Smartphones:

Information security risks, opportunities and recommendations for users

December 2010

enisa
European Network and Information Security Agency

About ENISA

ENISA is an agency of the European Union, established to contribute to a high level of network and information security within the EU by:

- giving expert advice on network and information security to national authorities and EU institutions;
- acting as a forum for sharing best practices;
- facilitating contacts between EU institutions, national authorities and businesses.

Together with EU institutions and national authorities, ENISA seeks to develop a culture of security for information networks across the EU. This report and other ENISA reports can be found on ENISA's website (http://enisa.europa.eu).

Contact details

Authors: Dr Giles Hogben (giles.hogben [at] enisa.europa.eu),

and Dr Marnix Dekker (marnix.dekker [at] enisa.europa.eu).

ENISA spokesperson: Ulf Bergstrom (ulf.bergstrom@enisa.europa.eu).

Legal notice

Notice must be taken that this publication represents the views and interpretations of the editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to ENISA Regulation (EC) No 460/2004. This publication does not necessarily represent the state-of-the-art in smartphone security and it may be updated from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

enisa
European Network and Information Security Agency

Executive summary

Eighty million smartphones were sold worldwide in the third quarter of 2010, accounting for 20% of the total of mobile phones sold (1). In the UK, Germany, France, Spain, and Italy the number of smartphone users increased to sixty million (2). Smartphones offer new opportunities in every sector of society (3) (4) – from mobile productivity to e-health, augmented reality and electronic payments.

Smartphones have a rich cocktail of features: an array of sensors, multiple radio and network interfaces, as well as gigabytes of storage and powerful processors. They are often within a meter of their owners 24 hours a day. In fact, smartphones have already realised many aspects of the vision of ambient intelligence which includes, for example, providing augmented reality applications, applications that adapt to and anticipate the user's physical environment using smart sensors – even providing smart health applications using biometric monitoring. Many of the security and privacy issues raised in the context of ambient intelligence apply to smartphones as well.

The objective of this report is to allow an informed assessment of the information security and privacy risks of using smartphones. Most importantly, we make practical recommendations on how to address these risks. The ultimate objective is to enable users, businesses and governments to take advantage of the opportunities offered by smartphones while minimising the information security risks to which they are exposed.

We assess and rank the most important information security risks and opportunities for smartphone users and give prioritised recommendations on how to address them. The report analyses 10 information security risks for smartphone users and 7 information security opportunities. It makes 20 recommendations to address the risks.

RISKS

- **R1 Data leakage:** a stolen or lost phone with unprotected memory allows an attacker to access the data on it.
- **R2 Improper decommissioning:** the phone is disposed of or transferred to another user without removing sensitive data, allowing an attacker to access the data on it.
- **R3 Unintentional data disclosure:** most apps have privacy settings but many users are unaware (or do not recall) that the data is being transmitted, let alone know of the existence of the settings to prevent this.

- **R4 Phishing:** an attacker collects user credentials (e.g. passwords, creditcard numbers) using fake apps or (sms,email) messages that seem genuine.
- **R5 Spyware:** the smartphone has spyware installed allowing an attacker to access or infer personal data. NB spyware includes any software requesting and abusing excessive privilege requests. It does not include targeted surveillance software (R7).
- **R6 Network spoofing attacks:** an attacker deploys a rogue network access point and users connect to it. The attacker subsequently intercepts the user communication to carry out further attacks such as phishing.
- **R7 Surveillance:** spying on an individual with a targeted user's smartphone.
- **R8 Diallerware:** an attacker steals money from the user by means of malware that makes hidden use of premium sms services or numbers.
- **R9 Financial malware:** malware specifically designed for stealing credit card numbers, online banking credentials or subverting online banking or ecommerce transactions.
- **R10 Network congestion:** network resource overload due to smartphone usage leading to network unavailability for the end-user.

OPPORTUNITIES

- **Sandboxing and capabilities:** most smartphones use sandboxes for apps and capability-based access control models.
- **Controlled software distribution:** gives providers *the opportunity* to have more control over app security by vetting apps submitted for security flaws and removing insecure apps.
- **Remote application removal:** functionality allowing removal of malware from devices after installation (NB caveats described in this section – e.g. the judgement about whether a particular app is malicious may not be clear-cut).
- **Backup and recovery:** most smartphones ship with convenient backup and recovery functions to address risks to data availability.
- **Extra authentication options:** smartphones can function as a smartcard reader, giving additional options for authentication and non-repudiation.
- **Extra encryption options:** several third-party applications are now offering encryption for smartphone voice calls, on top of the standard encryption provided by mobile network operators.
- **Diversity:** smartphones are diverse in terms of hardware and software, which makes it more difficult to attack a large group of users with one virus.

RECOMMENDATIONS

We provide a detailed set of measures which can be applied for each risk identified. The recommendations are structured according to the usage scenarios (consumer, employee, high official). In general, recommendations for consumers should be applied to employees and those for employees to high officials. Below is a summary of selected recommendations:

Consumers:

- **Automatic locking:** configure the smartphone in such a way that it locks automatically after some minutes.
- **Check reputation:** before installing or using new smartphone apps or services, check their reputation. Never install any software onto the device unless it is from a trusted source and you were expecting to receive it.
- **Scrutinize permission requests:** scrutinize permission requests when using or installing smartphone apps or services.
- **Reset and wipe:** before disposing of or recycling their phone, wipe all the data and settings from the smartphone.

Employees:

- **Decommissioning:** before being decommissioned or recycled, apply a thorough decommissioning procedure, including memory wipe processes.
- **App installation:** if any sensitive corporate data is handled or if the corporate network is accessible to the smartphone then define and enforce an app whitelist.
- **Confidentiality:** use memory encryption for the smartphone memory and removable media.

High officials:

- **No local data:** do not store sensitive data locally and only allow online access to sensitive data from a smartphone using a non-caching app.
- **Encryption software:** for highly confidential usage, use additional call and SMS encryption software for end-to-end confidentiality.
- **Periodic reload:** smartphones may be periodically wiped (using secure deletion) and reloaded with a specially prepared and tested disk image.

Table of contents

Target audience

The intended audience of this report includes

- IT officers (CIOs, CSOs, CTOs, etc) in business and public organisations to facilitate their evaluation and mitigation of the risks associated with adopting smartphones;
- Consumer safety bodies and consumers via consumer safety bodies) to enable them to minimise the risks of smartphone usage;
- European policymakers to aid them in deciding on research policy and measures required to mitigate risks.

Disclaimer

In this report, examples are given from a number of providers and products. These should be taken as examples only and there is no intention to single out a specific provider for criticism or praise. The examples provided are not necessarily those most representative or important, nor is the aim of this paper to conduct any kind of market survey or product evaluation.

Consulted experts

This paper was written with input from a group of experts from across government and business organizations. Their ideas and opinions were collected through surveys and reviews of intermediate drafts of this report. The experts consulted were:

Ajit Jaokar	Oxford University Next generation mobile applications Group
Alan Meeus	Microsoft (Windows Phone, Senior product manager)
Alberto Partida	European Central Bank, IT Security Expert
Aleksandras Spiridenkovas	Omnitel-TeliaSonera, Information Security Manager
Charles Brookson	GSMA, Security Group Chair
Erkki Kataja, Janne Uusilehto	Nokia
Eric Gauthier	France Telecom Orange
Frank Fransen	TNO, Information Security Expert
Friedger Müffke	OpenIntents
Dr Gabriele Lenzini	Interdisciplinary Centre for Reliability, Security and Trust, University of Luxembourg, Researcher
Felix Leder	Fraunhofer FKIE, Senior Researcher
Gintaras Bertasius	DnB Nord Bank, Information Security Officer
Gunnar Petterson	OWASP
James Moran	GSMA, Security Director
Pavel Balashov	Swedbank, Head of Identity Services Department
Jan van Bekkum	Shell, Chief Information Security Officer
Kari Kostiainen	Nokia Research Center
Liam Lynch, Hadass Harel	eBay
Leon Clarke, Nick Kralevich, Ben Laurie & others	Google Inc.
Matt Broda	Microsoft
Nader Henein, Daniel Jouan	Research in Motion
Eng. Peter Teufl	Secure Information Technology Center, Austria

Pieter Siekerman	The Saints, Lead iOS Developer
Piotr Kwiatkowsi	Inquso, Smartphone security expert
Rita Forsi	ISCOM, Italian Ministry of Economic Development, Communication Department, General Director
Rob Faber, Peter Hoogendoorn	Achmea, Security architect and Information Security Manager
Ronald Westerlaken	Fox-IT, Netherlands, Product Manager Mobile Security
Thom Schiltmans	Philips Healthcare, Sector IT Security Manager
Dr Ton van Gessel	Government and financial information security consultant
Viola Viederpass, Richard Roberts	Interpol

We would like to thank our colleague Laurent Beslay at the EDPS (European Data Protection Supervisor) for his input, and our colleagues at ENISA for their input and review.

Glossary and abbreviations

App	Software application for smartphones (aka application)
App-store	Software distribution channel for third-party software (aka marketplace)
Botnet	A collection of (malicious) software agents, or robots, which run without the user being aware of them.
Classified information	Information that is labelled in a government or business classification system for its degree of confidentiality; a typical classification system consists of several levels: *unclassified*, *restricted*, *confidential*, *secret* or *top secret*. Classified information usually means 'restricted' or higher.
GPS (Global Positioning System)	A satellite-based system, created and maintained by the USA, for providing location and time information
GSM	The most popular standard for mobile telephony systems in the world.
Unlocking	A process which removes smartphone restrictions; the restrictions usually concern changes to the smartphone OS or the installation of third-party software. Unlocking an iPhone is usually called *jail-breaking*, and unlocking an Android phone is usually called *rooting*.
LAN	A computer network that connects computers and devices in a limited geographical area such as a home, school or office building
LTE	Long Term Evolution – 3GPP standard supporting improved spectral efficiency and lower latency compared to previous standards. (aka 4G)
NFC (near field communication)	A short-range high-frequency wireless communication technology based on RFID, which enables the exchange of data between devices over a distance of about 10 centimetres
PAN (personal area network)	A network for interconnecting devices centred on an individual person's workspace (e.g. over Bluetooth)
Smartphone	Currently, most smartphones include the following characteristics : • small form factor: pocket-sized; • powerful processor (like common 1GHz processor models) and gigabytes of storage; • app-store (or applications marketplace); • multiple network connections for WAN, LAN, and PAN networking, over multiple radio interfaces like WiFi, GSM, UMTS, Bluetooth, etc. • a set of sensors including microphone, camera, GPS, accelerometer, magnetic field sensor, and (often internal) temperature sensor; • rich user interface, capable of rendering full web pages in a browser.
TLS (aka SSL)	A mechanism to protect Internet Protocol traffic from eavesdropping and tampering.
UMTS (aka 3G)	Universal Mobile Telecommunications System, Mobile telecommunications technology specified by 3GPP, part of the global ITU IMT-2000 standard.
Wardriving	The process of traveling around collecting information on wireless access point signals that can be used to get network access.
WAN	A computer network covering a broad area across regional boundaries.

