CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Authors Teemu Väisänen, Alexandria Farar, Nikolaos Pissanidis, Christian Braccini, Bernhards Blumbergs, and Enrique Diez

Defending mobile devices for high level officials and decision-makers

Tallinn 2015

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation.

www.ccdcoe.org
publications@ccdcoe.org

1. Abstract

High-level officials and decision-makers handle and store sensitive data with their own or with their organisations' mobile devices. The sensitive data may be owned by the person him/herself or by the organisation. These users do not always follow security policies, creating a risk of leaking this sensitive data. It is often impossible to assess all the places where data is accessed and/or stored.

The purpose of this study is to find mitigation mechanisms for a number of risks resulting from the usage of such systems without obeying security policies.

The study was done by analysing usage scenarios; their actors and the assets to be secured; related mobile threats; suitable mitigation mechanisms; and threats lacking good enough mitigation mechanisms.

The key results of this study are a set of threat descriptions and existing mitigation mechanisms, along with proposed new mechanisms for mitigation.

Results can be implemented by adding the described security controls and mitigation mechanisms to systems to improve their security.

Keywords: security awareness, security policies, mobile devices, COPE, BYOD, MDM, EMM, risk analysis

2. List of Abbreviations

4G	**4th generation for GSM**
AE	Authenticated Encryption
AES	Advanced Encryption Standard
AIDE	Advanced Intrusion Detection Environment
AIX	Advanced Interactive eXecutive
API	Application programming interface
AV	Anti-virus
BES10	BlackBerry Enterprise Service
BYOD	Bring Your Own Device
CAVP	Cryptographic Algorithm Validation Program
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CCM	Counter with CBC-MAC
CESG	Communications and Electronic Security Group
CHARGEN	Character Generator Protocol
COPE	Corporate owned - personally enabled devices
CPNI	The Centre for the Protection of National Infrastructure
CSC	Critical security control
DEP	Device Enrollment Program
DNS	Domain Name System
DoS	Denial-of-Service
DRM	digital rights management
DTU	Danish Technical University
EMM	Enterprise mobility management
ENISA	European Network and Information Security Agency
ESP	Encapsulating Security Payload
EU	European Union
FIPS	Federal Information Processing Standards
GCHQ	Government Communications Headquarters
GCM	Galois/Counter Mode
GD	Good Dynamics
GFE	Good for Enterprise
GID	Group ID
GPS	The Global Positioning System
GSC	Government Security Classification
GSM	Global System for Mobile Communication
HIDS	Host Based Intrusion Detection Systems
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IDS	intrusion detection systems
IM	instant messaging
IMEI	International Mobile Station Equipment Identity
IMSI	International mobile subscriber identity
IP	Internet Protocol
IPS	intrusion prevention systems
IPsec	Internet Protocol Security
IT	Information Technology
KSN	Kaspersky Security Network
LDAP	Lightweight Directory Access Protocol
LTE	Long-Term Evolution
MAC	Media access control
MAM	Mobile Application Management
MDM	Mobile device management
MFS	Multi-factor authentication
MitM	Man-in-the-Middle
MMS	Multimedia Messaging Service
NATO	North Atlantic Treaty Organisation
NFC	Near Field Communication
NIDS	Network intrusion detection systems
NOCs	Network Operations Centres
NSP	Network Security Platform
NTP	Network Time Protocol
OCB	Offset Codebook
OS	Operating system
OSSEC	Open Source SECurity
OTP	One-time password (or pad)
OWASP	The Open Web Application Security Project
PC	Personal computer
PIN	Personal identification number

PVS	Passive Vulnerability Scanner
QOTD	Quote Of The Day
RASP	Runtime Application Self-protection
RAT	Remote Access Trojan
RCS	Remote Control Systems
RNG	Random number generator
ROM	Read Only Memories
RSA	Rivest-Shamir-Adleman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SAE	System Architecture Evolution
SD	Secure Digital
SDK	Software development kit
SHA	Secure Hash Algorithm
SMC	Sophos Mobile Control
SMS	Short Message Service
SSD	Solid State Drive
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security
TPM	Trusted Platform Module
UID	Unique ID
UK	United Kingdom
US-CERT	United States Computer Emergency Readiness Team
VAS	Vulnerability Assessment Scanner
VoIP	Voice over IP
VPN	Virtual Private Network
WIPS	Wireless intrusion prevention system

3. Table of Contents

4. Table of Figures

5. Table of Tables

6. Executive Summary and Recommendations

Smartphones are an inevitable presence in everyday life. High-level officials and decision-makers use mobile devices to handle and store sensitive information that should be protected as well as possible.

However, those mobile devices are fundamentally unsecurable - it is impossible to have absolutely secure systems, even if users follow security policies. In addition to possibly poor cyber hygiene, such as free games that use malicious advertisements or inadequate settings in social network services, mobile devices can often be compromised without the user's knowledge. This could lead to disclosure of personal information or sensitive data with dire political and national consequences. Additionally, offensive campaigns can be staged against decision-makers through compromised mobile devices that can have detrimental effects.

This study describes and analyses threats and risks related to mobile device usage scenarios and presents countermeasures and mitigation mechanisms for them. This is done by analysing several public documents including security guidelines, checklists, security controls, presenting features of existing products (such as secure smart phones) and work of security researchers. In addition to these, new countermeasures and recommendations are presented.

The reader should be aware that there is no single rule to follow and no single security countermeasure that would mitigate all the risks related to mobile devices. Several risk mitigation techniques exists, and by combining them, the security of the whole system increases.

The detailed recommendations presented in this study include, but are not limited to:

- Improving user security awareness;
- Reinforcing security policies;
- Strong authentication;
- Monitoring accesses and behaviour of users and devices;
- Encrypt media and communication.

7. Introduction

The number of threats and attacks against mobile devices such as mobile phones, smartphones, tablets, and laptops has been increasing and their effects have become more dangerous [1] [2] [3] [4] [5] [6] [7] [8]. Still, more sophisticated attacks will arise in the future [9].

Being the perfect media convergence platform, mobile devices will continue to be first choice for all kinds of users [10]. They are typically used in a variety of locations outside the organisation's control [11]. Today, a lot of corporate data is situated outside the company [12]. It is hard or, in some cases, even impossible to assess all the places where data is accessed and/or stored [13].

Corporate data is data shared by the users of an organisation, generally across departments and/or geographic regions. Because enterprise data loss can result in significant security issues for all parties involved, corporations spend time and resources on careful and effective data modelling, solutions, security and storage. Compared to personal mobile subscribers, enterprises have more concerns about mobile device security and are willing to invest more effort to ensure their security [14]. Personal data is defined as any information about a specific or definable natural person. A person is considered definable if, for example, a connection to the person can be established by the information from the data combined with supplementary knowledge, even if such knowledge is available only by coincidence.

Another element worth considering is where data is processed: Corporate data, processed outside its perimeter border, adds complexity to any policy balanced approach. This is particularly true when considering the usage of portable devices (including the personally owned ones) where 'authorised' users may wish to use them for work purposes, for example using their own tablet computers to access, read and respond to work emails, or working in a home-office. It is evident that in this 'outbound' scenario the corporation must secure its data to the same extent as an 'inbound' scenario, and must not introduce unacceptable risks (such as malware) into corporate networks by failing to secure its own equipment.

Bring Your Own Device (BYOD) has become popular and it is inevitable that a mobile device includes both personal data and business data [14]. The same applies to Corporate Owned - Personally Enabled devices (COPE), which is the opposite approach to BYOD. Mobile devices are different from normal computers, as are the security controls used in them [15]. This affects, for example, the usability of security controls.

As presented in Burson-Marsteller's Twiplomacy study 2014 [16], world leaders tweet a lot: More than half of the world's foreign ministers and their institutions are active on Twitter and more than two-thirds (68 percent) of all governmental decision-makers have personal accounts. Individual smartphones and smartphone users frequently cross-over from their normal usage scenarios [17].

Security controls [18], guidelines [11], security checklists [19], and security policies [20] exist for securing mobile devices, developed applications [21] [22], for BYOD [23], and for increasing user awareness [24], however they do not target mobile devices used by high-level decision-makers. Few exceptions exist, such as European Network and Information Security Agency's (ENISA's) Smartphones security report [17], where one of usage scenarios is related to high officials. The second example is a collection of United Kingdom (UK) Government Communications Headquarters (GCHQ) Communications and Electronic Security Group (CESG) definitions for a security framework for end users working with OFFICIAL information and security controls for mobile laptops to be used for OFFICIAL and OFFICIAL-SENSITIVE information [25]. It should be noted, that in Government Security Classification (GSC) levels [26], in addition to OFFICIAL level of information, we are interested also in users who have clearance to access SECRET, TOP SECRET or similar levels of information.

