Discovery of Rogue Mobile Phone Towers

Jóannes í Sandagerði

Kongens Lyngby 2015
IMM-M.Sc.-2015-

Technical University of Denmark
Department of Applied Mathematics and Computer Science
Matematiktorvet, building 303B,
2800 Kongens Lyngby, Denmark
Phone +45 4525 3351
compute@compute.dtu.dk
www.compute.dtu.dk IMM-M.Sc.-2015-

Summary (English)

Since August/September 2014, multiple newspapers have claimed to have found evidence of rogue mobile phone towers, so called IMSI Catchers. An IMSI Catcher is capable of imitating a normal mobile phone tower, and thus is able to trick an unsuspecting phone to connect to it. Once a device has connected to the tower, it may become vulnerable to various “over-the-air” attacks as having identifying information stolen, eavesdropping on calls and texts. This project aims to propose a solution for discovering IMSI Catchers. We will document what identifying artefacts are transmitted by IMSI Catchers. We will document what software and hardware is required. Lastly, we will perform an empirical study of cells operating in Copenhagen. We will, using our proposed solution, attempt to determine whether we are able to detect an IMSI Catcher. The proposed solution is able to detect mobile towers, and we have shown that the discovery of IMSI Catchers, using our system is feasible. However, due to time-constraints preliminary results are inconclusive on whether any IMSI Catchers were found.

Summary (Danish)

Siden august/september 2014 har flere aviser hævdet at have fundet beviser for falske mobiltelefon tårne, såkaldte IMSI fangere. En IMSI fanger er i stand til at efterligne en normal mobiltelefon tårn og er således i stand til at narre en intetanende telefon til at oprette forbindelse til den. Når en enhed er tilsluttet tårnet, kan det blive sårbar over for forskellige "over-the-air" angreb som havende identificerende oplysninger stjålet, få aflyttet opkald og smser. Dette projekt har til formål at foreslå en løsning til at opdage IMSI fangere. Vi vil dokumentere hvad identificerende artefakter overføres af IMSI fangere. Vi vil dokumentere hvilken software og hardware er påkrævet til at bygge en IMSI fanger. Endelig vil vi udføre en empirisk undersøgelse af tårne, der opererer i København. Vi vil, ved hjælp af vores foreslåede løsning, forsøge at afgøre, om vi er i stand til at opdage en IMSI catcher. Den foreslåede løsning er i stand til at detektere mobile tårne, og vi har vist, at opdagelsen af IMSI fangere, ved hjælp af vores system er mulig. Men på grund af tids begrænsninger viser vores foreløbige resultater ikke klart, om nogen IMSI fangere blev fundet.

Preface

This thesis was prepared at the department of Informatics and Mathematical Modelling at the Technical University of Denmark in fulfilment of the requirements for acquiring an M.Sc. in Informatics.

Lyngby, 23-June-2015

Jóannes í Sandagerði

Jóannes í Sandagerði

Acknowledgements

I would like to thank my supervisors Christian D. Jensen, and Luke Herbert for their in work for this thesis. Additionally, I would like to thank Jens A. Bjørnager from Berlingske for his contributions to the data gathering process.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Motivation

Mobile networks are becoming ubiquitous, the number of mobile phone users worldwide in 2014 is estimated to be 4.55 billion [EMa14], and this number is growing steadily. Users are demanding and expecting to have access to mobile networks at all times and at all locations. As a result the mobile network infrastructure is large and ever growing. Customers increasingly demand higher network transfer speeds, and to meet this demand, network operators are always looking to upgrade their infrastructure to the latest and greatest technologies. However, for backward compatibility reasons, a large number of older Global System for Mobile Communications (GSM) networks are still in operation. Unfortunately, many of these older GSM networks are lacking many of the enhanced security and privacy measures that are offered by the newer technologies.

It is in the context of these GSM networks that this thesis is based. GSM networks have been documented to have a number of security issues. A number of researchers have shown that it is possible, using consumer available hardware and software, to build an IMSI Catcher [DPK+14, And11, SZC12, SHL11, HvH+14, GRB12, NM10]. These devices are able to acquire mobile phone identity information by tricking them to connect to a mobile phone tower. This data is claimed to be anonymized and randomly generated periodically, however research has shown that it may be possible to find metadata that indicates the owner of the mobile phone [DDBP08, Eng09, CCRS10]. Using a signal jammer, an attacker may be able to bar users from using the GSM networks [SZYC10]. Specially crafted Short Message Service (SMS) messages sent to a mobile phone causes the device to continuously crash and reboot [GM11]. Paging request messages being transmitted by the network operator, are broadcast messages that are sent to all mobile phones within an area. Using a mobile phone running a modified baseband software, researchers showed that it is possible to receive SMS messages intended for other recipients, de-authenticate all mobile phones connect to a network within a whole city [Gol12]. Finally, researchers have known for some time that some of the encryption schemes used in GSM communication are weak or have been broken [Noh, Noh10].

These are just some of the known problems that exist in GSM mobile networks.

The motivation for this project stems from recent discoveries of Rogue Mobile Phone Towers (RMPTs). A Rogue Mobile Phone Tower, which is sometimes referred to as an IMSI Catcher, is a device which is capable of imitating a normal Mobile Phone Tower, but which can be used for nefarious purposes. The fascinating thing about these IMSI Catchers, and which is a part of the motivation for this project is that in the last couple of years, there have been documented numerous cases where IMSI Catchers have been discovered in cities around the world.

In neighbouring Scandinavian countries, newspapers have made claims about having found evidence of IMSI Catchers. Most recently, the Norwegian newspaper Aftenposten, in collaboration with two independent security companies, claimed to have found evidence of RMPTs being employed in, and around, various politically, and financially important locations in Norway [BJHT14]. The validity of the newspapers' claims have been discussed, even refuted by the Norwegian Police Security Service PST [BJ15, NTB15]. Whichever party is correct in their claims, is not for this thesis to say. However, this, and other stories, have resulted in a growing public interest in the topic of security in mobile communication here in Denmark. A question that has been asked by many is: are, or have, similar devices ever been used here in Denmark? If so, by whom have they been used, and for what purpose?

These are some of the questions that this thesis will explore, and use as a basis for further research in the domain.

To understand why it is interesting to know whether a IMSI Catcher has been deployed here in Denmark, and in other countries, one must first understand a few things: What is a Mobile Phone Tower, and how does a *Rogue* Mobile Phone Tower differentiate from a normal tower.

What is a Mobile Phone Tower?
In short, it is a device that provides network connectivity for mobile phones on the wider mobile telephone network. A Mobile Phone will continuously search for towers to connect to, and based on selection criteria related to signal strength, the mobile station will connect to the tower, authenticate the Subscriber Identity Module (SIM) on the network, and if the subscriber is authorized on the network, the phone will then be a able to utilize the offered network services. A IMSI Catcher can be loosely compared to the function of an Access Point in a typical wireless local area network. Client devices wirelessly connect to the Access Point, which in turn can be connected to Wide Area Network, which then ultimately provide Internet connectivity to all devices connected to the AP. Further detailed explanations on how Mobile Phone Towers operate are given in Chapter 2.

Rogue Mobile Phone Towers
A Rogue Mobile Phone Tower is a tower, or more likely, a small mobile device, which imitates a normal tower. To a mobile station, the rogue tower is no different to a legitimate tower, and as a result, the mobile station will happily connect to the rogue tower if the selection criteria are met.

Terminology
The terminology used to refer to a *Rogue Mobile Phone Tower* varies from source to source. Other terms that have been observed:

IMSI Catcher, IMSI Grabber, Cell-Site Simulator, Fake Mobile Phone Tower, Stingray, Rogue BTS, Fake BTS, Weaponized Femtocell, etc..

The terms above generally all refer to the same type of device. A device which this thesis will refer to as an IMSI Catcher.

The term used for the proposed system for detecting an IMSI Catcher will be referred to as an IMSI Catcher-Catcher.

1.1 Objectives of the Thesis

The main objective of this thesis is to:

Propose a solution for discovering rogue mobile phone towers.

Based on the motivating context of Chapter 1, there is an interest in investigating whether Rogue Mobile Phone Towers are being used in Copenhagen, Denmark. With that in mind, this thesis will propose a solution for a system that is capable of detecting the presence of an IMSI Catcher. Using the proposed system we will perform measurements in various locations around Copenhagen.

Central to the work of this thesis is to document any detectable traits of a rogue mobile phone tower. This thesis will not be able to guarantee whether IMSI Catchers have been in use in Denmark prior to the start of the project, as that would require a backlog of data, which does not exist. However, this thesis will make an attempt at determining whether an IMSI Catcher is deployed, in the areas where our measurements were taken, and at the time the data was gathered.

Limitations of the project scope

- The first version of the proposed solution will only be able to detect any IMSI Catcher operating on the GSM 900 band. Expanding the system to function on the other GSM Bands would be trivial, however, in the interest of time and due to hardware limitations, only one major band has been chosen.
- The proposed solution requires that data be gathered and analysed at a later time. A system with live feedback would require some restructuring of the proposed solutions' software stack, and would likely take more time than is available for this project.

A more extensive statement of the objectives is as follows:

1. **Research:** Research and document background information need to be able to understand how a GSM900 network operates.
2. **Installation:** Acquirement of hardware and software necessary to create a system for scanning GSM900 frequencies for Mobile Phone Towers.
3. **Methods for discovering IMSI Catchers:** Analyse how an IMSI Catcher might work, and identify revealing artefacts of an IMSI Catcher.
4. **Identify Possible Target Locations:** Investigate possible locations, in Copenhagen, Denmark, where an IMSI Catcher could be likely found.
5. **Gather Data:** Using the produced hardware and software system, we aim to perform survey of mobile towers in the previously identified target locations.

6. **Data Extraction:** Produce a system for converting raw GSM tower data in to a form where we can determine whether the tower may be malicious or not.
7. **Analyse Data:** Analyse processed data for any suspicious activities that might stem from an IMSI Catcher.

1.2 Project Methodology

Build a prototype solution for detecting an IMSI Catcher. We will then, using aforementioned prototype, perform an empirical study of mobile phone towers in certain locations around Copenhagen, Denmark. We will seek to identify a set of predefined locations, where the likelihood of detecting an IMSI Catcher may exist. We will then proceed to mobilize our prototype and drive to each of those locations and perform the survey. Lastly, we will put theory to practice and attempt to determine whether any IMSI Catchers have been observed at the target locations.

This thesis has met its goals if we are able to successfully create a prototype IMSI Catcher-Catcher solution. Discoveries of an IMSI Catcher are not guaranteed, and may depend on a variety of factors, which will be discussed further in Chapter 4.

1.3 Organisation of the Thesis

The structure of the thesis reflects the goal given in Section 1.1. The thesis has been structured in such a way, that each chapter reflects and goes in to depth, and attempts to answer the questions set by the thesis objectives.

The chapters of this thesis contain the following material:

Chapter 1 Introduction:
This chapter states the objectives for the thesis and introduces the motivating context of IMSI Catcher and provides an overview of the structure of this thesis.

Chapter 2 Background:
This chapter provides the necessary background information required to

understand the basics of GSM networks. To produce an IMSI Catcher-Catcher it is necessary to have an understanding on how a Mobile Station (MS) discovers a Base Transceiver Station (BTS), how the BTS can identify itself to the MS and various other aspects of the communication between an MS and a BTS. With the basic understanding of GSM, we go to explain what it means when we say IMSI Catcher. We explain what it is, how it can be used, and what purpose an IMSI Catcher might serve.

Chapter 3 Building an IMSI Catcher-Catcher:
In this chapter we propose a system capable of detecting the presence of an IMSI Catcher, an IMSI Catcher-Catcher. The proposed solution is a Software Define Radio (SDR) based system. We will then explain the reasoning behind the system, how it performs, and how it compares to other existing, and possible solutions. Lastly in this chapter we document the software projects that have been used, and which function they perform in this project.

Chapter 4 Detecting an IMSI Catcher:
In this chapter, we will attempt to explore the various methods of detecting the presence of an IMSI Catcher. Based on the background knowledge that we have established, with how the GSM networks operate, what data is transmitted by a BTS, how MS will choose to select the cells that it chooses to camp on, etc. we are able to device a system that detects anomalies in a typical GSM network. We will document some of the known anomalies that can be detected by a device which has been set to receive on the right frequencies.

Chapter 5 Data analysis:
In this chapter we will document the process of gathering data that we will analyse using our IMSI Catcher-Catcher system. A justification for the data acquisition locations is given. Secondly we will do an analysis of the data and form a hypothesis on the results gained from the dataset.

Chapter 6 State of the Field:
This chapter looks in to the state of the field. It looks in to the work that has been done, in the creation of IMSI Catcher-Catchers as well as IMSI Catcher-Catchers solutions. In recent years, there has been a growing number of cases where IMSI Catcher-Catchers have been known to be used in the field. This chapter will investigate and summarize some of the discoveries that have been found. Lastly, this chapter will attempt to make a hypothesis on which parties that may have the benefit of using such a device, and for what purpose.

Chapter 7 Future Work:
In this chapter we explore possible future work that could be performed

on the basis on the work made in this thesis. We explore some of he shortcomings of this project, and what can be done to create a second prototype IMSI Catcher-Catcher.

Chapter 8 Conclusion:
This chapter concludes the thesis and provides a brief summary of the main contributions of this work. The contributions of the thesis are summarized. We determine whether we have met the goals that were identified at the onset, and a summary of the results of the thesis is given.

Appendix A :
This appendix documents the installation procedure required to setup the required software solutions used in this thesis.

Chapter 2

Background

Overview

This chapter will give some background information on mobile networking protocols. This chapter will provide sufficient background knowledge required for understanding how a GSM mobile network operates. Additionally, this chapter will introduce the term IMSI Catcher, what it is, how it operates, and what it is that makes an IMSI Catcher the focus of this thesis. Using the background knowledge gained, we should be able to create a prototype solution for detecting the presence of an IMSI Catcher. That will be covered in the following chapters.

2.1 GSM Networks

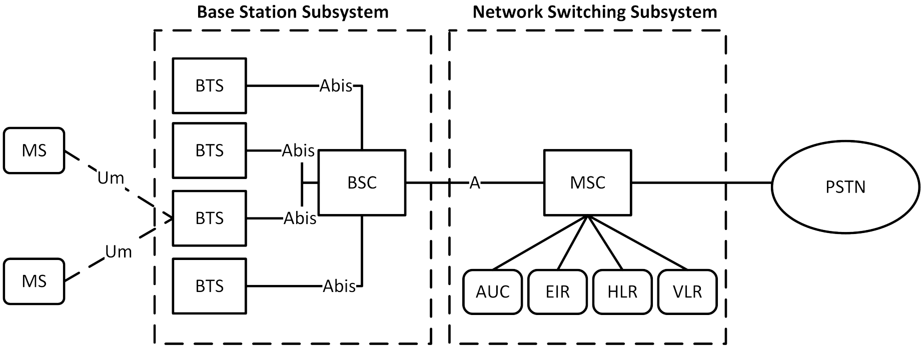


Figure 2.1: GSM Network Overview

The Figure 2.1 shows a general layout of a GSM mobile network. Below we explain the main components of this diagram, their function, and how the components communicate with each other.

A quick summary of the main components shown in this diagram. MS (Mobile Station) is typically a mobile phone. The BTSs (Base Transceiver Station) are what we have previusly referred to as a mobile tower. These two are the main components, and will be the main focus in this thesis. The rest of the components are explained further in the following section.

2.1.1 Interfaces in GSM

Air Interface

The air interface between the MS and the mobile phone tower, or Base Transceiver Station BTS is called *Um* interface. The name *Um* comes from the fact that this is the mobile equivalent of the *U* interface in ISDN networks. It is through this interface that the MS receives Broadcast Control Channel (BCCH) messages from the BTS.

The transmission protocol on this interface is *Link Access Protocol on the Dm-channel (LAPDm).*

It is on this interface, that the majority of the data, used in this thesis, has been collected. However, the exact details of how data is exchanged on this interface is out of scope for this thesis. Further details can be read in the GSM standard documents [ETS94, ETS06].

BSC/BTS Interface

The physical communication interface between the BTS and Base Station Controller (BSC) is called *Abis*. The *Abis* interface transmits traffic and signalling information between the BTS and the BSC. The transmission protocol on the interface is *Link Access Protocol on the D-channel* (LAPD) [ETS96c].

MSC/BSC Interface

The physical interface between the Mobile Service Switching Center (MSC) and the BSC is called the *A-interface* [OET98]. This interface carries data between the Network Switching Subsystem (NSS) and the Base Station Subsystem (BSS) with information about channel allocation, timeslots and other relevant data required by MSs that are being services by the BSS. The messages that are required for handling handover, routing, SMS exchange, are carried over this interface [OET98].

2.2 Components of a GSM network

2.2.1 MS

A mobile device, that is a part of the mobile network, called a Mobile Station (MS). An MS is a Mobile Equipment (ME) (a mobile phone, tablet, or other device capable of connecting to the mobile networks), which contains a SIM card.

2.2.2 SIM

The Subscriber Identity Module (SIM) is a smart-card provided by the network operator that is either inserted in to the ME, or can be found embedded in the ME. A SIM contains data identifying the MS on the mobile network.

A SIM contains the following data:

Integrated Circuit Card Identifier (ICCID)
An, up to 22 digits long, unique identifier used to identify each individual SIM card internationally. This identifier is typically physically burnt on the surface of the card, as well as stored on the chip. The IMSI may be changed, but an ICCID stays the same. This number may be considered as the Serial Number of the SIM card.

International Mobile Subscriber Identity (IMSI)
This number identifies the MS in the network. This is the identity of the MS and is used for among other, to determine whether a subscriber has a service contract with the network. See Section 2.2.14.

