Bachelor thesis
Computer Science

Radboud University

Catching IMSI-catcher-catchers: An effectiveness review of IMSI-catcher-catcher applications

Author:
Bauke Brenninkmeijer
4366298

First supervisor/assessor:
MSc, Fabian van den Broek
f.vandenbroek@cs.ru.nl

[Second supervisor:]
MSc, Joeri de Ruiter
joeri@cs.ru.nl

July 3, 2016

Abstract

The modern cell phone knows almost everything about you, from what you are going to do at what time to what you like and dislike. Alongside this, cell phones are becoming more widespread than ever before. These two factors make listening in on these devices very interesting for malicious agents. A way to do this is with an IMSI-catcher. A fake cell tower intercepting all communication. This is countered with an IMSI-catcher-catcher which detects these fake towers. An alternative to these catcher-catchers are apps which claim to do the same. In this paper we will take a look at how effective these apps are at detecting malicious networks and why they do or do not work.

Contents

Chapter 1

Introduction

In this day and age IMSI catchers for the public are not a thing of the past anymore. IMSI-catchers are devices used to, as the name indicates, catch a phone's IMSI (International Mobile Subscriber Identity). This is an unique identifier stored in the SIM. Originally IMSI-catchers only caught identifiers like IMSIs and IMEIs (physical identifier of the device), but this developed into a full size man in the middle device where all data could be intercepted[3]. These fake base stations can be used to intercept text messages, voice messages and data such as used for internet browsing [7]. They can also be used to track a handset, deliver geo-targeted spam messages [10] and even reconfigure APNs to install a more permanent man in the middle [11].

These devices abuse the fact that mobile devices choose strong signals over weak signals due to quality of service and battery usage. This enables attackers to setup a fake cell tower and have mobile devices connect to it. Normally, this would not be a problem, since all communication using UMTS (Universal Mobile Telecommunications System) or LTE uses mutual authentication and encryption, but since most networks provide backwards compatibility for GSM they are not secure. This is because GSM does not require a cell tower to authenticate to the cellphone, while the cellphone does have to authenticate to the cell tower with his SIM (Subscriber Identity Module). This creates the possibility to be connected to a cell tower that is fake or even malicious. A mobile device can easily be deluded to disable data encryption which puts the cell phone tower in full control of all communication since it can read the contents. This gives the ability to do full man-in-the-middle attacks, where the cell tower acts as cell tower towards the phone and as a phone towards the real cell tower.

An article written by the New York Civil Liberties Union states that the NYPD have used Stingrays over a thousand times between 2008 and 2015 [13]. Another article, written by the Washington Post, gave insight to the frequency of IMSI-catchers in Washington. They drove around in a car

with a CryptoPhone, a high security and privacy device capable of detecting IMSI-catchers. They detected 18 interception devices in less than two days of driving around [6]. This exemplifies IMSI-catchers are not an uncommon occurrence.

As a counter to these malicious cell towers, IMSI-catcher-catchers were developed. These devices search the available networks for suspicious cell towers. These fake networks can be identified by a range of characteristics, including strange area codes, identification numbers and sudden downgrades of encryption. But where an IMSI-catcher can be build at home for about a thousand euro [2] [8] or be bought off the shelf for 1,800$ [1], an IMSI-catcher-catcher is much more expensive to build yourself because of the more advanced hardware needed and the lack of existing open-source software. We could only find one commercially available, which costs €49,000 [5].

As an alternative, developers starting creating apps that could potentially do the same as these expensive devices. These apps did not have access to the same powerful hardware as the normal IMSI-catcher-catchers so these apps do not have the same functionality, but they come close nevertheless. These apps scan either the network you are connected to or every network that is available to the phone. In both cases they check if the networks have signs that could indicate if the device is connected to a malicious cell tower or one is near.

In our research we take three well known and popular IMSI-catcher-catcher apps and test them with our own fake network. This will either result in the confirmation that these apps do indeed work, work partially or do not work at all. This is an important subject of research since IMSI-catchers are not an anomaly anymore. The broad public will never buy a personal IMSI-catcher-catcher nor are these functional for consumers to carry around. What they do carry around is their phone, which most people have on them at all times. So if these apps work well, potentially every person could protect themselves against IMSI-catchers.