Additional security controls are used in the mobile phones of high-level officials and decision-makers [27], and there are additional security policies for using them [28]. Even so there have been security problems [29] [30] [31] [32] [33] related to their phones or laptops. In addition to this, some countries have threatened to ban

phone services, if they do not allow full access to them [34]. Based on a survey of three hundred IT security professionals, a company board of directors are most likely to ignore or flout security policies and procedures [35]. Similarly, the survey conducted by Nasuni finds that the greatest violators of IT cloud security policies have been top executives [36]. Several reasons have been presented for why security policies are not followed, for example, security policies are not simple enough nor understandable, they conflict with everyday processes, there are no mechanisms for enforcing policies, users are too ignorant [37] or they are in (too) high a position and believe that policies are not their concern [38]. Decision-makers and high-level officials have the most valuable information, which is of interest to other countries or competing organisations, as well as to individual hackers or hacker groups, which marks them as a high value targets.

Security policies are the foundation for information security through which management formally defines and places various information security obligations on an organisation's members. While most organisations have something in place, only few of them have truly effective information security policies, as well as enforcement and supervision mechanisms for them. On the other hand, 'unselective' policies might hamper the effective processing of information due to strict technical limitations. A balanced approach within the set of information security controls should start from the understanding of the nature of the data processed firstly, and sharing responsibilities for information security secondarily.

Problems arise when these systems are not used as security policies dictate. The user of the system does not, is not willing to, or cannot follow the security policies and hence makes the system insecure. In addition to not following security policies, it is possible that there are no security policies for each existing or still unknown use case. In this paper, the most tailored technical and non-technical security measures aimed to mitigate such conflicts are described and evaluated.

The level of security in the system can be defined by the value of three components: security, usability and functionality. Security means the restrictions, security controls, etc. Functionality means the features in the system, and usability means their ease of use. Moving towards security means less functionality and less usability.

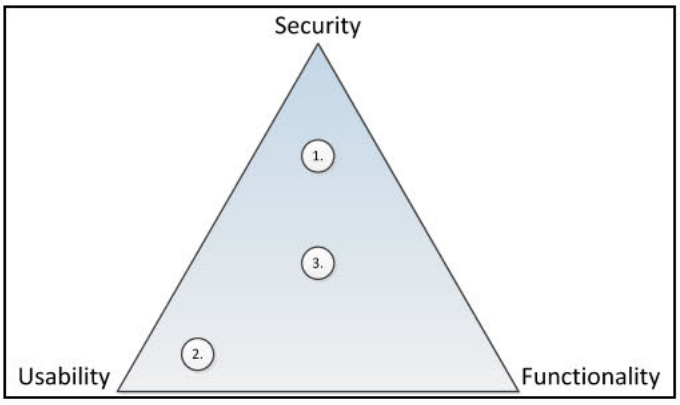


Figure 1. Security, Usability, and Functionality triangle

Bullet (1) in Figure 1 might describe a desired situation for a security manager of the system. Bullet (2) might be a desired situation for the user, and the optimal situation might be bullet (3) near the middle of the triangle, where usability, security and functionality are in balance.

These examples give an overview of the areas discussed in this paper: Devices used by high-level officials and decision-makers that must have an 'always connected' status, which cause additional threats, because their devices can't be isolated from networks or shut down. The way decision-makers use their mobile devices is

often in fundamental conflict with secure computing. Only the synergy of an enhanced technical situational awareness and proactive human vigilance could mitigate the severity of security breaches.

The main contribution of this study is in analysing risks related to mobile devices used by high-level officials and decision-makers, and describing mitigations to reduce these risks.

The paper continues with the section 8. 'Research process (methods)', which describes the methods used in this study. Section 9. describes usage scenarios, actors and assets. Then section 10. 'Threats' discusses existing threats and the following section 11. describes the risk analysis process we executed. The section 12. 'Literature Review' is divided into three subsections. The first includes reviews existing related guidelines, security controls and checklists, the second includes a review of commercial security products that can already be made available to make high-level officials' and decision-makers' usage scenarios more secure, and the third subsection reviews results and proposals from research world. Results of the risk analysis and their mitigation are presented in the section 13. 'Results'and new countermeasures to mitigate risks are proposed in section 14. 'New countermeasures, security controls and recommendations'. Finally, executive summary is in section 6. and we finish with our conclusions in the section 15.

8. Research process (methods)

In this study the most important risks related to mobile devices of high-level decision-makers are identified. This is done by 1) identifying the assets worth protecting in usage scenarios related to high-level officials, 2) identifying the potential threats or threat sources and potential vulnerabilities (including analysis of research publications, guidelines, security controls, checklists, commercial products, threat reports and security news related to mobile devices, and creating attack trees), and 3) identifying the likelihood and impact of identified threats and/or vulnerabilities.

After this we present existing commercial products, security controls, checklists, research proposals, and guidelines that can be used to mitigate these risks. Mitigation mechanisms for threats having greater likelihood and/or impact are presented. Thirdly, an analysis of the risks that cannot be mitigated by using these aforementioned techniques has been performed. Lastly, new countermeasures, recommendations and security controls for those risks that could not be mitigated in the previous step, are described and analysed. Mitigation techniques have been numbered (M1-M57) and presented in tables and are referenced in the text.

9. Usage scenarios, actors and assets to be protected

This study is focusing on the following usage scenario related to high officials described in [17]:

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 for business phone calls, Internet browsing, corporate email, expense management, customer relationship management, travel assistance, contact management, business social networking, video conferencing, scheduling tasks, and reading documents. In addition, it is used for dealing with sensitive information and/or tasks. [17]

If using GSC categorisation [26], the sensitive information locates at OFFICIAL-SENSITIVE, SECRET, or at TOP-SECRET level.

Usage in such a scenario is subject to security policies and the functionality of the smartphone may be restricted or customised, 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 [17]. This means that there are possibilities that high-level officials are using their work phones as consumers, e.g., for navigation, not work related social networking, gaming, photography, video recording, etc.

The following assets are especially worth protecting in usage scenarios of high-level officials and decision-makers: a) sensitive data (voice and video calls, messages, documents, intellectual property, innovations, etc.), b) privacy of the user (availability, location, traveling direction, contacts, behaviour, tasks, patterns, etc.), c) credentials (usernames, passwords, key patterns, private keys, session keys, certificates, etc.), d) transactions (calls, messages, contacts, money, etc.), e) reputation of the user (behaviour, customer relations, etc.), and f) sensors of the device (microphone, etc.).

As described in [39], governments and private organisations are targets of several sources of threat, such as state actors, terrorists, professional criminals, cyber vandals, scriptkiddies, hacktivists, internal actors and cyber researchers. From these, state actors and professional criminals cause high level threats to both governments and private organisations. Digital espionage by state actors and disruption of IT services done by professional criminals are high threats targeting both governments and private organisations. In addition to these, professional criminals are targeting private organisations with theft and the disclosure or selling of information, as well as with IT takeover. High level threat is defined as being a clear development which make the threat opportunistic or where measures have a limited effect. As described, various countries are developing the ability to carry out offensive cyber operations, however in addition, states could also hire services or buy products from other operators under a foreign banner, e.g., by pretending to be hacktivists. The intention of professional criminals is to earn money. [39] It should be noted, that when targeting high-level officials, they do this by selling services or stolen information, not directly as when targeting consumers.

This study does not concentrate on insider threats, as they are not thought to be likely in selected usage scenarios. As described in [40], insiders who commit IT sabotage attacks have personal predispositions, insiders who steal intellectual property are usually scientists, engineers, salespeople, or programmers, and insiders who commit frauds are usually low-level employees who use authorized access during normal working hours to steal or modify information.

10. Threats

Entities such as United States Computer Emergency Readiness Team (US-CERT) [1] [2], Fortinet [3], F-Secure [4], Webroot [5], ENISA [41] [17], the Open Web Application Security Project (OWASP) [42] [43] [44], the Centre for the Protection of National Infrastructure (CPNI) [45], Trend Micro [6], Norton [7] and Sophos [8] have described threats related to mobile devices and mobile applications. Attack patterns and tools that targeted personal computers (PCs) a few years ago have been migrated to the mobile ecosystem [10]. Different types of malware including rootkits, worms, ransomware, trojans and botnets, as well as phishing, and jailbreaking/rooting are listed in many of these reports and also in research papers. Malware can spread via interfaces and services unique to smartphones, including infrared, Near Field Communication (NFC), Wi-Fi-direct, Bluetooth, Short Message Service (SMS) and Multimedia Messaging Service (MMS). Kernel-level rootkits may be used to hide malicious user space files and processes, install backdoors and Trojan horses, log keystrokes, disable firewalls, antivirus software and Intrusion Detection Systems (IDS), and inclusion of the infected system into a botnet [46]. Several researchers think that there will be more sophisticated malware in the future [9]. As described by Vanja Svajcer [8] mobile malware has become a true threat to end users within the past few years. Examples of malware from 2004 to 2014 are presented in Figure 2.

Figure 2. 10 years of malware for mobile devices [8].

