networked Series
https://www.ettus.com/product/category/USRP_Networked_Series

[5] Android Radio Layer Interface
http://www.netmite.com/android/mydroid/development/pdk/docs/telephony.html