Christian

[Skriv et resume af dokumentet her. Resumeet er normalt en kort beskrivelse af dokumentets indhold. Skriv et resume af dokumentet her. Resumeet er normalt en kort beskrivelse af dokumentets indhold.]

[Skriv titlen på dokumentet]

[Skriv undertitlen på dokumentet]

# Abstract

An abstract of the report

# Report information

Group names, data.

# Introduction

There are over 5 billion mobile phones worldwide [1]. Phones have changes our lives, for some it is a very important part of our life. With over 5 billion phones, it is one of the most widespread types of technology.

The mobile technology has developed a lot since the early start. From the transportable phone to the latest Smartphones today.

## Android

Android is one of the most used operating system for smartphones and tablets. The android system is a free open source system from Google [2]. The android system does only work with devices equipped with a touchscreen [3]. There are over 100 million android devices, with 400.000 new devices every day [4]. HTC, Samsung and LG are some of the big mobile companies, who use android. They have their own skin, like HTCSence, but they use android as OS. The programs for android are called Apps. Apps can be downloaded from Android Market, where many apps are free, and some are for sale. There are over 200.000 apps available in Android Market, with 4.5 billion installed apps. [4]

The many apps can improve the users’ experience of android, but all these apps are not authorized by Google. It means, that Google do not control the porpoise of the app, e.g. sending personal information to a third part.

## IMEI

International Mobile Equipment Identity (IMEI) is a number which follows the mobile unit. If the SIM-card on a phone is replaced, the IMEI number will remain the same. When a phone connects to the mobile network, it will be identified by its IMEI. The IMEI can be a great weapon against cell phone thieves. If a cell phone is stolen, the police have the possibility to block the IMEI, so the phone cannot get access to the mobile network anywhere in the world, which will make the mobile useless as a mobile phone.

The IMEI is a unique number for a phone – in theory. There are examples of changing the IMEI of a phone, making it a copy of another phone.

The IMEI has a lot of opportunities, like combating theft, but also have some possibilities of illegal use.

# Problem analysis

The use of mobile technology has changed our way of life, and this change has consequences.

For some, the use of mobile phones can be a problem – an addiction. As a result of that, it can be concluded that technology has a lot of consequences – good and bad.

Many have a lot of personal information on the phone. With the new smartphones, there are the possibilities to manage your bank account. The owner in other words does not want anyone to get into his private information on the phone.

When IMEI identification was developed, the system seemed like a great system to identify the phones, but the system had other possibilities. If the IMEI number falls into the wrong hands, the phone can be tracked, controlled and many other things.

There are many issues and problems with this new technology. To increase the focus of the report, the report will focus on the possibilities of the IMEI.

The IMEI has many good uses for the police, and technical uses for the operators of the mobile network, but apps for Android can get the IMEI with a simple function.

If it’s only the authorities that have any use of the IMEI number, then why is it possible for the android apps to read the phones IMEI?

The report will illuminate the legal uses of the IMEI, and to try to show the reasons as to why apps can read the IMEI. The report will also describe some of the illegal uses of the IMEI, and describe the consequences of a stolen IMEI.

Therefore, the problem statement is:

“Why can apps on Android-phones get the IMEI, and what consequences can it have?”

Exactly why IMEI numbers can be read at all isn't clear. The most simple thing to do for the IMEI number would be to encrypt it, and obviously keep it hidden to the consumers. The companies could then keep logs of the IMEI numbers. Then, if a phone is stolen, the consumer could contact his or her's company and they would find the IMEI for the phone and lock it.

# Theory of IMEI, IMSI and Android

A mobile phone connect to the network by a GSM module. A GSM module can host thousands of mobile phones, and it use two information to recognize the phones from each other is the IMEI and the IMSI number [5]. The system of IMEI numbers was valid from 2003 [6]. The IMEI number is a 14 og 16 digits. As seen on Figur 1, the IMEI number is given, by a set of different digits. The first two digits, marked on the figure with “NN” is the Reporting Body Identifier. The Reporting Body Identifier is a geographic assign code. The next 6 digits, marked with a “XXXXYY” on the figure is the ME Type Identifier. ME stands for Mobile Equipment. Is identifiers which type of mobile phone it is. The “XXXX” is the original identifiers digits. In the beginning, the YY were set to “00” until they were needed. The “ZZZZZZ” on the figure is the digits for the serial number. The serial number is a unique number for every cellphone of a specific ME type. The last digits is a check digit, which is generated by a function of the other digits, and is uses for verifying the IMEI.