Another commonly described threat is related to the update process; it is possible that manufacturers of old devices will never apply patches to them or that the user does not install the patches, e.g., if the updating process is too difficult. For example in Finland, there are cases where markets are selling [47] phone models that will not receive any security updates [48]. These threats relate to all mobile device users, however this study is especially interested in threats related to the assets described in the section 9. 'Usage scenarios, actors and assets to be protected'. It is unlikely that high-level officials would have such an old smartphone model that it could not be upgraded. In the described usage scenarios the end user is a high-level official or a decision maker (e.g., working for governments or for a big organisation), they accesses sensitive or critical information with their devices, and/or for some reason, they do not follow properly the security policies of the organisation they are working for. Related studies exist, e.g., risk analysis of the Android platform in public safety and security (PSS) applications [49]. ENISA [17] rates risks, opportunities and recommendations according to consumers, employees and high officials.

Appendices in [45] include case studies to demonstrate some of the less obvious aspects of mobile device security. For example case study (5) describes how the iPad of a corporate executive was wiped and reset to factory defaults because the executive's young child had repeatedly entered an incorrect passphrase.

In [42], OWASP lists the following top ten mobile risks: 1) Weak server side controls, 2) insecure data storage, 3) insufficient transport layer protection, 4) unintended data leakage, 5) poor authorisation and authentication,

6) broken cryptography, 7) client side injection, 8) security decisions via untrusted inputs, 9) improper session handling and 10) lack of binary protection.

The following threats for corporate use of mobile devices are listed by CPNI in [50]: 1) physical compromise of a device, 2) logical compromise of a device, 3) user actions, 4) compromise of communications, 5) contamination of a device, 6) the compromised device used to pivot into the secure environment, and 7) bypass of security controls.

The following threats are described by ENISA in [17] to have either medium, high, or very high risk in usage scenarios related to high officials: 1) data leakage resulting from device loss or theft, 2) unintentional disclosure of data, 3) attacks on decommissioned smartphones, 4) phishing attacks, 5) spyware attacks, 6) network spoofing attacks, 7) surveillance attacks and 8) dialler-ware attacks. Other described threats have smaller risks in high-level officials' usage scenarios, or they do not relate to the assets described in the section 9. 'Usage scenarios, actors and assets to be protected'. It is claimed in [17] that, 8) dialler-ware attacks in which adversaries steal money from the user by means of malware that makes hidden use of premium SMS services or numbers, and 9) financial malware attacks have low likelihood and low impact in usage scenarios related to high officials.

The following risks coming from similar threats are described in report of OWASP and ENISA [21] [22]: 1) Unsafe sensitive data storage, attacks on decommissioned phones, and unintentional disclosure, 2) Spyware, surveillance and financial malware, 3) network spoofing attacks and surveillance, 4) unauthorised entities obtaining access to sensitive data or systems by circumventing authentication systems or by reusing valid tokens or cookies, 5) attacks on backend systems and loss of data via cloud storage, 6) data leakage because of malicious applications, 7) unintentional disclosure of personal or private information and illegal data processing, 8) unauthorised access to paid-for resources, 9) lack of security patches, updates and secure distribution, and 10) runtime interpretation of code giving an opportunity to provide unverified input to be interpreted as code. In addition to the described risks, [21] and [22] describe security controls to mitigate these risks. The described risks relate mostly to usage scenarios of consumers, but all of the described security controls should be considered for mitigating risks in usage scenarios of high-level officials.

In addition to these threats, the following are important for this study: An unauthorised entity gaining physical access to the mobile device, the user does not follow security policies and information leaks from computers to smartphones. All of the mentioned threats have relations, e.g., in real life if the unauthorised entity gains physical access to the device, usually it is much easier also to access wireless communication after reading Wi-Fi passwords from the device. All threats could be categorised under the four basic threat consequence types: unauthorised disclosure, deception, disruption, and usurpation. They have been presented in Table 1.

Table 1. Threat consequences [51]

Threat consequence	Description
Unauthorised disclosure	A circumstance or event whereby an entity gains access to information for which the entity is not authorised.
Deception	A circumstance or event that may result in an authorised entity receiving false data and believing it to be true.
Disruption	A circumstance or event that interrupts or prevents the correct operation of system services and functions.
Usurpation	A circumstance or event that results in control of system services or functions by an unauthorised entity.

The next sessions present the selected threats and attack trees with more details.

10.1. T1: Disclosure of information

Disclosure of information can be unintentional (accidental) or intentional (malicious).

Unauthorised disclosure is a circumstance or event whereby an entity gains access to information for which the entity is not authorised [51]. Disclosure of information can be unintentional, unauthorised, or both. When the revealed information is sensitive, the impact of unintentional disclosure might be high.

Users are not always aware of all the functionality of smartphone applications, e.g., cameras might add location coordinates to photos taken or social network service to messages [41].

Unintentional disclosure may be the result of, e.g., lending the mobile device to a family member. This scenario then goes under the next section. It can be also result of getting an unauthorised physical access to device, and, perhaps in the simplest case, disclosing information about locations where the user has visited. Sometimes it is also possible that disclosure of media access control (MAC) and Internet Protocol (IP) addresses happens, e.g., if it is possible to ping the device.

Information can leak also via the smartphone. Security researchers at Ben Gurion University have found a way to infiltrate a closed network to lift data from an isolated computer using little more than a cellphone's FM radio receiver. At MALCON 2014, security researcher Mordechai Guri with the guidance of Prof. Yuval Elovici from the cyber security labs at Ben Gurion University in Israel presented a breakthrough method ('AirHopper') for leaking data from an isolated computer to a mobile phone without the presence of a network [53]. A presentation of the attack can be watched [54].

The accelerometers in many smartphones could be used to decipher what you type into your PC keyboard — including passwords and email content — according to computer scientists at Georgia Tech [55]. The technique depends on the person typing at their computer with their mobile phone on the desk nearby. The vibrations created by typing onto the computer keyboard can be detected by the accelerometer of the phone and translated by a program into readable sentences with as much as 80 percent accuracy. [56]

10.2. T2: Unauthorised device usage

An example: a professor gives his work laptop to his granddaughter. This would be more common rather if he forgets the unlocked laptop at cafeteria where one of his students finds it and opens it. In both cases the unauthorised user (granddaughter or a student) has access to the device, however the impact might vary a great deal. If the professor is lucky, the granddaughter will just play installed games with the laptop and cause no real harm other than consuming battery. This could cause a short Denial-of-Service (DoS) attack if the professor has forgotten the battery charger. If the student is malicious, she could, e.g., try to access his records, modify teaching material, or just wipe everything on the laptop.

Mechanisms such as automatic locking of the device (M15), remote monitoring of user activities (M24, M27), multi-factor authentication (M5), etc. exist and are used in commercial products, as presented in the section 12.2. 'Existing countermeasures and security controls'. They provide mechanisms that prevent using it in wrong locations, at wrong time, or using it 'wrongly' and this prevents obtaining information for which the user is (perhaps) not authorised (M7, M24, M27). Usually these mechanisms are used only when the device is used to access sensitive material in email servers. These kinds of use cases have additional security controls and authentication mechanisms. In some cases it might be required that the unauthorised entity is not able to use the system at all, which means also common usage such as playing games, drawing, or surfing web pages. Several more advanced mechanisms to provide solutions for this threat exist, as described in the sections 12.2. 'Existing countermeasures and security controls' and 14. 'New countermeasures, security controls and recommendations'.

Attack trees have been presented in the following tables. The goal is described in the top cell, the attacks in the leftmost column, and subcategories, details and example attacks in the middle and right columns.

The attack tree in the Table 2 presents a case where no proper security controls exist after the adversary has gained an access to the device, and can use the device, start applications, etc.

Table 2. Attack tree of the actual data if there are no proper security controls after there is a possibility to use the device.

Goal: Do something nasty		
Gain unauthorised access to information.	Gain the possibility to use the device.	Login to a locked device, see Table 3.
Deceive an authorised entity receiving false data to believe it to be true.		Get an unlocked device, see Table 4.
Intercept or prevent correct operation of system services and functions.		Get a remote access to the device. See Table 6, Table 7 and Table 8.
Gain unauthorised control of system services or functions.		

One countermeasure against attacks related to unauthorised login is multi-factor authentication (M5).

Before the adversary can use the device as a normal user, there must be physical access to it and the adversary must have an unlocked device, receive the device in a state where login is already complete, or be able to login to the device. The attack tree in Table 3 presents attack vectors that can lead an adversary being able to login to a device they have physical access to. Some of the attacks in Table 3 relate also to a goal where an adversary needs to access sensitive data in encrypted storage instead of being able to login to the device. It is assumed that no multi-factor authentication has been used.

Table 3. Attack tree of login to a locked device.