Chapter 2

Preliminaries

2.1 GSM

GSM is a cell phone communication standard developed by the European Telecommunications Standards Institute. GSM describes one of the protocols for communication on the second generation of cellular networks, also called 2G. GSM is the most used 2G protocol and amounts for 80% of the total subscribers. GSM's first usage was in 1991 and thus has been around for over 25 years. GSM is now the global standard for mobile communication and as of May 2016 there are approximately 4.7 billion mobile subscribers [9].

2.1.1 Architecture

The network of GSM is structured top down and can be split into two categories. On the bottom is the Base Station Subsystem (BSS) which consists of a base transceiver station (BTS) and a base station controller (BSC). The top part is the Network Switching Subsystem (NSS), but this is irrelevant for this paper so we will not go into further detail about this.

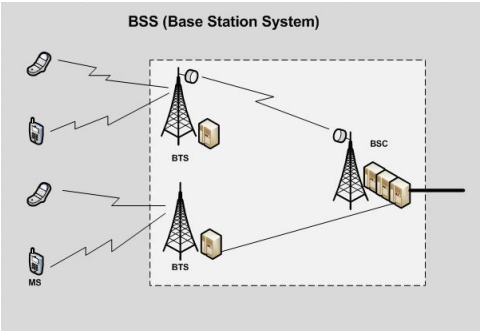

Figure 2.1: The Base Station Subsystem

The BSS handles communication between mobile stations (MS), like cellphones, and the network switching subsystem. The GSM coverage areas are split into cells, with each cell containing a BTS. This is because base transceiver stations are the first connection point of a cellphone when connecting to the cell network meaning they have to be available everywhere. These stations have a limited capacity and are deployed more or less frequently depending on the geographic characteristics and population density. A base station contains equipment for sending and receiving radio signals, antennas and hardware to encrypt and decrypt communication. When connecting to such a tower a cell phone has to identify and authenticate itself. This is needed to make sure the mobile agent is in fact a real user with a SIM card, otherwise everything with an antenna could connect to the cell network. However, this authentication is not mutual, meaning the base station does not have to authenticate itself towards the mobile station. This creates a very serious vulnerability which all GSM operating IMSI-catchers abuse. Anyone can setup a fake base station without any mobile agent noticing any difference with a real base station.

A base transceiver station has multiple parameters of identification which it broadcasts at all times. The first one is the Mobile Country Code (MCC) which specifies the country the base station is located in. For the Netherlands this is 204. The second parameter the Mobile Network Code (MNC) which specifies to which network the cell tower belongs within the specified country code. The network we use in this paper is Tele2 and for Tele2 this code is 02. The third parameter is the Location Area Code (LAC). This is a code specific for the area the tower serves. The fourth parameter is the Cell ID (CID) which is an identification number for the cell tower. A parameter that is not broadcast but important for detecting IMSI-catcher is the absolute radio frequency channel number (ARFCN). This is the frequency on which a tower is broadcasting.

The base station controller controls these base stations, dozens or sometimes hundreds at the same time. It controls the frequency and channel the BTS broadcasts on. It also handles the situation when a mobile station moves from one cell to another, a so-called handoff. When these cells are allocated to different base station controllers this handoff is handled by the network switching subsystem.

2.1.2 Encryption

Encryption of GSM is divided in four variants. There is A5/0, A5/1, A5/2 and A5/3. A5/0 means there is no encryption and everything is communicated in the clear. A5/1, A5/2 and A5/3 are all actual encryptions of which only A5/3 is still regarded as safe. A5/1 can be broken by using rainbow tables whereas A5/2 is broken in real time by using a ciphertext-only attack.

Encryption is an important part of IMSI-catchers since these towers do

not have the private keys of the cell phones, which normal base stations have to verify the SIM is of a genuine user. Because of this reason, IMSI-catchers often tell connected devices to downgrade their encryption to A5/0, in which no private keys are needed, or into the breakable A5/1 and A5/2. This way the fake cell tower can communicate with the connected devices while reading all the content. This also means the fake cell tower can possibly set-up a man-in-the-middle attack between the targeted phone and the real network. Downgraded encryption is also one of the aspects an IMSI-catcher-catcher can check for.