Figur 1: The figure shows the structure of the IMEI number. [6]

The IMEI numbers has been extended by two digits since its first origin.

When the IMEI number is sticks to the cellphone, the IMSI sticks to the SIM-card. The IMSI is similar to IMEI and stands for International Mobile Subscriber Identity. Where the IMEI is like the chassis number of a car, the IMSI is the registration number [8]. The IMSI determents who’s paying for the mobile traffic. The IMSI number is a 14 or 15 digits number, and it is, like the IMEI, generatet by a certain system [7]. As seen on Figur 2, the IMSI number start with 3 digits, described as “MCC”. The “MCC” stands for Mobile Country Code, and is a specific code, given for which country the SIM-card is issued. The “MNC” is the Nobile Network Code, and is a code, specific for the operator associated with the SIM-card. It can be 2 og 3 digits long. The last 10 digits is the “MSIN” or the Mobile Subscriber Identification Number. Together, these 14 or 15 digits will be the IMSI.



Figur 2: The figure shows the structure of the IMSI number. [7]

When a cellphone connects the the mobile network, it will send and identify it self with the IMEI and IMSI.

## Android

Android is a OS for smartphones and tablets developed by Google. Google is a multinational company, which make a lot of net based solution like Gmail, Google search, Google Translate etc. Common for all is, that it is free. The core of Android is based on a Linux kernel, with GNU software. The Linux kernel is the core of the system, where the OS GNU software is built on. Android is then a bouilton to the GNU, with the first release in 2008. Several cellphone producents, who uses Android, makes their own skin for Android, like HTC Sense.



Figur 3: The structure of the Android system.

The structure of Android is described on Figur 3. All the drivers and necessary processes is in the Linus kernel. Then there is a lot of libraries, which the Android runtime use to start up. It is the Android Runtime, which control and coordinate the system, where the libraries is read by the runtime. The kernel is the basic structure, which make the runtime possible to start. Then there is the application framework, and the applications, which make the Apps possible on Android.

# Theft of cellphones and IMEI

**Cellphone Theft**

In 2008, 139.3 million smart phones were either handed over the counter in the local shops, or shipped to a buyer somewhere in the world. By the end of the fourth quarter of 2008 alone 38.1 million unites had been sold. According to Gartner, a US research firm, that's an increase of 3.7 percent if you compare it to the same quarter of 2007. Overall the increase in sales when comparing 2007 to 2008 proved to be as high as 13.9 percent.

With all these phones being handed out to customers around the world legally, it makes you wonder just how many phones are being sold illegally?

Statistically every one in five smart-phone is a fake. Crafted to look the model of any one of the most popular smart-phones.

What that means is that there's a 20 percent chance that the Nokia-phone your friend, colleague or even yourself own is actually a Nokia. In many cases the manufacturers of these copies will put a name that very much resembles the name of the real model. In some cases they will just put the original logo on the phone and sell it even still.

These kinds of phones make up for one of the major dangers in cell-phone theft and cell-phone copying. As they can easily come with malicious software installed onto them, or if they are bought with a subscription, the sim-card might be coded to apply for expensive SMS-services obviously this will be kept completely unknown to the owner of the phone untill the bill for the month arrives.

This kind of software can potentially also be installed on a regular phone. According to the metropolitan police service, there's stolen 10.000 phones on average each month [9].

If a phone is stolen, and not reported as such, the thief, or new buyer can use the phone in your name. There's the obvious making calls, sending texts and other use of traffics and services on your bill. However you can easily set up a paid call-line, and make several calls to that line from the stolen phone and make huge profit. Furthermore, as the number and phone is adressed to the original owner, anyone with acces to the phone can go ahead and do whatever they want, and it'll be in the original owner's name.