Goal: Login to a locked device.		
Bypass locked screens.	Use other credentials to change or remove PIN codes or patterns.	Steal other credentials from external services.
	Use vulnerabilities in screen locking mechanisms.	Use emergency calls [57] or read unlock pattern from the screen surface.
Get access to user credentials inside the device.	Get and brute force credentials.	Use a previously installed malware able to access credentials and to send them to an external service to be processed.
		Access credentials stored in an unencrypted storage.
		Access credentials stored in an encrypted storage.
	Get credentials using side channel attacks.	Electromagnetic emission [58]
		Power monitoring attacks: Simple or differential power analysis [59]
		Acoustic cryptanalysis [60].
		Vibration attacks [56].
		Timing attacks
		Differential fault analysis
		Get credentials from the memory using cold boot attacks [61] .
Modify existing or add new user credentials to the device and use them to login.	Use exploits of certain vulnerabilities.	Use previously installed malware providing a remote connection.
		Use vulnerabilities in remotely connectable software running in the device.
Get pattern or PIN code from the screen.	Read fingerprints and patterns from the screen.	Smudge attacks [62].

	Spy credentials beforehand.	Shoulder-surfing [63] locally.
		Shoulder-surfing remotely using binoculars or other vision enhancing devices such as miniature cameras.
Use social engineering to get user credentials.	Use phishing [64] such as voice phishing, spear phishing [65], clone phishing and rogue Wi-Fi access points [66].	Man-in-the-Middle (MitM) attacks.
		Uniform resource locator (URL) obfuscation attacks.
		Cross-site scripting attacks.
		Clickjacking attacks [67].
		Pre-set session attacks.
		Observing customer data.
		Exploiting client-side vulnerabilities.
	Use pretexting [68].	Pretexting via phone.
		Pretexting via customer service, via delivery person, via tech support [69].
	Use baiting.	Baits in files [70], fake web sites [71], in social networks, etc.
Blackmail or torture to get user credentials.	Blackmail the user.	-
	Blackmail an admin or other people who can, e.g., reset the credentials.	-
Guess user credentials.	Collect information for the guesses. Combine this with social engineering.	Gather information about users credentials in other services and devices you are able to access. Perhaps the user has used the similar passwords or parts of passwords in them.
		Collect information about user's family, interests, hobbies, pets, favorite food, book, movies, etc.
		If possible, ask for hints from the device, sometimes they are easier than the actual password.
	Collect technical information about the authentication procedure	Discover if the device model has some requirements, e.g., for length of passwords, PINs or patterns.
		Discover if there are limits for login attempts.
		Discover if the password is case-sensitive or only numbers, etc.
Bribe to get user credentials.	Bribe the user.	-
	Bribe an admin or other people who can, e.g., reset the credentials.	-
Find written user credentials.	Collect information about the user's habits. Combine this with social engineering.	As urban legends tell, written credentials can be found, e.g., under the user's tables or from wallets.

10.3. T3: Unauthorised physical access into a device's memory and storage

The loss of mobile devices is increasing: Around 2% of British mobile phone users reported their mobile phones stolen in 2009 [72]. About 3.1 million American adult consumers were victims of smartphone theft in 2013, which was double the number stolen during 2012 [73]. Not only have normal consumers lost their devices but also government officials [29] [32] [33]. When a mobile device is stolen or lost, anyone who has physical access to it can potentially access all the information in the device, and expose the owner, contacts and the organisation to serious risk [74].

Losing or stealing the device is not only way to get unauthorised physical access to the device. Another way is buying a used device. ENISA describes a study in which mobile phones were bought second-hand on eBay, 4 out of the 26 business smartphones contained information from which the owner could be identified while 7 contained enough data to identify the owner's employer. As described, the research team managed to trace one smartphone to a senior sales director of a corporation, recovering a lot of information. [17].

If the device is not wiped before decommission (M30), it is possible for the adversary to access sensitive and/or personal information in the device, e.g., by using forensic tools.

This threat is closely related to data leaks resulting from device lost or theft. Tools and attack vectors used to access the data might be the same, however the adversary might be different. Some of the countermeasures such as remote wiping (M8) are suitable for both cases, however it should be noted that in some cases, if a device contains sensitive information, it should not be decommissioned at all but destroyed and recycled instead (M30).

An adversary with enough resources will most likely be able to access the data stored on a mobile device, even if the device is locked. Several different level attack vectors exist; from buying an old used device to stealing an unlocked device from the user, and even stealing a locked device from a physically locked car and afterwards accessing the password from memory with a cold boot attack [75] [76]. Poor encryption practices for mobile devices might lead to severe information leakage [10]. In some phone models encryption features have been claimed to be too poor for companies [77]. It should be noted that some phone models support hardware accelerated encryption (M43) only when using the device with specific enterprise security features [78]. This means that a normal user cannot enable all the security features without connecting the phone to an enterprise. In the event of a lost phone or tablet, many companies don't know what data is actually on the device, and because of this, the potential ramifications of lost mobile device can't be fully assessed [12].

Countermeasures against data leakage after the device is lost or stolen are encryption (M3), remote wiping and remotely locking the device (M8). Some of the existing applications, phone models and Mobile Device Management (MDM) systems providing such functionalities have been presented in the section 12.1. 'Existing guidelines, checklists and lists of security controls'.

Even if the adversary could not break the encryption of storage, she has several attack vectors to login into the device. Login can be done via hacking the pattern, password or personal identification number (PIN) code used in the device via a malicious software such as a key logger [79], via social engineering [80], via blackmailing via smudge attacks [81], or human error such as giving the device to be played, e.g., to a granddaughter. After a successful login, there might be consequences such as access to, modifying, or removing information for which the entity is not authorised, or even breaking parts of the device. These can be done accidentally or with purpose.

10.4. T4: Get physical access to the device

Before being able to login to the device or getting an unlocked device, the adversary must have a physical access to it. The attack tree for this is presented in Table 4. Similarly, before being able to physically break into the encrypted storage of the device, the adversary must have physical access to the device.

Table 4. Attack tree of getting a physical access to the device.

Goal: Get a physical access to the device.	
Steal the device.	Steal the device, e.g., from user's car or an apartment.
	Steal the device directly from the user.
	Steal the device from inside the organisation property.
	Steal the device from inside other properties.
Blackmail or torture to get the device.	Blackmail the user.
	Blackmail an admin.
	Blackmail a person working in a device repair organisation.
	Blackmail other people (e.g., a family member) who have physical access to the device.
Find the lost device.	Follow the user and make him/her to leave/miss the device.
	Randomly discover the lost device.
'Use' the device.	Access the device (without stealing it) when the user is not present.
Bribe to get the device	Bribe the user.
	Bribe the admin.

	Bribe a person working in a device repair organisation.
	Bribe other people (e.g., a family member) who have physical access to the device.
Get the device from the user	Ask the device from the user.
Get a decommissioned device	Buy the device second-hand.
	Find the device, e.g., from an organisation's recycle bin.

This threat can be mitigated, e.g., by training the user as well as security officers, administrators and support personnel in the organisation (M11).

10.5. T5: An unauthorised remote access to a device

There are several attack vectors leading to the compromise of smartphones, as presented in [82] [83] [10] [84] [85].

As described in [10], drive-by downloads have embraced mobile platforms, and just as any other device, mobile platforms are targeted by the vulnerability scanning capabilities of exploit kits. There is malicious code, worms and Trojans targeted to mobile devices. Mobile malware takes a significant part in malware statistics. Malware is increasingly targeting mobile platforms, with mobile Trojans coming in first. This is due to the increasing use of mobile devices, the increased sophistication of attacks but also due to the weaker/immature security mechanisms implemented on these platforms. An increased sophistication in malware has been reported, especially on mobile platforms. Code obfuscation and use of multiple channels are some characteristics of the complexity of malware. There is a growing market for stolen user data [86]. This means that information stealing malware is on the rise. Given the increased use of mobile devices and the sophistication of attacks, information stealing malware is here to stay. In 2013, for example, financial Trojans (e.g. Zeus, SpyEye, Citadel67) have been used to implement two-factor authentication attacks on mobile platforms [10]. In some cases the malware tries to infect both the PC as well as the smartphone used as a second channel for authentication in order to manipulate, e.g., online banking transactions [39]. When targeting high-level officials, the purpose is not necessarily directly money, but rather getting access to multiple authentication factors.

Malware may be used to send messages to premium-rate SMS services or to call premium numbers. Such attacks are called diallerware attacks. This way the adversary can steal money from the smartphone user indirectly, because the cost of these will be put by the operator to his/her phone invoice. Ransomware is another class of malware trying to get money from the user. This is done by restricting access to the phone and by demanding a ransom paid in order for these restrictions to be removed. In addition to these, financial malware attacks can be used to steal credit card numbers, or online banking credentials, e.g., by using key loggers or intercepting SMS authentication codes [17] [41]. Money theft is much more common with consumers than high-level officials and decision-makers: If the adversary gained access to the smart phone of a high-level official or decision maker, there would be more important information to be stolen than credit card numbers and it would not be wise to expose themselves via expensive SMSs or calls on the invoice. In addition to this, the impact of losing money is not as high for high-level officials and decision-makers than for consumers.