Authentication Key (K_i)
The key K_i is a 128 bit value that is for authenticating the SIM on the network. This value is generated by the network operator, and stored on the card when it is created. A copy of K_i is stored on the networks' Authentication Center (AUC).

Location Area Identification (LAI)
The SIM card stores information about the last network LAI which the MS has been connected to. If the MS is power cycled, it will read the LAI stored on the SIM and search for that LAI again. See Section 2.2.11.

Data
Contacts, SMSs, and other user created data.

The LAI storage on the SIM is a storage where the network operator, can choose to store a list of networks that the MS should recognize, and prefer, over other discovered networks. Information stored could be the names of known networks e.g.:

Without a LAI list, the phone might simply display: ***MNC: 01***

With a predefined LAI list, provided by the operator, the phone could display: ***TDC A/S***

2.2.3 GSM TDMA

In 2G GSM networks, signals are transmitted using Time Division Multiple Access (TDMA). TDMA is a method of sharing access to a limited frequency range, which is the case of allocated frequency range for GSM networks, by transmitting signals in different timeslots. GSM divides each 200kHz channel into eight 25kHz timeslots [ETS15a].

2.2.4 BTS

A Base Transceiver Station (BTS), is what an MS will connect to, via the Air interface, for network connectivity. The BTS is also sometimes referred to as a *cell*, or a *cell tower*. A BTS provides network connectivity to MSs that are within its range. Previously in this thesis, we have referred to a Mobile Phone Tower, for the rest of the thesis we will refer to them as a BTS/Cell.

All GSM BTSs will continuously transmit information about their existence, current system configuration, and other information required by MSs before they are allowed and able to access the network. The information transmitted by the BTS is organized in eight different **System Information** type messages, where each contain different parameters.

System Information type 1 through 4 are transmitted on the Broadcast Control Channel (BCCH). Type 5 and 6 are only transmitted during an already established individual radio link in downlink direction in a multiplexed service channel called Slow Associated Control Channel (SACCH). System Information messages are sent in a cyclic order on the TDMA frames.

For this thesis, the messages of interest, are the ones that are transmitted on the BCCH. We will primarily be looking at the **System Information Type 3** messages. Type 3 messages contain identifying information about the cell such as its ID, network operator, area code, and other parameters which are relevant for work in IMSI Catcher and IMSI Catcher-Catcher development.

Figure 2.2 is an illustration on what a BTS typically might look like.

Typically, cell sites are installed in such a way that there is no interference among neighbouring cells [OET98]. Figure 2.3 illustrates how a number of cells may be distributed in a cityscape.

2.2.5 BSC

Base Station Controller (BSC), sometimes referred to as the radio switch, is a components that manages multiple BTSs in one area. The BSC is responsible for setting up radio channels and signalling to the MSC, as well as monitoring

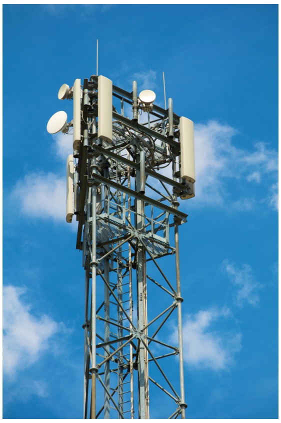


Figure 2.2: Cell tower [Pug10]

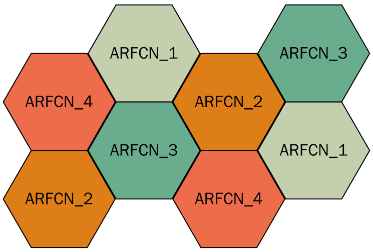


Figure 2.3: Cell sites

access to the network portion of the connection. Additionally, a BSC handles handover [1]between BTSs that it controls [OET98].

2.2.6 BSS

Base Station Subsystem consists of BTSs and BSCs, and is responsible for handling traffic and signalling between MEs and the NSS.

[1] Handover, is the act of transitioning an MS between BTSs, BSCs,channels, etc. without interrupting the network traffic for the MS [OET98].

2.2.7 MSC

Mobile Service Switching Center is a core part of the GSM mobile networks. An MSC handles MS handover switching between other MSCs, routing calls and messages, as well as interfacing with other networks e.g. the Packet Switched Telephone Network (PSTN).

The MSC is comprised of four components: Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), and Authentication Center (AUC).

HLR
A database with all MSs that are registered with the network operator. Information about the location of each MSs is also stored here.

VLR
A database store with information about visitors who have roamed within the MSCs service area.

EIR
The database store with information on the identity of every ME. The register is used to check whether a *me* has been reported stolen, or barred from some reason.

AUC
The authentication center stores security information, e.g. encryption keys for all subscribers of the network.

2.2.8 MCC

Mobile Country Code is a 3 digit number, which identifies a country of domicile of the MS. E.g.:

Denmark, has been allocated ***238***

Faroe Islands, have been allocated ***288***

2.2.9 MNC

Mobile Network Code (MNC) this is a 2-3 digit number that identifies the network operator. Mobile Country Code (MCC) and MNC, sometimes referred to as the “MCC/MNC tuple” is a value that uniquely identifies the network operator on the GSM Public Land Mobile Networks (PLMNs).

Example: **TDC A/S** has the MNC **01**

A list of MNCs currently being utilized in Denmark is given later in the paper, see Table 2.1.

2.2.10 LAC

A Location Area Code (LAC) is a 16 bit number given to identify an area. Wireless mobile networks are typically organized in areas that cover large geographical areas and are operated by several BTSs. The LAC is used when routing calls and messages to MSs.

2.2.11 LAI

Location Area Identification number. This number uniquely identifies a location area within a GSM PLMN. The LAI is broadcast on the downlink BCCH channel over the *Um* interface from the BTS to the MS. A *BTS* will continuously transmit broadcast beacons on the active ARFCNs [ETS15b].

The number consists of three components:

- Mobile Country Code (MCC), the same as in IMSI
- Mobile Network Code (MNC), the same as in IMSI
- Location Area Code (LAC)

2.2.12 CI

The Cell Identity (CI) is a 2 octet value that is used to identify a BTS. The value can be encoded using full hexadecimal representation; e.g. ***45393***.

2.2.13 CGI

If we add a CI to the LAI then we get the *Cell Global Identification.* This is a value that is used to identify a cell within an LAI.

2.2.14 IMSI

IMSI or International Mobile Subscriber Identity. This is an identification number that is provided by the network operator to allow identification of the mobile device on the network. The number is typically stored on the Subscriber Identity Module (SIM).

The number consists of three components:

- Mobile Country Code (MCC)
- Mobile Network Code (MNC)
- Mobile Subscriber Identity Number (MSIN), this is also the phone number

The first 3 digits of an IMSI are the MCC, then 2-3 digits for MNC and the last 9-10 digits are the MSIN. In total a maximum of 15 digits form the IMSI [ETS96d].

2.2.15 IMEI

IMEI or International Mobile Equipment Identity. This number identifies the Mobile device on the GSM/UMTS network. The IMEI uniquely identifies a specific mobile device. This is used for, among others, to allow law enforcements to identify and track a lost/stolen mobile phone [ETS14].

2.2.16 TMSI

Temporary IMSI, this is a pseudo-random number that is generated on the mobile subscribers device. This number is used in the communication between the subscriber and the network provider, whenever there is a data communication.

The IMSI number is typically constant, and to help mask that number and keep the IMSI number private, an TIMSI number is transmitted instead.

Many of these numbers, and others, can be obtained by an attacker, if he is able to operate a rogue mobile tower.

2.3 IMSI Catchers

> *"multi-channel, software-defined, two-way electronic surveillance radios for authorized law enforcement and government agencies for interrogating, locating, tracking and gathering information from cellular telephones"*
>
> –[Tra13]

The quote above is from the product description given in a patent application for the *Stingray*, an IMSI Catcher device. There are multiple implementations of IMSI Catcher available, however the name *Stingray* is often used interchangeably with the term IMSI Catcher. The quote above describes quite well what an IMSI Catcher is capable of. In essence, an IMSI Catcher is a device that is capable of imitating a legitimate Mobile Phone Tower. The IMSI Catcher may act as a man-in-the-middle, which lies between the user and the network operator. An IMSI Catcher is able to acquire information about a users' mobile phone, whether a user is present in an area, the contents of the voice calls, SMS messages and more.

One of the reasons that it is possible to create a device that imitates a BTS, and which is able to trick MSs to connect it, lies in the fact that the verification of identity between BTS and MS is only one way. The BTS will authenticate the MS, decide whether the MS is allowed on the network or not. However, the MS will ***not*** authenticate the identity of the BTS. Additionally, the decision on whether to use encryption or not, lies with the BTS. When a MS wants to connect to a BTS, the BTS will transmit a "CIPHERING MODE COMMAND" to the MS. This message indicates the ciphering ciphering algorithm that the BTS suggests. The MS will then reply with the ciphering modes that it supports, or send a "CIPHER MODE REJECTED" message, or a "CIPHER MODE COMPLETE" message. After receiving the complete message, the network will change to the newly agreed upon mode [OET98]. The interesting thing about this handshake process, is that the BTS dictates what type of encryption mode to use.

Mobile phones will automatically attempt to connect to a mobile phone tower. When deciding which tower to connect to, the mobile phone will, among others, attempt to choose the tower with the highest signal strength. An IMSI Catcher can force unsuspecting MSs to connect to it by providing a higher signal strength, than the surrounding real mobile phone towers. By providing the highest signal strength, the mobile phones will automatically attempt to authenticate themselves with the IMSI Catcher.

An IMSI Catcher can also operate as an Man In The Middle (MITM). That is when the IMSI Catcher forwards calls and messages on to the phone network. The attacker can do this forwarding in a number of ways. The simplest on being, by using a second mobile phone, and forward calls and messages through that phone. The problem with this solution is that the Caller ID will not match the one of the originating phone [DPK$^+$14]

Why the term IMSI Catcher?
When an MS wakes from a cold start and connects to a BTS for the first time it will transmit certain identifying information to the BTS. Specifically, the phone will among other, transmit an IMSI number to the BTS. Section 2.2.14 describes the IMSI number. The BTS receives the IMSI number, and passes it through to the MSC. The MSC will then check for this number in the HLR and verify whether the MS is a subscriber on the network, or if he is a ‘foreign user’, and thus is ‘roaming’ the network. We have previously established that an IMSI Catcher is capable of imitating a legitimate BTS and thus gain access to certain data from the MS. Where IMSI Catcher get their name from is the fact that they are able to harvest the IMSI numbers from MSs that connect to it. This IMSI number can then potentially be used by an attacker for nefarious purposes, such as tracking the movements of an individual [DDBP08].

MSs can be tricked into performing a Location Update, which results in the IMSI number being transmitted to the BTS. A location update occurs, when an MS connects to a LAC that differs from the one used by the currently serving BTS.

An attacker who would want to gather IMSI Catcher numbers can configure an IMSI Catcher to imitate surrounding BTSs, by using the same MNC and MCC, but trick the MS to performing a Location Update by using a different LAC [SZC12].

Availability of IMSI-Catchers

In this section we list some of the available IMSI Catcher products. This will not be an extensive and complete list, however it simply serves to document that these devices are available to purchase for certain entities. A majority of the device manufacturers only provide them for sale to military, law enforcement, and intelligence agencies. At the time of writing, a widely available commercial solution has not been found by the author of this thesis.

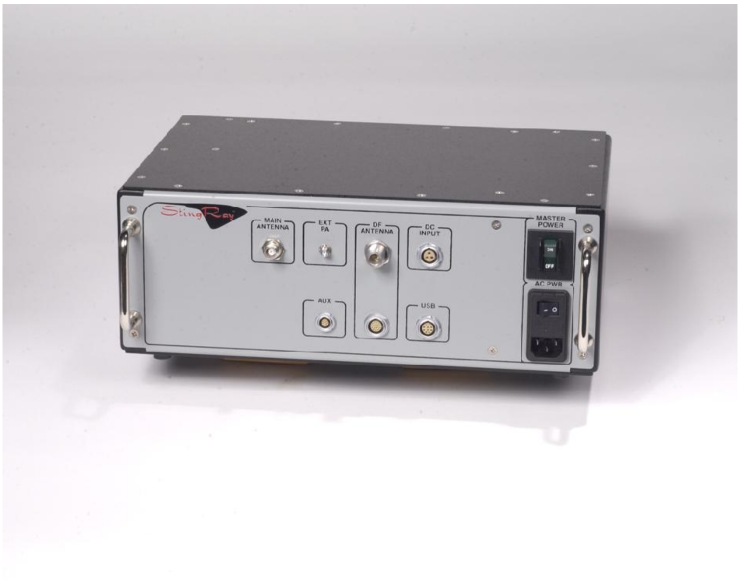


Figure 2.4: Stingray Trademark application [Tra13]

The Figure 2.4 is an illustration from the patent application for one of the better known IMSI Catchers. A large portion of the news articles on this topic refer to this specific device. The figure also illustrates the size of such a device. In the media, it has often been referred to a “rogue mobile phone tower”, “fake cell tower”, or similar, which can be deceiving. Compared to the size of a regular BTS as seen in Figure 2.2, these devices can be small and very mobile. An attacker could easily hide such a device in a backpack, Christiania bike, trolley, or other innocent looking vehicle of transportation, and thus get close to the victims.

Other devices that all perform similar functions are available: Intercept [Int], PKI [PKI], Septier [Sep], Patent [Pat03]

2.4 IMSI Catcher-Catcher

An IMSI Catcher-Catcher is a device that is able to detect the presence of an IMSI Catcher. The primary focus of this project will be to investigate the required technology for identifying an IMSI Catcher, i.e. to build an IMSI Catcher-Catcher. The following chapter will propose the design for an IMSI Catcher-Catcher. In Chapter 4 we will describe some of the methods for detecting an IMSI Catcher.

2.5 Cell Selection Process

Normal Cell Selection

The GSM Standard document 05.08 describes how an MS, which has no prior knowledge of which channels have BCCH carriers, shall search for channels with BCCH carriers.

An MS shall search all channels within its bands of operation, and for each channel, the MS shall take readings of received signal strength and calculate an **RLA_C** *(Received Level Averages)* for each. The MS shall take an average of five samples on each channel, and the measurement samples shall be spread over a time-period of three to five seconds. An MS is allowed to camp on a cell after decoding all relevant BCCH data [ETS05].

Cell Reselection Selection

In [ETS05] it is described that an MS shall read and synchronize BCCH information from six of the strongest non-serving cells[2]. Every five seconds the MS shall calculate the Path loss criterion parameter (C1) and Reselection criterion parameter (C2) for the serving cell, and re-calculate the C1 and C2 for non-serving cells.

Following is a list of conditions, that will cause the MS to reselect cell to camp.

1. The serving cell is barred.

[2] Cells that the MS is not currently camped on.

2. The C1 value on the current cell falls below 0 for five seconds, which indicates that the path loss is high.
3. The calculated value C2 for non-serving suitable cells exceeds the value of C2 for the serving cell.
4. The calculated value C2 for non-serving suitable cells exceeds the value of C2 by at least Cell Reselect Hysteresis (CRH)[3].
5. Downlink signalling failure counter (DSC) expires.

If any one of the given criteria is met, then the MS will initiate what is called a cell reselection. It will find a new BTS to camp on [ETS05].

2.6 Mobile Networks

In most countries, the radio frequencies are centrally regulated by an entity within the state. This ensures that radio communication, when performed by various operators, does not interfere with the communication by other operators. In Denmark, this regulation, is performed by *Erhervsstyrelsen*.

Mobile Operators in Denmark:

- TDC Mobile A/S
- Telenor A/S
- Telia Mobile AB
- Hi3G Denmark ApS (3)

Erhvervsstyrelsen provides a list of Network Providers, and their respective Mobile Network Codes. Below is a complete list of the network providers, in Denmark, that have been allocated a MNC.

The values shown in the Table 2.1 will be referred back to when performing analysis of the data gathered for this thesis.

[3] Value is in dB, and is received from the serving cell on the BCCH.

MNC	Network Operator
01	TDC A/S
02	Telenor
03	MACH Connectivity
04	NextGen Mobile Ldt T/A CardBoardFish
05	Dansk Beredskabskommunikation
06	Hi3G
07	Mundio Mobile
08	Voxbone
09	Dansk Beredskabskommunikation
10	TDC A/S (forsøgsdrift)
11	Dansk Beredskabskommunikation (forsøgsdrift)
12	Lycamobile Denmark Ltd
13	Compatel Limited
15	Ice Danmark ApS
16	Tismi BV
20	Telia
23	Banedanmark
28	CoolTEL
30	Interactive digital media GmbH
43	MobiWeb Limited
66	TT-Netværket P/S
77	Telenor

Table 2.1: MNC values, and Network Operators in Denmark

Chapter 3

Building an IMSI-Catcher-Catcher

Overview

This chapter will describe hardware and software tools required for building an IMSI Catcher-Catcher device. This chapter describes a possible system for detecting an IMSI Catcher. The proposed solution used software radios, and we will attempt to justify the decision for this choice.

See Figure 5.1 for a photo of the hardware setup.

3.1 Software Defined Radio

A Software Define Radio is a hardware component where the radio frequency communication is defined in software. What this means, is that we can have one hardware component, that is capable of Transmission (Tx), Reception (Rx) or both Transmission and Reception (Tx/Rx), in a dynamic range of frequencies.

3.2 Hardware

We will acquire a Software Define Radio (SDR), specifically an Universal Software Radio Peripheral 2 (USRP2). This is one of the main components needed for transmitting and receiving data on the frequencies relevant for Mobile GSM communication. However, for the USRP to be fully functional we require a transceiver, which comes as a daughterboard for the USRP.

Transceiver?

