# Abstract

# Introduction (Christian)

## Mobile usage today

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. [5]

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.

[1] http://www.bbc.co.uk/news/10569081
[2] http://source.android.com/source/licenses.html
[3] http://www.gartner.com/it/page.jsp?id=1764714
[4] http://googleblog.blogspot.com/2011/05/android-momentum-mobile-and-more-at.html
[5] http://googleblog.blogspot.com/2011/05/android-momentum-mobile-and-more-at.html

# Problem analysis

## Problem definition

# Statement of problem

# Theft of cellphones and IMEI (Nicolai)

## 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 Nckia. 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 day.

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 succesfully 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".

# Usage of IMEI

## Law of IMEI (Christian)

## Legal use of IMEI number

The IMEI number is used to prevent stolen mobile phones from accessing a network and being used to make phone calls. 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. [6]

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. [7]

Shopping centers in the UK are tracking their costumer’s every move. They track their costumer’s by monitoring the signal produced by the costumer’s cell phone. The phone is tracked by placing receivers around the shop the system then use a triangulation method by measuring the distance from the phone to three receivers.

The system does not identify the owner, but only the phone’s 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.

### 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

[6] http://www.gsm-security.net/faq/imei-international-mobile-equipment-identity-gsm.shtml
[7] http://www.gsm-security.net/faq/imei-international-mobile-equipment-identity-gsm.shtml

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. [8]

### What can apps use IMEI to?

When an application is launched it checks the device 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 devises that is allowed to run the application. This could be used to determine if the phone is fast enough to run the application. [9]

## Illegal use

### Control of the phone (Thais)

### Surveillance of phone traffic (Dag)

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[10] 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[11].

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 without a court order[12] 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 GB there is one camera for every 14 citizen which is a whole lot more than there is in Denmark.

### Copy of identity (Rasmus)

On the GSM network, an identity is based on two numbers: The IMEI number, which is bound 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 IMEI number are used to identify the phone, when it

[8] http://www.mobilsiden.dk/tips/imei-nummer,lid.1513/
[9] http://www.gsm-security.net/faq/imei-international-mobile-equipment-identity-gsm.shtml
[10] http://abcnews.go.com/blogs/headlines/2006/12/can_you_hear_me/
[11] http://seattletimes.nwsource.com/html/nationworld/2003474824_bugs130.html
[12] http://www.dr.dk/P1/Kanten/Udsendelser/2009/03/18091353.htm

connects to a signal transmitter. In Android it is very easy for an app to get both the IMEI and IMSI number. The app simply has to call the TelephonyManager[13] library, and then use the getDeviceId()[14] function to get the IMEI number, and the getSubscriberId()[15] function to get the IMSI number. 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 terrorist 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[16]. 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[17]. 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 unabeling 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 (Rasmus)

### Examples of IMEI abuse (Thais)

### Why allow apps to read IMEI?

## Conclusion (and followup on the statement of problem)

## Litterateur

[13] http://developer.android.com/reference/android/telephony/TelephonyManager.html
[14] http://developer.android.com/reference/android/telephony/TelephonyManager.html#getDeviceId()
[15] http://developer.android.com/reference/android/telephony/TelephonyManager.html#getSubscriberId()
[16] Do You Trust Your Phone - Aniello Castiglione, Roberto De Prisco, and Alfredo De Santis, Dipartimento di Informatica ed Applicazioni “R. M. Capocelli”, Universit`a di Salerno, Via Ponte don Melillo, I-84084 Fisciano (SA), Italy
[17] Do You Trust Your Phone - Aniello Castiglione, Roberto De Prisco, and Alfredo De Santis, Dipartimento di Informatica ed Applicazioni “R. M. Capocelli”, Universit`a di Salerno, Via Ponte don Melillo, I-84084 Fisciano (SA), Italy