1. Introduction

Smartphones are now an essential tool in all sections of European society, from top government officials to businesses and consumers (4). In the UK, Germany, France, Spain, and Italy alone, the number of smartphone users has increased to 61 million (2). As an illustration of the monetary value flowing through smartphones, eBay expects 1.3 to 1.5 billion Euro in transactions to be conducted through its iPhone app in 2010 (5).

Smartphones are famous for their versatility – in a single day a smartphone may be a contactless wallet (6), a barcode reader, a satellite navigation system, an email or social network client, a WiFi hotspot, and be used to make a phone call. Given the growing importance of smartphones, we believe it is important to assess the privacy and security risks of these devices.

In this report we give an overview of the key information security risks and opportunities for smartphone users (in chapters 2 and 3). We also provide practical advice to address the risks (in chapter 4) and we conclude with some recommendations for research and industry (in chapter 5).

We stress that the risks should be balanced against the potential benefits of smartphones [1]. A description of the many potential benefits in terms of, for example, cost-savings, increased efficiency and a better quality of life is outside the scope of this report. To give just one example however, smartphones are being used as smart-health sensors, allowing heart patients to stay at home safely, while having their heart issues controlled and monitored by medical staff. In this way smartphones increase a patient's quality of life and, at the same time, save healthcare costs (7).

[1] *As with the risks, the criteria for such a balance depend on the usage scenario – more critical usage scenarios should give more priority to security. This paper is not intended to replace a project specific risk assessment.*

2. Information security risks

In this chapter we give an overview of the most important information security risks of using smartphones. We start by explaining our approach and the scope of our analysis.

2.1 Usage scenarios

Risks vary depending on how the smartphone is used. We have therefore defined three different usage scenarios and described risks and recommendations for each scenario.

Usage scenario	**Description**
Consumer (C)	The phone is an integral part of a person's daily life – e.g. private phone-calls, social networking, messaging, navigation, gaming, online banking, on-the-go entertainment, location based services, Internet browsing, micro-blogging, email, photography, video recording, e-health, etc.
Employee (E)	The smartphone is used by an employee in a business or government organization. It is used for business phone calls, Internet browsing, corporate email, expense management, customer relationship management, travel assistance, contact management and business social networking, video conferencing, scheduling tasks, and reading documents. In some cases workflow applications are run on the smartphone, e.g. to fill in forms as part of an employee task. Usage in this scenario is subject to IT (security) policies, set by the employer's IT officer. The smartphone is used for personal use in a limited way.
High official (H)	The smartphone is used by a high or top-level official in a business or government organisation, or by his or her close aide. The smartphone is used as in usage scenario E but in addition it is used for dealing with sensitive information and/or tasks. Usage in this scenario is subject to security policies and the functionality of the smartphone may be restricted or customized, for example by adding cryptographic modules for protecting call-confidentiality.

It should be noted that individual smartphones and smartphone users frequently *cross-over* from one usage scenario to another. This in itself has important implications for the management of security risk. For example, a business smartphone with sensitive client data may be taken outside Europe on holiday by an employee (a subject for further investigation would be whether or not this represents cross-border data flow). A smartphone may be used for personal social networking during weekends (scenario C) and for handling sensitive email on working days (scenario E). We have included some recommendations to address this specific issue in our recommendations. In general, recommendations for consumers should be applied to employees and those for employees to high officials.

individual smartphones and smartphone users frequently cross-over from one usage scenario to another. This in itself has important implications for the management of security risk

2.2 Approach

In information security, *risk* is the product of the likelihood and the impact of a *threat* against the information assets of an organization or an individual (8). Threats exploit one or more *vulnerabilities*. The *likelihood* of a threat is determined by the number of underlying vulnerabilities, the relative ease with which they can be exploited and the attractiveness for an attacker. For each risk covered in this chapter we refer the reader to the underlying vulnerabilities.

The *impact* of a threat can be determined by the value of the assets affected by the threat. Throughout this report we use the following list of possible affected assets:

- Personal data
- Corporate intellectual property
- Classified information [see Glossary and abbreviations]
- Financial assets
- Device and service availability and functionality
- Personal and political reputation

The risks were determined in consultation with the expert group. The experts were asked to indicate the likelihood (from very low to very high) and impact (from very low to very high) of each risk in each of the three usage scenarios.

The average value of each risk is reported in this chapter. The scheme is summarized in the diagram below.

Likelihood **Impact**	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very low (1)	1	2	3	4	5
Low (2)	2	4	6	8	10
Medium (3)	3	6	9	12	15
High (4)	4	8	12	16	20
Very high (5)	5	10	15	0	25

High risks are coloured red, medium risks are coloured yellow, and low risks are coloured white.

Caveat: the objective of the risk assessment is to give readers an understanding of the most significant risks, to enable them to minimise their exposure. Therefore we do not put any absolute value on the likelihood and impact of threats – e.g. a 'High' likelihood is not intended to be an estimate of the number of times a threat will occur in a year. We also do not offer a comparative risk assessment of the use of smartphones versus other technologies fulfilling the same functionalities.

Individuals and organizations are encouraged to make their own risk assessments and weigh the risks against the potential benefits in their own specific cases.

Furthermore, it should be noted that vulnerabilities and risks vary greatly across different smartphone models and the impact and likelihood of a threat may vary greatly across individuals and organizations, even within the same usage scenario. For example, for certain employees in certain organizations, a confidentiality breach affecting a smartphone address book may have a big impact (e.g. by revealing customer relations, notes on customers, secret pin numbers, or passwords), while for others the impact may be small (revealing only the phone numbers of family and friends). Individuals and organizations are encouraged to carry out their own risk assessments and weigh the risks against the potential benefits in their own specific cases. This paper is not meant to replace a project-specific organisational risk assessment.

2.3 Scope

We focus on the risks for the user or his or her organisation. At the end of this chapter we briefly discuss risks to other parties. We only cover threats which are typical for smartphones or are increased by smartphones. For example, a brute-force attack on a password is not included, because the risk of this attack is not typical for smartphones nor is it increased by smartphones. The risk of phishing, on the other hand, *is* included because there are aspects of smartphone platforms which increase the risk of phishing.

This paper covers the 'top ten' risks to smartphone users resulting from threats directly affecting the device or platform. However, as part of a project-specific organisational risk assessment, the following areas of risk should also be covered:

- Risks from the use of remote or cloud backup services (readers may refer to the ENISA paper Cloud Computing: Benefits, Risks and Recommendations for further information on this aspect (9)). It should be noted in particular, that:
  - Many smartphone platforms make considerable use of remote and/or cloud-based services.
  - These services are often implemented without the availability of alternative services.
  - Data stored in cloud services is processed by the cloud service provider and data confidentiality, integrity and availability therefore depend on the level of security offered by the cloud provider.
- Attacks on online services used by smartphones, such as injection attacks, etc.
- Attacks on authentication systems used by smartphones, such as password guessing.

- Attacks on or via online services used by smartphones such as cross-site scripting.
- Attacks on web browsers, e.g. CSS history attack, browser fingerprinting, etc.
- Risks which exclusively affect a single smartphone model or a single organization.

Note that we do not cover risks related to national security (e.g. the risk of not being able to eavesdrop on mobile phone communication, as claimed in the case of Saudi Arabia's temporary ban on Blackberries (10)).

2.4 Overview of risks

Risks are ordered according to an average rating across the different usage scenarios. Recommendations can be found in Chapter 4.

R1. Data leakage resulting from device loss or theft

Threat description	The smartphone is stolen or lost and its memory or removable media are unprotected, allowing an attacker access to the data stored on it.		
Rating	**Likelihood**	**Impact**	**Risk**
Consumer (C)	High	Medium	Medium
Employee (E)	Medium	High	High
High official (H)	Medium	Very high	High
Vulnerabilities	[6.7 Lack of user awareness][6.4 Encryption weaknesses]		
Assets	All		

Smartphones, being both valuable and pocket-sized, are likely to be stolen or lost. In a recent UK government survey, 2% reported their mobile phone was stolen last year (11). If data on the smartphone memory or its removable media is not sufficiently protected (by encryption) then an attacker can access that data.

Smartphones are often the user's primary repository of personal data because they are carried around all the time and are always available.

Smartphones often contain valuable information such as credit card data, bank account numbers, passwords, contact data, and so on. They are often the user's primary repository of personal data because they are carried around all the time and are always available. Users sometimes protect sensitive information by storing it in an obfuscated form (see example below). Business phones often contain corporate emails and documents and may contain sensitive data. In the case of scenario H the impact is very high, because the smartphone could contain classified information, e.g. classified emails.

The likelihood is rated lower in scenarios E and H because the users are more aware of the risks of theft or loss and because protective measures, such as memory encryption and auto-locking the device, are enforced more often by an IT officer.

Note that even when encryption is implemented, weaknesses may exist in the implementation of encryption in smartphones (12) (13). This is not to suggest that encryption is not recommended, but to encourage caution in selecting the solution used.

Example: 'When Buck looked at my colleague's phone, he found two 4-digit numbers stored in his address book under the names 'M' and 'V'. A search through his text messages revealed a few from [service provider] informing him that a new credit card, ending in a specific number, had just been mailed to him. Buck guessed that 'M' and 'V' were PIN codes for the Virgin credit card and a Mastercard - and he proved to be correct on both counts.' (14)

R2. Unintentional disclosure of data

Threat description	The smartphone user unintentionally discloses data on the smartphone.		
Rating	**Likelihood**	**Impact**	**Risk**
Consumer (C)	Very high	High	High
Employee (E)	High	Medium	High
High official (H)	High	Very High	High
Vulnerabilities	[6.3 User permissions fatigue] [6.2 Covert channels/weak sandboxing] [6.6 No privacy protection best practices][6.7 Lack of user awareness]		
Assets	[Personal data] [Personal and political reputation]		

Most apps have privacy settings for controlling how and when location data is transmitted, but many users are unaware (or do not recall) that the data is being transmitted, let alone know of the existence of the privacy setting to prevent this.