2.2 IMSI-catchers

As stated in the introduction, IMSI-catchers are devices to intercept cell data by pretending to be base transceiver stations. Generally speaking IMSI-catchers can be divided into two categories. On one side you have the off-the-shelf IMSI-catchers sold by specialised companies to governments and law enforcement. Government agencies and security agencies often use heavily customised software which is tailor-made for their specific devices.

On the other side you have the home-made devices. Consumers and researchers do not have the same means as powerful agencies and therefore often use a home-made solution. This mostly consists of a self-made or bought radio transmitter in combination with open source software like OpenBTS. As you will read in the research section, so did we for this paper.

As stated in the encryption part, GSM allows for a full man-in-the-middle. This changes when connecting to a 3G or 4G networks where the flaws of GSM are no longer around. Because of this, networks that do not serve GSM anymore are fairly well protected against man-in-the-middle attacks. But where an IMSI-catcher might not be able to man-in-the-middle anymore, it can still do its original activity of catching IMSIs. The exchange of information like the IMSI is part of the set-up of a connection and thus can still be done on 3G and 4G networks.

2.3 OpenBTS

OpenBTS is a software defined radio developed and maintained by Range Networks. It replaces the functionality of the base station controller and partly the base transceiver station. The software itself runs from a computer or laptop and needs a peripheral to function. These peripherals are devices designed specifically for the purpose of software defined radios. Software defined radios have the ability to serve on multiple frequencies and change their frequency just by a simple configuration. This gives these devices the ability to adapt to changing situations very fast. If the device has multiple

antennas, it can even serve multiple frequencies at the same time, basically having the same capabilities as a real base station.

Chapter 3

Research

We want to test the effectiveness of IMSI-catcher-cather apps. To do this, we ran our own fake base station which will function as an IMSI-catcher. We have gathered three popular apps, namely Snoopsnitch, Cell Spy Catcher and Android IMSI-catcher detector, to detect IMSI-catchers. These apps will be active when connected to the fake network with different settings. This will give an indication about how well apps can function as IMSI-catcher-catchers and give insight in how these apps check whether a network is malicious or not. This will also show what indicators a cell phone can check for to detect fake networks. We will then see if these apps detect the fake networks correctly. Additionally we will use these apps in daily life to get a feel for their user experience and false detection rate.

3.1 Test setup

The implementation of the research setup was fairly basic. We had a Lenovo R60e running Ubuntu 10.10. This is an old version of Ubuntu but had proven to effective in combination with our software defined radio: OpenBTS 2.6. Both aren't the most modern versions but sufficed for this project. OpenBTS is a software defined radio, capable of imitating radio components with the right hardware. Our hardware was the USRP (Universal Software Radio Peripheral) 1 from Ettus Research. This is the first basic software defined radio developed by Ettus Research with a low price, making it attainable to consumers.

Originally we tried running OpenBTS 5.0 which supports 64-bit operating systems and included many new features. This was being installed on Ubuntu 14.04 but unfortunately we did not succeed in this due to the many out-dated required dependencies.

Our fake base station did not perform a man-in-the-middle attack but executed just plain IMSI-catching. There was no network connection available when connected to our base station as to make it quite obvious it is

not a suited network for devices. When connecting to the network the IMSI and IMEI of the phones were logged. With regard to IMSI-catching nothing else was being done.

The network that was set-up had certain limitations. Since we do not have the private keys of phones, our connections were limited to the unencrypted A5/0 cipher mode. As stated in the preliminaries, this is a sign for phones that they might be connected to an IMSI-catcher.

For our testing we use two mobile devices. An LG G3 running the CloudyG3 2.5 ROM, which is based on android 5.0. This device contained a SIM card from Tele2. Our second device is the Nexus 4 running Android 6.0 stock. This device contains a SIM card from Lebara mobile. Tele2 has its own cell towers in the Netherlands while Lebara does not. Lebara uses the cell towers of KPN in the Netherlands, but uses other telecom providers' networks in other countries.

To make sure we didn't interfere with official networks, the antenna was positioned in a Faraday cage. By doing this, only phones inside the Faraday cage could connect to our network.

Our testing exists of running multiple IMSI-catcher-catcher apps at the same time while being connected to our fake base station. The apps are Snoopsnitch, Cell Spy Catcher and Android IMSI-Catcher Detector. The first two can be found on the Play Store, while Android IMSI-Catcher Detector has to be downloaded from Github [1]. Once connected we determine whether the apps detected the fake base station as such.