Many transceivers are available for the USRP1, however for our purposes, we will use the SBX 400-4400 MHz Rx/Tx (40MHz). The SBX is capable of Tx/Rx on a wide range of frequencies, which is needed for being able to receive most of the used frequencies in typical mobile communication.

Below is a list of technologies, used in mobile communication, and their associated frequency bands:

- GSM: 900/1800 MHz
- UMTS, HSDPA, HSPA+: 900/2100 MHz
- LTE: 800/1800/2600 MHz

3.3 Antenna

Having the SDR, is not enough, we need an antenna that has the capability of transmitting and receiving on the desired frequency ranges.

We will acquire an **VERT900**, 824-960 MHz, 1710-1990 MHz Quad-band Cellular/PCS and ISM Band. The Vert900 is not capable of sending and receiving on all frequencies used in mobile communication. Therefore, we might need another antenna that is capable of transmitting in the higher frequency ranges, used in some 3G and 4G technologies. For this purpose, we will acquire an **LP0965**. This antenna operates within the frequency range 850 MHz to 6.5 GHz, which makes it capable of sending and receiving on the relevant frequency ranges used in mobile communication.

3.4 Clock Modifications

One of the issues that this project experienced, was the fact that the internal clock, in the USRP1 is not sufficiently precise for transceiving GSM data.

Looking at the GSM 05.10 technical specification document we can read this quote:

> *"The BS shall use a single frequency source of absolute accuracy better than 0.05 ppm for both RF frequency generation and clocking the timebase. The same source shall be used for all carriers of the BS."*
>
> \- [ETS96b]

This quote dictates the level of precision required by the clock used in a BS to operate successfully as a Cell in a mobile network. The clock is used to calibrate the RF frequency generation.

In most RF frequency generation devices there is a certain clock drift that happens over time. This clock drift may result in a frequency offset and thus the BS being imprecise in the frequency that it has been set to generate traffic on. For instance setting the device to Tx/Rx on the frequency 801.01MHz, it may in reality be centering on a slightly different frequency.

As an example, say that we have set the Universal Software Radio Peripheral (USRP) to operate as a BTS with the ARFCN 47 on E-GSM 900:

$$
\begin{array}{l}
890.0 + 0.2 \cdot ARFCN + 45 \Rightarrow \\
890 + 0.2 \cdot 47 + 45 = 944.4 MHz
\end{array}
$$

Table 3.1: Calculating frequency from ARFCN

What we have calculated here is the downlink frequency (BTS to MS). We then set the BTS to Tx on the frequency calculated above. However, due to clock drift, the actual frequency set by the USRP, might actually differ from the desired frequency [Ope14].

When an MS is turned on from a cold start, it will attempt to search all ARFCNs within the bands supported by the device [ETS05]. So, if the BTS from above is running on a frequency that differs from the one that is expected by the MS, then the MS might not be able to discover the cell. Further explanations are at Section 2.5.

Band	Lower Band, Fl(n)	ARFCN	Upper band, Fu(n)
P-GSM 900	$Fl(n) = 890 + 0.2 \cdot n$	$1 \leq \mathrm{n} \leq 124$	$Fu(n) = Fl(n) + 45$
E-GSM 900	$Fl(n) = 890 + 0.2 \cdot n$	$0 \leq \mathrm{n} \leq 124$	$Fu(n) = Fl(n) + 45$
	$Fl(n) = 890 + 0.2 \cdot (n - 1024)$	$975 \leq \mathrm{n} \leq 1023$	
R-GSM 900	$Fl(n) = 890 + 0.2 \cdot n$	$0 \leq \mathrm{n} \leq 124$	$Fu(n) = Fl(n) + 45$
	$Fl(n) = 890 + 0.2 \cdot (n - 1024)$	$955 \leq \mathrm{n} \leq 1023$	
ER-GSM 900	$Fl(n) = 890 + 0.2 \cdot n$	$0 \leq \mathrm{n} \leq 124$	$Fu(n) = Fl(n) + 45$
	$Fl(n) = 890 + 0.2 \cdot (n - 1024)$	$940 \leq \mathrm{n} \leq 1023$	
DCS 1800	$Fl(n) = 1710.2 + 0.2 \cdot (n - 512)$	$512 \leq \mathrm{n} \leq 885$	$Fu(n) = Fl(n) + 95$
PCS 1800	$Fl(n) = 1850.2 + 0.2 \cdot (n - 512)$	$512 \leq \mathrm{n} \leq 810$	$Fu(n) = Fl(n) + 80$
GSM 450	$Fl(n) = 450.6 + 0.2 \cdot (n - 259)$	$259 \leq \mathrm{n} \leq 293$	$Fu(n) = Fl(n) + 10$
GSM 480	$Fl(n) = 479 + 0.2 \cdot (n - 306)$	$306 \leq \mathrm{n} \leq 340$	$Fu(n) = Fl(n) + 10$
GSM 850	$Fl(n) = 824.2 + 0.2 \cdot (n - 128)$	$128 \leq \mathrm{n} \leq 251$	$Fu(n) = Fl(n) + 45$

Table 3.2: Formulas for calculating frequencies

Issues

We were unable to get the USRP1 to correctly recognize the SBX daughterboard. Our issues were that the USRP1 would only recognize the SBX as a generic daughterboard. The incorrect identification of daughterboard resulted in the USRP1 to Tx/Rx on frequencies that differed from the one requested. This meant that, when scanning for BTS on specific frequencies, we were unable to receive any BCCH messages, as the device was actually listening on the wrong frequency.

The solution, which is also the one that was used for this thesis, is to acquire an USRP2, or a newer SDR from Ettus and transfer the SBX over to that device.

3.5 Software

To control the SDR we will use a generic laptop running Ubuntu Linux operating system. Ubuntu 12.04 LTS or Ubuntu 14.04 LTS 32 bit is recommended. The majority of the software projects used in this thesis have been developed on 32 bit systems, and as a result it is recommended to use the same, as using a 64 bit Operating System might cause compilation issues.

3.5.1 Ettus UHD Driver

This is the driver package required to interface with the Ettus Research hardware components. With this package it is possible to control the SDR, transmit/receive data to and from the device.

3.5.2 Gnu Radio

Gnu Radio (GR) is a software development toolkit for interacting with software defined radio equipment. GR provides signal processing blocks that can be used to process data streams received from a hardware radio, or to send data streams out to a hardware radio which then transmits it Radio Frequency (RF) signals [Gnu15].

GRs offers a simple way of performing complex software based signal processing by using what it calls ‘blocks’. Blocks perform signal processing functions, and can be connected together to form a complex signal processing application.

GR is widely used by hobbyists as well as in the academic world. Recently, GR and radio equipment from Ettus was used in transmitting uplink radio commands to an abandoned NASA space craft [Mal14].

For this thesis GR is a core component and is used for all direct interaction with the radio peripheral. GR is used for receiving and storing RF data on disk. One of the great things about being able to receive data, and store it on disk, is that the stored data gives an exact image of the ‘state of the world’ at the time it was received. It also allows us to perform complex data analysis after the fact, and should there be any disputes about results derived from the data, third parties will be able to perform independent analysis and form their own conclusions.

Additionally, parts of mobile communication is encrypted and may be instantly decipherable. A malicious attacker could in theory, using GR, massively gather encrypted communication data, store it on disk. And as the encryption technologies used in mobile communication are broken or hardware becomes powerful enough to brute-force the encryption schemes, an attacker may be able to decrypt the file contents and gain access to raw communication data.

3.5.3 Airprobe

Airprobe, is a suite of projects developed to implement an air-interface Section 2.1.1 analysis tool for the GSM standard [Air15]. Airprobe is structured in three parts: Acquisition, DeModulation, and Analysis. In this thesis, we have primarily used two tools from the Airprobe suite: **gsm-tvoid** and **gsm-receiver**.

gsm-tvoid
This tool uses GR to gather and digitize RF received from the SDR. Using this tool, a user can center on a specific ARFCN (frequency), and from that frequency scan for GSM data. Not all channels are in use at any given location, and thus this scan may return nothing, however, when a cell is active within range of the equipment, the tool will output a file with raw GSM data.

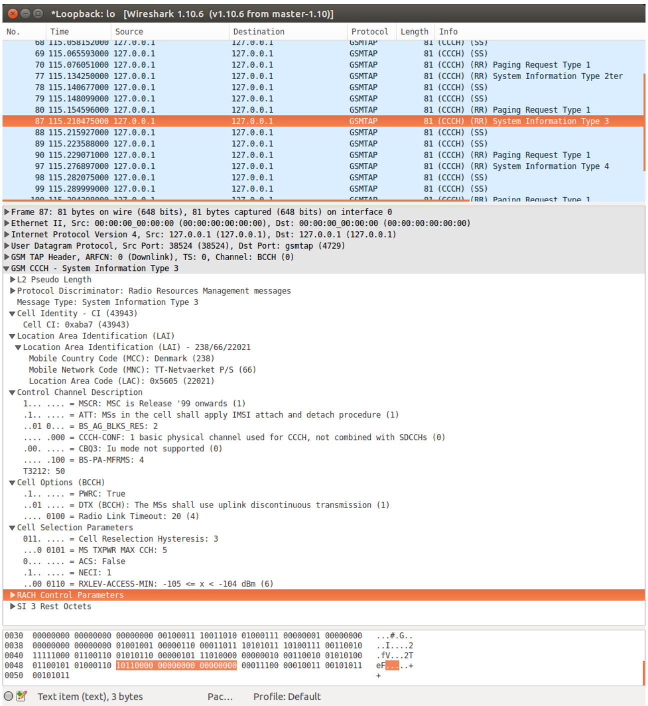
gsm-receiver
Gsm-receiver is able to demodulate the raw GSM data. It is able to demodulate both live captures as well as capture files from disk. This tool takes GSM capture data, converts it in to GSMTAP (Section 3.5.4) packets, wraps them in a User Datagram Protocol (UDP) packets and finally transmits them on the Loopback Interface (lo). If we start a Wireshark capture on the lo interface, we are able to view the data contained in the original raw RF captures.

Figure 3.1 shows the output after a GSM capture has been converted to GSMTAP packets. This figure only shows a snipept of the packets contained in this specific capture file. However, we are able to see that the capture contains information about a BTS. We are able to read the Cell Identity (CI), Location Area Identification (LAI) and other parameters that have been transmit by this BTS in this BCCH message.

Osmocom projects

Osmocom is a group of research projects that focus on doing research in various types of mobile communication [OSM15c]. The **Osmocom** project used in this thesis is the library *libosmocore*, a library containing a collection of utility functions that were shared among the **OsmocomBB** and **OpenBSC** projects.

OsmocomBB was one of the early projects that dealt with developing an Open Source (OS) implementation of the GSM baseband stack. This project gave researchers a cheap system for testing and analysing the security issues in the GSM protocols. Using a modified Motorola C123[1] [Osm10] and the OsmocomBB

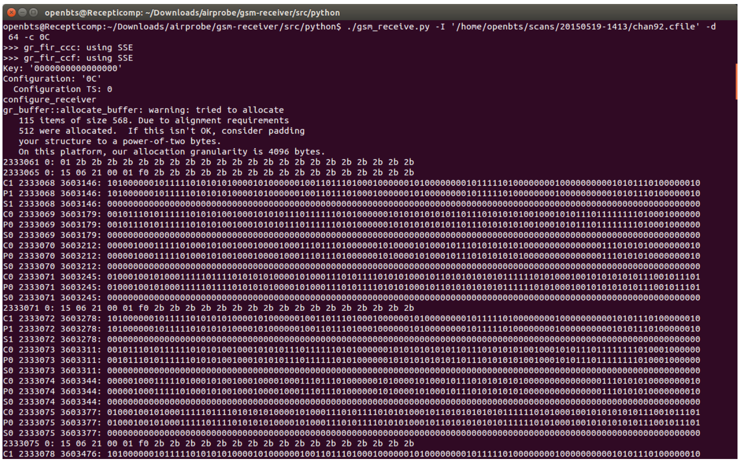


```
*Loopback: lo   [Wireshark 1.10.6  (v1.10.6 from master-1.10)]
No.     Time          Source       Destination  Protocol  Length  Info
     68 115.058152000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (SS)
     69 115.065593000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (SS)
     70 115.076051000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 1
     77 115.134250000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (RR) System Information Type 2ter
     78 115.140677000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (SS)
     79 115.148099000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (SS)
     80 115.154596000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 1
     87 115.210475000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (RR) System Information Type 3
     88 115.215927000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (SS)
     89 115.223588000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (SS)
     90 115.229071000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 1
     97 115.276897000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (RR) System Information Type 4
     98 115.282075000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (SS)
     99 115.289999000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (SS)
    100 115.294298000 127.0.0.1    127.0.0.1    GSMTAP        81 (CCCH) (RR) Paging Request Type 1

▶Frame 87: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
▶Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
▶Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
▶User Datagram Protocol, Src Port: 38524 (38524), Dst Port: gsmtap (4729)
▶GSM TAP Header, ARFCN: 0 (Downlink), TS: 0, Channel: BCCH (0)
▼GSM CCCH - System Information Type 3
 ▶L2 Pseudo Length
 ▶Protocol Discriminator: Radio Resources Management messages
  Message Type: System Information Type 3
 ▼Cell Identity - CI (43943)
   Cell CI: 0xaba7 (43943)
 ▼Location Area Identification (LAI)
  ▼Location Area Identification (LAI) - 238/66/22021
    Mobile Country Code (MCC): Denmark (238)
    Mobile Network Code (MNC): TT-Netvaerket P/S (66)
    Location Area Code (LAC): 0x5605 (22021)
 ▼Control Channel Description
   1... .... = MSCR: MSC is Release '99 onwards (1)
   .1.. .... = ATT: MSs in the cell shall apply IMSI attach and detach procedure (1)
   ..01 0... = BS_AG_BLKS_RES: 2
   .... .000 = CCCH-CONF: 1 basic physical channel used for CCCH, not combined with SDCCHs (0)
   .00. .... = CBQ3: Iu mode not supported (0)
   .... .100 = BS-PA-MFRMS: 4
   T3212: 50
 ▼Cell Options (BCCH)
   .1.. .... = PWRC: True
   ..01 .... = DTX (BCCH): The MSs shall use uplink discontinuous transmission (1)
   .... 0100 = Radio Link Timeout: 20 (4)
 ▼Cell Selection Parameters
   011. .... = Cell Reselection Hysteresis: 3
   ...0 0101 = MS TXPWR MAX CCH: 5
   0... .... = ACS: False
   .1.. .... = NECI: 1
   ..00 0110 = RXLEV-ACCESS-MIN: -105 <= x < -104 dBm (6)
 ▶RACH Control Parameters
 ▶SI 3 Rest Octets

0030  00000000 00000000 00000000 00100011 10011010 01000111 00000001 00000000   ...#.G..
0038  00000000 00000000 01001001 00000110 00011011 10101011 10100111 00110010   ..I....2
0040  11111000 01100110 01010110 00000101 11010000 00000010 00110010 01010100   .fV...2T
0048  01100101 01000110 10110000 00000000 00000000 00011100 00010011 00101011   eF.....+
0050  00101011                                                                  +
```

Figure 3.1: Wireshark showing GSMTAP packages



```
openbts@Recepticomp: ~/Downloads/airprobe/gsm-receiver/src/python
openbts@Recepticomp:~/Downloads/airprobe/gsm-receiver/src/python$ ./gsm_receive.py -I '/home/openbts/scans/20150519-1413/chan92.cfile' -d
 64 -c 0C
>>> gr_fir_ccc: using SSE
>>> gr_fir_ccf: using SSE
Key: '0000000000000000'
Configuration: '0C'
  Configuration TS: 0
configure_receiver
gr_buffer::allocate_buffer: warning: tried to allocate
   115 items of size 568. Due to alignment requirements
   512 were allocated.  If this isn't OK, consider padding
   your structure to a power-of-two bytes.
   On this platform, our allocation granularity is 4096 bytes.
2333061 0: 01 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
2333065 0: 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
C1 2333068 3603146: 1010000001011111010101010000101000000010011011101000100000010100000000010111110100000000010000000000101011101000000010
P1 2333068 3603146: 1010000001011111010101010000101000000010011011101000100000010100000000010111110100000000010000000000101011101000000010
S1 2333068 3603146: 00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
C0 2333069 3603179: 00101110101111110101010010001010101110111111010100000010101010101011011101010101001000101011101111111110100010000000
P0 2333069 3603179: 00101110101111110101010010001010101110111111010100000010101010101011011101010101001000101011101111111110100010000000
S0 2333069 3603179: 00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
C0 2333070 3603212: 00001000111110100010100100010000100011101110100000010100001010001011101010101010000000000000000111010101000000000010
P0 2333070 3603212: 00001000111110100010100100010000100011101110100000010100001010001011101010101010000000000000000111010101000000000010
S0 2333070 3603212: 00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
C0 2333071 3603245: 01000100101000111110111101010101000010100011101011110101010001011010101010101111110101000100101010101011100101110 1
P0 2333071 3603245: 01000100101000111110111101010101000010100011101011110101010001011010101010101111110101000100101010101011100101110 1
S0 2333071 3603245: 00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
2333071 0: 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
C1 2333072 3603278: 1010000001011111010101010000101000000010011011101000100000010100000000010111110100000000010000000000101011101000000010
P1 2333072 3603278: 1010000001011111010101010000101000000010011011101000100000010100000000010111110100000000010000000000101011101000000010
S1 2333072 3603278: 00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
C0 2333073 3603311: 00101110101111110101010010001010101110111111010100000010101010101011011101010101001000101011101111111110100010000000
P0 2333073 3603311: 00101110101111110101010010001010101110111111010100000010101010101011011101010101001000101011101111111110100010000000
S0 2333073 3603311: 00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
C0 2333074 3603344: 00001000111110100010100100010000100011101110100000010100001010001011101010101010000000000000000111010101000000000010
P0 2333074 3603344: 00001000111110100010100100010000100011101110100000010100001010001011101010101010000000000000000111010101000000000010
S0 2333074 3603344: 00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
C0 2333075 3603377: 01000100101000111110111101010101000010100011101011110101010001011010101010101111110101000100101010101011100101110 1
P0 2333075 3603377: 01000100101000111110111101010101000010100011101011110101010001011010101010101111110101000100101010101011100101110 1
S0 2333075 3603377: 00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
2333075 0: 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b 2b
C1 2333078 3603476: 1010000001011111010101010000101000000010011011101000100000010100000000010111110100000000010000000000101011101000000010
```

Figure 3.2: Gsm-receiver terminal output

software, it is possible to run your own BTS [Osm15a], perform Denial of Service (DoS) attacks on MSs [Gol12], and more.