**IMEI Theft**

If a phone is stolen, one should immediately get it locked. This can be done through submitting the IMEI number, that your phone is carrying. If your phone is stolen, and you do not get your IMEI locked, the new owner can potentially just keep buying new pre-paid cards, and do whatever he or she wants to do in your name, and you wouldn't even know about it, as there would no longer be a bill to recieve. Every phone should, in theory, carry it's own unique IMEI number. So if a theif get's a hold of a phone, and changes the billing information/address, he has successfully stolen just the hardware of the phone and the IMEI number. The ability to use a phone completely anonymously carries great value in the crime-world. In India a group of 3 men went to stores and implanted fake (invalid) IMEI numbers in phones. The article doesnt describe what the purpose was, but one could imagine that they then kept the original (valid) IMEI numbers to themselves, or for trading purposes.

The way an IMEI number is stolen from a phone is simply by changing the IMEI shown on the phone. The location varies depending on what model it is. Then you change the IMEI inside the actual software of the phone. In India it was done using something called "The Spiderman Kit".

# Android Apps (Anders)

What is Andoid app, and how do they work? Do they “sniff” the IMEI number and for what reason?

# Usage of IMEI

## Law of IMEI

The problem of combatting abuse of IMEI is that it is a global problem. UK has made laws, which make it illegal to change the IMEI on a phone [10]. There are several similar laws around the world, with the porpoise to prevent illegal activities, using the IMEI. The problem is the lack of a global law of IMEI abuse. When it is legal to change the IMEI of a telephone in the UK there are no law about it in China, which will make it possible to legal change the IMEI in China, and sent it to the UK, og other countries with more strictly laws.

There are no global laws, but there is a Central Equipment Identity Register (CEIR), which is a database of stolen and lost IMEI. The central is located in Ireland, and is maintained by GSMA (GSM Assosiasion) [11].

There are many countries that check this CEIR, far from all.

There is therefore no worldwide cooperation against stolen phones using the IMEI number.

## Legal use

The IMEI number is used to prevent stolen mobile phones from accessing a network and being used illegally. In case the phone is stolen the owner can contract their network carrier and tell them to disable their phone using its IMEI number. When the carrier has blocked the phone, the phone is unable to connect to any network. With the IMEI number the phone can easily be blocked from the network. Even if you change your SIM card, the phone will still be blocked, because the IMEI number is stored on the phone itself and not on the SIM card [12].

When a carrier gets the message that a phone has been stolen or lost, they contact CEIR (Central Equipment Identity Register) which will blacklist the device. This will make the phone unusable [12].

Shopping centers in the UK are tracking their costumers’ every move. They track their costumers by monitoring the signal produced by the costumer’s cell phone. The phone is tracked by placing receivers around the shop. The system then uses the triangulation method, by measuring the distance from the phone to the three closest receivers, to see their customers’ position [13].

The system does not identify the owner, but only the phones IMEI number. It is the operator only that can match the IMEI number to the personal information about the owner. Path Intelligence, the developer of the technology says that the equipment is just a tool for market research [13].

### What does the user, use the IMEI to?

When the user tries to connect to the mobile network, the phone first looks for an operator where the phone has permission to connect. Then the IMEI number is checked in a central register of all usable IMEI number. If the IMEI number has been reported stolen, the police get notified with the information of the location and when the phone last was used. And if the phone is blacklisted the phone does not get permission to connect to the network. [14]

### What can apps use IMEI to?

When an application is launched it checks the device’s IMEI number and from that number the phone can see the device brand and model. The application can then compare it with a list of devices that is allowed to run the application. This could be used to determine if the phone is fast enough to run the application. [12]

### How does the application get access to the IMEI number?

When an application needs to read the IMEI number, the application has to get permission from the user as seen on Figur 4. The application gets permission though “The Manifest File”, in order to use the methods “TelephonyManager”. This manifest file is the file that later asks the user, if the application is allow to use the command “getDeviceId()” [16]. This command will get the IMEI number and the application can use it however it wants. [17]