Users are not always aware of all the functionality of smartphone apps. Even if they have given explicit consent, users may be unaware that an app collects and publishes personal data[2]. Location data, for example, is often used in social networks – in messages or uploaded photo metadata, in augmented reality apps, micro-blogging posts, etc. Most apps have privacy settings for controlling how and when location data is transmitted, but many users are unaware (or do not recall) that the data is being transmitted, let alone know of the existence of the privacy setting to prevent this. Unintentional disclosure of location data may help attackers to track and

[2] *It goes without saying that, without informed consent, this kind of analysis can violate (if it uniquely identifies the user) the right to privacy of the individual concerned, as defined in European data protection law..*

trace users and so allow, for example, stalking, robbery or the hijacking of trucks containing valuable goods.

A fundamental underlying vulnerability is the difficulty of collecting meaningful consent for the processing of all the personal data available on a smartphone. Certain types of data collection naturally lend themselves to integration with user consent, without having to assume the persistence of a decision. For example, file upload involves the user in selecting the file and thus giving consent (to that file being uploaded) as an integral part of the process. Other types of data are more problematic and location data is a good example, as it is not feasible for the user to have to consent every time a new location is disclosed.

Example: *Location data is often included in image files. Users, by giving an app access to the image files, may be unintentionally disclosing their whereabouts. An interesting demonstration of the extent of information disclosed is provided by the web site icanstalku.com which (for awareness raising purposes) collates data disclosed via GPS data embedded in images.*

R3. Attacks on decommissioned smartphones

Threat description	The smartphone is decommissioned improperly allowing an attacker access to the data on the device.		
Rating	**Likelihood**	**Impact**	**Risk**
Consumer (C)	Medium	Medium	Medium
Employee (E)	High	High	High
High official (H)	Medium	Very high	High
Vulnerabilities	[6.7 Lack of user awareness][6.4 Encryption weaknesses]		
Assets	All		

Due to a growing awareness of identity theft many people and organizations now destroy or wipe computer hard drives before decommissioning. However, the same thing is not yet happening with smartphones. At the same time, more and more devices are being recycled. According to market analysts ABI Research, by 2012 over 100 million mobile phones (15) will be recycled for reuse each year. As previously mentioned, smartphones contain large amounts of sensitive information which may be valuable to an attacker. They are an increasingly attractive target for 'smartphone dumpster divers'.

According to market analysts, by 2012 over 100 million mobile phones will be recycled for reuse each year. As previously mentioned, smartphones contain large amounts of sensitive information which may be valuable to an attacker. They are an increasingly attractive target for 'smartphone dumpster divers'.

Example: *In a recent study, mobile phones were bought second-hand on eBay and, out of the 26 business smartphones, 4 contained information from which the owner could be identified while 7 contained enough data to identify the owner's employer* (14). *The research team managed to trace one smartphone to a senior sales director of a corporation, recovering call history, address book entries, diary, emails, etc*.

R4. Phishing attacks

Threat description	An attacker collects user credentials (such as passwords and credit card numbers) by means of fake apps or (SMS, email) messages that seem genuine.		
Rating	**Likelihood**	**Impact**	**Risk**
Consumer (C)	Medium	High	Medium
Employee (E)	Medium	High	Medium
High official (H)	Medium	Very high	High
Vulnerabilities	[6.5 Weak app distributor authentication mechanisms][6.7 Lack of user awareness]		
Assets	All		

Phishing attacks are a well-known threat for users of traditional PCs. Phishing attacks are actually platform independent, because the attacker does not need to attack the user's device in any way. However, there are a number of reasons why the risk of phishing is important for smartphone users:

- Smartphones have a smaller screen, which means that attackers can more easily disguise trust cues that users rely on to decide on submitting credentials; e.g. cues that show whether the website uses SSL.

attackers can more easily disguise trust cues that users rely on

- App-stores provide a new way of phishing by allowing attackers to place fake apps in the app-store, disguising them as legitimate apps (such as in the 09Droid case (16))
- Smartphones provide additional channels that can be used for phishing, e.g. SMS (SMiShing (17)). Users may be less cautious about SMS phishing messages.

app-stores provide a new way of phishing by allowing attackers to place fake apps in the app-store, disguising them as legitimate

- Smartphones are a new type of device and users may not be aware of the fact that phishing is a risk on smartphones as well.

R5. Spyware attacks

Threat description	The smartphone has spyware installed, allowing an attacker to access or infer personal data. Spyware covers untargeted collection of personal information as opposed to targeted surveillance.		
Rating	**Likelihood**	**Impact**	**Risk**
Consumer (C)	High	Medium	High
Employee (E)	Medium	High	Medium
High official (H)	Medium	Medium	Medium

Vulnerabilities	[6.1 Vulnerabilities leading to malware installation][Ability to unlock phones][Reputation vulnerabilities][6.2 Covert channels/weak sandboxing]
Assets	[Personal data][Personal and political reputation]

Spyware is malicious software that covertly collects information about users and their activities to use it for marketing purposes, such as profiling or targeted advertisements. Such spyware is often apparently bona fide software, installed with the user's consent, which requests and abuses privileges over and above those required for the stated purpose of the app.

The amount of personal data, sensitive documents and credentials stored and processed by smartphones makes them an interesting target for spyware. Furthermore, smartphones provide covert channels through which data may be disclosed (by an application) to an attacker. Even when it seems there is a legitimate need for an app to send data over a particular channel, the permission model of smartphones is not always granular enough to protect users against abuse. For example, a weather app may ask permission to use location data and to connect to the Internet, which seems legitimate (to get fresh location-based weather data). The app may however abuse this permission by sending location-data to advertisement servers for marketing purposes.

Example: *A recent study published in OSDI'10 TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones* (18) *found that of 30 apps studied, 2 sent the phone number, IMSI, and ICC-ID to a remote server, 7 sent the device ID to content servers and 15 sent location data to advertisement servers. In no case was the user's consent obtained either explicitly or implicitly.*

Smartphones provide covert channels through which data may be disclosed (by an application) to an attacker. Even when it seems there is a legitimate need for an app to send data over a particular channel, the permission model of smartphones is not always granular enough to protect users against abuse.

Example: *SMobile describes* (19) *a study of 48,694 applications in the Android market, which found that one in every five applications requests permissions to access private or sensitive information that an attacker could use for malicious purposes. One out of every twenty applications has the ability to place a call to any number without interaction with or authority from the user.*

Furthermore, data access by apps is sometimes exempt from explicit user permissions. For example, in iOS, the address book is accessible to all apps. No special status is given to the user's own contact details in the address book, meaning that, apart from the large amounts of personal data this exposes, the user's own phone number is also accessible, which can be used for unsolicited marketing. Another important vulnerability is the fact that on the iPhone the keyboard cache is accessible to all apps; although this does not include sensitive information such as passwords, it does contain a lot of private information.

Example: *The [iPhone] keyboard cache contains all the words ever typed on the keyboard, except the ones entered in password fields. This is supposed to help auto completion but effectively acts as a key-logger, storing potentially private and confidential names and numbers* (20)*.*

It is possible in some cases to extract high-level events from collections of low-level (sensor) events. For example, an analysis of magnetic field and acceleration data over a period of days yields information about the activities and movements of the user. If the user works in an office near a magnetic field and lives somewhere without one (which is not unlikely), the magnetic field sensor data could be used (in combination with other data) to deduce his or her location. Bayesian analysis of sensor data sets could be used to determine activities and even to classify individuals for marketing purposes. The combination of sensors on smartphones increases the possible channels through which data can be collected and increases the chance that privacy-sensitive information can be inferred.

Example: *The app Jigsaw* (21) *is able to recognise user activities based on an analysis of microphone, GPS and accelerometer for patterns characteristic of routine activities. For example, the jolts produced when the user is walking depend on whether the phone is in a trouser or jacket pocket, so the software can recognise both patterns. It is designed to minimise the drain on the phone's battery.*

Example: *The app Sensor Logger* (22) *records changes in the phone's accelerometer and magnetic field sensors over a period of 50 seconds and attempts to determine the activity (walking, standing, sitting) in which the user is engaged. (This is not in itself an attack but demonstrates the possibilities.)*

R6. Network Spoofing Attacks

Threat description	An attacker deploys a rogue network access point (WiFi or GSM) and users connect to it. The attacker subsequently intercepts (or tampers with) the user communication to carry out further attacks such as phishing.		
Rating	**Likelihood**	**Impact**	**Risk**
Consumer (C)	Medium	Medium	Medium
Employee (E)	Medium	High	Medium
High official (H)	Medium	High	High
Vulnerabilities	[6.7 Lack of user awareness]		
Assets	All		

Rogue WiFi hotspots and Bluetooth devices can be used to intercept and tamper with the network communication to the smartphone.

Rogue WiFi hotspots and Bluetooth devices can be used to intercept and tamper with the network communication to the smartphone. Rogue Internet gateway names may be configured on the smartphone by a malicious SMS configuration message. In this attack, a spoofed service configuration SMS is used to change the default access point used by the phone (23). A more complicated spoofing attack relies on mounting a rogue GSM base station. The hardware required to set up such a base station has become relatively inexpensive. This attack is not feasible on 3G networks because of network integrity keys. A rogue WiFi hotspot or other spoofed network nodes can be used as a means to carry out several other attacks, e.g. phishing, SSL downgrade attacks, eavesdropping, etc (making it less likely using 3G networks). [3]

Security indicators (such as a 'trusted SSL connection' indicator) are harder to find on smartphones or are missing.

Theoretically speaking, such attacks should be detectable by the user. However, in practice most users do not pay attention to trust cues such as SSL certificates or whether a site uses SSL[4]. For smartphone users the risk is even higher because security indicators (such as a 'trusted SSL connection' indicator) are harder to find or missing on smartphones.