OpenBSC is a project which aims to be a complete *GSM network in a box* [Osm15b]. OpenBSC aims to implement the functionality which in a typical GSM network is performed by: BSC, MSC, HLR, AUC, VLR, and EIR.

The research work made in many of of the Osmocom projects have found its way in to other projects which deal with GSM/3GPP networks. As an example, the Airprobe Section 3.5.3 project relies heavily on Osmocom projects.

OpenBTS

OpenBTS is an open source cellular infrastructure software solution. It is a collection of software modules, that allows users to setup their own 2G GSM and UMTS/3G mobile network [Ied15] that operate over software defined radios. OpenBTS uses Session Initiation Protocol (SIP) and Private Branch Exchange (PBX) to connect calls between users. Using OpenBTS, SDR and a few other software projects, it is possible to operate a low-cost Voice Over Internet Protocol (VOIP) based mobile network [Ope15].

OpenBTS is a highly configurable project, and a great number of GSM configuration flags[2]can set by the user. For example, it is possible to set the LAI values to any desired valid value. What this means is that a user is able to configure the network to any other network, e.g. it is possible to configure the MCC to **238**, MNC to **01**, andLAC **12233**. The MS will then be able to see this network, and assume that it is a legitimate **TDC A/S** network, and if the signal strength is sufficiently high, the MS will connect to the cell.

In the context of this project, a user is able to freely create their own BTS. Or even, a nefarious user, could use it as a basis for harvesting MS data.

Asterisk

An open source telephony switching and PBX service [AST]. This project is being used by OpenBTS, and other projects, for its switching functionality. Asterisk offers switching functionality for phone to phone calls, as well as allowing connectivity to the greater PSTN and VOIP services.

[1] Other models will also work. These phones can be bought online cheaply.

[2] Setting options that can be set.

SMQueue

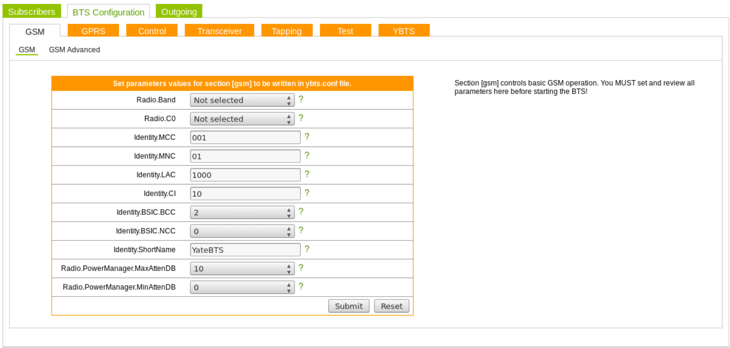
SMQueue is an extension to the SIP protocol for Instant messaging [BRS+02]. SMQueue offers functionality for sending and receiving SMS messages over the SIP protocol. This technology is an essential part of projects that attempt to implement a complete GSM network, such as OpenBTS [SMQ14], and YateBTS.

SIPAuthServe

A daemon which provides SIP authentication services [SMQ14]. This project is used by, among others, the OpenBTS project. This project keeps track of registered subscribers and will authenticate them with the service.

Yate and YateBTS

Yet Another Telephone Engine (Yate) is another software based mobile telephony engine [Yat15a]. Yate is a telephony engine that handles much of the underlying telephony technologies required to operate a mobile network. YateBTS, similar to OpenBTS, implements the GSM and General Packet Radio Service (GPRS) radio access network [Yat15b]. YateBTS is additionally able to receive signals from MSs, and pass them through to a VOIP connection. One of the areas where YateBTS differs from OpenBTS is a high focus on usability. Developers behind YateBTS have developed a front-end and configuration utility that simplifies some of the complex configurations that are required for setting up a working mobile network.



Set parameters values for section [gsm] to be written in ybts.conf file.

Radio.Band	Not selected
Radio.C0	Not selected
Identity.MCC	001
Identity.MNC	01
Identity.LAC	1000
Identity.CI	10
Identity.BSIC.BCC	2
Identity.BSIC.NCC	0
Identity.ShortName	YateBTS
Radio.PowerManager.MaxAttenDB	10
Radio.PowerManager.MinAttenDB	0

Section [gsm] controls basic GSM operation. You MUST set and review all parameters here before starting the BTS!

Figure 3.3: YateBTS configuration screen [Yat14]

Openmoko

Openmoko was a project that aimed to develop a mobile phone that ran on a purely open source software stack [FSO09]. They believed that mobile phones should be able to run on an open architecture, in the same way that desktop systems have a plethora of available operating systems to chose from [Ope08].

3.5.4 Wireshark and GSMTap

Wireshark is a network protocol analyzer tool [WS215]. Wireshark is able to capture network interface traffic, which can consequently been analyzed. Wireshark has built-in support for vast amounts of network traffic protocols e.g. UDP, Transmission Control Protocol (TCP), Internet Control Message Protocol (ICMP), and GSMTAP. With this tool, it is possible to inspect the contents of the each frame, and view detailed descriptions of packet flags and contents. This project relies heavily on GSMTAP.

GSMTAP
GSMTAP is a pseudo-header format, used to encapsulate frames from a GSM Um (Section 2.1.1) interface into UDP packets [GSM13]. In this project, as was explained in Section 3.5.3, Airprobe reads raw RF GSM data and transmits it back out again as GSMTAP packets on the lo interface. Using Wireshark it is then possible to capture these packets and view the exact contents of the transmitted data.

tshark
tshark is a command line implementation of the Wireshark utility [tsh15]. We have used this tool for a program that automates the conversion of GSM raw data to Wireshark pcap files containing GSMTAP packets. Pcap files are then exported to XML files which are easily parsed by other programs.

3.5.5 My own scripts

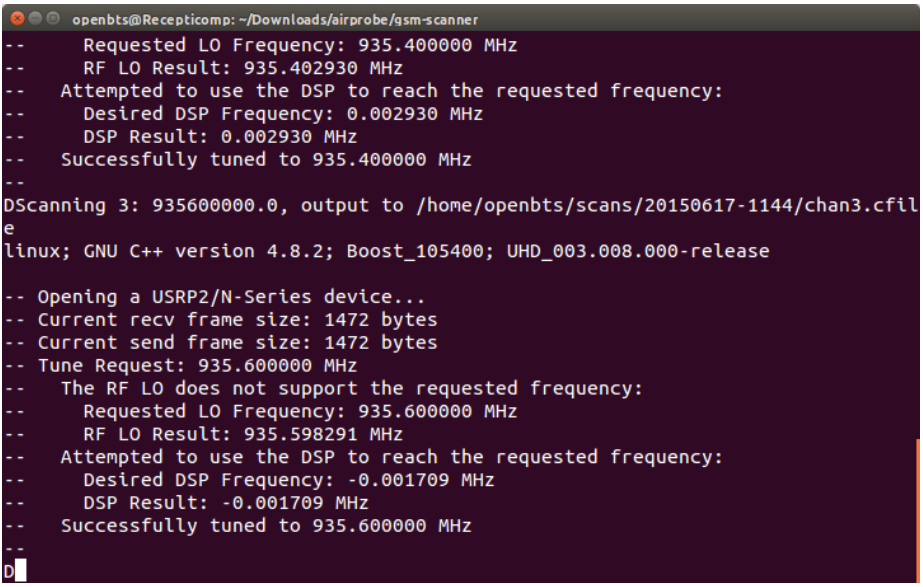
For this project, a number of projects have been written to simplify the process of data analysis. In this section, a brief overview of the individual components is given. Each component is described, and some of the design decisions are given and justified.

Scanner

This tool uses the USRP and does a scan of all channels in the GSM 900 band.

Time for each scan: 3.5s The reasoning behind this, was partially practical, and with some basis in how a MS may operate under normal circumstances. The length of the scan determines the amount of data that can be gathered on each ARFCN. When started, the system will scan all **124** ARFCNs for 3.5 s. and store the data on the computer as a raw data capture file.

For practical reasons, the length of scanning was set to 3.5 s, as the total time required for scanning at each location was on average 10 minutes. Increasing the length of each channels' scan would logically also increase the total scan length. It was estimated that, any number lower than this might result in a decrease of data resolution.



```
--     Requested LO Frequency: 935.400000 MHz
--     RF LO Result: 935.402930 MHz
--   Attempted to use the DSP to reach the requested frequency:
--     Desired DSP Frequency: 0.002930 MHz
--     DSP Result: 0.002930 MHz
--   Successfully tuned to 935.400000 MHz
--
DScanning 3: 935600000.0, output to /home/openbts/scans/20150617-1144/chan3.cfil
e
linux; GNU C++ version 4.8.2; Boost_105400; UHD_003.008.000-release

-- Opening a USRP2/N-Series device...
-- Current recv frame size: 1472 bytes
-- Current send frame size: 1472 bytes
-- Tune Request: 935.600000 MHz
--   The RF LO does not support the requested frequency:
--     Requested LO Frequency: 935.600000 MHz
--     RF LO Result: 935.598291 MHz
--   Attempted to use the DSP to reach the requested frequency:
--     Desired DSP Frequency: -0.001709 MHz
--     DSP Result: -0.001709 MHz
--   Successfully tuned to 935.600000 MHz
--
D
```

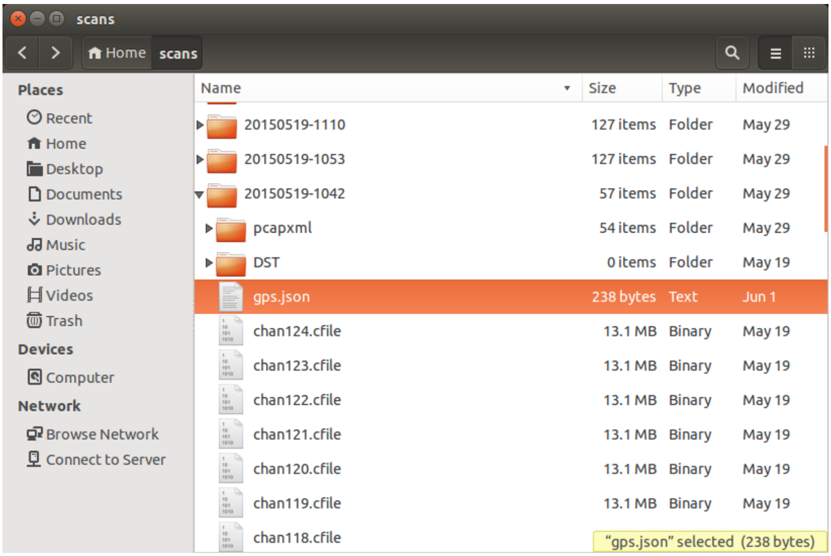
Figure 3.4: Scanner script running

Figure 3.4 shows the scanner running a scan of all 124 ARFCN channels. Additionally, to prove the exact location of each scan, the script will poll an Universal Serial Bus (USB) attached smartphone for Global Positioning System (GPS) coordinates, and consequently dump the received GPS data into a file on disk.

Figure 3.5 shows an example of the output received from the smartphone.

```
{"class":"TPV","tag":"RMC","device":"tcp://localhost:4352",
"mode":3,"time":"2015-05-19T12:01:43.000Z", "ept":0.005,
"lat":55.700400000,"lon":12.591238333, "alt":58.000,
"epx":7.667,"epy":7.916,"epv":0.000, "track":0.0000,
"speed":0.000,"climb":-3.000,"eps":15.83}
```

Figure 3.5: GPS Coordinate output



Name	Size	Type	Modified
20150519-1110	127 items	Folder	May 29
20150519-1053	127 items	Folder	May 29
20150519-1042	57 items	Folder	May 29
pcapxml	54 items	Folder	May 29
DST	0 items	Folder	May 19
gps.json	238 bytes	Text	Jun 1
chan124.cfile	13.1 MB	Binary	May 19
chan123.cfile	13.1 MB	Binary	May 19
chan122.cfile	13.1 MB	Binary	May 19
chan121.cfile	13.1 MB	Binary	May 19
chan120.cfile	13.1 MB	Binary	May 19
chan119.cfile	13.1 MB	Binary	May 19
chan118.cfile			

"gps.json" selected (238 bytes)

Figure 3.6: Completed scan output

Converter

The output from the scans above come in the form of raw RF capture files. These files are not directly processable, at least not for the software projects used in this thesis, and need to be converted into a form where we can programmatically extract necessary data. Above in Section 3.5.4 we gave an overview on *Wireshark* and *GSMTap*. These two applications allow us to convert the RF data files into *Wireshark pcap XML files*. Converting to XML files, allows us to extract the data out of the dataset, which is relevant for identifying IMSI Catchers.

convert_cfile_to_xmlpcap.py
This script will traverse the output directory from the scanner script in Section 3.5.5, and then using *TShark* and *Airprobe* will automatically convert each

individual RF file to *pcap xml* files.

```
1  <proto name="gsm_a.ccch" showname="GSM CCCH - System Information Type 3" size="23" pos="58">
2    <field name="gsm_a.rr.l2_pseudo_len" showname="0100 10.. = L2 Pseudo Length value: 18" size="1" pos="58" show="18" value="12" unmaskedvalue="49"/>
3    </field>
4    <field name="gsm_a.dtap.msg_rr_type" showname="Message Type: System Information Type 3" size="1" pos="60" show="0x1b" value="1b"/>
5    <field name="" show="Cell Identity - CI (6286)" size="2" pos="61" value="188e">
6      <field name="gsm_a.bssmap.cell_ci" showname="Cell CI: 0x188e (6286)" size="2" pos="61" show="0x188e" value="188e"/>
7    </field>
8    <field name="" show="Location Area Identification (LAI)" size="5" pos="63" value="32f8100461">
9      <field name="" show="Location Area Identification (LAI) - 238/01/1121" size="5" pos="63" value="32f8100461">
10       <field name="e212.mcc" showname="Mobile Country Code (MCC) : Denmark (238)" size="2" pos="63" show="238" value="32f8"/>
11       <field name="e212.mnc" showname="Mobile Network Code (MNC) : TDC Mobil (01)" size="2" pos="64" show="1" value="f810"/>
12       <field name="gsm_a.lac" showname="Location Area Code (LAC) : 0x0461 (1121)" size="2" pos="66" show="0x0461" value="0461"/>
13     </field>
14   </field>
15   ...
16 </proto>
```

Figure 3.7: XML pcap file

Figure 3.7 shows a small section from one of the converted XML files. This snippet shows one BTS that was discovered in the scans performed in Copenhagen.

"...Cell CI: 0x188e (6286) ..." on line 6 shows the Cell Identifier of the discovered BTS.

"...Mobile Country Code (MCC) : Denmark (238) ..." on line 10 shows the

MCC of the discovered BTS.

"...Mobile Network Code (MNC) : TDC Mobile (01) ..." on line 11 shows the MNC of the discovered BTS.

"...Location Area Code (LAC) : 0x0461 (1121) ..." on line 12 shows the LAI of the discovered BTS.

It is this data we will analyse further in Chapter 5. From this data we should be able to determine whether we have discovered a potential IMSI Catcher in our scans.

Extractor

For extraction of IMSI Catcher relevant data, we have written a script that automates this process. **analyse_xml_pcap_files.py**
This script will traverse all XML files created by the **convert_cfile_to_xmlpcap.py** script, extract elements relevant to detecting an IMSI Catcher, and then dump them in a SQLite database.

Storing things in an easy to access database will simplify future work on the project, as well as creating a history of all BTSs that have been discovered, and on what location they have been discovered. The exact purpose of this database, and how we can further use this data will be expound up further in Chapter 5.

Future work?

See Chapter 7.

Where to find the code?

All source code written for this project can be found on my GitHub repository for this thesis [San15].

Analysis

Detailed analysis, and actual IMSI Catcher-catching is detailed in Chapter 5.

Installation Instructions

Instructions for installing the required software is found in Appendix A. A note for the instructions document: basic knowledge of Linux system is assumed, as well as some knowledge of operating the Linux command line is expected.

3.6 Reach

We have been unable to determine the exact distances that we are able to detect cells from. However, the distance that the proposed solution is able to detect cells, may vary based on a variety of factors. Rayleigh fading being one of them. Rayleigh fading is a statistical model which shows that the strength of a signal that passes through a transmission medium will vary randomly, or fade according to the Rayleigh distribution [Skl97]. A variation of weather (rainy, cloudy), the number of vehicles present in the area between transmitter and receiver, may affect the signal strength. As a result, without doing thorough testing where an average is calculated, it may be difficult to determine the exact distances that we are able to receive cells from.

3.7 Summary of Setup

Table 3.3 shows a complete summary of the software and hardware that is being used for the proposed prototype in this thesis.

Below are product websites for the acquired hardware components:

USRP1
`http://www.ettus.com/product/details/USRPPKG`

USRP2
This product has been discontinued and been replaced by the newer models USRP N200 and USRP N210.