When the user buys an application it asks for permission to some “mother-categories”. Here it is the “Phone calls”

“This permission deals with reading the state of the phone and identity. This can be a bit of questionable permission as it allows apps to read the IMEI, IMSI and 64-bit unique ID of the phone. Apps can use this for finding out about piracy, but this is not transparent. The state of the phone deals with an app being able to read if you are on the phone or not.” [18]

Figur 4: Shows a app, trying to get permission to read the IMEI. [15], edited.

## Illegal use

How can the IMEI/IMSI number be abused?

### Control of the phone (Thais)

How the phone can be controlled with the IMEI number.

### Surveillance of phone traffic

Within the last few years, it has become more common to monitor cellphones in search of terrorists, drug dealers, mafia bosses, etc. That’s a good idea but what happens when governments intelligence agencies start monitoring regular people?

It’s become a fact that the intelligence agencies can monitor yours and my cellphones [19] and the problem is that it’s actually a violation of privacy rights. The article says that the FBI can use your cellphone to monitor everything you say to people, even when it’s powered off. The only solution to solve this problem is to take the battery out of your cellphone. [20]

One of the dangers of the surveillance is that it can be interrupted by “crackers” (crackers are the evil edition of hackers), which means it potentially can be used to terror activities. Another danger is the question; who are watching those who are watching us? We don’t really know what the intelligence agencies are using the mined data for.

In Denmark, we are being monitored as well by the Danish intelligence agency, PET. After the second “terror law” got adopted by the Danish government, PET was now allowed to monitor people via their e-mails, phone calls, text messages, and where they go without a court order [21] but it was only allowed if it could be proofed that it had a connection to terrorism. We aren’t really known for such monitoring in Denmark as they are in Great Britain. In the Great Britain there is one camera for every 14 citizen which is a whole lot more than there is in Denmark.

### PET (Danish Security and Intelligence Service)

It started back in the 1920's with Copenhagen Explorer Police, which was the first established political department that was the first intelligence department in Denmark. In the first years they operated in Copenhagen only, but after a few years the police chiefs in the country districts got a reporting duty to the department.

In 1939, a new nationwide intelligence service came to life under the chief of the state police. It was called the "Sikkerhedspolitiet" (Security police). The service was taken down during WWII and was reestablished in 1945 under the name "Commissioner of Police's intelligence department".

6 years later, in 1951 happened a general re-organizing in the service which resulted in a change of the name to "Politiets Efterretningstjeneste" (Danish Intelligence Agence - DIA).

Until 1960 the Copenhagen Police, Frederiksberg Police, Southern and Northern Birk Police were excepted from the reporting duty to the Commissioner of Police, but through the years 1960-66 the DIA overtook the intelligence work within those 4 police districts and has since been nationwide. [22]

#### Organization

The DIA is a part of the Danish police. Organizational the service represents a department within the State Police (Department G). Due to the intelligence agency's special duties the commissioner of the service reports directly to the Secretary of Justice.

DIA has through time adapted the organization and resources accorded to the actual threat- and communityimage. It's the intention that DIA's structure must support the service's overall strategy about an intensive focus on the operative- and monitoringpurposes, and the service's extern coordinated role.

The personal consists of 700 employees, officers, office personal, lawyers, academics, communication people, interpreters, and technicians. [23]

#### Duties today

Their main duties today are counter terrorism, counter extremism, and counter espionage. The intention is to keep our country free from terrorist attacks, but also securing VIP's like politicians, the royal, and other exposed persons like the Muhammed cartoonist Kurt Westergaard. They employ their own bodyguards to protect the VIP's. They monitor both domestic and foreign terror cells like Taliban and al-Qaeda by listening to their phone calls, watching their activities, reading their e-mails, and they work together with both Europol and Interpol in the war against terrorism.