Example: *At the Blackhat 2009 conference a presenter used a rogue WiFi hotspot to mount an SSL downgrade attack* (24) *and was thus was able to capture 20 email passwords from security professionals.*

R7. Surveillance attacks

Threat description	An attacker keeps a specific user under surveillance through the target user's smartphone.		
Rating	**Likelihood**	**Impact**	**Risk**
Consumer (C)	Low	High	Medium
Employee (E)	Low	High	Medium
High official (H)	Medium	Very high	High
Vulnerabilities	[6.1 Vulnerabilities leading to malware installation]		

[3] *Even in the case of GSM an encryption-on indicator can indicate a fake base station.*

[4] *This is well-demonstrated by the case of New Zealand's BankDirect which accidentally allowed a certificate to expire. The mistake was fixed within 12 hours, during which time about 300 customers were presented with a security alert when visiting the bank's website. Server logs show that all but one of 300 users dismissed the warning (65).*

Assets	[Personal data] [Classified information]

Smartphones can be used to keep a targeted individual under surveillance[5]. Smartphones contain multiple sensors such as a microphone, camera, accelerometer and GPS. This, combined with the possibility of installing third-party software and the fact that a smartphone is closely associated with an individual, makes it a useful spying tool.

Given short-term physical and logical access to a device, it is possible to install comprehensive spying tools on it (25). Sometimes the user can be tricked into helping the attacker by installing malicious apps (see example below). There are also already several examples of legitimate software (26), whose express purpose is to allow an attacker to keep the mobile user under surveillance. Furthermore, even tools that are not designed for spyware may be configured covertly to allow for tracking (27).

The GPS sensor deserves particular attention in this regard since it is a source of highly sensitive personal information – e.g. information about when someone is not at home can be useful to burglars. As mentioned above, even a combination of seemingly innocuous sensor data (e.g. magnetic field history) could be used to deduce sensitive information about an individual and their environment.

Smartphones contain multiple sensors such as a microphone, camera, accelerometer and GPS. This, combined with the possibility of installing third-party software and the fact that a smartphone is closely associated with an individual, makes it a useful spying tool.

Example: *The app Tap Snake, ostensibly a simple snake game, captures GPS location data and uploads it to a remote server* (28).

Example: *On the iPhone, apps obtain read and write access to the address book by default* (20), *which allows an attacker (through malware) to add a rogue*

[5] *This attack should not be confused with illegitimate untargeted mass-collection of data as described in [R5. Spyware attacks].*

email address ('email@ofattacker.com') to existing email addresses and receive email correspondence.

R8. Diallerware attacks

Threat description	An attacker steals money from the user by means of malware that makes hidden use of premium SMS services or numbers.		
Rating	**Likelihood**	**Impact**	**Risk**
Consumer (C)	High	High	High
Employee (E)	Medium	Medium	Medium
High official (H)	Low	Low	Low
Vulnerabilities	[6.1 Vulnerabilities leading to malware installation] [Reputation vulnerabilities] [6.3 User permissions fatigue][6.2 Covert channels/weak sandboxing][6.7 Lack of user awareness]		
Assets	[Financial assets]		

Certain smartphone API calls cost the user money, e.g. SMS (including micropayments), phone calls, and data over metered GSM/UMTS. If an attacker can install an app on the user's smartphone, which is able to make such API calls covertly or trick the user into giving consent to their use, they can steal money from the smartphone user. The risk of this attack for consumers is judged as high because they are usually on a more limited budget and are more likely to download rogue apps.

An attacker steals money from the user by means of malware that makes hidden use of premium SMS services or numbers.

Example: *Scammers are distributing corrupted versions of shareware games for smartphones which make calls to premium-rate numbers across the globe, racking up expensive bills without the phone owner's knowledge* (29) .

R9. Financial malware attacks

Threat description	The smartphone is infected with malware specifically designed for stealing credit card numbers, online banking credentials or subverting online banking or ecommerce transactions.		
Rating	**Likelihood**	**Impact**	**Risk**
Consumer (C)	Medium	High	High
Employee (E)	Low	High	Medium
High official (H)	Low	Low	Low
Vulnerabilities	[6.1 Vulnerabilities leading to malware installation]		
Assets	[Financial assets]		

Financial malware is software specifically designed to steal credentials or perform man-in-the-middle attacks on financial applications or web services. Like PCs, smartphones are also vulnerable to banking malware.

Financial malware may be a simple key-logger collecting credit card numbers, or it may be more sophisticated and intercept SMS authentication codes to attack online banking applications.

Financial malware may be a key-logger collecting credit card numbers, or it may be more sophisticated and intercept SMS authentication codes to attack online banking applications. Another strategy is for an attacker to submit an app to an app-store, impersonating a real banking app. If users download and use the app, the attacker can mount a man-in-the-middle attack on banking transactions.

Smartphones have been relatively safeguarded from malware (compared to PCs). This may be due to the efforts from platform vendors (see opportunities

[3.1 Sandboxing and capabilities], [3.2 Controlled software distribution] and [3.3 Remote application removal]) or simply because traditional PCs still provide an easier and more interesting target for attackers. Nonetheless, malware for smartphones is a serious risk (30).

Example: *ZeuS Mitmo (Man in the Mobile)* (31) *is an example of an attack that exploits the combined features unique to the smartphone. ZeuS Mitmo combines the SMS and Web attack vectors to target online banks via the smartphone.*

R10. Network congestion

Threat description	Network resource overload due to smartphone usage leading to network unavailability for the end-user.		
Rating	**Likelihood**	**Impact**	**Risk**
Consumer (C)	Low	Low	Low
Employee (E)	Low	Low	Low
High official (H)	Low	Low	Low
Vulnerabilities	[Inadequate resource provisioning]		
Assets	[Device and service availability and functionality]		

The uptake of smartphones and mobile Internet increases the risk of network congestion. Network congestion can occur in two ways:

- Signalling overload: always-on smartphone apps are constantly polling the network for updated information. For every bit of data sent, a large number of signalling messages are sent (e.g. keep-alive messages). A typical smartphone generates 8 times more signalling traffic than a laptop with a USB dongle (32) .
- Data capacity overload: Cisco estimates that mobile data traffic will double every year through 2014, increasing 39 times between 2009 and 2014 (33). Mobile data traffic will grow at a compound annual growth rate

of 108 percent between 2009 and 2014, reaching 3.6 million terabytes per month by 2014.

To address signalling overload, there are mechanisms that change how often a smartphone switches between idle and active mode, such as the 3GPP Fast Dormancy mechanism (34).

In terms of data capacity (as opposed to signalling load), solutions such as LTE and WiMAX promise improvements in spectral efficiency, the amount of data that can be transmitted over the air using the same amount of allocated spectrum (35). At the same time, however, it has been argued that average data demand per network user will outstrip data capacity by 2013 and there are concerns that ‘wireless technology is approaching theoretical limits of spectral efficiency’ (36).

- ***Signalling overload: always-on smartphone apps are constantly polling the network for updated information. A typical smartphone generates 8 times more signalling traffic than a laptop with a USB dongle.***
- ***Data capacity overload: Cisco estimates that mobile data traffic will double every year through 2014, increasing 39 times between 2009 and 2014.***

In the longer term in Europe, the risk is reduced by the fact that spectrum is being released by the cessation of analogue TV and 2G services, which is likely to be made available for such applications. However, it is worth noting that while on average, this threat may not be very serious, critical events such as natural disasters which cause a sudden peak in demand (for example the 2010 Eyjafjallajökull volcano eruption) may be create conditions which put data networks used by smartphones under severe strain.

Example*: A widely publicized case was AT&T’s first introduction of the iPhone, which caused massive disruption of their data network* (37)*. This seems to be a problem in many EU countries as well. The Italian Telecommunications Authority recently warned of ‘network collapse’ due to smartphone and 3G card usage* (38).

Example: *There was also a complete loss of data connectivity at Microsoft's annual company meeting at Safeco Field in Seattle when tens of thousands of highly connected employees gathered together in a single place.*

Measures should (and are already being) implemented to ensure the resilience of data services to cope with the increasing demand from smartphones. Governments and operators should continue to work together to explore available options, such as quality of service (QoS) provisions for emergency service levels of mobile data. For further reference, see the ENISA report *Gaps in standardisation related to resilience of communication networks* (39).

2.5 Risks to other parties

All the risks covered previously are risks to the end-user of the smartphone (or his friends, family, colleagues or employer). In this paragraph we briefly discuss the risks for parties (people, organizations or services) other than the user.

R11. Distributed malware attack

Smartphones could be used to launch distributed attacks, just as traditional PCs are now used as parts of larger botnets. Although currently smartphones are not being targeted for such attacks, this may change as mobile devices are becoming more popular and more connected and the complexity and the number of vulnerabilities in these platforms is increasing. Smartphone botnets could be used for familiar crimes such as spam, click fraud and DDoS. Since smartphones interface with cellular networks, they could also be used for new distributed attack scenarios; e.g. SMS spam and DDoS on telephony networks. Such attacks could be used to support wider attacks on, for example, other infrastructure (40). Mobile phone coverage is becoming increasingly vital, especially in the event of an emergency, so smartphones open up new possibilities for DDoS attacks with potentially serious impacts.

Mobile phone coverage is becoming an increasingly critical service, especially in the event of an emergency, so smartphones open up new possibilities for DDoS attacks with potentially serious impacts.

Example: *The DoCoMo i-mode virus* (41) (42) *had access to call interfaces (tel: tags, which were available to malicious emails at the time of the cited article) and caused the user's device to dial emergency numbers (112 in Japan). Since the number of vulnerable devices at the time was small, this is unlikely to have had a significant impact but, in today's environment, such an attack could have flooded emergency numbers.*

R12. Collection of environmental data

Smartphones can be used to collect data in the physical vicinity of the phone. For example, they can be used for wardriving (see glossary) or the logging of MAC addresses on WiFi networks. Smartphones are also powerful spying tools, and can be conveniently used to collect confidential information in restricted areas, record confidential conversations, and so on.

3. Information security opportunities

From an information security perspective, smartphones have certain advantages over traditional PCs and mobile handsets. In this chapter we give an overview of the main information security opportunities for smartphone users . Note that any concrete security benefit provided depends heavily in all cases on the extent to which the opportunities are exploited in practice.

We have ordered the opportunities taking into account the rating from the experts consulted when writing this report. The experts were asked to rate on a scale ranging from no opportunity, through minor and medium opportunities, to major opportunity.

3.1 Sandboxing and capabilities

Description	Most smartphones use sandboxes for apps and capability-based access control models.
Rating	Major

Some smartphone vendors use sandboxes for third-party software. Sandboxing is a security mechanism for separating running applications by default. This is an opportunity from a security point of view because, if correctly implemented, an application in a sandbox cannot access or manipulate the data or functions of other applications for malicious purposes.