The ENISA report also mentions that mobile spyware applications might become strong tools for advanced persistent threats (APTs) targeting BYOD environments. It should be noted, that multiple espionage examples exist [87] [66]. For example, some devices might include preinstalled software which have strange behaviour [85].

The authors of [82] have listed attacks against mobile device under the following three categories: 1) attacks from the Internet, 2) infection from compromised PC during data synchronisation, and 3) peer smart-phone attack or infection.

This study is not interested in common mass targeted financial or spamming malware targeted with stealing money, e.g., by sending SMSs to costly numbers or sending spam. Instead, the study is interested in mobile remote access surveillance tools or Trojans (also called Spyphones) that are able to access everything in the phone, including their sensors. Such Trojans are sometimes used for parental control, however also for personal, corporate and governmental espionage.

In 2014, Kaspersky Lab presented research results from the Darkhotel (also known as Tapaoux) espionage campaign, which has been stealing sensitive data from selected corporate executives and high-tech entrepreneurs traveling abroad and staying in luxury hotels. The adversary seemed to know in advance when victims will arrive and depart from their high-end hotels. In Darkhotel, the adversary tricks the victim into downloading and installing a backdoor that pretends to be an update for legitimate software. This backdoor has been used to download more advanced theft tools to collect data. [66]

In Blackhat USA 2013 attacks against MDM systems [84] [88] [89] were presented. They showed how MDMs should disable access to secured information from 3rd party applications, but how they fail. Shaulov and Brodie have categorised such Trojans into three categories: 1) commercial surveillance tools, such as FlexiSpy, 2) customisable code which might be open source, 3) law enforcement tools such as FinFisher. Presented in Table 5 are the capabilities of tools in these three categories, which are approximately the same, however the infection vectors as well as the price differs.

Table 5. Properties of three mobile remote access Trojans (aka Spyphones) [89].

Capability	FlexiSpy	AndroRAT	FinFisher
Real-time listening on to phone calls	YES	YES	YES
Surround recording	YES	YES	YES
Location tracking via Global Positioning System (GPS)	YES	YES	YES
Retrieval of text	YES	YES	YES
Retrieval of emails	YES	YES	YES
Invisible to the user	YES	YES	YES
SMS C&C fallback	YES	YES	YES
Infection vector	Physical	Repackage	Exploit?
Cost	$279	Free	287000 €
Activation screen	YES	NO	NO

Other examples of such malware tools are DaVinci Remote Control Systems (RCS) by the Hacking Team, LuckyCat, Red October's mobile component, DarkComet Remote Access Trojan (RAT), XtremeRAT, BlackShades RAT, njRAT, HackingTeam RCS, ShadowTech RAT and Gh0st RAT.

FinFisher (also known as FinSpy) is marketed as spyware through law enforcement channels. It can be installed by exploiting vulnerabilities. These products have been sold to repressive and non-democratic states known for monitoring and imprisoning political dissidents [90], however there is always a risk that some hostile countries target these same products or copies of them against high-level officials and decision-makers of other countries or large organisations in other countries.

Containerisation can be bypassed with the techniques presented in Table 6.

Table 6. Attack tree of containerisation bypass

Goal: Bypass containerisation

Android: Listen events from logs, open up the heap, and search wanted information.	Use root privileges.
	Use ID of user that uses the secure container.
iOS: Get notified about events and pull related events from the UI class.	Load malicious dylib into memory and hook using standard Objective-C hooking mechanisms.

Before bypassing containerisation, the privileges have been escalated.

Table 7. Attack tree of privilege escalation.

Goal: Escalation of privileges		
Android: Remote control of sensors, read SMSs, manipulate clipboard, modify proxy settings, take pictures, record audio or video, etc.	Exploit advertisement libraries [91].	Exploit DNS vulnerabilities
Android: Root the device.	Exploit existing vulnerabilities in the OS.	
iOS: Install backdoors.	Load a malicious dylib using standard Mobile Substrate methods. Remove/hide any trace of the Jailbreak. Jailbreak detection mechanisms can be hooked or patched.	
Get credentials, etc	Exploit existing implementation-based or design-based vulnerabilities [44].	

Before privilege escalation, the device has been infected.

Table 8. Attack tree of infecting the device.

Goal: Infect the device	
Android: Make the user install a malicious application or install it through vulnerabilities.	Use phishing, see Table 3.
	Insert the application to market (e.g., Google Play store). Use two stage approaches to bypass security controls of Google Bouncer [83], turn any legitimate application into a malicious one without breaking an application's signature [92], or bypass certificate chain validation and inject malware into other applications [93].
	Use zero day vulnerabilities.
iOS: Jailbreak the device	Get physical access to the device, see Table 4.
	Use zero day vulnerabilities.

A backdoored application that looks and feels like the original app can be issued instructions and can send data to a Command and Control console via SMS. Payloads include grabbing a list of the installed apps and sending a text message to another device. Keep in mind that any Hypertext Transfer Protocol (HTTP) based communication can be monitored and even blocked by any devices at the perimeter but on the other hand any SMS based communication is only interacting with the mobile modem and thus bypasses any controls in the network. [94]

Anti-virus (AV) software (M22) and monitoring tools (M24, M27) have been used to detect malicious software and remote attacks.

10.6. T6: Social engineering attacks

Social engineering typically refers to psychological manipulation of people into performing wanted actions or getting confidential information from them.

As described in Table 3, social engineering can be used to get inside a locked device by using targeted phishing, pretexting and baiting attacks. In addition to these, social engineering includes diversion theft, quid pro quo,

tailgating (piggy-backing), and shoulder surfing attacks. This is a different type of attack than getting credentials to login to devices or installing malware to the mobile device.

Smartphones are a new type of device and users may not be aware of the fact that phishing is a serious risk on smartphones as well. Actually, phishing attacks are platform independent because the adversary does not need to attack the user's device in any way [41]. Phishing attacks can lead to user installing malicious applications, which can lead to privilege escalation and eventually bypassing secure containerisation.

As described by [10], mobile devices constitute main targets/channels to obtain user credentials: In this context social engineering approaches target users over various channels supported in mobile devices such as voice, instant and short messages and rogue apps, and these channels come to complement email as common phishing delivery method. [10]

Some spear phishing emails look so legitimate, that it is difficult for a user to assess whether they are unsafe and because of this, end users cannot reasonably be expected to have the capabilities to circumvent it [39]. Technical measures alone cannot solve this, in addition training is required.

Reasons why the risk of phishing is important for smartphone users have been described in [41]: 1) Smartphones have a smaller screen, which means that adversaries can more easily disguise trust cues that users rely on to decide on submitting credentials; e.g. cues that show whether the website uses Secure Socket Layer (SSL), 2) app-stores provide a new way of phishing by allowing adversaries to place fake apps in the app-store, disguising them as legitimate apps (such as 09Droid), and 3) smartphones provide additional channels that can be used for phishing, e.g. SMS (SMiShing). Users may be less cautious about SMS phishing messages [41].

Social engineering attacks can lead to any of the previous and following threats. The adversary may get passwords used for storage encryption (T3.), get an unlocked device (T2.2.) or credentials to login (T2.1.) or be able to access it remotely (T2.3.), or help in network spoofing (T7.), etc.

Possible proactive countermeasures against social engineering attacks is training (M11). Reactive countermeasures are AV (M22) and monitoring (M24, M27).

10.7. T7: Network spoofing attacks

In this case an unauthorised entity gets access to traffic sent/received by the system and does something wrong. This threat consequence may lead to or be a result of, for example, wiretapping/eavesdropping/listening, disruption, modification, corruption, interception of the traffic, different types of penetrations, dropping or delaying the traffic, or Man-in-the-Middle (MitM) attacks. Sensitive information (such as user location, International Mobile Station Equipment Identity (IMEI), International mobile subscriber identity (IMSI), unencrypted traffic, usage patterns) may be leaked, communicating partners may think the data is accurate and consistent even if it is not, etc.

Unsecured file transfers might lead to severe information leakage [10]. In [17], the likelihood of network spoofing attacks is described to be medium and their impact high, totalling the risk to be high.

Current mobile devices and other technologies have several countermeasures against network spoofing, implemented at different communication layers. Listing all of them is out of scope for this document, however some special cases such as using end-to-end encryption of Voice over IP (VoIP) calls and text messages, monitoring technologies (M20), tunnelling techniques such as Virtual Private Network (VPN) (M14), forcing proper Wi-Fi encryption (M17) and voiding malicious Wi-Fi access points (M9, M25), and disabling wireless interfaces (M33) when they are not needed will be shortly described in sections 12.1. 'Existing guidelines,

checklists and lists of security controls' and 12.2. 'Existing countermeasures and security controls'. Other mechanisms to provide mitigation mechanisms for this risk are described in sections 12.2. 'Existing countermeasures and security controls' and 14. 'New countermeasures, security controls and recommendations'.