### Copy of identity

On the GSM network, an identity is based on two numbers: The IMEI number, which is bound to a specific phone. This number can usually be found by pressing “\*#06#” on the phone, but it is also located under the battery, and it also appears on the bill when purchasing the phone. In case a cellphone is stolen, you can contact your network provider, and have that exact phone blocked on all networks.

The other number is the IMSI number – this number is tied to the SIM-card, which again is tied to the individual user of that SIM-card. Both the IMEI and the IMSI number are used to identify the phone, when it connects to a signal transmitter. On Android it is very easy for an app to get both the IMEI and IMSI number. The app simply has to call the TelephonyManager library, and then use the getDeviceId() function to get the IMEI number, and the getSubscriberId() function to get the IMSI number [16]. In theory the app could then silently transmit these numbers to a remote server, and a criminal would be able to alter these on to another phone.

It is in fact illegal to alter the IMEI number – this is because the only apparent reason to alter the IMEI number is if the phone was stolen and blacklisted. But organized criminals like terrorists may be interested in obtaining IMEI- and corresponding IMSI numbers to hide their identity and to make it harder for the authorities to trace them.

There have already been a number of reported Trojan horses on the Android platform, which obtained the IMEI and IMSI numbers and established encrypted data connections to remote servers and transmitted the infected phones IMEI and IMSI numbers [24]. At least three of the known Trojans for Android were spread using fake Chinese clones of the Android Market. In these markets popular apps where repackaged in order to contain the Trojan. This is may be the easiest method to obtain IMEI and IMSI numbers. Another, more sophisticated method to obtain this sensitive data is to build a GSM transmitter – this can be built with regular electronic equipment, which can be found in most electronic stores [24]. A cellphone will in theory connect to the signal transmitter with best connectivity, thus getting the best signal. A custom built transmitter will then be able to decode the encrypted phone signal, and extract the IMEI and IMSI numbers.

To prevent these attacks, one would simply disallow roaming, thus disabling the phone to connect to other service providers, and unknown network transmitters. One would also have to have an updated anti-virus application to prevent infections on the phone.

## Illegal IMEI implants

Manufacturers of cheap cellphones in China have been unable to put a genuine IMEI number on their phones. This caused a lot of phones to be unusable in many western countries, due to the fact that you need an IMEI number to connect to a signal transmitter. But in India, phones with illegitimate IMEI numbers and even phones without IMEI numbers would be allowed to work just fine. That was until April 15th, 2009, where India decided that phones without a genuine IMEI number weren’t serviceable. This rendered up to 25 million unusable cellphones in India, from one day to another. The reason why phones was sold without a genuine IMEI number, is that only two instances, British Approvals Board of Telecommunications and the North America's PCS Type Certification Review Board was allowed to issue IMEI numbers to cellphone manufacturers. In December 2008, the Telecommunication Terminal Testing & Approval Forum in China was allowed to issue IMEI numbers to cellphones manufactured in China. [25]

## Examples of IMEI abuse (Thais)

Concrete examples with people who has been a victim of identity theft through the change of an IMEI number.

## Difference between tablets and smartphones

Since tablets, at least tablets with 3G connectivity, also have IMEI- and IMSI numbers [26], they are also potential victims to identity theft. But since the tablets are generally used in different ways [27] than smartphones, they might pose an even bigger threat if exploited. It seems that tablets are used as a replacement of laptops – which suggests that tablets are used for work and to handle more sensitive data than smartphones. Again, if a criminal where to only obtain the IMSI and IMEI numbers, he would only be able to use the victim’s subscription as if it was his own. Sensitive personal information is not vulnerable to this kind of attack. On the other hand, if a tablet is infected with one of the above mentioned Trojans, it criminals would be able to obtain vital information – especially if the tablet were used to hold company data. A smartphone on the other hand, is more likely to be used to communicate, where the tablet is likely to be used to actually work, due to the bigger screen, which improves the productivity experience.

## Consequences of an stolen/copied IMEI (Nicolai)

#### Mobile operators

Their function in case of a stolen phone. Abuse of power to gain control over innocent people’s phones.

The consequences for the operator.