Both these features reduce the possibilities for malware because rogue applications are not able to access third-party application data or functionality unless explicitly granted permission by the application developer.

Moreover smartphone operating systems are often based on a capability-based access control model. In this model, individual processes are granted separate privileges (called capabilities) which are limited by default, following the principle of least privilege. In Symbian, for example, processes need to have special capabilities to access certain API calls on the device and, for some API calls, this requires the software to undergo a test and certification programme (43).

Both these features reduce the possibilities for malware because rogue applications are not able to access third-party application data or functionality unless explicitly granted permission by the application developer.

Example: *The Symbian security model specification* (44) *states: 'In Symbian OS v9 there is a more fine-grained security model which allows privileged access to be granted based on 'capabilities'. These capabilities are based on clearly defined groupings of what each API is designed to do. For example, if an API is associated with reading user data, it will require the capability "ReadUserData".*

Caveat: clearly, the effectiveness of sandbox implementations varies across different smartphone OSs and with it the effectiveness to protect against malware. Furthermore, although the granting of permissions must be done explicitly in a capability-based model, developers may still grant excessive privileges. Secondly, such measures are perceived as an obstacle by some developers and the ease with which developers can make apps for a smartphone is an important success-factor for a smartphone vendor.

3.2 Controlled software distribution

Description	Widespread use of controlled software distribution gives providers *the opportunity* to have more control over app security by vetting apps submitted for security flaws and removing insecure apps.
Rating	Medium

An information security opportunity with respect to traditional PCs is offered by the 'walled garden' approach many smartphone vendors take to third-party software; by default, users can only add applications from a centrally controlled distribution channel. On many smartphone platforms, it is unusual for users to install software from other sources and this sometimes requires unlocking (sometimes known as 'jail-breaking' or 'rooting') the smartphone. For example, statistics show that less than 10% of iPhone users unlock their device (45) to allow installation of software from other sources.

On most traditional PCs, by contrast, it is easy for users to install software from a variety of sources. This allows for so-called 'drive-by download' attacks, which are a common way for attackers to infect PCs. This means that app-store owners *have the opportunity* to perform a security review of apps before admitting them to the app-store and to remove apps from circulation which are subsequently shown to have security flaws.

App-store owners have the opportunity to perform a security review of apps before admitting them to the app-store and to remove apps from circulation which are subsequently shown to have security flaws.

Compared to other software distribution models *and depending on the review process implemented*, the walled-garden approach makes it more difficult for cyber attackers to spread malware because:

- the attacker has to pass the review process to have his or her malware admitted to the marketplace;

- importantly, even if an attacker manages to get malware onto the marketplace, moderators can intervene at a later time, by removing the application from the market and thus limiting the number of affected users;
- controlled distribution limits the vectors or channels which can install malware on the device.

> ***Even if an attacker manages to get malware onto the marketplace, moderators can intervene at a later time, by removing the application from the market and thus limiting the number of affected users;***

The approach mirrors many Linux software distribution models in which users can select additional software (a package) by selecting it from a controlled repository. The main difference with Linux distributions is that the review is not performed by a community of experts and that it is often not a very public and transparent process.

Example: *Apple's App Store review guidelines* (46)*, state that: 'Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used. Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected.'*

Caveat: this only applies where the app-store implements effective security controls. Questions have been raised about whether the app-store owner can be an independent and expert judge as to whether an app should be admitted to or removed from the app-store (*Quis custodiet ipsos custodies*). If not properly implemented, this may actually be detrimental to security by fostering a misplaced sense of trust in app security. Finally, it is worth noting that if even 1% of users unlock their devices, this still means that an average sized SME using these devices is likely to have several users with unlocked devices.

3.3 Remote application removal

Description	Some smartphone platforms have a built-in remote application removal function which allows the removal of malware from devices after installation.
Rating	Medium

In order to mitigate risks of malware, some smartphone OSs have built-in functions that allow the remote removal of applications from smartphones. This functionality is also sometimes referred to as a 'remote kill-switch'. It provides the opportunity for vendors to remove malware from users' devices even when it is already installed.

This functionality is also sometimes referred to as a 'remote kill-switch'. It provides the opportunity for vendors to remove malware from users' devices even when it is already installed.

A related opportunity is that successful implementation of this mechanism may also be a precedent for other kinds of ex-post-facto software removal which may be very beneficial in the fight against malware. The possibility of neutralising malware which is already installed on users' PCs is much sought after in the fight against botnets, for instance. It is often problematic (legally and contractually) to remove malware from a user's PC, even if the malware is threatening the user himself and others.

Example of existing policy: the Android Market Business and Program Policies (47) states*: Product Removals: From time to time, Google may discover a Product on the Market that violates the Android Market Developer Distribution Agreement or other legal agreements, laws, regulations or policies in force from time to time. In such an instance, Google retains the right to remotely remove those applications from your Device at its sole discretion. If that occurs, Google will make reasonable efforts to recover the purchase price of the product, if any, from the originating Developer on your behalf. If Google is unable to recover the full amount of the purchase price, it will divide any recovered amounts between the affected users on a pro rata basis.*

Example of usage: *Google recently removed two apps via the remote kill-switch built into Android. The (free) apps had first been admitted to the marketplace, and were later removed because they did not work as advertised by the app developer.*

Caveat: remote application removal has, however, raised some objections, mainly related to privacy and unfair censorship. In general, it should be noted that public perception appears to be very sensitive towards any mechanism which is seen to invade the user's device, even if used exclusively for his or her benefit. Although not an information security issue per se, the security opportunities of implementing such mechanisms have to be considered against such a background, especially when less invasive mechanisms such as signature revocation could be used with a similar effect.

Less invasive mechanisms such as signature revocation could be used with a similar effect

- The judgement about whether a particular app is malicious may not be clear-cut so there is the potential for 'false positives' that result in the removal of apps that were not acting maliciously. Additionally, there may be concerns that a remote kill mechanism may be used for purposes other than to protect the end-user, for, for example, commercial purposes[6]. A coherent and effective industry-wide policy and mechanism for revoking and even sharing information about suspicious applications and vulnerabilities may be a useful development in order to mitigate such risks.
- In addition to laws that address accessing a user's device and causing damage, there are also laws that address storing information on or retrieving information from a user's device that may be implicated. For example, Article 5.3 in the updated 2002/58 directive of 25

The judgement about whether a particular app is malicious may not be clear-cut

[6] *A recent case involved the removal of a book (Orwell's 1984) which had been paid for from Kindle services, an e-reader service which also operates on smartphone) (68). Amazon, the vendor who removed the content, later issued an apology, stating: 'We are changing our systems so that in the future we will not remove books from customers' devices in these circumstances.'*

November 2009 (commonly known as the ePrivacy Directive) states: *Member States shall ensure that ... the gaining of access to information already stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access ... as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*. This law raises questions about whether remote removal of an app would be considered to be gaining access to information stored on a user's device without sufficient consent and/or whether this was strictly necessary to deliver the service requested by the user. A more defensible approach under laws such as the ePrivacy Directive could be to revoke the digital signature of the app and thus disable it.

- The possibility of removing apps remotely is not acceptable for security reasons in some cases. For example, in a military usage scenario the presence of certain apps is critical and the possibility of app removal performed by a third-party would not be acceptable.

In a military usage scenario the presence of certain apps is critical and the possibility of app removal performed by a third-party would not be acceptable.

- The mechanism usually only covers the removal of malicious apps which are installed via the official software distribution channel (app-store). Although there are currently few known examples in smartphones, attacks may also be carried out via mechanisms and protocols built into bona-fide software. For example, a recently reported vulnerability allowed a website to automatically load a simple PDF document containing a font which caused a buffer overflow giving unrestricted access to the phone for an attacker (48).
- If the mechanism is not securely implemented, it could be abused by attackers, and be used in a denial of service attack or commercial sabotage.

3.4 Better backup and recovery

Description	Some smartphones ship with convenient backup and recovery functions to address the risk to data availability of failure, loss, or theft.
Rating	Medium

Smartphones are often well integrated with local or remote backup and recovery services. For example, some platforms automatically back up contacts, calendar or emails to a remote service. Smartphone applications, furthermore, often rely on network-based storage and backup. Overall this can make recovery of data in the event of a device failure, theft or loss quicker and more convenient and increase overall service availability.

In some cases, smartphones can even be located remotely via the network, allowing the user to recover a lost device more easily. Additionally, some smartphones can be disabled and wiped remotely (and data may be easily recovered by the owner). This, combined with above-mentioned backup and recovery services, can be used to mitigate the risks associated to theft and loss.

In some cases, smartphones can even be located remotely via the network, allowing the user to recover a lost device more easily

Example: *Blackberry Protect is a security application which* (49) *'allows you to wirelessly backup, restore and locate your phone. In the event that your phone is misplaced, lost or stolen, it provides features like: remote device wipe, remote device lock, 'Lost and Found' screen, locate device on a map, remote activation of the phone's loud ringer, and wireless device backup and restore.'*

Caveat: although not covered in this report, the extent of this opportunity clearly depends on the security of the backup services used (see 2.3 Scope)

3.5 Extra authentication and non-repudiation options

Description	Smartphones are equipped with a smartcard reader, which gives additional options for authentication and non-repudiation.
Rating	Medium

Smartphones can be used to improve the process of online authentication and provide a mechanism for non-repudiation. Smartphones lend themselves to such applications because:

- The SIM card used in smartphones is a smartcard (50) and, with the appropriate software, licences and certificates in place, can be used for PKI-based authentication and digital signatures (51). Although unavailability of smartcards and readers is not the only impediment to the uptake of PKI, this feature of smartphones could be one factor in encouraging the use of PKI and digital signatures for the authentication of users and transactions.
- Smartphones may also take advantage of the shared secret between the SIM card and the HLR (Home Location Register) using the 3GPP standard Generic Bootstrapping Architecture (GBA) (52).
- Smartphones may also be used to create one-time-password codes without using SMS or network connections.

The SIM card used in smartphones is a smartcard and, with the appropriate software, licences and certificates in place, can be used for PKI-based authentication and digital signatures.

Example: *Google Authenticator* (53) *is a mobile application that allows the generation of two-step verification codes on a smartphone without a network connection.*

Caveat: not all smartphones have security mechanisms such as a trusted display, which is needed for the implementation of a safe digital signature process (to show the user which document is being signed).