We connected in two ways. Once where we maintained the connection and waiter a few minutes to disconnect and once where we disconnect after only a few seconds as to imitate a real IMSI-catcher.

3.2 Android vs. iOS

Since both Android and iOS have quite big shares in the current cellphone distribution, we took a look at both to determine whether the operating systems were suitable for our purpose.

iOS releases neither high-level nor low-level baseband information through the public API. Some baseband information is available through a private API that was leaked on the internet, but we do not have access to this. Because of the low accessibility of this required data, there are no IMSI-catcher-catcher application available on the App Store. Since apps on iOS can only be sideloaded on jailbreaked devices, there are no application easily available for iOS to detect IMSI-catchers.

This left us with Android. A search on the Play Store gave us multiple results for IMSI-catcher-catcher application and related applications.

[1] https://github.com/CellularPrivacy/Android-IMSI-Catcher-Detector

3.3 Used apps

3.3.1 SnoopSnitch

Snoopsnitch is an app developed by Karsten Nohl et al. which detects IMSI-catchers and SS7 attacks [12]. SS7 in short is the backbone of telephone communication, which can also be attacked. This app uses diagnostic data from Qualcomm chipsets to detect attacks. This data is parsed and GSM, UMTS and LTE packages are extracted. These packages are then stored in a local database. This database is scanned regularly by the Snoopsnitch service running in the background and notifies the user when something new has been detected since the last analysis. The gathering of this data, since it is so low level, does require root access on the phone. This might be a turnoff for consumers.

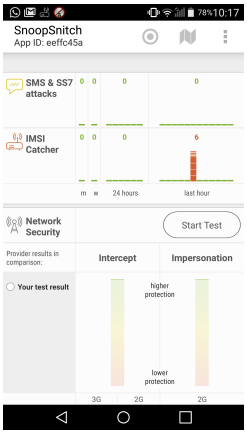

Figure 3.1: Snoopsnitch displaying a detected attack.

Since Snoopsnitch needs a Qualcomm chipset and the additional diagnostic data, a device needs certain specifications to be able to use this app. Unfortunately, the Nexus line of phones did not meet these specifications because it did not have access to the Qualcomm chipset data and thus Snoopsnitch does not work on the Nexus 4. So for the testing of this app we will limit ourselves to the LG G3, on which it does work.

Snoopsnitch uses multiple attributes to determine whether a network is fake or not. The main attributes are changes in LAC and CID in combination with the ARFCN. Changes in the ARFCN while the LAC and CID stay the same or the other way around where the ARFCN stays the same but LAC and CID change are signs an IMSI-catcher might be at work.

In figure 3.1 we displayed the main screen of Snoopsnitch, in which detected IMSI-catcher attacks can be seen.

3.3.2 Cell Spy Catcher

Cell spy catcher is an app that basically detects unknown networks. To do this it has has a learning period in which it learns which networks are nearby. This period can be set by the user, but is two days by default. It learns all the networks present in the area traveled in the two days, which should give a fair impression of the usual networks present in the area. The part that does the actual IMSI-catcher-catching is it compares the list of detected networks to the list of networks it is currently detecting. When it finds an unknown network the app gives a warning. These warnings range from low to high threat, depending on what has changed in the network.

Low indicates a never before seen network. Medium indicates a never before seen network with a changed LAC or CID. High indicates that the network and the LAC have never been seen before. Although this way of detection does work, we do not agree with the levels of warning. Anyone with any knowledge about cell towers and networks will set his LAC to something non-alarming. A malicious agent without enough knowledge to change the LAC is not likely to do much damage. We understand this is not always the case, but we think in the majority it is.

As expected, not all networks you will visit are found in the two day learning period. This results in many false warnings while going outside the learning zone and sometimes even within the learning zone. This happens when a new cell tower is placed or an existing tower is changed.

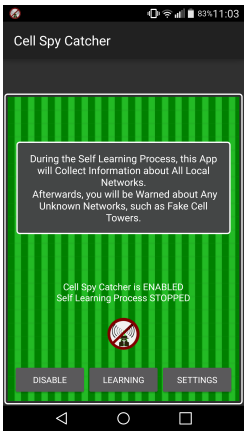

Figure 3.2: The main screen of Cell Spy Catcher.