Hardware	**Description**
USRP2	Software Defined Radio
SBX 400-4400 MHz	Daughterboard for the USRP
Vert900	Antenna capable of transmitting and receiving data on necessary frequencies
Software	
Ubuntu 14.04 LTS	Operating System used
UHD Drivers	Required drivers to control the USRP
Airprobe	Software project for analysing GSM signals
Wireshark	Network protocol analysis tool, used for receiving and storing GSM packets
TShark	Based on Wireshark, a command line network protocol analysis tool
Raw Data to Pcap Script	Script used to automatically convert raw data from the USRP to data we can process
Data filtration and extraction	Processed data needs to be filtered and desired items are filtered out
Additional	
Laptop	Controls the software and hardware
Inverter	Powering the hardware in the car
Smartphone	Used only for receiving a GPS signal when out scanning

Table 3.3: Specification table

SBX
`http://www.ettus.com/product/details/SBX`

Vert900
`http://www.ettus.com/product/details/VERT900`

LP0965
`http://www.ettus.com/product/details/VERT900`

3.8 Expected Outcomes

Using the hardware and software mentioned in Table 3.3, we believe that we will have a working prototype solution for an IMSI Catcher-Catcher. Using this hardware we expect to be successful at detecting an IMSI Catcher.

Additionally, with the tools shown in Table 3.3, we would also be able to build a prototype IMSI Catcher. Having a prototype solution that may imitate the functionality of an IMSI Catcher may be valuable for testing out the theory for how an IMSI Catcher operates. Additionally, we will be able to test some of the cell selection scenarios. We should be able to test how an MS is attached to a cell, and what parameters can be set to trick the device to connect to our IMSI Catcher. We may also be able to test a scenario where an MS is locked to a BTS, something that may be done by an aggressive IMSI Catcher.

Using the knowledge on how an IMSI Catcher actually operates, and how simple in reality it is, to create and run a private BTS may prove valuable when we will continue to the detection of an IMSI Catcher. Using the same hardware with only software modifications, we are able to build an IMSI Catcher-Catcher. Using the proposed system, we should be able to detect an IMSI Catcher. To test it, we will empirically study whether any IMSI Catcher are to be found in Copenhagen, Denmark.

The hardware listed above, may also provide further value to the university, as the same hardware could be used for a number of other potential projects. The following section will briefly mention some of the potential future projects, that could be performed with a similar hardware set-up.

3.9 Other Project Opportunities

Further projects could include a security assessment of the various technologies and protocols used within mobile communication. This could be to assess the cryptographic properties used by the various mobile communication standards.

Improving the IMSI Catcher-Catcher design. Creating a fully battery operated SDR based IMSI Catcher-Catcher. We could explore the feasibility of replacing the laptop with a smaller computer, such as a Raspberry Pi or similar. This would drastically reduce the size of the prototype. It may additionally be valuable to explore whether a smaller SDR would be equally feasible. One of the project that recently has caused some stir in the SDR community is the RTLSDR [Rtl15]. The RTL-SDR is a DVB-T TV tuner dongle, based on a RTL2832U chipset, which can be used as a low cost SDR. Combining a Raspberry Pi, and one of these RTL-SDR devices, it might be feasible to create a cheap and highly mobile solution for detecting IMSI Catchers. This device may not be as powerful and quick to scan as the proposed solution, but it would be cheap, and therefore it would be possible to acquire multiple copies of this design. The units could then be designed to operate in conjunction, and distribute the scanning of channels.

Investigating the security of other wireless radio communication technologies. This could for example be to investigate the security in systems used for communicating between aeroplanes and the ground. Credit card terminals, used within airborne aeroplanes, have been known under certain circumstances, to not enforce encryption in the transmission between the aeroplane and the ground. Combining information about aeroplane traffic, that we also are able to receive and decode, we can strategically place a receiver to catch any data transmission coming from CC terminals within the aeroplanes.

Another project may be to create a system for detecting active mobile stations within an environment. This could be a system that is able to detect the usage of a mobile phone, in an environment where mobile phone usage has been prohibited [VAIGCPC01].

Chapter 4

Detecting an IMSI-Catcher

Overview

In this chapter we will investigate some of the possible ways of detecting the presence of an IMSI Catcher. Based on the background knowledge that has been given, we will analyse that data transmit by a BTS and how it may be used to identify good BTSs from bad BTSs.

4.1 Cell History

A clear indicator of suspicious activity would be any sudden changes in the number and specific configuration parameters received by discovered cells.

Our proposed solution will construct a database containing data from received cells. Each entry in the database is attached to a specific GPS coordinate, and a timestamp. Whenever a new cell is discovered, its configuration parameters are read, extracted, and added to the database. For any subsequent discoveries of cells that have previously been seen, the process of adding the cells information to the database is repeated.

To offer complete coverage of a city network operators typically operate a large number of cells. As a result, using our proposed solution for detection of IMSI Catcher within a city, the number of data points collected will likely be large. To prevent a rapid growth of the database, and to minimize the amount of computation required for matching new cell discoveries with previous discoveries, our solution will perform an update on the cell already in the database. For each subsequent discovery of cell, the system will match the received cells' parameters with ones already in the system. If there is a complete match, and the cell has been discovered before, the system will update the 'time last discovered' timestamp.

A database containing information about cells present at a number of locations, is vital in the detection of an IMSI Catcher. Other existing IMSI Catcher-Catcher solution employ similar technologies. Two Android IMSI Catcher-Catcher projects AIMSICD and SnoopSnitch both generate a reference database for matching discovered cells against [SRL15b, Sec15], see Chapter 6. The security company commissioned by Aftonposton to do re-do the analysis of IMSI Catchers in Norway, **Delma**, uses a similar solution for detecting IMSI Catchers [McK15b].

A reference survey is best done independently of network operators. That is, the investigator should perform their own survey of the target area, rather than rely on cell tower data received from network operators. Data received from network operators may be incomplete, erroneous, or possibly not completely representative of the current situation at a specific location. Additionally, the legality of using an IMSI Catcher is debated, and any legal use of an IMSI Catcher will likely not be shown in data received from the network operator [McK15b].

4.2 IMSI Catcher Artefacts

4.2.1 Neighbouring Cells

Dabrowski et al. describe a method for locking a MS, which has already been connected to the IMSI Catcher network. If a cell transmits an empty list of neighbouring cells, then the MS will not know which other cells to search for. A cell transmits information about a number of neighbouring cells, that the MS uses in its cell selection process. If a cell transmits an empty neighbouring cells list, or a neighbouring cell list that only contains unreachable cells (non existing cells), then it will make it impossible for the MS to perform a normal cell reselection. An thus, the MS is locked on the cell [DPK+14].

Detection
Look for an empty list of neighbouring cells, or a list of neighbouring cells that does not exist in the surrounding area.

```
...
<field name="" show="List of ARFCNs = 54 48" size="16" pos="61"
    value="00000000000000000020800000000000"/>
</field>
...
```

Figure 4.1: List of Neighbouring Cells/List of ARFCNs

Figure 4.1, a snippet from the output of our scans, show a 'List of ARFCNs', which is also referred to as a 'List of neighbouring cells'. If this list was empty, it may be cause for suspicion.

4.2.2 Sudden Appearance of New Cell

A sudden appearance of a new previously unseen cell in a location is cause for suspicion. After having performed a survey analysis, if the system is able to detect a cell on a channel, which previously was unoccupied, it may be the result of an IMSI Catcher operating in the area.

Detection
This anomaly can be detected by performing a survey analysis of the location. A variance in the number of channels which are occupied by cells is cause for further investigation.

Note: See Section 3.6. This could potentially be the result of a difference in distance that the RF signals are able to travel. As a result, the number of cells discovered at a specific location, may vary from time to time.

4.2.3 Wrong LAC Used

By analysing the network infrastructure of the country where the analysis is performed, it is possible to determine what LACs are used in the country. This analysis can be done by working with that network operators operating in the country, to attempt to acquire this information. A survey analysis can also help determine the LACs values that are expected in the country.

Detection
A cell which has the LAC parameter set to a value which should not be found in the target country, then this may be cause for investigation.

4.2.4 Sudden varying LACs

If a discovered cell provides a LAC which differs from other cells, in the same area, by the same network operator, then this might be an indicator of an IMSI Catcher Section 2.3. Cells within the same are, and are operated by the same network operator, are typically on similar LACs.

Detection
Using cell history database. If a cell provides a LAC which differs from ones used by other cells value of other cells from the same network operator. This may be cause for suspicion. It is possible that it could be a misconfigured cell. However, LAC and MNC will typically be the same in an area.

4.2.5 Cell LAC Changes

A discovered cell, which has previously been discovered, offers a LAC value that is different from initial reading. This can potentially be an IMSI Catcher which is imitating a legitimate cell, and trying to trick MS to sending an location update message Section 2.3.

Detection
Using a cell history database. It is then possible to detect sudden changes in LAC value for a cell at an area.

4.2.6 Cell Changes Channel

A discovered cell, which has been previously been discovered at a location, is served on a different channel. Cells typically stay on the same channel [DPK$^+$14]. This could be an indicator of an IMSI Catcher imitating another cell, but which transmits on a different channel as to not cause interference.

Detection
Using cell history database. This can be detected by matching the discovered cell, which has been known to transmit on a certain channel at this location, suddenly is found to transmit on a different channel.

4.2.7 Suspiciously High Hysteresis

A cell may enforce a high CRH value. If the serving cell enforces a higher CRH value than the C2 value that the MS is able to calculate from neighbouring cells, then the MS may not be able to reselect to another suitable cell**??**, [SZC12]. Setting a high CRH the cell may prevent the MS from camping on another cell.

Detection
Using cell history database. It may be possible to form a pattern of expected CRH values used by network operators within the area of investigation. Anomalies here may be cause for investigation.

4.2.8 Cell Reselection Value Anomaly

A cell is able to provide a much higher signal strength than surrounding cells. MSs will calculate their reselection values **??**, and are likely tricked in to connecting to the cell. The IMSI Catcher system proposed by Song et al. uses this for their advantage when tricking MSs to connect to their system [SZC12].

Detection
Continuously monitoring the Reselection criterion parameter (C2) values, it may possible to discover a sudden increase in the reselection values. Which may be the result of an IMSI Catcher operating at a very targeted location.

4.2.9 Service Denial

When an IMSI Catcher tricks a MSs to camp on a cell, may extract the IMSI number, and then when the MS attempts to access the network, the IMSI Catcher barr from access to the network. This is a pattern know to be exhibited by IMSI Catchers [McK15b].

Detection
Connecting to a network, and analysing the result. If the MS is quickly denied

service and barred access to the network. Then it may be a indicator of an IMSI Catcher.

4.2.10 Ciphering Mode

When a MS connects to a cell, there occurs a ciphering mode negotiation. If the cell offers no ciphering, it might be cause for suspicion. It is possible that there is a reasonable explanation for why the cell offers no encryption, the MS is roaming on a foreign network (and thus the network operator, does not have the Authentication Key (K_i) which corresponds to the one on the MS)[DPK+14]. Certain ciphering suites are known to be weak:

A5/0
No ciphering used. No encryption is offered by the cell.

A5/1
This ciphering mode is known to be weak. Biryukov et al. already in 2000 showed that it was feasible to break the A5/1 encryption on a consumer PC [**?**]. Other researchers have supported the claim that the encryption is broken [EJ03, BBK08].

A5/2
This ciphering mode has also been shown to be breakable [EJ03, BBK08].

Detection
Using a system which is capable of connecting to discovered cells. If the MS connects to the cell and receives an Ciphering Mode where they cell offers either no encryption, or encryptions which are known to be weak, it may be cause for suspicion.

4.2.11 Multiple Cells on Channel

Multiple cells are discovered to be transmitting on the same channel. Network operators will typically attempt to deploy cells on different channels as not to cause interference amongst other cells in the same area [OET98].

There might be a reason why multiple cells occupy the same channel. If two cells are transmitting not far from each other, and both are emitting on the same BCCH frequency, then must be a way for subscribers to distinguish between them. For that purpose the GSM standard provides the Base Station Colour Code (BCC) parameter. The cells can set the BCC parameter, a parameter that can help MSs distinguish between the two cells. The BCC shall be locally unique [ETS96a].

Detection
Using cell history database. A scanned channel is found to be occupied by multiple cells. If two cells are found to operate on the same channel, then the BCC should be checked for both cells.

4.2.12 Cell Found in Neighbouring Cell List other Network

Cell from *Network A* is found found in handover list of *Network B*. This may be an indicator of an IMSI Catcher trying to trick an MS which is camping on a cell, to perform a reselection to the IMSI Catcher cell [SZYC10].

Detection
Checking which network each cell in a Neighbouring Cell list belongs to. If there is a discrepancy in which network the initial cell belongs to and which network the neighbouring cells belong to, then this is a cause for suspicion.

4.2.13 Signal Jammer

Signal jamming. An attacker may deploy a signal jammer which blocks GSM RF signals in an area. An attacker could target a specific list of channels, by looking at the neighbouring cell list of cells in the target location. The attacker may then transmit jamming signals on target channel frequencies. A MS will then be unsuccessful at scanning the ‘neighbouring cell’ channels for cells. As a result, the MS will attempt to scan all channels in the bands supported by the device. The attacker may then be successful at tricking MS at connecting to his IMSI Catcher-Catcher [DPK+14]

Detection
Using a reference database of cells in a location. It might be possible to detect this anomaly if cells, which previously were known to operate on certain channels have suspiciously disappeared, and only a previously unknown cell is found. It may also be possible to detect this artefact by using a spectrum analyser to look for sudden increase in noise levels.

4.2.14 Traffic Forwarding

An IMSI Catcher could be acting as a MITM, and forwarding MSs calls, data and SMS messages to the public telephone system [DPK^{+}14], see Section 2.3. IMSI Catchers, which operate as MITM sometimes forward their traffic simply by relaying the traffic through another MS and on to the mobile network. If **Alice** makes a call to **Bob**, **Bob** will see the caller ID of **Mallet** (the IMSI Catcher).

Detection
Performing periodic test calls. If a MS is camped on a IMSI Catcher, which acts as a MITM, the calls made from the MS may have their caller IDs masqueraded by one of the attacker.

4.3 Summary of Artefacts

Table 4.1 shows a summary of the IMSI Catcher artefacts which have been discovered for in the making of this thesis. An IMSI Catcher artefact is generally a cause for further investigation. The given artefacts that may be detected, as well as methods for detecting the artefact (if detection is possible). In previous chapters a basic understanding of the communication that occurs MS ⇔ BTS.

IMSI Catcher Artefact	Detection Method
Neighbouring Cells	Analyse NC list
Sudden Appearance of New Cell	Cell Database
Wrong LAC used	Cell Database
Sudden Varying LACs	Cell Database
Cell LAC Changes	Cell Database
Cell Changes Channels	Cell Database
Suspiciously High Hysteresis	Cell Database
Cell Reselection Value Anomaly	Network Fingerprinting
Service Denial	Attempting to Camp on Cells
Ciphering Mode	Read Cipher Indicator
Multiple Cells On Channel	Cell DB & Sanity check
Cell Found in Neighbouring Cell List	Network Fingerprinting
Signal Jammer	Cell Database, Watching Noise Levels
Traffic Forwarding	Periodic Test Calls

Table 4.1: IMSI Catcher Artefacts

4.4 Finding an IMSI Catcher

There are many artefact which may give indication of whether an IMSI Catcher is operating within an area. However there are number of artefacts that an IMSI Catcher may display, it can be challenging to guarantee that an IMSI Catcher has been detected. All of the artefacts given in this chapters all act to give an indication that something nefarious may be occurring in the location of the scan.

4.4.1 Where Is The Needle?

Using the tools and methods given in this thesis, we have a chance at detecting an IMSI Catcher. However, the detection will depend on a variety of factors which will be covered further in the section Section 4.4.2. Most of the artefacts shown in this chapter, give an indication that there may be something nefarious going on, and which should raise suspicion. However, as has been mentioned earlier, they are not guarantees in themselves.

We have chosen to list all these artefacts, some of which may only be minor causes for suspicion. A system, like the one proposed in this thesis could implement automatic checks for all of these artefacts, and thus result in a system which is able to create a qualified guess at determining whether a cell is nefarious or not.

The author of this thesis maintains that a system for detecting IMSI Catchers should err or on the safe side, and raise many warnings, rather than potentially missing a detection, due to the system being having set the bar too high.

Our research has shown that it is vital to perform a full cell tower survey at the target location, at a time before the expected tests are to be performed. A large number of the IMSI Catcher artefacts are best detected if there is a reference model which can be compared against for any new cell discoveries. Industry professional security analysts have found, working with network operators, with acquiring an overview of cells that they operate in areas, can be troublesome.

4.4.2 Why No Needle?

Detecting an IMSI Catcher can be a complecated processed. Ourresearch has shown that there can be many factors that can affect the outcome of a network analysis. The authors of the Aftenposten news story, where evidence was put forward, that claimed to prove the existence of IMSI Catchers, can attest to the complexity of detecting IMSI Catchers. One must have a thorough understanding of mobile network technologies to be able to determine whether an IMSI Catcher-study provides sufficient evidence, or not.

Add to the fact that IMSI Catcher device can be highly mobile. IMSI Catcher can be placed in moving/parked vehicles, placed in a back pack, hidden behind a tree, operated from a low flying aeroplane, and so on. When the detection of these device can be so difficult as it has been shown to be [BJ15], getting a court order to gain access to a vehicle/building where a IMSI Catcher is suspected to be operating, is likely a lengthy process, and thus giving the operator time to move/remove the device.

Chapter 5

Data Analysis

Overview

In this chapter we will perform an analysis of the survey data. We will describe our methodology for performing the survey. And using information given in previous chapters, this thesis will analyse the survey data for IMSI Catchers. After the analysis, we will discuss the results, and determine what went wrong, well, and what can be improved. Next we will form an hypothesis and discuss who and why anyone would use an IMSI Catcher.