3.6 Extra encryption options

Description	Smartphones allow users to use end-to-end encryption for phone calls and SMS more easily.
Rating	Medium

Smartphones come with more processing power and third-party encryption applications are easily available to end-users. For call confidentiality, traditional handset users rely on encryption offered by the mobile network operator.

Crypto-modules for additional protection are expensive and are typically only used by top-officials. However several third-party applications are now offering encryption for smartphone voice calls, on top of the standard encryption provided by mobile network operators[7]. This allows users to take advantage of increased protection and confidentiality of their telephone calls against, for example, eavesdropping attacks (54) (55).

Caveat: note, however, that most smartphones do not have the same integrity controls as a standard smartcard reader; thus a malicious app could limit the effectiveness of the end-to-end encryption. Secondly, the use of such solutions must be in accordance with local regulatory provisions governing the use of encryption technologies. Finally, the security of such solutions depends strongly on the key management procedures implemented.

3.7 Device and OS diversity

Description	Smartphones are diverse in terms of hardware and software, which makes it more difficult to attack a large group of users with one virus.
Rating	Minor

[7] *The Wassenaar Arrangement may be applicable to certain encryption schemes.*

Smartphones are not yet standardized in many respects. There is currently a variety of hardware manufacturers and a wide spread of operating systems. For example, four different operating systems have large shares of the market (56). This is an advantage because it drives up the costs for malware developers and reduces the effectiveness of malware.

Diversity drives up the costs for malware developers and reduces the effectiveness of malware.

Caveat: it has been reported on the other hand that criminals instead focus on exploiting other software that *is* common across different platforms, e.g. Java ME, a cross-platform Java runtime for mobile devices (30). It should also be mentioned that device and OS diversity complicates software development as well as security patching and that it makes the standardization of security measures more difficult. In any event, as the market share of smartphones compared to conventional mobile phones increases, OS diversity will not prevent malicious programs from propagating among mobile users.

4. Information security recommendations

In this section we make practical recommendations for smart smartphone end-users, IT officers and CISOs dealing with smartphones. We take a pragmatic risk-based approach, prioritising the high risks.

Our recommendations target end-users as well as IT officers. As a general recommendation, it is important that IT officers raise awareness of the risks, and issue advice and guidelines for end-users. At the same time it should be mentioned that years of raising awareness have done little to prevent large-scale virus outbreaks on PCs. Apart from advice and guidelines, IT officers should make separate rules about smartphones in the security policy of their organizations. Furthermore, when feasible, policy breaches should be *prevented* by technical means, for instance by using default configurations, security software, or mobile device management software, for example (57) (58) (59).

We reiterate that smartphone users frequently cross over from one usage scenario to another. In order to mitigate any potential risks this introduces, IT officers should anticipate and even assume that this will occur and issue policy and guidance on safe use. For example, a policy might include statements on the personal use of apps which are given unrestricted access to an address book containing business contacts. In general, recommendations for consumers should be applied to employees and those for employees to high officials.

Smartphone users frequently cross over from one usage scenario to another. In order to mitigate any potential risks this introduces, IT officers should anticipate and even assume that this will occur and issue policy and guidance on safe use

We are aware of the fact that some of the recommendations concern measures that have a significant impact on usability. These measures should be implemented with special care, and we have marked these recommendations with an asterisk (*).

4.1 Addressing the risk of device theft or loss

Risks addressed		**Recommendations**
R1. Data leakage resulting from device loss or theft	**C**	**Automatic locking:** configure the smartphone in such a way that it locks automatically after some minutes. Some smartphones allow visual passwords to ease the use of auto-lock features. **Regular backups:** given the amount of personal data on smartphones, make regular backups of the data on their smartphone and removable media. **Note IMEI number:** note the IMEI number of their devices and report the loss or theft of their devices to their service providers in a prompt manner.
	E	IT officers should have policy rules covering: **User-to-smartphone authentication:** configure smartphones to lock automatically after a short time period. **Continuity:** make regular backups of data on smartphones by, for instance, an automatic backup procedure. **Classified data on smartphones:** do not store or process classified data (see Glossary) on smartphones. **Confidentiality:** memory encryption should be used for the smartphone memory and removable media used in smartphones. Checking the security properties of encryption schemes or requiring certification is recommended. For example, vulnerabilities were found for the iPhone encryption system (12) (13). ***Remote-wipe:** if encryption or user-to-device authentication is weak then remote-wipe or auto-wipe (automatically wipe after x failed access attempts) mechanisms should be available, to allow wiping the memory in case of theft or loss. Frequent backups are

		a prerequisite for implementing auto-wipe (see Continuity). ***Minimize local data:** the amount of sensitive data that is locally stored on smartphones should be kept to a minimum and, where possible, online services with non-caching apps should be used.
	H	In addition to E, IT officers should have policy rules on: **Certification of smartphones:** only use devices which are certified according to, for example, FIPS 140-2, the UK CESG Assisted Product Scheme (CAPS) or Common Criteria EAL 2+ (or higher[8] depending on the sensitivity of the use-case). ***Remote-wipe:** remote wipe (see E) should be available and, in addition, to prevent an attacker from disabling remote-wipe by blocking network-connectivity, the smartphone may be configured to automatically wipe in case of blocked network connectivity for a given period. False positives (coincidental network failure) can be reduced by performing a credential check. ***No local data:** sensitive data should not be stored locally and online access to sensitive data only allowed from a smartphone using a non-caching app. ***Two-factor authentication:** user-to-device authentication should rely on two factors; e.g. a PIN and a Bluetooth-enabled smartcard reader.

[8] *Note that there are very few off-the-shelf devices providing higher levels of certification, so customisation may be required to achieve this.*

4.2 Addressing the risk of unintentional disclosure of data

Risk addressed		Recommendations
R2. Unintentional disclosure of data	C	**Scrutinize permission requests:** scrutinize permission requests when using or installing smartphone apps or services. For example, a social networking app may request access to the smartphone’s address book in order to publish it on the Internet. Such a request should be treated with caution. **Review default privacy settings:** review the default privacy settings of smartphone apps or services and, if needed, change the settings; e.g. settings about whether or not to attach location data to images, to social network posts, etc.
	E	IT officers should raise awareness of this risk and issue guidelines that include the items under C.
	H	Idem

4.3 Addressing the risk of attacks on decommissioned phones

Risk addressed		Recommendations
R3. Attacks on decommissioned smartphones	C	**Reset and wipe:** before disposing of or recycling the phone, wipe all the data and settings from the smartphone. This goes beyond a factory reset of the smartphone’s settings.
	E	IT officers should have policy rules on: **Decommissioning:** before being decommissioned or recycled, pass used phones a thorough decommissioning procedure, including memory wipe processes. Include removable media and memory. For wiping memory, use a standard procedure, such as the NIST standard (60) (61).
	H	Idem

4.4 Addressing the risk of phishing attacks

Risk addressed		Recommendations
R4. Phishing attacks	**C**	**Be sceptical:** take a sceptical approach to messages, content and software, especially when it is coming from unknown sources via SMS, Bluetooth, email, or otherwise. For preventing phishing apps (a form of phishing) see 4.5 C, but note that most forms of phishing do not rely on malware.
	E	IT officers should create awareness of this risk. For preventing phishing apps (a form of phishing) see 4.5 E, but note that most forms of phishing do not rely on malware.
	H	Idem

4.5 Addressing the risks of malware attacks

Risk addressed		Recommendations
R5. Spyware attacks R8. Diallerware attacks R9. Financial malware attacks	**C**	**Check reputation:** before installing or using new smartphone apps or services, check their reputation using app-store reputation mechanisms and, if possible, with friends, family or colleagues. It is good practice to install apps only from well-known sources. Never install any software onto their devices unless they know and trust the source of that software and they were expecting to receive it. This refers to any software or application that users receive on their devices through any channel, e.g. by download over WAP/web, attached to an SMS, MMS, instant message or email, through Bluetooth™, infra-red or

		data connection, via synchronisation with a computer or from a memory card or other temporary storage device read by the phone. Never ignore or override security prompts displayed by their devices unless they are confident that they fully understand the risks associated with these actions. **Check resource usage and phone bill:** check resource usage and phone bills or prepaid balances. Mobile malware can sometimes be detected by monitoring in this way, especially when premium rate services are being defrauded or abused.
	E	IT officers should have policy rules on: **Authorization:** configure smartphones to require a PIN or password before new apps are installed, otherwise even relatively short periods of physical access to the device can allow the installation of malware or spyware. Requiring a password before installing new applications also prevents against certain social engineering attacks. **Resource control:** monitor resource usage of smartphones for anomalies. To limit the impact of fraud or abuse on premium rate services, limit premium resources, e.g. by the mobile network provider or by a mobile device management solution as mentioned in the introduction of this chapter. ***App installation:** if any sensitive corporate data is handled on the smartphone or if the corporate network is accessible to the smartphone, then define a whitelist of apps which are allowed to be installed. Regarding the white-listing of apps, many apps are given easy read-access to the contact data or the address book on the smartphone, but this data should be treated as highly sensitive.
	H	In addition to E, IT officers should have policy rules

		on: ***Periodic reimage:** periodically wipe (using secure deletion) and reload the smartphone with a specially prepared and tested disk image.

4.6 Addressing the risks of network spoofing

Risk addressed		**Recommendations**
R6. Network spoofing attacks	**C**	**Cautious use of hotspots:** use public WiFi hotspots with caution and configure the smartphone so that it does not connect automatically. It is recommended that only trusted networks and hotspots be used for sensitive matters, e.g. ebanking, ecommerce, and emailing.
	E	IT officers should have policy rules on: **Communications confidentiality:** communication of corporate data should be encrypted (using VPN or SSL). **Pre-installing server certificates:** pre-install public key certificates of corporate servers (email, intranet) and configure clients to deny other certificates.
	H	In addition to E, IT officers should have policy rules on: **Encryption software:** for highly confidential usage, use additional call and SMS encryption software for end-to-end confidentiality.

4.7 Addressing the risk of surveillance attacks

To address the risk of R7. Surveillance attacks all previously-mentioned recommendations should be followed.

5. Conclusions

In this report we have given an overview of the main information security risks and opportunities for smartphone users, and we have provided practical recommendations for end-users and IT-officers on how to address the risks. However, we conclude by raising some issues which cannot be addressed by end-users or IT officers.