3.3.3 Android IMSI-Catcher Detector

The Android IMSI-catcher detector is an app developed by the community, mostly existing of members from the XDA-forums. The XDA-forum is the biggest forum for android development. AIMSICD, as it is called in short, is an app with a lot of options. Years of development have created a very functional app with a lot of potential. The app's startscreen shows you your device's network information like IMEI, SIM information like the country, operator ID, IMSI and a lot more.

The second screen gives an overview of nearby cell tower, but this did not appear to be working for us.

The third screen is a database viewer, in which you can see all the networks the app has detected so far. It shows detailed information about these cell towers like CID, LAC, MCC and even the coordinates. The app has the option to download OpenCellID data, which is an open database with cell tower information. When downloaded, these towers also show up in the database viewer as well as the antenna map viewer.

The fourth screen is an antenna map viewer. It takes the local area from OpenStreetMap and puts dots on the locations of cell towers. This way the user has a visual overview of where the cell towers are located. The fifth and last option of the app is the command interface in which the user can execute custom commands. The only IMSI-catcher related option is a little check box that says "Toggle Attack Detection". The status of this is shown as a persistent notification. This is the part that is relevant to IMSI-catcher since this would indicate whether you are connected to an IMSI-catcher or not.

3.4 Different network configurations

In this section we give a technical overview of the network configurations we used for testing. We used a random network setup, a test network setup and an imitating setup.

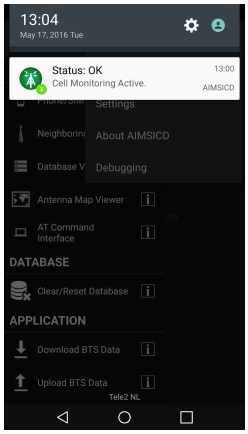

Figure 3.3: The AIMSICD notification.

3.4.1 Random configuration

In this setup we used an MCC of 204, which is predetermined for the Netherlands, and an MNC of 98, which is not allocated to any network in the Netherlands. Thus the MNC of 98 was free for us to use and not have any interference with other networks. The LAC was set to 1000 which did not correspond to cell towers around it.

3.4.2 Test configuration

The setup of the test network is very standard because it has properties described by the GSM specification. Test networks have a MCC of 001 and a MNC of 01. The brand and operator were, as described in the specification, specified as 'Test' and 'Test Network' respectively. The LAC was again set to 1000.

3.4.3 Imitating configuration

In this testing the network used the same settings as the local Tele2 network. These networks had a configuration as follows: MCC=204, MNC=02, LAC=12500 and CID=105966340. We copied every aspect except for the CID which we altered so it wouldn't interfere with the other nearby cell towers. The CID of the nearby Tele2 tower was 105966358, so we chose our CID to be close to that.

3.5 Results and discussion

We discuss the results of each app in combination with each network configuration. We will also outline how the apps compare to each other with respect to the network configuration as some will perform better under certain circumstances. An overview of the results can be found in Figure 3.1, 3.2 and 3.3.

Table 3.1: Results long connection LG G3

	Snoopsnitch	Cell Spy Catcher	Android IMSI-Catcher Detector
Willekeurige configuratie	X	X	
Test configuratie	X	X	
Imitatie configuratie	X		

3.5.1 Random configuration

On the LG G3, Snoopsnitch and Cell Spy Catcher found the network and reported some level of danger, both in the short and the long connection tests. Snoopsnitch even determined it was an IMSI-catcher, while Cell Spy Catcher only reported a new network with medium threat level. It did this because the location area code and mobile network code had changed. AIMSICD, unfortunately, did not find anything suspicious and did not ring an alarm. This is odd, since it did see the network as it was listed in their database viewer. The app did also not respond in any other way to the network.

3.5.2 Test configuration

The test network was detected as being malicious by Snoopsnitch and Cell Spy Catcher on the LG G3 and only by Cell Spy Catcher on the Nexus 4. We have strong doubts Snoopsnitch and cell spy catcher detected it as being a test network since neither have any specific documentation about test networks, but admittedly this does not matter for the purpose of IMSI-catching. As per expectation, these results do not differ much from the random network results, because not much has changed with respect to the mobile stations.