5.1 Data Analysis

5.1.1 Methodology

In this thesis we perform an empirical study of cell tower survey data around Copenhagen, Denmark. The data was gathered by mobilizing our hardware and software system, setting it up in a vehicle and then going to target locations and performing complete scans of the GSM 900 band channels at each location. The complete band scan took ~10 minutes, and each channel was scanned for

3.5s. All scans were performed while the vehicle was stationary. We have chosen to perform the surveys while stationary to reduce possible errors. In the initial survey performed by Aftenposten, some of the measurements were performed while the equipment was moving. This was one of the things that PST maintained were cause of their 'erroneous' results [BJ15].

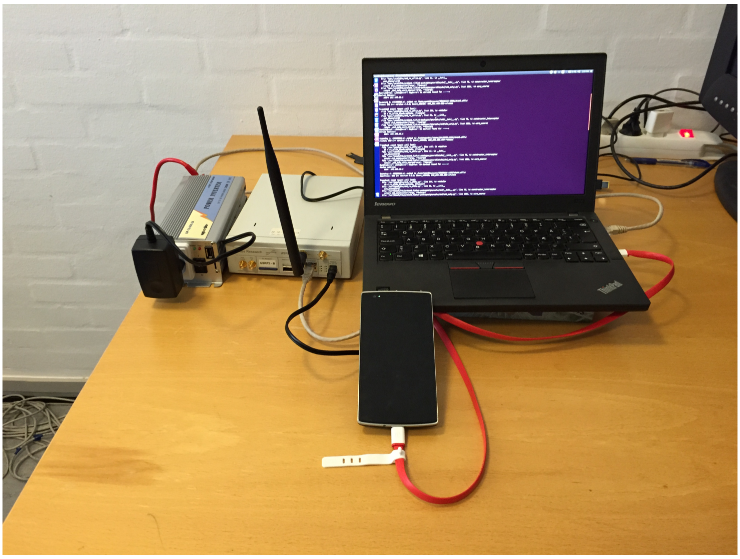


Figure 5.1: Hardware Setup

The Figure 5.1 shows the complete setup before it was put in a car. The components shown in the picture, from left to right:

- 12V-220/240V Inverter
- USPR2
- Laptop
- In front: Android Phone (External GPS Input)

Power to the components came from a 12V-220/240V inverter that was plugged in to the 12V output (cigarette lighter receptacle) in the vehicle. The laptop had sufficient battery capacity to be able run purely on battery. If the laptop was running low on power, we were able to recharge it by using the inverter. The mobile phone, is only used for receiving GPS reference data.

5.1.2 Locations

The Figure 5.2 shows the locations where we have performed scans in the search of IMSI Catchers. The locations were chosen based on an attempt at identifying areas of interest, and where we believe that an attacker would likely deploy and IMSI Catcher.

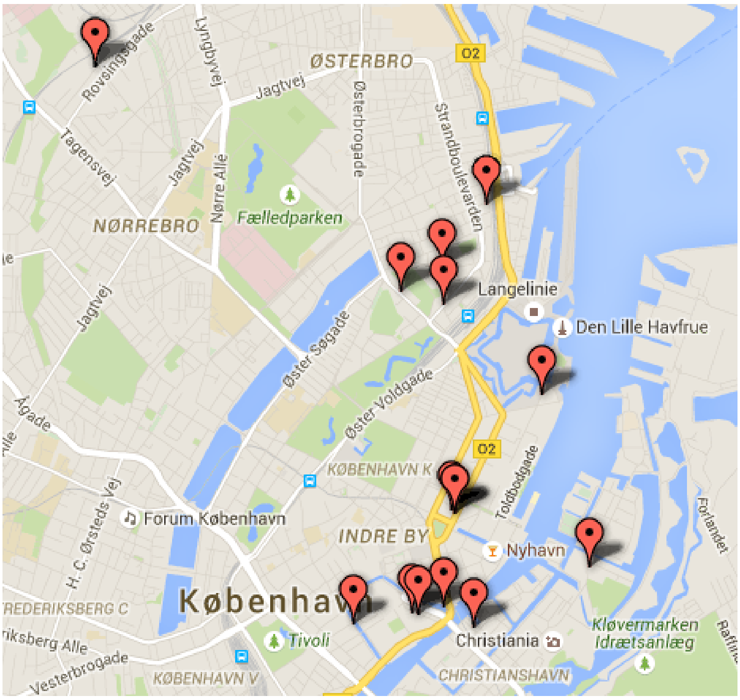
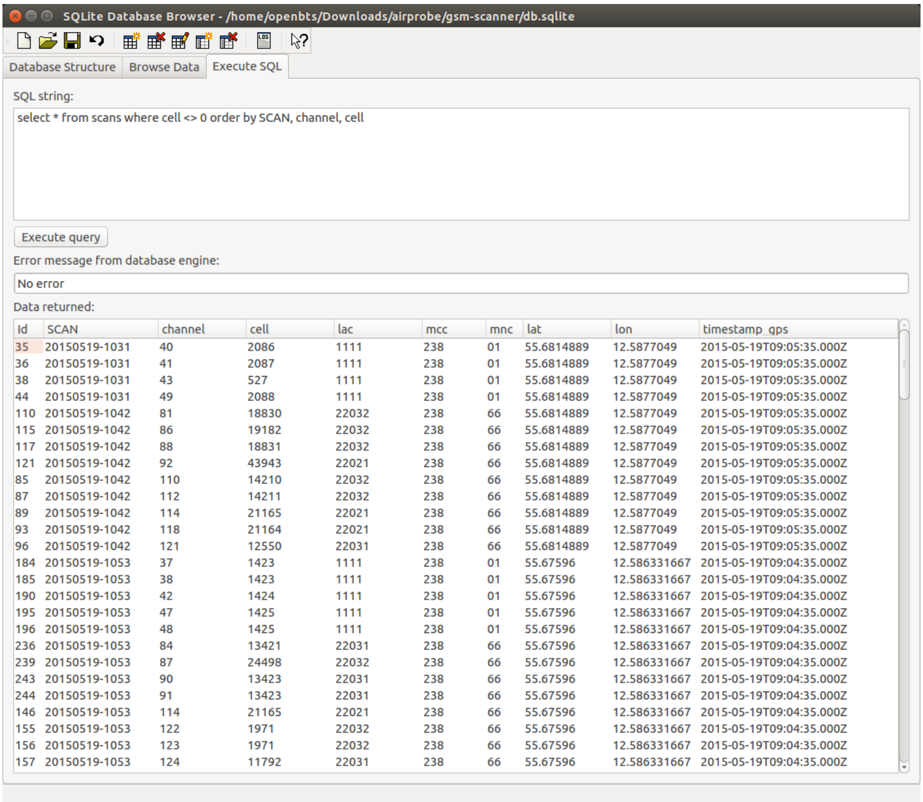


Figure 5.2: Survey Locations

We chose to perform the cell scans at areas where we assume an attacker may gain the most from deploying an IMSI Catcher. The areas chosen were predominantly financial, political, and areas that may be of interest to foreign entities.

5.2 Results

The Figure 5.3 shows an example of the output retrieved from the surveys. In Figure 3.7, even though this is just a snippet of the data which is output from Airprobe, we have access to a large number data points from each cell.



SQLite Database Browser - /home/openbts/Downloads/airprobe/gsm-scanner/db.sqlite
Database Structure
Browse Data
Execute SQL
Execute query

SQL string:

```
select * from scans where cell <> 0 order by SCAN, channel, cell
```

Error message from database engine:

No error

Data returned:

Id	SCAN	channel	cell	lac	mcc	mnc	lat	lon	timestamp_gps
35	20150519-1031	40	2086	1111	238	01	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
36	20150519-1031	41	2087	1111	238	01	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
38	20150519-1031	43	527	1111	238	01	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
44	20150519-1031	49	2088	1111	238	01	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
110	20150519-1042	81	18830	22032	238	66	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
115	20150519-1042	86	19182	22032	238	66	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
117	20150519-1042	88	18831	22032	238	66	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
121	20150519-1042	92	43943	22021	238	66	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
85	20150519-1042	110	14210	22032	238	66	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
87	20150519-1042	112	14211	22032	238	66	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
89	20150519-1042	114	21165	22021	238	66	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
93	20150519-1042	118	21164	22021	238	66	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
96	20150519-1042	121	12550	22031	238	66	55.6814889	12.5877049	2015-05-19T09:05:35.000Z
184	20150519-1053	37	1423	1111	238	01	55.67596	12.586331667	2015-05-19T09:04:35.000Z
185	20150519-1053	38	1423	1111	238	01	55.67596	12.586331667	2015-05-19T09:04:35.000Z
190	20150519-1053	42	1424	1111	238	01	55.67596	12.586331667	2015-05-19T09:04:35.000Z
195	20150519-1053	47	1425	1111	238	01	55.67596	12.586331667	2015-05-19T09:04:35.000Z
196	20150519-1053	48	1425	1111	238	01	55.67596	12.586331667	2015-05-19T09:04:35.000Z
236	20150519-1053	84	13421	22031	238	66	55.67596	12.586331667	2015-05-19T09:04:35.000Z
239	20150519-1053	87	24498	22032	238	66	55.67596	12.586331667	2015-05-19T09:04:35.000Z
243	20150519-1053	90	13423	22031	238	66	55.67596	12.586331667	2015-05-19T09:04:35.000Z
244	20150519-1053	91	13423	22031	238	66	55.67596	12.586331667	2015-05-19T09:04:35.000Z
146	20150519-1053	114	21165	22021	238	66	55.67596	12.586331667	2015-05-19T09:04:35.000Z
155	20150519-1053	122	1971	22032	238	66	55.67596	12.586331667	2015-05-19T09:04:35.000Z
156	20150519-1053	123	1971	22032	238	66	55.67596	12.586331667	2015-05-19T09:04:35.000Z
157	20150519-1053	124	11792	22031	238	66	55.67596	12.586331667	2015-05-19T09:04:35.000Z

Figure 5.3: Database of found cells

Armed with the survey dataset and a matrix of IMSI Catcher detection matrix, an analysis can be performed.

Unfortunately, due to time-constraints that were the result of numerous issues encountered when getting all of the hardware and software to perform the necessary tasks, a thorough data analysis was completed in time for this delivery.

However, we were able to perform a preliminary analysis of the survey data. We look for some of the IMSI Catcher artefacts that were given in the Table 4.1. Some of the artefacts in the aforementioned table require access to data, that we do not have access to with the proposed solution. Additionally, a majority of the artefacts given in the 'IMSI Catcher Artefacts' table, require a survey dataset, which has been gathered over a period of time.

Late in the project, after reading the methodology used by the security company which was commissioned to perform an analysis of the mobile networks in Norway [McK15b]. We have seen the importance of having a cell survey history.

The artefacts that we were able to, given the time-constraints, check against were: Multiple Cells On Channel
Wrong LAC Used
Sudden Appearance of New Cell
We also attempted to match discovered cells against both Mastedatabasen, and OpenCellId

The results of the preliminary analysis were such that we were unable to conclude that we had found any IMSI Catchers.

Chapter 6

State of the Field

Overview

In this chapter we give an overview of the current developments in area of IMSI Catchers and the detection of such devices by using IMSI Catcher-Catchers.

6.1 Related Work

An American hardware manufacturer, known for creating penetration testing and vulnerability assessment products, has recently announced a device capable of detecting IMSI Catchers, its called the Pwnie Pro [Gal15, Pwn15]. This device looks very similar to a typical wi-fi router, a small box with some antennas sticking out the back. The manufacturer claims that the device will be able to detect whether an IMSI Catcher is within close vicinity of the device. Without having any access to the device, it is difficult to assess exactly how it detects a potential IMSI Catcher. However, as has been discussed at length previously in this paper, there are certain aspects of the GSM mobile communication standards, that if used by an IMSI Catcher, are distinguishable from a legitimate mobile cell tower. This device, we suspect, uses some of the same techniques as has been used in this paper to identify potential IMSI Catcher, albeit packaged in a more consumer friendly product.

At DEFCON 18, 2010, Chris Paget, a security researcher showed that it was possible for relatively little money to build an IMSI Catcher by using commercially available software and hardware components [Pag10]. He showed that, by using a SDR (USRP1), OpenBTS, and some of the other software projects mentioned in the Chapter 3, that it he was able to build his own BTS. This BTS he then showed that he could convert a BTS in to an IMSI Catcher.

Dabrowski et al documented the work required for building an IMSI Catcher-Catcher [DPK$^+$14]. The authors built two prototype IMSI Catcher-Catchers devices, one mobile and one stationary. The mobile IMSI Catcher-Catcher was built on Android devices. The stationary device was built using a small computer, and a SDR. They showed two models for building an IMSI Catcher-Catcher and showed to benefits and advantages of both methods.

Song et al. demonstrated a method for building a Fate BTS which could be used to acquire IMSI numbers from target phones [SZC12]. Their Fake BTS was built on a SDR-based system. In the paper they demonstrated two types of attack, that they could perform using their system: IMSI/IMEI catch attack, and an then a method of jamming target IMSI number service. They showed that once they had received the IMSI number from a target device, they could decide whether the device should be allowed service or not.

6.2 Mobile IMSI Catcher-Catchers

In the research field, there are two major open source Android projects that aim to solve the problem of detecting an IMSI Catcher.

Snoopsnitch

Nohl et al. one of the security researchers at Security Research Labs (SRLabs), have developed the Android application SnoopSnitch which is able to detect the presence of an IMSI Catcher and suspicious BTSs [SRL15b]. Using a number detection methods, they are able to determine whether a discovered cell is suspicious or not. If there is a suspicion, then the app will show a warning to the user. In addition, to detecting IMSI Catchers the app offers users to upload cell discoveries to a central database online GSM Map[SRL15a]. GSM Map gathers data from SnoopSnitch users around the world, and uses aggregate data from the users to generate a security report, which details the numbers of passive, active, impersonation, or user impersonation attacks have been discovered in each country.

To detect impersonation attacks (the IMSI Catcher acts as a MITM), SRLabs will periodically automatically call and send texts to the users' phone. Upon receiving a message/call, the app is able to determine whether the Caller ID differs from SRLabs' Caller ID.

AIMSICD

Similar to SnoopSnitch, AIMSICD is an open source Android IMSI-Catcher Detector app project, started by SecUpwN [Sec15]. This project is a similar project to SnoopSnitch, in that is aims to detect IMSI Catchers. AIMSICD does not offer the automatic impersonation attack detection, that SnoopSnitch offers, but it offers many of the other detection functionalities.

Cryptophone and others

Cryptophone is an Android-based secure mobile phone. The phone runs a heavily modified version of the Android OS, and contains a number of enhancements to the OS which increase the security of the phone [GSM]. The main feature, which is relevant to this thesis, is the Baseband firewall (BF). The BF will detect suspicious mobile baseband activity. For example, the device will give warnings when the connection to the basestation is unencrypted. The phone has been used by journalists around the world for detecting IMSI Catchers. For example, the phone was used in the discoveries in Norway [BJHT14], and also the recent discoveries in UK [Che15].

Similar security is also offered by the Blackphone by Silent Circle, and Tiger/S and Tiger/R by Sectra [Sec12].

Android Kickstarter

An interesting development, is that on the crowd-funding platform Kickstarter, users were attempting to collect money to fix a security issue in the Android operating system [Col14]. Users were collecting money to fund the fixing an issue where the OS would not show whether the air interface connection was encrypted or not.

6.3 News

There have been numerous news stories around the world, where journalists have discussed whether IMSI Catchers have been operating in their country. Below we show some of the stories that have been in the news in the last couple of years.

In Moscow 2013, the are allegations that the Moscow Metro has installed IMSI Catcher devices for finding stolen mobile phones. The Moscow Metro claims to have installed devices which are capable of tracking an SIM over range of 16 m, and if the IMSI is wanted (claimed to be stolen) then the system will create a path of the device's movement.s Experts suggest that Russians are likely using the devices for surveillance [Far13].

In Denmark at Version2 in 2014, journalists have made an attempt at discovering whether any IMSI Catcher are to be found in Denmark. They travelled around Copenhagen with an Android device running AIMSICD. The results of their analysis were unsuccessful and the version of the app that they were running turned out to have some issues [jB14].

In the United States, a large number of stories have circulated about the law enforcements' usage of IMSI Catcher. In February of 2015, the FBI had claimed publicly that they used IMSI Catcher in the hunt for 'bad guys'. Asked about the FBI's usage about Stingrays, the FBI Director James Comey publicly stated "It's how we find killers, it's how we find kidnappers, it's how we find drug dealers, it's how we find missing children, it's how we find pedophiles. It's work you want us to be able to do." [Koe15].

This is just one of many news stories from the US regarding this topic.

On 10 June, 2015 the British newspaper Sky News published the results of a survey that they had performed in and around the London, UK area. Again here, the newspaper made use of the Cryptophone for making their analysis. The newspaper published results which were indicative of IMSI Catchers operating in London [Che15].

The Oslo Saga

PST There has been much discussion about whether the are IMSI Catcher being used in Norway. Aftenposten first in December 2014 publish some articles where they claimed to have found evidence of IMSI Catchers around strategically important locations in Oslo, Norway [BJHT14]. The discoveries were made with the use of CryptoPhone 500 devices Section 6.2.

Soon after, the PST published claims that the discoveries made by the newspaper Aftenposten were erroneous. PST claims that the newspaper made a number of errors in their methodology, e.g. they were mobile when performing the cell scannings, and that a number of the suspicious artefacts that the newspaper claimed to be evidence of IMSI Catchers could be explained with sufficient knowledge on mobile networks [BJ15, NTB15].