- **Device access control and off-the-shelf memory encryption:** the risks associated with theft and loss are relatively high, especially for employees and high officials. We have made recommendations for end-users and IT officers to take necessary precautions, but they are dependent on what is offered off-the-shelf by smartphone vendors and developers.
- **Standardized privacy and security settings**: the third highest risk does not concern an attack but the unintentional disclosure of data by the user. The combination of smartphones and social networking apps make it easy for users to upload large amounts of personal data. Developers of smartphone apps and services should choose default settings with security and privacy in mind (the principle of security and privacy by default). In this regard, there is currently a lack of industry-standard guidelines on privacy for developers.
- **Patch management:** some platforms still lack mature update features and despite the obvious opportunity for improving security, app-stores can create a potential bottleneck in the distribution of patches by creating an extra hurdle to clear before distribution. Furthermore the testing of patches such as OS updates which must interface with several different models presents serious challenges.
- **Safety of third-party software and the OS:** sandboxing, capability-based access control in smartphone operating systems, controlled software distribution, and remote application removal are key opportunities for improving smartphone security. Both controlled software distribution and remote application removal are topics that raise discussions on censorship, big-brother effects, unfair competition, etc., but most experts agree that the ‘walled-garden’ approach could help to reduce the impact of malware. There is, however, currently no industry standard or best practice on the review and removal of apps.
- **Web standards for apps:** while many desktop applications have migrated into the browser, the opposite is occurring for many smartphone apps; many

web sites are being turned into apps on multiple platforms. However standards are now emerging, such as W3C widgets (62), which in the longer term promise to evolve into a single standard for both web applications and smartphone apps. These new standards will allow access through the smartphone browser to the full range of smartphone capabilities. It is vital that security and privacy are given high priority in the design and implementation of these standards.

Looking into the future we do not only see information security risks, but information security opportunities. We look forward to following up on this preliminary report by analysing specific risks, opportunities and recommendations in more detail.

6. Appendix: Vulnerabilities

Below we describe classes of vulnerabilities which may be present in a smartphone, for use as a reference.

6.1 Vulnerabilities leading to malware installation

1. Patching weaknesses

- In walled-garden app-store models, any patch has to find its way through the app-store vetting process before it can be applied to a device. Despite an obvious opportunity for improving security, app vetting schemes are a bottleneck in the distribution of patches. This is a serious obstacle to the timely patching of apps, which in a fast moving industry may be required frequently.
- Thoroughly testing that a patch does not break any applications is challenging even for only one or just a few products. Managing a security update system for tens of different products (some of them based on very different platforms and operating systems, some of them already many years old, etc.) would be extremely challenging. If security patches are not thoroughly tested for all models, automatic updates could deliver more harm than benefits to users. Thus, deploying such an infrastructure would be very challenging for many manufacturers.
- Several OSs still rely on users to confirm or even discover individual updates of apps, which is a serious problem for patching security flaws.

2. Limited capabilities for 3rd party security solutions (centralised security management)

Many platforms allow only limited functionality for third-party security services. For example, on some platforms, apps are not allowed access to processes unless they are signed by the same developer certificate. Some platforms do not allow certain types of apps to run in the background. This makes it difficult to provide security services which rely on monitoring the activities of applications. This places more responsibility in the hands of the OS and app-store providers. Although this has obvious opportunities for improving security (see [3.3 Remote application removal]), it nevertheless creates a significant single point of failure in the event that the provider’s defences prove inadequate.

3. Reputation vulnerabilities

Vulnerabilities in reputation systems applied to apps might allow an attacker to inflate the reputation of an app artificially and thus gain undue trust from users. These vulnerabilities include lack of voter authentication, the possibility of multiple votes, votes not being weighted according to the importance of the target app, etc. (further information can be found in the ENISA report (63))

4. Lack of code/app review processes

Due to market forces, recent mobile platforms tend to be very open and developer friendly to encourage adoption. This is because of current trends in which third-party application developers have an increasingly important role in mobile device ecosystems. Furthermore application signing infrastructures and operating system level security frameworks are sometimes considered a major hurdle for the development of applications by third-parties.

5. Signed ≠ trusted

Users may think that signed apps are more trustworthy than unsigned apps when there may be no such implication. Clearly in some cases, the app signature is an assertion that the app has been checked according to certain criteria but, in other cases, it may be simply a mechanism to establish the origin of the application. The risks from malware and spyware are increased with respect to older phones since mechanisms available for users to distinguish trusted from untrusted apps (reputation systems, digital signatures) are open to abuse and misinterpretation.

6. Ability to unlock phones

These vulnerabilities are of a rather different category, in that the user of the device is aware that he or she is disabling certain security measures, and indeed almost certainly wants to work around them. However an unlocked phone allows the user to install apps which are not subject to the vetting processes used in app-stores. This leads to a situation where users are often not aware that they are executing code which has not been subject to any review process and which operates with root privileges.

6.2 Covert channels/weak sandboxing

There are several loopholes in sandboxing schemes. For example, if the keyboard cache (the database of the words most frequently typed by the user) is publicly available (which it often is), this effectively allows apps to access personal data from the user and usage data from other apps. Many apps are also granted access to the user address book, which usually contains highly sensitive information (e.g. users hide bank account details as address book entries). Network interfaces may also be used to transmit private data covertly between apps or to an attacker; e.g. a backdoor in an SMS app is easy to implement.

In some smartphone platforms, location data is added to photo filenames or in file metadata. If these photos are made available to other apps or uploaded to social networking sites, users will be asked for permission to access the gallery, but not location data. This therefore constitutes a covert channel. For example, a user might post a photo on a public blog or micro-blogging site, without realising that the filename contains the location of the data.

6.3 User permissions fatigue

Many platforms request user consent for app access to different types of data and messaging (e.g. push notifications) on the phone at installation time. There are several problems with this:

- Compared to PCs and laptops, user interfaces are usually more limited, meaning that, for example, storage of credentials on the device is more probable and user authentication cannot be so frequent (biometric authentication is one possible solution). For example, a request for user authentication is more invasive on a smartphone than on a PC and the fraction of a user's attention which can be devoted to dealing with security-related decisions is even smaller than in larger form-factor environments.
- Users do not have the time or commitment to evaluate permissions requests even though it is restricted to a once-per-install request.
- Permissions are not detailed enough to convey the risks of giving consent – e.g. granting access to the frequently typed words list in the keyboard cache may sound harmless to many users, but this could reveal passwords.
- Some data types naturally lend themselves to integration with user consent, without having to assume the persistence of a decision. For example, file upload naturally involves the user in selecting the file and therefore presents little difficulty. Other types, however, cannot be managed in this way. It is not feasible for the user to provide input every time their location, temperature, acceleration, magnetic field, etc are disclosed.

- It is often very difficult for users to examine and/or change the permissions they have granted after the initial request.
- There is no means to set global policies for permissions granted, e.g. 'do not install any apps which request location data for marketing purposes'.

6.4 Encryption weaknesses

Various high-profile weaknesses have been found in some implementations of smartphone encryption, rendering data protection on the devices close to useless (12) (13). These weaknesses come into play when an attacker gains physical access to the device through theft or loss. Additionally the effectiveness of encryption mechanisms depends strongly on the procedures and technical measures used to manage cryptographic keys.

6.5 Weak app distributor authentication mechanisms

It is often easy to impersonate a trusted brand such as a banking app. There may be no PKI or other trust infrastructure to assure the identities of developers.

6.6 No privacy protection best practices

This applies especially to developers – there are no privacy best practices available for smartphone developers. Given the privacy risks outlined in [Information security risk], many of which rely on features specific to smartphones, this is an important issue.

6.7 Lack of user awareness

This is no different from other platforms but is, nevertheless, a factor in some risk scenarios. For example, unintentional disclosure of data often relies on users' lack of awareness of the implications of consenting to certain kinds of data disclosure.

7. References to other related best practice guides

- BSI, Germany (in German) Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen https://www.bsi.bund.de/ContentBSI/Publikationen/Broschueren/mobile/index_htm.html
- BSI, Germany (in German) Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte https://www.bsi.bund.de/cae/servlet/contentblob/487520/publicationFile/30774/oefmobil_pdf.pdf
- Burton Group tele-briefings, e.g. 20.07.2010 Evaluation Criteria for Smartphone Device Management
- CIS iPhone secure configuration guide: https://www.cisecurity.org/tools2/Iphone/CIS_Apple_Iphone_Benchmark_v1.2.0.pdf
- Datamation Smartphone Security Best Practices: Five Tips http://itmanagement.earthweb.com/mowi/article.php/3881096/Smartphone-Security-Best-Practices-Five-Tips.htm
- Finnish site for Finnish nationals using smartphones: http://www.ficora.fi/mobiiliturva/english/index.html
- FIPS 140-2 Security Policy BlackBerry Cryptographic Kernel http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp593.pdf
- Fraunhofer BlackBerry Enterprise Solution for Microsoft Exchange Security Analysis http://testlab.sit.fraunhofer.de/downloads/certificates/Certification_Report-06-104302.pdf
- Smartphone Security Risks by Gartner analyst John Girard http://www.computerworld.com/s/article/345297/Smartphones_Need_Smart_Security
- GSMA advice to help minimise the risk of users experiencing security problems: http://gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/security-accreditation-scheme/security-advice-for-mobile-phone-users/index.htm
- Help Net Security http://www.net-security.org/secworld.php?id=8646
- ISACA White Paper http://www.isaca.org/Knowledge-Center/Research/Documents/SecureMobileDevices-Wht-Paper-20July2010-Research.pdf
- NIST Guidelines on Cell Phone and PDA Security http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf
- Policy and Guidance for the Use of BlackBerry by the Australian Government http://www.dsd.gov.au/_lib/pdf_doc/library/Blackberry_March_06.pdf
- Secure Information Technology Centre Austria (in German) http://www.a-sit.at/pdfs/Technologiebeobachtung/Studie_IPhone_v1.0.2.pdf and http://www.a-sit.at/pdfs/Technologiebeobachtung/Studie_Blackberry_v1.0.2.pdf
- TechRepublic Smartphone enterprise security risks and best practices http://blogs.techrepublic.com.com/smartphones/?p=1935

Bibliography

1. **Gartner.** Smartphone Sales Increased 96 Percent. [Online] 2010. http://www.gartner.com/it/page.jsp?id=1466313.

2. **comScore.** European Smartphone Market Grows 41 Percent in Past Year. [Online] 2010. http://www.comscore.com/Press_Events/Press_Releases/2010/9/European_Smartphone_Market_Grows_41_Percent_in_Past_Year.

3. **New Bricklyn.** Magic Toothbrush iPhone app. [Online] http://www.newbricklyn.com/.