10.8. T8: Lack of security patches, updates and secure distribution

It is possible that manufacturers of old devices will never apply the associated patches to them or the user does not install patches, e.g., if the updating process is too difficult. For example, markets in Finland have been selling [47] models of smartphones that won't get any security updates [48]. Android version fragmentation has been visualised, e.g., by OpenSignal [95] [96].

It has been claimed in [97] that 97% of top paid Android and 87% of top paid iOS applications, and 80% of the most popular free Android and 75% of the most popular free iOS applications have been hacked. It is also claimed that these numbers are not getting any lower.

In this study, the likelihood of having devices that can't be updated is assumed to be low. If the device has a modified OS, the likelihood that the updating process takes much longer than in devices using the newest OS version is high but the risks can be mitigated for some time until the patch is available to the modified OS version with additional security controls such as hardened security policies, and extra careful monitoring with existing intrusion prevention systems (IPSs) and IDSs. Insecure distribution is more likely, e.g., because of hijacked Wi-Fi access points or malicious cell towers.

Table 9. Android platform versions in October/November 2014 [98].

Version	Codename	Application Programming Interface (API)	Distribution
2.2	Froyo	8	0.6%
2.3.3-2.3.7	Gingerbread	10	9.8%
4.0.3-4.0.4	Ice Cream Sandwich	15	8.5%
4.1.x	Jelly Bean	16	22.8%
4.2.x		17	20.8%
4.3		18	7.3%
4.4	KitKat	19	30.2%

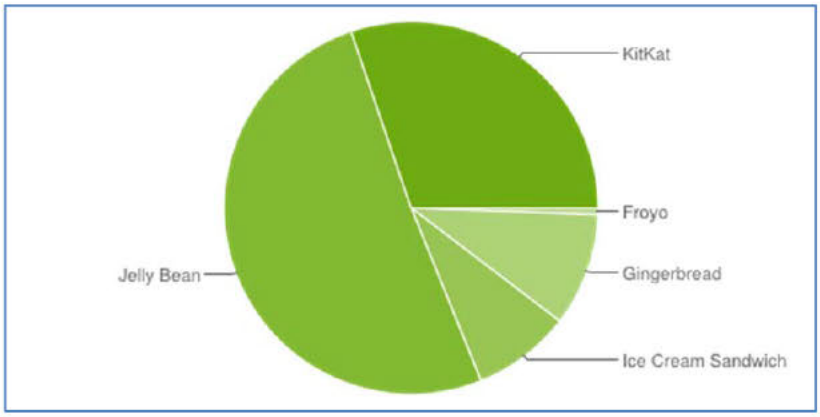


Figure 3. Android platform versions in October/November 2014 [98].

We should also mention that there are open source third party Read Only Memories (ROMs). For example, CyanogenMod is the most popular Android custom firmware with more than 10 million installations. At the

Ruxcon Security Conference in Australia, an unnamed security researcher revealed that CyanogenMod developers 'copy-pasted' Oracle's 'sample code for Java 1.5' and this puts Android devices with CyanogenMod at risk of MitM attacks.

Lack of security patches, updates and secure distribution can lead to decreasing security, e.g., by presenting bugs.

10.9. T9: Jailbreaking and rooting of devices

Jailbreaking and rooting and unlocking tools, resources and processes are constantly updated and have made the process easier than ever for end-users. Many users are lured to jailbreak their device in order to gain more control over the device, upgrade their operating systems (OSs) or install packages normally unavailable through standard channels. While having these options may allow the user to utilise the device more effectively, many users do not understand that jailbreaking can potentially allow malware to bypass many of the device's built in security features. The balance of user experience versus corporate security needs to be carefully considered, since all mobile platforms have seen an increase in malware attacks over the past year. Mobile devices now hold more personal and corporate data than ever before, and have become a very appealing target for adversaries. Overall, the best defence for an enterprise is to build an overarching mobile strategy that accounts for technical controls, non-technical controls and the people in the environment. Considerations need to not only focus on solutions such as MDMs, but also policies and procedures around common issues of BYOD and user security awareness (M11) [99].

10.10. T10: Personal, political and organisational reputation

Losing reputation is possible, because it can be the result of many other threats that have been realised. For example, disclosure of sensitive material unintentionally or intentionally, exposure of sensitive data to unauthorised entities, losing the device in insecure locations, or using the mobile device maliciously instead of as an authorised user, can lead to a decrease in personal, political and organisational reputation.

A way to plant false evidence such as call records, locations, etc. on the smartphone is described in [100]. The scenario is to put decoy data such as innocent numbers on the smartphone, so that the real data escapes forensics. This technique can work also vice versa just to plant false evidence in a way to harm someone's reputation for example plant compromising material in a victims smartphone. Presumably it will be an arms race between programs like this and programs that harvest data from your phone.

10.11. T11: Denial-of-Service (DoS) attacks

Mobile devices have limited resources and are vulnerable to DoS attacks [101].

DoS attacks can be categorised into the following: 1) consumption of computational resources such as bandwidth, memory, disk space or processor time, 2) disruption of configuration information such as routing information, 3) disruption of state information such as unsolicited resetting of TCP sessions, 4) disruption of physical network components, and 5) obstructing the communication media between the intended users and victim so that they cannot communicate adequately [102]. In smart phones, DoS attacks might be caused by jamming radio channels, with MMS message flooding and incoming phone call flooding attacks, battery exhaustion attacks [103] or disabling the smartphone by using smartphone blocking functions.

DoS attacks can be targeted also against systems such as Domain Name System (DNS), and cause serious problems in the usage of mobile device. Several services such as DNS, Network Time Protocol (NTP), Character

Generator Protocol (CHARGEN), Quote Of The Day (QOTD), Kad, and Quake Network Protocol can be exploited to act as reflectors in distributed DoS (DDoS) attacks [104]. DDoS attacks have been categorised in [105].

DoS may also be the result of malicious or incidental usage of the device after getting physical access into a device, and locking or wiping it due to too many failed login attempts.

Mitigation mechanisms against DoS attacks in mobile devices are, e.g., host-based firewalls (M38), IDS and IPS (M27).

11. Risk analysis

Risk is the product of the likelihood and the impact of a threat against the information asset of an organisation or an individual [106].

This study uses the following risk value scheme; likelihood, impact and risk have values Very Low (1), Low (2), Medium (3), High (4) and Very High (5). The risks were determined by indicating the likelihood (from very low (1) to very high (5)) and impact (from very low (1) to very high (5)) of each risk.

The risk analysis is based on the threats T1-T11 described in section 10. 'Threats', and is done by 5 members of NATO CCDCOE.

Table 10. Identified threats and their estimated likelihood and impact.

Threat	Description	Likelihood	Impact
T1.	**Disclosure of information.**	4,00	5,00
T1.1.	- Unintentional disclosure of information.	4,20	4,60
T1.2.	- Intentional disclosure of information.	2,80	5,00
T2.	**An unauthorised use of the device.**	1,50	5,00
T2.1.	- Login to a locked device.	1,20	5,00
T2.2.	- Get an unlocked device.	2,00	5,00
T2.3.	- Get a remote access to the device.	2,20	4,80
T3.	**Unauthorised physical access into a device (memory, storage, etc.).**	2,25	4,00
T4.	**Get a physical access to the device.**	3,00	3,25
T4.1.	- Steal the device.	2,80	3,60
T4.2.	- Blackmail or torture to get the device.	1,00	2,80
T4.3.	- Discover the lost device.	2,00	3,00
T4.4.	- Use the device when the user is not present.	1,00	3,20
T4.5.	- Bribe to get the device.	1,00	3,20
T4.6.	- Get the device from the user by asking it.	2,60	2,80
T4.7.	- Get a decommissioned device.	1,20	2,80
T5.	**Unauthorised remote access to a device. (See T2.3.)**	2,20	4,80
T5.1.	- Bypass containerisation.	2,00	5,00
T5.2.	- Escalate privileges.	2,20	5,00
T5.3.	- Infect the device.	3,00	4,20
T6.	**Social engineering attacks.**	3,25	4,00
T.6.1.	- Attacks via phishing, voice phishing, spear phishing, clone phishing, rogue Wi-Fi access points.	3,40	4,00
T6.2.	- Pretexting attacks, e.g., via phone, customer service, delivery persons or tech support.	3,00	3,60
T6.3.	- Baiting attacks via baits in files, fake web sites, social networks, etc.	3,00	3,80
T7.	**Network spoofing attacks.**	3,00	4,20
T8.	**Lack of security patches, updates and secure distribution.**	1,80	5,00
T9.	**Jailbreaking and rooting of devices**	2,40	2,80
T10.	**Reputation of the user**	2,40	3,60
T11.	**DoS attacks**	2,60	2,00

There are several ways to calculate the total risk. One of the simplest ones is multiplying values of likelihood and impact, and use thresholds for risk levels (e.g., 5 or larger for medium level and 15 or more for high level. It should be noted that the readers of this study are encouraged to carry out their own risk assessments and weigh the risks against the potential benefits in their own specific usage scenarios.