#### Client

Consequences for the clients.

# Conclusion (and follow-up on the statement of problem)

# Litterateur

[1] BBC, “Over 5 billion mobile phone connections worldwide”, 9. July 2010

[2] Android.com, “Licenses”, visited 19/9/2011, <http://source.android.com/source/licenses.html>

[3] Gartner.com, “Gartner Says Sales of Mobile Devices in Second Quarter of 2011 Grew 16.5 Percent Year-on-Year; Smartphone Sales Grew 74 Percent”, August 11, 2011.

[4] Google Code Blog, “Android: momentum, mobile and more at Google I/O”, 5. October 2011.

[5] ewh.ieee.org, ”GSM”, <http://ewh.ieee.org/r10/bombay/news5/GSM.htm>

[6] GSM Association, “IMEI Allocation and Approval Guidelines”, 1. September 2010.

[7] Liu, Zhen Yu. Xie, ShengLi. Lai, Yue. “A Parallel Method in the 3G Firewall”. 2009.

[8] Goode, A. J. “Forensic extraction of electronic evidence from GSM mobile phones”, 2003.

[9] Metropolitan Police. “Safeguarding your mobile phone”. Visited 19. September 2011. <http://www.met.police.uk/crimeprevention/phone.htm>

[10] UK Government. “Mobile Telephones (Re-programming)”. Act 2002. <http://www.legislation.gov.uk/ukpga/2002/31/pdfs/ukpga_20020031_en.pdf>

[11] IT- og telestyrelsen. “Din mobiltelefon eller SIM-kort er blevet stjålet”. Visited 19. september 2011. <http://borger.itst.dk/lov-og-ret/adgang-til-internet-og-telefonlinjer/mobiltelefonen-er-stjalet-hvad-gor-du/din-mobiltelefon-eller-sim-kort-er-stjalet-hvad-gor-du>

[12] GSM Security. ”What is IMEI”. Visited 19. September 2011. <http://www.gsm-security.net/faq/imei-international-mobile-equipment-identity-gsm.shtml>

[13] Richards, Jonathan. ”Shops track customers via mobile phone”. 16. May 2008. The Times.

[14] Birkjær, Andreas. “IMEI-nummer”. 3. September 2006. Mobilsiden.dk

[15] Picture of app permissions. <http://www.androidtapp.com/android-wallpaper-apps-falsely-accused-of-spyware-and-stealing-sensitive-user-data-fud/comparison-of-android-app-permissions-of-popular-backgrounds-app-versus-jackeey-wallpaper-apps/>

[16] Android Developer. “TelephonyManager”. Visited 19. September 2011. <http://developer.android.com/reference/android/telephony/TelephonyManager.html>

[17] Android Developer. “Application Fundamentals”. Visited 19. September 2011. <http://developer.android.com/guide/topics/fundamentals.html>

[18] Kolobaric, Daniel. ”Guide to Android Application Permissions”. 26. May 2011.

[19] ABC news. “Can You Hear Me Now?”. 5. December 2006.

[20] Coughlin, Kevin. “Even if they’re off, cellphones allow FBI to listen in”. 13. December 2006.

[21] Mchangama, Jacob. “Telefonaflytning uden retskendelse”. 18. Marts 2009.

[22] PET. “History”. Visited 19. September 2011. <http://www.pet.dk/Organisation/Historie.aspx>

[23] PET. “Organisation”. Visited 19. September 2011. <http://www.pet.dk/Organisation.aspx>

[24] Castiglione, Aniello. Prisco, Roberto de. Santis, Alfredo de. “Do You Trust Your Phone?”. 2009.

[25] ChinaTechNews.com Editorial Team. “Chinese Mobile Phones Lacking IMEI Numbers Face Death In India”. 7. April 2009.

[26] Apple Support. “iPad: How to find the serial number, UDID, IMEI, ICCID, and Cellular Data Number”. 28. February 2011.

[27] Biggs, John. “10 Reasons To Buy A Tablet (And 5 Reasons Not To)”. Visited 19. September 2011.