4. **Computerwoche.** Die Kanzlerin bekommt ihr Merkel-Phone. [Online] http://www.computerwoche.de/netzwerke/mobile-wireless/1910789/.

5. **Reuters.** EBay CEO says volume on iPhone app could triple. [Online] 2010. http://www.reuters.com/article/idUSTRE65160V20100602.

6. **PCMAG.COM.** Google's Schmidt Shows Off 'Gingerbread' NFC Phone. [Online] 2010. http://www.pcmag.com/article2/0,2817,2372746,00.asp.

7. **The Tech Journal.** Monitor your Body On Your Android Cellphones. [Online] 2010. http://thetechjournal.com/tech-news/monitor-your-body-on-your-android-cellphones.xhtml.

8. **International Organization for Standardization.** ISO/IEC 27005. 2008.

9. **ENISA.** Cloud Computing Security Risk Assessment. [Online] 2009. http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

10. **BBC.** Saudi Arabia begins Blackberry ban, users say. [Online] 2010. http://www.bbc.co.uk/news/world-middle-east-10888954.

11. **Cellan-Jones, Rory.** Government calls for action on mobile phone crime. *BBC.* [Online] 2010. http://news.bbc.co.uk/2/hi/technology/8509299.stm.

12. **Marienfeldt, B.** iPhone business security framework. [Online] 2010. http://marienfeldt.wordpress.com/2010/03/22/iphone-business-security-framework/.

13. **Wired.** Hacker Says iPhone 3GS Encryption Is ‘Useless’ for Businesses. [Online] 2009. http://www.wired.com/gadgetlab/2009/07/iphone-encryption/.

14. **New Scientist.** The pocket spy: Will your smartphone rat you out? [Online] 2009. http://www.newscientist.com/article/mg20427301.100-the-pocket-spy-will-your-smartphone-rat-you-out.html.

15. [Online] http://www.abiresearch.com/press/1015-Recycled+Handset+Shipments+to+Exceed+100+Million+Units+in+2012 .

16. **F-Secure.** Warning On Possible Android Mobile Trojans. [Online] January 2010. http://www.f-secure.com/weblog/archives/00001852.html.

17. **Wikipedia.** SMiShing. [Online] http://en.wikipedia.org/wiki/SMiShing.

18. *Proceedings of the 9th USENIX Symposium on Operating Systems Design and Implementation (OSDI).* **William Enck, et al.** 2010. 9th USENIX Symposium on Operating Systems Design and Implementation.

19. **SMobile Systems.** Threat Analysis of the Android Market. [Online] 2010. http://threatcenter.smobilesystems.com/wp-content/uploads/2010/06/Android-Market-Threat-Analysis-6-22-10-v1.pdf.

20. *iPhone Privacy.* **Seriot, N.** s.l. : Blackhat, 2010.

21. *The Jigsaw Continuous Sensing Engine for Mobile Phone Applications.* **H. Lu, et al.** s.l. : ACM, 2010. SenSys.

22. **Smith, C.** Sensor Logger Test . [Online] 2010. http://www.androlib.com/android.application.uk-co-md87-android-sensorlogger-wnqz.aspx.

23. *Hijacking Mobile Data Connections.* **Mobile Security Lab.** s.l. : Blackhat, 2008.

24. *More Tricks For Defeating SSL In Practice.* **Marlinspike, M.** s.l. : Blackhat, 2009.

25. **TSH Software Group.** THE SPY PHONE . COM. [Online] http://www.thespyphone.com/.

26. **Retina-X Studios.** Mobile-Spy. [Online] http://www.mobile-spy.com/.

27. **Privacy International.** Privacy international identifies major security flaw in Google's global phone tracking system. [Online] 2009. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-563567.

28. **PCWorld.** Android Game Is a Spy App in Disguise. [Online] 2010. http://www.pcworld.com/article/203512/android_game_is_a_spy_app_in_disguise.html?tk=hp_new.

29. **CNET.** Malware found lurking in apps for Windows Mobile. [Online] 2010. http://news.cnet.com/8301-27080_3-20006882-245.html.

30. **Kaspersky Lab.** Mobile Malware Evolution: An Overview, Part 3. [Online] 2009. http://www.securelist.com/en/analysis?pubid=204792080.

31. **S21sec.** ZeuS Mitmo: Man-in-the-mobile (I). [Online] 2010. http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html.

32. **Airvana.** Solving the mobile network signalling overload. [Online] 2010. http://viewer.zmags.co.uk/publication/d5f7ecee#/d5f7ecee/4.

33. **CISCO.** Visual Networking Index: Global Mobile Data Traffic Forecast Update. [Online] 2010. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.

34. **3GPP.** Release 8. [Online] 2010. http://www.3gpp.org/Release-8.

35. **Rysavy Research / 3G Americas.** HSPA to LTE-Advanced: 3GPP Broadband evolution to IMT-Advanced (4G). [Online] 2009. http://www.3gamericas.org/documents/3G_Americas_RysavyResearch_HSPA-LTE_Advanced_Sept2009.pdf.

36. **Rysavy Research (sponsored by RIM).** Mobile Broadband Capacity Constraints and the Need for Optimization. [Online] 2010. http://www.rysavy.com/Articles/2010_02_Rysavy_Mobile_Broadband_Capacity_Constraints.pdf.

37. **Ars Technica.** How smartphones are bogging down some wireless carriers. [Online] 2010. http://arstechnica.com/gadgets/news/2010/02/how-smartphones-are-bogging-down-some-wireless-carriers.ars.

38. **Repubblica.** Calabrò: "Troppi smartphone la Rete rischia il collasso". [Online] 2010. http://www.repubblica.it/tecnologia/2010/07/06/news/smartphone_collasso_rete-5421817/?ref=HRER2-1.

39. **ENISA.** Gaps in standardisation related to resilience of communication networks . [Online] 2009. http://www.enisa.europa.eu/act/it/library/deliverables/gapsstd.

40. **US dpt of Homeland Security.** Cyber Storm: Securing Cyber Space. [Online] 2010. http://www.dhs.gov/files/training/gc_1204738275985.shtm.

41. **Japan.inc.** WW-12 -- Stupid Browser Phone Tricks. [Online] 2001. http://www.japaninc.com/ww12.

42. **Nikkei Business Publications.** ニュース・ウォッチ　モバイル 携帯電話にメール・ウイルス ドコモのiモードで2月発生｜日経コミュニケーション｜日経BP記事検索サービス. [Online] 2001. http://bizboard.nikkeibp.co.jp/kijiken/summary/20010305/NCC0337H_428183a.html.

43. **Nokia.** Symbian Platform Security Model. [Online] 2009. http://wiki.forum.nokia.com/index.php/Symbian_Platform_Security_Model.

44. How has Symbian Signed evolved with Symbian OS v9? [Online] 2005. https://www.symbiansigned.com/How_has_Symbian_Signed_evolved_with_Symbian_OS_v9.pdf.

45. **ReadWriteWeb.** New iPhone App Piracy Statistics Reveal "Try Before You Buy" Mentality is a Myth. [Online] 2009. http://www.readwriteweb.com/archives/new_iphone_app_piracy_statistics_reveal_try_before_you_buy_myth.php.

46. **Apple.** App Store Review Guidelines. [Online] 2010. http://developer.apple.com/appstore/guidelines.html.

47. **Google.** Android Market Business and Program Policies. [Online] http://www.google.com/mobile/android/market-policies.html.

48. Apple Security Breach Gives Complete Access to Your iPhone. [Online] 2010. http://gizmodo.com/5603319/.

49. **Blackberry.** Inside BlackBerry Protect. [Online] 2010. http://blogs.blackberry.com/2010/07/introducing-blackberry-protect/.

50. **Bundesamt fur Sicherheit in der Informationstechnik.** Offentliche Mobilfunknetze und Sicherheitsaspekte. [Online] https://www.bsi.bund.de/cae/servlet/contentblob/487520/publicationFile/30774/oefmobil_pdf.pdf.

51. **ETSI.** Mobile Commerce (M-COMM); Mobile Signature Service; Security Framework. [Online] 2003. http://docbox.etsi.org//EC_Files/EC_Files/tr_102206v010103p.pdf.

52. **3GPP2.** Generic Bootstrapping Architecture (GBA) Framework. [Online] 2008. http://www.3gpp2.org/public_html/specs/S.S0109-0_v2.0_080222.pdf.

53. **Google.** Google Authenticator. [Online] 2010. http://www.google.com/support/a/bin/answer.py?hl=en&answer=1037451.

54. *Real Time Cryptanalysis of A5/1 on a PC.* **A. Biryukov, A. Shamir, D. Wagner.** s.l. : Fast Software Encryption Workshop 2000, 2000.

55. **Casper Tech Mobile Cryptography.** Mobile encryption devices. [Online] http://www.caspertech.com/voice-encryption/mobile-crypto/.

56. **Gartner.** Gartner Says Android to Become No. 2 Worldwide Mobile Operating System in 2010 and Challenge Symbian for No. 1 Position by 2014. *Gartner newsroom.* [Online] 2010. http://www.gartner.com/it/page.jsp?id=1434613.

57. **Inquso.** Secure Phone - device life cycle management. [Online] http://www.inquso.se/en/product.

58. **Funambol.** Funambol solutions: Device management. [Online] http://www.funambol.com/solutions/devicemanagement.php.

59. Excitor Mobile Device Management. [Online] http://www.excitor.com/.

60. **NIST.** Guidelines for Media Sanitization. [Online] http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

61. US Department of Defense directive 5220.22-M. [Online] http://www.usaid.gov/policy/ads/500/d522022m.pdf.

62. W3C widgets. [Online] http://www.w3.org/TR/widgets/.

63. **E. Carrara, G. Hogben.** Reputation-based Systems: a security analysis. [Online] 2007. http://www.enisa.europa.eu/act/it/oar/reputation-systems/reputation-based-systems-a-security-analysis.

64. Invalid banking cert spooks only one user in 300. [Online] http://computerworld.co.nz/news.nsf/UNID/FCC8B6B48B24CDF2CC2570020018FF73?OpenDocument&pub=Computerworld.

65. **Computerworld.** Invalid banking cert spooks only one user in 300. [Online] 2005. http://computerworld.co.nz/news.nsf/UNID/FCC8B6B48B24CDF2CC2570020018FF73.

66. Amazon Erases Orwell Books From Kindle . [Online] 2009. http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html?_r=1.