3.5.3 Imitating configuration

With the LG G3, only Snoopsnitch detected that the network was fake. After being connected and receiving the welcome text it started triggering alarms, telling you your phone is connected to an IMSI-catcher. Cell spy catcher did not find anything, but this was to be expected since cell spy catcher mainly checks the attributes of networks like MCC, MNC, LAC and CID and these have not changed in a meaningful way in an imitation network. And last, Android IMSI-catcher detector also did not detect the network as being fake or malicious.

The Nexus 4 had the same results, except for the result from Snoopsnitch which could not be installed. Cell spy catcher did not detect anything strange, and neither did AIMSICD. We suspect this is for the same reasons as on the LG G3.

Table 3.2: Results short connection LG G3

	Snoopsnitch	Cell Spy Catcher	Android IMSI-Catcher Detector
Willekeurige configuratie	X	X	
Test configuratie	X	X	
Imitatie configuratie			

Table 3.3: Results long and short connection Nexus 4

	Cell Spy Catcher	Android IMSI-Catcher Detector
Willekeurige configuratie	X	
Test configuratie	X	
Imitatie configuratie		

3.5.4 User experience

Since apps that are meant to be used by a lot of people have to be very easy to use and have an clear and simple user interface, we will talk shortly about the user experience the apps provided. Starting of with Snoopsnitch, the app provided a clear overview of recent detections and an indication of the security level of your current connection. The other options are hidden under three dots in the right top corner. This is not an new app design and was very common 2-3 years ago. This app would be quite usable by non-experienced users. Cell spy catcher was different. There's one main screen with buttons to enable the service, go to the FAQ and go to settings. The network info is positioned in the middle, but without any formatting. When the user figures out how the app works, it's fairly well designed since the core options are all quickly accessible but for a new user it would be a lot harder to even figure out what the app does. AIMSICD is the only app from these three that tries to follow some user interface guidelines provided by Google. That's why this app does quite well in this regard. It has the swipeable menu on the left side which contains all the relevant items. We would say AIMSICD provides the best user experience, quickly followed after Snoopsnitch and lastly Cell spy catcher.

3.5.5 Discussion

As the results show, some apps work fairly well while others do not. While Snoopsnitch was quite convincing in being capable of detection, the other two disappointed. This raises the question whether we should use these apps. Are they useful enough for people to use them and are they accessible enough for the broad public? And the answer we must draw from this is no. Snoopsnitch is promising but has a lot of requirements, which most people

cannot deliver. We do not recommend Cell Spy Catcher and AIMSICD as their performance was not great or absent. Cell Spy Catcher also detects a lot of false positives, which might make people ignore the warnings, although the warning might be correct and there has been a detection of an IMSI-catcher. This reduces effectiveness quite much and decreases the appeal of Cell Spy Catcher to levels that it is not that interesting for the broad public anymore. Lastly, there is AIMSICD which sadly did not work very well in our research, yet it seems to work quite well for others. This might be a good subject for future research. But looking at our results, we must conclude that AIMSICD is not very capable at detecting IMSI-catchers and therefor is not appealing to the public.

Chapter 4

Related Work

In this paper we have only talked about how to protect your own device, but to remove the IMSI-catcher exploit for once and for good more substantial measures have to be taken. Since this problem exists primarily because base station need not authenticate themselves towards mobile stations, this can easily be fixed by authenticating. However, this would require changes in the GSM protocol, as well as the firmware of base stations.

As a reaction to this, research was conducted towards fixing the IMSI-catcher exploit without having to change the infrastructure. Van den Broek et al.[14] discussed an approach using pseudonyms, where the IMSI is replaced by an pseudonym which can only be authenticated by the home network, rendering it useless to intermediate providers. This would resolve the problem where people can be tracked via IMSIs since phones would not try to authenticate with their IMSI to a base station anymore. In their solution the only things that need to change are some properties on the SIM and the authentication with the home network. Both can be implemented quite easily.