The latest developments in Norway happened claim that the network operators in Norway do not have any way of detecting any suspicious mobile network activity within their networks. On June 25, 2015, the newspaper publishes a follow article where they put forward additional evidence that mobile surveillance is occurring in Norway [JFHT15]. The newspaper commissioned British security solutions company Delma MSS Ltd., to perform a thorough analysis of the mobile networks in Oslo, and have another attempt at determining whether any IMSI Catchers were to be found in the city. On June 25, 2015, they published the results of their findings [McK15a, McK15b]. According to a number of security experts, e.g. Karsten Nohl from SRLabs, the findings made by Delma are clear indicators of IMSI Catchers [FJRHT15].

Another aspect of the story is that, in January 2015, the Norwegian Stortinget requested a "statement" from the industry and to government to determine whether "fake base stations" (IMSI Catchers) are being used in Norway [Sto15]. June 25, 2015 the report has been completed and they have put forward their results.

> *"«I Norge brukes falske basestasjoner og passivt overvåkingsutstyr i hovedsak av tre brukergrupper; egne myndigheter, fremmede stater, og kriminelle», skriver arbeidsgruppen."*
>
> –[JFHT15]

At the time of this writing, the story is still expected to continue unravelling.

Chapter 7

Future Work

Overview

This chapter will mention future work for the proposed solution, and what can be done further in the development of a system for detecting IMSI Catchers.

Future Work

Stationary Device

Similar to the one created by Dabrowski et al, an idea would be to create a mobile IMSI Catcher-Catcher that could continuously monitor a location permanently, or over a longer period of time [DPK^{+}14]. The device would continuously monitor the area for any appearance or disappearance of suspicious cells.

Continuous monitoring equipment could be installed at location vulnerable and exposed locations. Alternatively, a stationary device could be used as a counter intelligence measure.

An example scenario would be to deploy an IMSI Catcher-Catcher inside/outside an embassy. If a nation state, malicious entity, or other, were to target an employee or visitor of the embassy, then they might deploy an IMSI Catcher outside the premises. Using the IMSI Catcher, the attacker may be able to determine whether a person of interest has visited the embassy. A, or multiple, strategically placed IMSI Catcher-Catcher devices could help detect such a threat to the privacy of the individual.

Maps

A system for displaying discovered cells on a map would increase the usability of the system greatly. We would develop a system that gave the user quick feedback on the cell discovery history, that is, the system would displaying all previously discovered cells on a map, and any new cells would be highlighted.

Future work might include creating a central storage database for cell discoveries. We could create central storage where users of the framework may upload and share their discoveries with the rest of the public. A central, crowd sourced storage, will provide a larger and more complete cell tower dataset. Additionally, we would create a way for the framework to perform lookups on this central database for checking, and to match new cell discoveries with ones made by other users of the system.

Another obvious feature that we would implement is to add functionality for matching all cell discoveries with other cell databases that already exist online. There is an official Danish cell tower database maintained by *Erhvervsstyrelsen* called *Mastedatabasen* [Erh15]. Mastedatabasen provides information about information about existing, and planned cells in Denmark. The database provides the following data on each cell: location coordinates, address, owner of the cell, and mobile technology (GSM, LTE, UMTS, etc.). One issue with this database is that it does not provide cell configuration parameters. The database does not contain information such as LAI, Neighbouring Cells, and CRH. However, when a cell is discovered by our system, we should be able to check against Mastedatabasen whether a cell should exist at the discovery location. The results from this check are not guaranteed to be correct, and should only prove to be an additional indicator on whether a cell is suspicious or not.

OpenCellID is world's largest collaborative community project that collects GPS positions of cell towers [Ena15]. Users install an app on their device which collects information about BTSs. Users can then chose to upload the collected data to the OpenCellID database. One of the differences with this service and the one from Mastedatabasen is that the OpenCellID dataset contains information about MCC, MNC, LAC, and each data-point contains a timestamp of the time the BTS was seen.

The weakness with this system is that the data does not come from official sources. And there may exist gaps in the dataset if no user has performed any measurements in an area. And lastly, data in the dataset may be out of date, and as a result can not guarantee to reflect the reality of BTSs in an area.

Both of the mentioned web-services have their shortcomings, however, combining these two services, and potentially additional services, will only increase the precision of the predictions that the system is able to make.

Using Devices Which Connect to the Network

Future work on an IMSI Catcher-Catcher solution would be build the hardware based on components that have mobile phone modules built-in. As an example, Delma, the security company which was commissioned to do an analysis of whether IMSI Catchers operated in Norway, used SIMCOM (e.g.[Sim07]) modules [McK15a]. These modules are capable of connecting to the mobile networks. Using a system that is able to authenticate and connect to a mobile network we are able to gain access to additional information that may prove useful for detecting an IMSI Catcher. When searching for cells, as was described in Section 2.5 the MS will calculate C1 and C2 values. These values provide further evidence of whether a cell may be suspicious.

We can then also build a system that authenticates with the network. In the authentication process we will be able to receive the message where the BTS provides what type of ciphering to use for the connection. Using our SDR-based system, we are not able to receive this data, as our system will not perform any authentication with the BTS. Our system is simply a passive device that gathers all broadcast data being transmit by the BTS.

Large Scale Analysis

It would be interesting to perform a large scale and longer term investigation of the Copenhagen, Denmark. In the research done in the making of this thesis, we have gained much valuable knowledge, which would make a large investigation more likely to succeed. It would be interesting to perform surveys over a long period of time. This ties in with the work that has been done on the cell database system. With a large survey dataset it will be easier to estimate whether any of the discovered cells are suspicious or not.

Instant Decoding Of GSM Data

If we were to develop a system that was able to directly decode incoming radio messages, rather than having them go through the various processes used in this project, we would be able to decrease the time from scan to result drastically.

We might be able to develop a system which is capable of providing instant feedback about the status of cells at the current location. Additionally, an instant feedback with cell status would make the system even more mobile.

Implement Detection Metrics

The IMSI Catcher-Catcher framework proposed in this thesis would benefit from a system that would automate the data gathering and reporting of errors. This could be similar to the solution found in Android IMSI Catcher Detector applications AIMSICD and SnoopSnitch. These two, both give the user instant feedback, when the app is able to detect any network anomalies.

Develop a Complete Framework

Develop a complete framework, which would work independently of the type of SDR being used to receive GSM signals. The goal would be to develop a complete software solution that could be installed on a users laptop, connect a SDR, and run the program to start detect IMSI Catchers.

There exist the two Android applications, SnoopSnitch and AIMSICD. However, both of these apps rely on the user having specific Android device models, as well as the device has to be 'rooted'[1]. This limits the apps to mainly being used by individuals with a certain level of technological prowess. The Android based solutions are excellent, but an SDR-based solution may be superior in certain ways. For example, it may be able to perform complex computations and store large amounts of data, which the Android apps may be limiting factor for the Android apps.

[1] 'Rooted' means that that OS on the device is 'unlocked' and the user may install applications that are able gain access to features, that in a 'non-rooted' device are lock. These apps

Add Support For Other Bands

In the interest of keeping the scope of this project at a reasonable size, which would allow the author to perform a full system prototype, we chose to limit our system to only perform analysis of the GSM 900 band. There are multiple other bands that may be of interest, see Table 3.2. Adding support for more bands would increase the ability of the system to detect IMSI Catchers, as an IMSI Catcher may be operating on any of the other GSM Bands.

require ‘root’ to be able to access radio data.

CHAPTER 8

Conclusion

Overview

This chapter will summarize the results of this thesis. We conclude the thesis, and we will summarize the work that was made in the project.

Conclusion

At the start of this thesis we set the goal to “Propose a solution for discovering rogue mobile phone towers.”.

Through the course of the project we have acquired considerable amounts of background knowledge required, start building a system which is capable of detecting a rogue mobile phone tower (IMSI Catcher). We have gained an understanding of the basic workings of a GSM network. We have investigated and documented what a IMSI Catcher is. We have learnt how an IMSI Catcher operates, what it is capable of doing, and why someone would want to operate an IMSI Catcher, and for what purpose anyone would use an IMSI Catchers. We have documented the detectable artefacts of an IMSI Catcher, and what can be done to detect these artefacts. Secondly we have identified what technologies can be used to build a system for detecting an IMSI Catcher. We have documented what type of hardware to use, and what software to use. We have analysed a large number of software projects that are relevant to the area of IMSI Catchers and IMSI Catcher-Catchers.

Using the expertise acquired through the course of this project we have proposed a complete solution (hardware/software) for detecting the presence of an IMSI Catcher.

The proposed solution was then used to perform a cell survey around specific locations around Copenhagen, Denmark. We proved that we were able to use our solution to detect cells, and that we were able to gain access to broadcast cell data, which we then are able to analyse further. Lastly, we aimed to perform an analysis of the gathered survey data, in the hopes of detecting an IMSI Catcher. Unfortunately, due to time constraints, a complete and repeated survey was not performed, as well as a thorough analysis of the gathered data will need further work.

However, in this thesis we built and demonstrated a system which is capable of discovering rogue mobile phone towers.

Abbreviations

ARFCN Absolute radio-frequency channel number. xiii, 11, 36

BCC Base Station Colour Code. 15

BCCH Broadcast Control Channel. 15

BTS Base Transceiver Station. 6, 9, 16, 21, 30, 31, 35

C1 Path loss criterion parameter. 31

C2 Reselection criterion parameter. 13, 31

CRH Cell Reselect Hysteresis. 13, 30

GPS Global Positioning System. 9

GSM Global System for Mobile Communications. 1, 2, 6, 15, 18, 24, 32

IMSI International Mobile Subscriber Identity. 13

IMSI Catcher IMSI Catcher. x, 1–6, 9–20, 23–27, 29–32, 36

IMSI Catcher-Catcher A device capable of detecting an IMSI Catcher. 3, 5, 6, 10, 15, 23, 29–32

LAC Location Area Code. 11, 12, 31

LAI Location Area Identification. 30

MCC Mobile Country Code. 31

MITM Man In The Middle. 16

MNC Mobile Network Code. 12, 31

MS Mobile Station. 6, 10–16, 31

Neighbouring Cells A list of ARFCNs, which represents neighbouring cells.. 30

NSM National Sikkerhetsmyndighet (National Security Authority) is a cross-sectoral professional and supervisory authority within the protective services in Norway. The directorate reports to the Minister of Defence (mil. sector). 25

OS Open Source. 32

PST Norwegian Police Security Service. 2

RF Radio Frequency. 11, 15

RMPT Rogue Mobile Phone Tower. 2

SDR Software Define Radio. 6, 31, 32

SIM Subscriber Identity Module. 3

SMS Short Message Service. 2, 16

APPENDIX A

Installation

This section provides information on how to install the necessary software to run the tools that have been used for this project.

Dependencies:

```
apt-get install python-numpy \
python-qt4 libqwt5-qt4-dev qt4-dev-tools \
python-qwt3d-qt4 \
libqwtplot3d-qt4-dev python-qt4-dev \
libxt-dev libaudio-dev libpng-dev \
libxi-dev libxrender-dev libxrandr-dev \
libfreetype6-dev libfontconfig-dev \
python-lxml python-cheetah oss-compat \
swig g++ automake1.9 libtool libusb-dev \
libsdl1.2-dev python-wxgtk2.8 guile-1.8-dev \
libqt4-dev python-opengl fftw3-dev \
libboost-all-dev libcppunit-dev doxygen \
python-qwt5-qt4

jack portaudio19-dev

gsl:
./configure
```

```
make
sudo make install

sdcc:
Download a SDCC version < 3
sudo cp -r * /usr/local
```

Compiling GNU radio:
`http://gnuradio.org/redmine/projects/gnuradio/wiki/UbuntuInstall#Precise-Pangolin-120`

```
./configure --with-boost \
--disable-all-components --enable-usrp \
--enable-omnithread --enable-mblock \
--enable-pmt --enable-gnuradio-examples \
--enable-docs --enable-doxygen \
--enable-gnuradio-core --enable-gr-wxgui \
--enable-gruel --enable-gr-utils \
--enable-gr-usrp --enable-gr-usrp \
--enable-gr-qtgui --enable-gr-audio --enable-gr-uhd

make
sudo make install
```

ETTUS UHD
`http://code.ettus.com/redmine/ettus/projects/uhd/wiki/UHD_Linux`

```
sudo bash -c 'echo "deb http://files.ettus.com/binaries/uhd/repo/
    uhd/ubuntu/'lsb_release -cs' 'lsb_release -cs' main" > /etc/
    apt/sources.list.d/ettus.list'
sudo apt-get update
sudo apt-get install -t 'lsb_release -cs' uhd
```

UHD Configuration: To see what device is connected run: `http://files.ettus.com/manual/page_identification.html`

```
uhd_find_devices

udh_download_images
```

To calibrate the clock on the device: Installing the clock

```
https://code.google.com/p/clock-tamer/wiki/ClockTamerUSRPInstallation
https://web.archive.org/web/20121114100606/http://thre.at/kalibrate/
```

After we have installed the clock, we need to burn this information to the USRP motherboard:

```
./usrp_burn_mb_eeprom --values="mcr=52e6"
```

A.1 Configuring OpenBTS

We need to configure:

Asterisk

SMQUEUE

OpenBTS

Denmark uses 900 and 1800

A.2 Configuring Clock

```
kal -R A:0 -A 0 -v -s GSM900 -F 52M > ~/kaloutput.txt
kal -R A:0 -A 1 -v -s GSM900 -F 52M > ~/kaloutput.txt
```

Open kaloutput.txt and find the lines containing that look like:

```
"chan: 37 (942.4MHz + 32.305kHz) power: 4276.09"
```

This means that there is a BTS in the surrounding area that is transmitting on the ARFCN 37, and that our clock is operating at 32.305kHz faster than the found BTS. To fix this we can calibrate with

```
kal -A 0 -v -c 37 -b 900 -F 52M
```

A.2.1 Yate

```
cd /usr/src
svn checkout http://voip.null.ro/svn/yate/trunk yate
cd yate/
./autogen.sh
```

```
./configure
make install-noapi

cd /usr/src
svn checkout http://voip.null.ro/svn/yatebts/trunk yatebts
cd yatebts/
./autogen.sh
./configure
make install
```

A.3 Mobile Phone Stuff

If you have a mobile phone enter one of the codes below. To do so open up your Dialpad on the phone and enter either of these codes:

```
*#*#4636#*#*
*#*#197328640#*#*
*#0011#
```

iPhone:

```
*3001#12345#*
```

HTC:

```
*#*#7262626#*#*
```

IMSI Number:

```
238022730455866
```

A.4 Clock

Why are clocks so important? http://openbts.org/w/index.php?title=Clocks

http://www.box73.de/product_info.php?products_id=1869 http://www.box73.de/product_info.php?products_id=1870

NOTE: this is a good guide:
http://www.serverfault.sk/2013/07/customizing-backtrack-for-usrp-old-unfinished-note

A.5 OSMO

```
http://itp.junglebrains.com/setting-up-your-own-cellular-network-software-0-2-us
```

Need to install this to be able to install openbsc/openbsc

```
sudo apt-get install libdbi-dev libdbd-sqlite3
```

```
Clone OpenBTS
```

```
ybts.conf
```

If we set the Handover we might trap users that have connected to our network from ever getting released again.

A.6 OpenBTS

Install the UHD drivers Plug the SD Card in to your computer Use the UHD tool ‘usrp2_card_burner_gui.py’ to load an FGPA and FW to your SD card.

```
sudo ./uhd_images_downloader.py
```

This will download images and store them in ‘/usr/share/uhd/images’

To see which images are available run:

```
\$ ls ‘/usr/share/uhd/images’
```

Locate the ‘DEVICE_fw.bin’ and/or ‘DEVICE_fgpa.bin’, select your SD card and click ‘Burn SD Card’.

Now plug the card back in to the USRP2 and plug in the power. It will boot.