As can be seen from the Table 10, there are several threats having high likelihood and/or impact. The following sections give examples of ways to mitigate these risks. Certain threats, such as financial malware described in section 10.5. 'T5: An unauthorised remote access to a device' had low likelihood and low impact, so specific mitigation mechanisms against it weren't analysed, although AV software and monitoring tools can be used to detect such malware. The same with T4.2., blackmailing and torturing of the user, T4.4. using the device when

the user is not present, and T4.5. use of bribery to obtain the device. These threats have lower likelihood and impact than several other threats, so their mitigation mechanisms have not been analysed.

Figure 4. presents the attack tree and relationship of threats at high level.

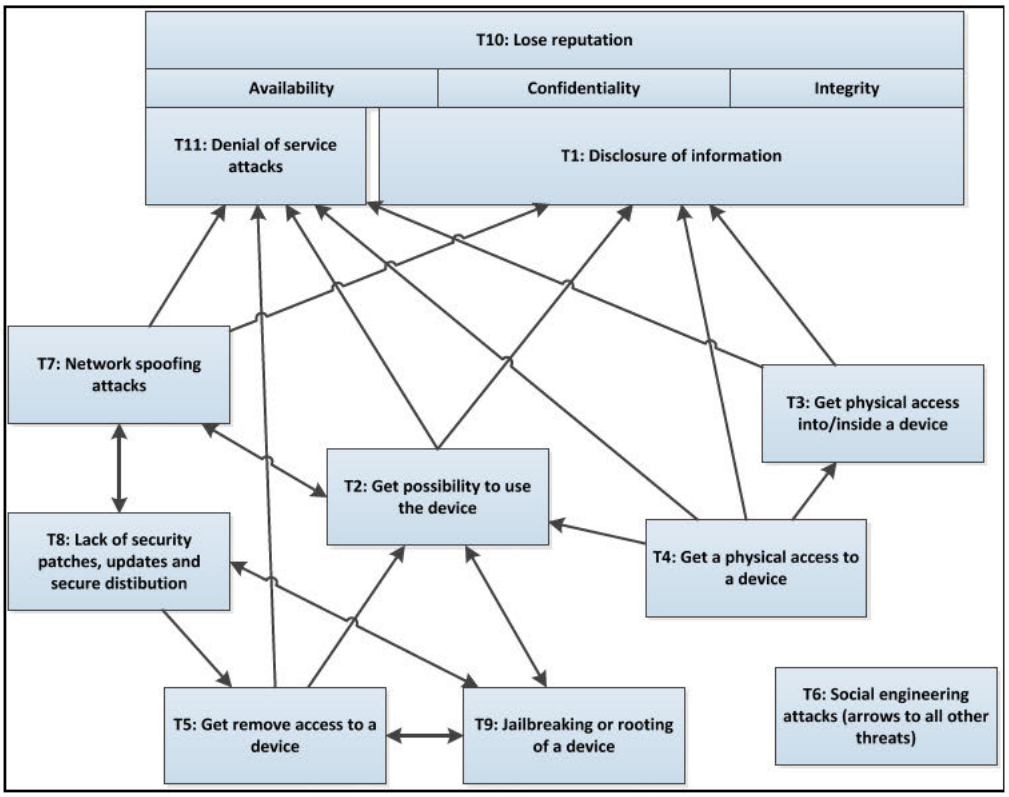


Figure 4. Overview of the attack tree.

As it can be seen from Figure 4, there is no point mitigating only one or few of the presented threats, because of the connections between them.

12. Literature Review

This chapter is divided into different sections. The first section gives examples from existing guidelines, checklists and security controls lists. The second section gives an overview of existing security controls already used in commercial secure mobile devices. The third section discusses security controls and countermeasures which have been presented by researchers but which have not been widely deployed in commercial products.

12.1. Existing guidelines, checklists and lists of security controls

Several common guidelines and precautions for securing mobile devices exist. All of these mechanisms mitigate the risk of lost and stolen devices already exist in commercial mobile phones and applications. These risk mitigation mechanisms do not affect only high-level officials, but also common consumers.

12.1.1. National Institute of Standards and Technology (NIST)

NIST Special Publication 800-124 [11] includes guidelines for managing the security of enterprise mobile devices. Some specific examples such as performing vulnerability scans and penetration tests are mentioned. The mitigation strategy for securing mobile devices in locations outside the organization's control is layered; the first layer involves requiring proper authentication, the second layer involves protecting sensitive data (M1, M2, M3), and the third layer involves user training and awareness (M11). Organisations should assume that all mobile devices are untrusted unless the organisation has properly secured them and is able to monitor their security continuously while in use with enterprise applications and data [11].

12.1.2. SANS Institute

SANS's monthly OUCH! security awareness newsletter for computer users lists using PIN codes, passwords, pattern locks, remote tracking and wiping, encryption, backups as effective precautions, and gives four step to follow if a device is stolen: 1) reporting the lost or stolen device (M11), 2) tracking the device (M7) or wiping the data from it (M8), 3) contacting network service or phone providers (M9, M11), and 4) recovering data from backups to a replacement device (M10, M21) [74].

SANS provides guidelines for creating policies for the use of handheld devices in corporate environments [20], critical security controls (CSCs) [107], security checklists for mobile devices [19] and guidelines for improving user awareness [24]. SANS' security checklist for mobile devices version 1.3 [19] includes procedures and descriptions related to developing and evaluating use cases, performing risk assessment (M32), reviewing and updating policies (M32), training and awareness programs (M11), considering COPE and/or BYOD models (M28), sandboxing (M18), configuration profiles (M42), validating minimum security settings, lifecycle processes, and antivirus/malware protection (M22). The same document includes checklists for policies, lifecycle, security settings, applications, COPE, and for BYOD. For example, the 5th procedure in the Policies checklist proposes evaluating forensic examination (M29) before and after foreign travel, and the 18th procedure in the same checklist describes that sensitive data should be minimised and deleted when not needed, and sensitive information stored on the device should be off-loaded to the PC and deleted from the handheld device, if possible (M2).

SANS CSC 3 [18] describes security controls for hardware and software on mobile devices, laptops, workstations, and servers. The first security control CSC 3-1 is to establish and ensure the use of standard secure configurations of the OSs by configuring, validating and updating images of the OS. Hardening should be used and it is described typically to include 1) removal of unnecessary accounts such as service accounts (M31), 2) disabling or removal of unnecessary services (M31), 3) configuring non-executable stacks and heaps (M33), 4) applying patches (M16), 5) closing open and unused network ports (M13), 6) implementing IDSs and/or IPSs (M27), 7) use of host-based firewalls (M35) [18]. Using secure images (M10, M16, M21) enable quick wiping and installation, or giving a new clean device for the user every day (M19, M53). This relates to the fourth

security control CSC 3-4 which describes that compromised systems should be re-imaged with the secure build. Implementing automatic patching tools and processes (CSC 3-2) must be thought out carefully, because there might be use cases where updates include other vulnerabilities or do not work correctly, e.g., with other software in devices. Therefore, it might be sometimes be required that system administrators do manual remote updating and the system does not update itself automatically (M16). It is described in CSC 3 [18] that rather than starting from scratch, organisations should start from publicly developed, vetted, and supported security benchmarks, security guides, or checklists such as the Center for Internet Security Benchmarks Program [108] or the NIST National Checklist Program [109]. In addition to deploying security controls described in CSC 3, the organisation should measure the effectiveness of their automated implementation and gather information from technical sensors [18].

SANS CSC 17 [110] describes security controls for data protection. The first is deploying approved hard drive encryption software to mobile devices and systems that hold sensitive data (M3, M6). The same applies to memory cards and internal memory used in smartphones.

As described in [24], computers are used to store, process and transfer data valuable to organisations. Because of this, they have been the primary target for cyber adversaries. To protect against attacks, numerous technical papers have been released on how to secure or harden OSs. Cyber adversaries have shifted their focus away from targeting computers to targeting people because this attack vector is easier. The paper compares 'humanOS' to other OSs, and gives examples how to improve security awareness and human behaviour to be more secure (M11) [24].

12.1.3. European Network and Information Security Agency (ENISA)

ENISA describes the following opportunities for securing smartphones: 1) sandboxing (M18) and capability-based access control models (M34), 2) controlled software distribution (M16), 3) remote application removing (M23), 4) convenient backup and recovery functions (M10), 5) additional authentication options such as smartcards (M5), 6) additional encryption of voice calls (M20), and 6) diversity of hardware and software. For high-level officials, ENISA presents the following recommendations: 1) do not store sensitive data locally (M2) and allow online access to sensitive data from a smartphone using a non-caching application (M2), 2) encrypt calls and SMS for end-to-end confidentiality (M20), and 3) wipe smartphones periodically (M21) and reload them with a specially prepared and tested disk images (M21) [17].