There have been other papers regarding the use of phones as IMSI-catcher-catchers. Dabrowski et al. researched the possibility of widespread IMSI-catcher-catchers by using phones [4]. In contradiction to our research, they created their own application. The chose to not use root access, as to enlarge the potential user base. Their app divides the area in 150 x 100 meter tiles which are set in a learning mode at the start. To signal a tile being ready for evaluation, at least entering the tile area twice and scanning of the tile are necessary. When data from the surrounding 8 tiles has also been gathered, the tile is seen fit for evaluation. This is done to prevent false positives from neighbouring cell towers. When a tile was in the evaluation phase it would check for unknown networks and alarm the user when finding a new one. In their experience the phones could identify their fake base station quite reliable. This gave us confidence the consumer apps would be able to detect something as well.

Chapter 5

Conclusions

We can say that although some apps are capable of warning the user of IMSI-catcher presence, to work well these apps require high privileges and low level access to baseband chipsets to offer some level of protection. This does not mean they completely protect you against IMSI-catchers, but it should give the user a warning at least. Although the results of Cell Spy Catcher and AIMSICD were not convincing at all, at least Cell Spy Catcher can be used to check whether the local network configuration has changed, but AIMSICD just did not work at all. Since we tested it on two phones, the possibility of some form of missing compatibility is very small. Snoopsnitch only works on some phones requiring specific hardware and root access. Although two-thirds of the phones contain this hardware, this might not be the same in the future. Root access is also a threshold for the average user, reducing the number of people who can use the app even further.

Snoopsnitch was by far the most competent one among the ones we tested and actually told you with confidence when you were being attacked, while Cell Spy Catcher gave you a mere warning with some info. This would not be enough to alarm a person without much knowledge about cell networks. The point that does stand out with this is that Snoopsnitch needed very low level diagnostic data from Qualcomm chipsets and root access to work. Since this was the only app really detecting the networks, means that it is really hard to detect fake networks with only the towers identifiers like Cell Spy Catcher uses.

In conclusion, IMSI-catcher-catcher apps are still early in development with regard to dedicated IMSI-catcher-catchers. They have a worse detection rate, false positives or require unusual high level access and therefor are not recommendable to the public. With the constant development of phones and software, this might more interesting to research in a few years.

Bibliography

[1] Imsi-catcher on alibaba. https://www.alibaba.com/product-detail/IMSI-catcher_135958750.html.

[2] Chris Paget aka Kristin Paget. Practical cellphone spying, 2010. At DEFCON 19.

[3] R. Bott and J. Frick. Method for identifying a mobile phone user or for eavesdropping on outgoing calls. July 25 2001. EP Patent App. EP20,000,107,879.

[4] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. Imsi-catch me if you can: Imsi-catcher-catchers. In *Proceedings of the 30th annual computer security applications Conference*, pages 246–255. ACM, 2014.

[5] DFRC. Imsi-catcher detector. http://www.dfrc.ch/solutions/imsi-catcher-detector/.

[6] Craig Timberg for The Washington Post. Tech firm tries to pull back curtain on surveillance efforts in washington. http://wapo.st/1qgzImt.

[7] Nico Golde, Kevin Redon, and Ravishankar Borgaonkar. Weaponizing femtocells: The effect of rogue devices on mobile telecommunications. In *NDSS*, 2012.

[8] Bryan Harmat, Jared Stroud, Daryl Johnson, Bill Stackpole, and Sylvia Perez-Hardy. The security implications of imsi catchers. In *Proceedings of the International Conference on Security and Management (SAM)*, page 57. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2015.

[9] GSMA Intelligence. Definitive data and analysis for the mobile industry. https://www.gsmaintelligence.com/.

[10] P Muncaster. Chinese cops cuff 1,500 in fake base station spam raid, 2014. http://www.theregister.co.uk/2014/03/26/spam_text_china_clampdown_police/.

[11] M Solnik and M Blanchou. Cellular exploitation on a global scale: The rise and fall of the control protocol. *Black Hat USA*, 2014.

[12] Snoopsnitch Team. Imsi catcher score. https://opensource.srlabs.de/projects/snoopsnitch/wiki/IMSI_Catcher_Score.

[13] New York Civil Liberties Union. Nypd has used stingrays more than 1,000 times since 2008. http://www.nyclu.org/news/nypd-has-used-stingrays-more-1000-times-2008.

[14] Fabian van den Broek, Roel Verdult, and Joeri de Ruiter. Defeating imsi catchers. pages 340–351, 2015.