A.6.1 Discovering Channels

If you run "kalibrate" you will find the channels where other BTS are transmitting.

```
‘uhd_fft.py -f 950.4 -W -A TX/RX’
```

http://www.rtl-sdr.com/rtl-sdr-tutorial-analyzing-gsm-with-airprobe-and-wireshark/

Wireshark:
System Information Type 2
List of ARFCNs: Neighbouring Cell tower Channels

Filters:

```
e212.mcc == 238
```

This will display all packages with LAC set to Denmark (238)

A.6.2 Wireshark

To run Wireshark as a non user do:

```
sudo apt-get install wireshark
sudo dpkg-reconfigure wireshark-common
   answer yes to the prompt
sudo usermod -a -G wireshark \$USER
gnome-session-quit --logout --no-prompt
```

Bibliography

[Air15] *airprobe*. https://svn.berlin.ccc.de/projects/airprobe/. Version: 2015

[And11] ANDROULIDAKIS, Iosif: Intercepting mobile phone calls and short messages using a GSM tester. In: *Communications in Computer and Information Science* 160 CCIS (2011), S. 281–288. http://dx.doi.org/10.1007/978-3-642-21771-5_30. – DOI 10.1007/978–3–642–21771–5_30. – ISBN 9783642217708

[AST] *Asterisk.org*. http://www.asterisk.org/

[BBK08] BARKAN, Elad ; BIHAM, Eli ; KELLER, Nathan: Instant ciphertext-only cryptanalysis of GSM encrypted communication. In: *Journal of Cryptology* 21 (2008), Nr. 3, S. 392–429. http://dx.doi.org/10.1007/s00145-007-9001-y. – DOI 10.1007/s00145–007–9001–y. – ISBN 978–3–540–40674–7

[BJ15] B. FOSS, Andreas ; JOHANSEN A., Per: *PST avviser Aftenpostens mobilavsløringer - Aftenposten*. http://www.aftenposten.no/nyheter/PST-avviser-Aftenpostens-mobilavsloringer--7960066.html. Version: 2015

[BJHT14] B. FOSS, Andreas ; JOHANSEN A., Per ; HAGER-THORESEN, Fredrik: *Secret surveillance of Norway's leaders detected - Aftenposten*. http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html. Version: 2014

[BRS+02] B. Campbell, Ed. ; Rosenberg, J ; Schulzrinne, H ; Huitema, C ; Gurle, D: *Session Initiation Protocol (SIP) Extension for Instant Messaging.* https://www.ietf.org/rfc/rfc3428.txt. Version: 2002

[CCRS10] Cazacu, Virgil ; Cobârzan, Laura ; Robu, Dan ; Sandu, Florin: Localization of the Mobile Calls Based on SS7 Information and Using Web Mapping Service. In: *Acta Universitatis Sapientiae - Electrical and Mechanical Engineering* 2 (2010), Nr. 112, S. 114–122. – ISSN 20655916

[Che15] Cheshire, Tom: *Fake Mobile Phone Towers Operating In The UK.* http://news.sky.com/story/1499258/fake-mobile-phone-towers-operating-in-the-uk. Version: 2015

[Col14] *Kickstarter » Android Privacy Indicator - Identify Cell Network Tampering by Privacy Collective.* https://www.kickstarter.com/projects/1760935672/android-cipher-indicator-identify-cell-network-tam. Version: Dezember 2014

[DDBP08] De Mulder, Yoni ; Danezis, George ; Batina, Lejla ; Preneel, Bart: Identification via location-profiling in GSM networks. In: *Proceedings of the 7th ACM workshop on Privacy in the electronic society - WPES '08* (2008), 23. http://dx.doi.org/10.1145/1456403.1456409. – DOI 10.1145/1456403.1456409. – ISBN 9781605582894

[DPK+14] Dabrowski, Adrian ; Pianta, Nicola ; Klepp, Thomas ; Mulazzani, Martin ; Weippl, Edgar: IMSI-catch Me if You Can: IMSI-catcher-catchers. In: *Proceedings of the 30th Annual Computer Security Applications Conference.* New York, NY, USA : ACM, 2014 (ACSAC '14). – ISBN 978–1–4503–3005–3, 246–255

[EJ03] Ekdahl, Patrik ; Johansson, Thomas: Another attack on A5/1. In: *IEEE Transactions on Information Theory* 49 (2003), Nr. 1, S. 284–289. http://dx.doi.org/10.1109/TIT.2002.806129. – DOI 10.1109/TIT.2002.806129. – ISSN 00189448

[EMa14] EMarketer: *Smartphone Users Worldwide Will Total 1 . 75 Billion in 2014.* http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536. Version: Januar 2014

[Ena15] *OpenCellID - OpenCellID.* http://opencellid.org/. Version: 2015

[Eng09] Engel, Tobias: *Locating Mobile Phones using SS7*. http://events.ccc.de/congress/2008/Fahrplan/events/2997.en.html. Version: 2009

[Erh15] *Mastedatabasen*. https://www.mastedatabasen.dk/VisKort/PageMap.aspx. Version: 2015

[ETS94] *ETS 300 554 - European digital cellular telecommunications system (Phase 2); Data Link (DL) layer General aspects (GSM 04.05)*. http://www.etsi.org/deliver/etsi_i_ets/300500_300599/300554/01_60/ets_300554e01p.pdf. Version: 1994

[ETS96a] *GSM 03.03 - Version 5.0.0 - Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification (GSM 03.03)*. http://www.etsi.org/deliver/etsi_gts/03/0303/05.00.00_60/gsmts_0303v050000p.pdf. Version: 1996

[ETS96b] *GSM 05.10 - Version 5.0.0 - Digital cellular telecommunications system (Phase 2+); Radio subsystem synchronisation (GSM 05.10) - gsmts_0510v050000p.pdf*. http://www.etsi.org/deliver/etsi_gts/05/0510/05.00.00_60/gsmts_0510v050000p.pdf. Version: 1996

[ETS96c] *GSM 08.56 - Version 5.0.0 - Digital cellular telecommunications system; Base Station Controller - Base Transceiver Station (BSC - BTS) interface; Layer 2 specification (GSM 08.56)*. http://www.etsi.org/deliver/etsi_gts/08/0856/05.00.00_60/gsmts_0856v050000p.pdf. Version: 1996

[ETS96d] *TS 123 003 - V12.6.0 - Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 12.6.0 Release 12) - ts_123003v120600p.pdf*. http://www.etsi.org/deliver/etsi_ts/123000_123099/123003/12.06.00_60/ts_123003v120600p.pdf. Version: 1996

[ETS05] *TS 100 911 - V8.23.0 - Digital cellular telecommunications system (Phase 2+); Radio subsystem link control (3GPP TS 05.08 version 8.23.0 Release 1999)*. http://www.etsi.org/deliver/etsi_ts/100900_100999/100911/08.23.00_60/ts_100911v082300p.pdf. Version: 2005

[ETS06] *TS 144 006 - V6.4.0 - Digital cellular telecommunications system (Phase 2+); Mobile Station - Base Stations System (MS - BSS) interface Data Link (DL) layer specification (3GPP TS 44.006 version 6.4.0 Release*

6). http://www.etsi.org/deliver/etsi_ts/100900_100999/100938/08.04.00_60/ts_100938v080400p.pdf. Version: 2006

[ETS14] *Digital cellular telecommunications system (Phase 2 +); Lawful Interception requirements for GSM GLOBAL SYSTEM FOR.* 2014

[ETS15a] *TS 145 001 - V12.1.0 - Digital cellular telecommunications system (Phase 2+); Physical layer on the radio path; General description (3GPP TS 45.001 version 12.1.0 Release 12).* http://www.etsi.org/deliver/etsi_ts/145000_145099/145001/12.01.00_60/ts_145001v120100p.pdf. Version: 2015

[ETS15b] *TS 145 002 - V12.4.0 - Digital cellular telecommunications system (Phase 2+); Multiplexing and multiple access on the radio path (3GPP TS 45.002 version 12.4.0 Release 12).* http://www.etsi.org/deliver/etsi_ts/145000_145099/145002/12.04.00_60/ts_145002v120400p.pdf. Version: 2015

[Far13] Farivar, Cyrus: *Moscow Metro says new tracking system is to find stolen phones; no one believes them | Ars Technica.* http://tinyurl.com/moscow-metro-tracking. Version: 2013

[FJRHT15] Foss, Andreas B. ; Johansen, Per A. ; Redaksjon, Aftenposten ; Hager-Thoresen, Fredrik: *Ekspertene om mobildataene - Aftenposten.* http://www.aftenposten.no/nyheter/iriks/Ekspertene-om-mobildataene-8069272.html. Version: Juni 2015

[FSO09] *FSO - Openmoko.* http://wiki.openmoko.org/wiki/OpenmokoFramework. Version: 2009

[Gal15] Gallagher, Sean: *This machine catches stingrays: Pwnie Express demos cellular threat detector | Ars Technica.* http://tinyurl.com/ars-pwnie. Version: 2015

[GM11] Golde, Nico ; Mulliner, Collin: *C3TV - SMS-o-Death.* http://media.ccc.de/browse/congress/2010/27c3-4060-en-attacking_mobile_phones.html#video. Version: 2011

[Gnu15] *GNU Radio.* http://gnuradio.org/redmine/projects/gnuradio/wiki. Version: 2015

[Gol12] Golde, Nico: *C3TV - Let Me Answer That for You.* http://media.ccc.de/browse/congress/2012/29c3-5216-en-attacking_mobile_terminated_service_in_gsm_h264.html#video. Version: 2012

[GRB12] Golde, Nico ; Redon, K ; Borgaonkar, Ravishankar: Weaponizing femtocells: The effect of rogue devices on mobile telecommunications. In: *Annual Network & Distributed …* (2012). https://www.isti.tu-berlin.de/fileadmin/fg214/Papers/femto_ndss12.pdf

[GSM] GSMK: *GSMK Cryptophone 500*. http://www.cryptophone.de/en/products/mobile/cp500/

[GSM13] *GSMTAP - OsmocomBB*. http://bb.osmocom.org/trac/wiki/GSMTAP. Version: 2013

[HvH+14] Hadžiali, Mesud ; Škrbi, Mirko ; Huseinovi, Kemal ; Ko, Irvin ; Mušovi, Jasmin ; Hebibovi, Alisa ; Kasumagi, Lamija ; Hadzialic, Mesud ; Skrbic, Mirko ; Huseinovic, Kemal ; Kocan, Irvin ; Musovic, Jasmin ; Hebibovic, Alisa ; Kasumagic, Lamija: An approach to analyze security of GSM network. In: *2014 22nd Telecommunications Forum Telfor (TELFOR)*, IEEE, November 2014. – ISBN 978–1–4799–6191–7, 99–102

[Ied15] Iedema, Michael ; MacDonald, Brian (Hrsg.): *Getting Started with OpenBTS*. O'Reilly Media, Inc., 2015. – 122 S. http://books.google.com/books?hl=en&lr=&id=ZMyZsbvPmJkC&oi=fnd&pg=PR3&dq=Getting+Started+with+D3&ots=vaUtzUHe-G&sig=1XEfQyYmr3xftmrbYEYDfqUkKlk. – ISBN 9781491910658

[Int] *GSM IMSI/IMEI/TMSI Catcher*. http://en.intercept.ws/catalog/2531.html#desc

[jB14] j, Jakob Mø l. ; Boye, Magnus: *Påjagt efter falske basestationer i København med open source-app / Version2*. http://www.version2.dk/artikel/paa-jagt-efter-falske-basestationer-i-koebenhavn-med-open-source-ap Version: 2014

[JFHT15] Johansen, Per A. ; Foss, Andreas B. ; Hager-Thoresen, Fredrik: *Teleselskapene mangler utstyr og rutiner for åavsløre mobilspionene - Aftenposten*. http://www.aftenposten.no/nyheter/iriks/Teleselskapene-mangler-utstyr-og-rutiner-for-a-avslore-mobilspionene html. Version: Juni 2015

[Koe15] Koebler, Jason: *The FBI Admits It Uses Fake Cell Phone Towers to Track You / Motherboard*. http://motherboard.vice.com/read/

fbi-admits-it-uses-fake-cell-phone-towers-to-track-you. Version: Februar 2015

[Mal14] Malsbury, John: *How to Talk to a 36-year-old Space Probe (ISEE-3) with GNU Radio, a USRP, and a Big Dish | John Malsbury.* http://www.jmalsbury.com/how-to-talk-to-a-36-year-old-space-probe-isee-3-with-gnu-radio-a-usrp-
Version: 2014

[McK15a] McKay, Gordon: *MFA-CP-007-D-Supplement.* http://mm.aftenposten.no/2015/06/23-mobilspionasje/pub/MFA-CP-007-D-Supplement.pdf. Version: Juni 2015

[McK15b] McKay, Gordon: *MOBILE NETWORK FORENSIC ANALYSIS.* http://mm.aftenposten.no/2015/06/23-mobilspionasje/pub/MFA-CP-007-D.pdf. Version: Mai 2015

[NM10] Nohl, Karsten ; Munaut, Sylvain: *GSM Sniffing.* http://events.ccc.de/congress/2010/Fahrplan/attachments/1783_101228.27C3.GSM-Sniffing.Nohl_Munaut.pdf. Version: 2010

[Noh] Nohl, Karsten: *Decrypting GSM phone calls | Security Research Labs.* https://srlabs.de/decrypting_gsm/

[Noh10] Nohl, Karsten: *BlackHat-USA-2010-Nohl-Attacking.Phone.Privacy-wp.pdf.* https://media.blackhat.com/bh-us-10/whitepapers/Nohl/BlackHat-USA-2010-Nohl-Attacking.Phone.Privacy-wp.pdf. Version: 2010

[NTB15] NTB: *IMSI-catchere - PST avviser mobilavsløringene - www.digi.no/juss_ og_ samfunn.* http://www.digi.no/juss_og_samfunn/2015/03/26/pst-avviser-mobilavsloringene. Version: 2015

[OET98] Olsson, A ; Ericsson. ; Telia.: *Understanding telecommunications. 2.* Studentlitteratur, 1998. – 677 s S. – ISBN 9144002149, 9789144002149

[Ope08] *Why Openmoko - Openmoko.* http://wiki.openmoko.org/wiki/Why_Openmoko. Version: 2008

[Ope14] *Clocks - OpenBTS.* http://openbts.org/w/index.php/Clocks. Version: 2014

[Ope15] *OpenBTS | Open Source Cellular Infrastructure.* http://openbts.org/. Version: 2015

[Osm10] *MotorolaC123 – OsmocomBB.* http://bb.osmocom.org/trac/wiki/MotorolaC123. Version: 2010

[Osm15a] *Network From Scratch - OpenBSC.* http://openbsc.osmocom.org/trac/wiki/network_from_scratch. Version: 2015

[Osm15b] *OpenBSC project homepage.* http://openbsc.osmocom.org/trac/. Version: 2015

[OSM15c] *OsmocomBB.* http://bb.osmocom.org/trac/. Version: 2015

[Pag10] Paget, Chris: *Defcon 18 - Practical Cellphone Spying - Chris Paget.* https://www.youtube.com/watch?v=DU8hg4FTm0g. Version: 2010

[Pat03] *Method for identifying a mobile phone user or for eavesdropping on outgoing calls.* https://www.google.dk/patents/EP1051053B1?dq=EP20000107879&cl=en. Version: Juli 2003

[PKI] *3G UMTS IMSI Catcher | PKI Electronic Intelligence GmbH Germany.* http://www.pki-electronic.com/products/interception-and-monitoring-systems/3g-umts-imsi-catcher/

[Pug10] Pug50: *Pug50 on Flickr.com.* https://www.flickr.com/photos/pug50/. Version: 2010

[Pwn15] *Pwn Pro.* https://www.pwnieexpress.com/product/pwn-pro/. Version: 2015

[Rtl15] *About RTL-SDR - rtl-sdr.com.* http://www.rtl-sdr.com/about-rtl-sdr/. Version: 2015

[San15] Sandagerdi, Jóannes ⁝ *Thesis repository.* https://github.com/flippingtables/airprobe. Version: 2015

[Sec12] *Sectra Communications.* http://communications.sectra.com/. Version: 2012

[Sec15] SecUpwN: *Android IMSI-Catcher Detector by SecUpwN.* https://secupwn.github.io/Android-IMSI-Catcher-Detector/. Version: 2015

[Sep] *Septier IMSI Catcher.* http://www.septier.com/146.html

[SHL11] Song, Yubo ; Hu, Xili ; Lan, Zhiling: The GSM/UMTS phone number catcher. In: *Proceedings - 3rd International Conference on Multimedia Information Networking and Security, MINES 2011* (2011), S. 520–523. `http://dx.doi.org/10.1109/MINES.2011.153`. – DOI 10.1109/MINES.2011.153. ISBN 9780769545592

[Sim07] Simcom: *Simcom SIM908*. `http://www.simcom.eu/index.php?m=termekek&prime=1&sub=41&id=0000000228`. Version: 2007

[Skl97] Sklar, B.: Rayleigh fading channels in mobile digital communication systems. I. Characterization. In: *IEEE Communications Magazine* 35 (1997), Nr. 9. `http://dx.doi.org/10.1109/35.620535`. – DOI 10.1109/35.620535. – ISSN 0163–6804

[SMQ14] *BuildInstallRun – rangepublic*. `https://wush.net/trac/rangepublic/wiki/BuildInstallRun`. Version: 2014

[SRL15a] SRLabs: *GSM Security Map*. `http://gsmmap.org/`. Version: 2015

[SRL15b] SRLabs: *Wiki - SnoopSnitch - SRLabs Open Source Projects*. `https://opensource.srlabs.de/projects/snoopsnitch`. Version: 2015

[Sto15] *Justis- og beredskapsministerens redegjørelse om falske basestasjoner*. `https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Hva-skjer-nyheter/2014-2015/Justis--og-beredskapsministerens-redegjorelse-om-falske-basestasjoner/`. Version: Januar 2015

[SZC12] Song, Yubo ; Zhou, Kan ; Chen, Xi: Fake BTS attacks of GSM system on software radio platform. In: *Journal of Networks* 7 (2012), Februar, Nr. 2, 275–281. `http://dx.doi.org/10.4304/jnw.7.2.275-281`. – DOI 10.4304/jnw.7.2.275–281. – ISSN 17962056

[SZYC10] Song, Yubo ; Zhou, Kan ; Yao, Bingxin ; Chen, Xi: A GSM/UMTS selective jamming system. In: *Proceedings - 2010 2nd International Conference on Multimedia Information Networking and Security, MINES 2010* (2010), S. 813–815. `http://dx.doi.org/10.1109/MINES.2010.172`. – DOI 10.1109/MINES.2010.172. ISBN 9780769542584

[Tra13] *Trademark Status & Document Retrieval, Stingray.* http://tsdr.uspto.gov/#caseNumber=76303503&caseType=SERIAL_NO&searchType=documentSearch. Version: 2013

[tsh15] *tshark - The Wireshark Network Analyzer 1.12.2.* https://www.wireshark.org/docs/man-pages/tshark.html. Version: 2015

[VAIGCPC01] Vales-Alonso, J. ; Isasi De Vicente, F. ; González-Castano, F. J. ; Pousada-Carballo, J. M.: Real-time detector of GSM terminals. In: *IEEE Communications Letters* 5 (2001), Nr. 6, S. 275–276. http://dx.doi.org/10.1109/4234.929611. – DOI 10.1109/4234.929611. – ISSN 10897798

[WS215] *Wireshark - Go Deep.* https://www.wireshark.org/. Version: 2015

[Yat14] *Network in a Box - YateBTS.* http://wiki.yatebts.com/index.php/Network_in_a_Box. Version: 2014

[Yat15a] *Yate.* http://yate.ro/. Version: 2015

[Yat15b] *YateBTS.* http://yatebts.com/. Version: 2015