12.1.4. Finnish Communications Regulatory Authority

The Finnish Communications Regulatory Authority has guidelines for securing mobile devices, the first set of these guidelines [111] contains the following six pieces of advice: 1) use a code or pattern to lock the phone, 2) enable automatic locking with proper delay (M15), 3) use passwords that are good enough, e.g. the PIN code can be more than four numbers, 4) setup the phone to not show notifications of SMSs, instant messaging (IM), news, etc. on the screen when the phone is locked, 5) update the phone OS and applications to the newest versions frequently (M16), and 6) download applications only from reliable sources (M16).

The second set of guidelines [112] contains the following six general advisories: 1) be careful when using cloud services, 2) enable remote alarm, locking and wiping services (M8), 3) remove personal information from the phone when selling, disposing or returning it (M30), 4) be careful when buying a used phone, 5) be aware that there is malware also for mobile phones and 6) buy a new phone after the manufacturer stops updating the phone.

The third set of guidelines [113] by the Finnish Communications Regulatory Authority gives the following advice: 1) encrypt the phone's memory and the memory card (M3), 2) enable wireless interfaces, such as Wi-Fi, Bluetooth, NFC and the Global Positioning System (GPS), only when they are needed (M13), 3) use AV software (M22), 4) root the device only if you know what you are doing, 5) use VPN-connections when you use the

phone in open WLANs or in foreign countries (M14), 6) use MDM systems for management of mobile devices (M23) and VPN connections to secure reading of emails (M14).

12.1.5. Communications-Electronics Security Group (CESG)

CESG has a collection of guidelines [114] for securing mobile devices. There are different guidance documents for enterprises [115], different OSs, application development, and for third party applications [116]. With these guidelines, CESG assists organisations with understanding the risks associated with deploying certain devices in their networks, and to describe mitigation mechanisms which can be applied to manage these risks [117].

It is mentioned [117] that CESG strongly recommends not using BYOD and if such are used, the user needs to be made aware that they will be handing over full management and control to the department and all existing data on the device will be wiped.

Sophos provides a MDM and CESG guidelines [117] concentrating on Sophos Mobile Control (SMC) in UK government organisations.

CESG lists 12 general security recommendations for mobile end user devices working with OFFICIAL information or with BYOD products [118]: 1) assured data-in-transit protection (M14, M20), 2) assured data-at-rest protection (M2, M3), 3) authentication (M4), 4) secure boot (M35), 5) platform integrity and application sandboxing (M18), 6) application whitelisting (M26), 7) malicious code detection and prevention (M22), 8) security policy enforcement (M46), 9) external interface protection (M13), 10) device update policy, 11) event collection for enterprise analysis (M23, M24, M27), and 12) incident response (M27).

12.1.6. Centre for the Protection of National Infrastructure (CPNI)

CPNI [119] provides information and security guidelines for a range of mobile devices, for implementers [45], for managers [120], and a briefing for executives [121].

CPNI and MWR InfoSecurity mention in [50] that it is strongly recommended that jailbroken devices are not allowed to access corporate resources and that all employees are made clearly aware of this fact.

The following solutions have been described [50]: 1) incident management including incident response procedures and policies and training of the users to understand the procedure following the incident (M11), 2) secure software distribution (M16) including prevention of installation of third-party applications to COPE devices and training of the user if allowed to access application marketplaces (M11), 3) access to only certain part of the data (M34), e.g., allowing management staff to access only a graph of changes in sales figures in their iPad, but not gain access to the actual data, 4) technical controls including MWR's security guide for implementers.

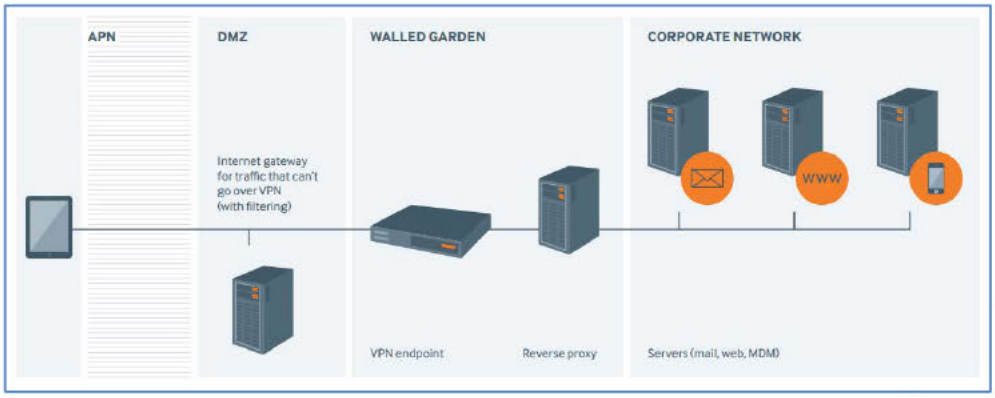


Figure 5. Model for secure mobile access to corporate resources [50].

12.1.7. Open Web Application Security Project (OWASP)

The OWASP Mobile Security Project has listed top ten mobile risks, it provides information and guidelines for developers to secure different platforms and to build secure mobile applications, and it gives its top 10 mobile security controls.

The following security controls are listed as the top 10 mobile controls by OWASP [122]: 1) identify and protect sensitive data, 2) handle password credentials securely on the device (M6), 3) ensure sensitive data is protected in transit (M14, M20), 4) implement user authentication, authorisation and session management correctly (M4, M5, M6), 5) keep the backend services and the server secure, 6) secure data integration with third party services and applications, 7) pay specific attention to the collection and storage of consent for the collection and use of the user's data, 8) implement controls to prevent unauthorised access to paid-for resources (wallet, SMS, phone calls, etc.), 9) ensure secure distribution/provisioning of mobile applications (M16), and 10) carefully check any runtime interpretation of code for errors. All of these include several security controls.

OWASP gives guidelines for securing the storage to follow [123]:

- Keep only the sensitive data that you need (M2), many eCommerce businesses utilise third party payment providers to store credit card information for recurring billing. This offloads the burden of keeping credit card numbers safe.

- Only use strong cryptographic algorithms (M17), use approved public algorithms such as Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA) public key cryptography, and Secure Hash Algorithm (SHA)-256 or better for hashing. Do not use weak algorithms, such as MD5 or SHA1. Note that the classification of a 'strong' cryptographic algorithm can change over time. The Cryptographic Algorithm Validation Program (CAVP) in [124] is a good default place to go for validation of cryptographic algorithms.

- Ensure that random numbers are cryptographically strong and ensure that random algorithms are seeded with sufficient entropy (M6).

- Only use widely accepted implementations of cryptographic algorithms, so do not implement an existing cryptographic algorithm on your own (M17).

- Always ensure data integrity and authenticity. Use cryptographic cipher modes that offer both confidentiality and authenticity via Authenticated Encryption (AE) mode under a uniform application programming interface (API) (M17). Recommended modes include improving cipher block chaining message authentication code (CBC-MAC) mode with a counter (CCM) [125] mode, using Galois/Counter Mode (GCM) [126] and Offset Codebook (OCB) [127] mode.

In the third bullet, it would be possible to use also additional hardware to generate random numbers (M17, M43), e.g., as in [128].

12.1.8. Other guidelines and recommendations

Arxan proposes in [97] the following security controls relevant to high officials and decision-makers: 1) all applications should be built in a way that maintains the confidentiality of the application/code, 2) high-value mobile applications should include Runtime Application Self-protection (RASP), 3) software that is used to enable mobile wallets and payment applications should be protected with secure crypto (M6) and application hardening, 4) determining if existing applications are exposed to risks that are unique to mobile environments, including penetration testing (M12), exploring vulnerabilities from reverse-engineering and tampering, application repackaging, intellectual property and data theft exposure, cryptographic key exposure (M6), and system compromise.

WebRoot recommends in [129] that companies follow the following four recommendations: 1) establish device control policies, 2) enforce device-level security, 3) develop and deliver mobile workforce security training and 4) let business drive mobile device security policies and training.

Palo Alto Networks [130] lists 10 things that a firewall should do: 1) identify and control applications on any port, 2) identify and control circumventors, 3) decrypt outbound SSL and control Secure Shell (SSH), 4) provide application function control, 5) systematically manage unknown traffic, 6) scan for viruses and malware in all applications, on all ports, 7) enable the same application visibility and control for all users and devices, 8) make network security simpler with the addition of application control, 9) deliver the same throughput and performance with application control fully activated and 10) support the exact same firewall functions in both hardware and virtualised form factors. It should be noted, that it is not possible to run all such functionalities in firewalls of mobile devices.

It should be noted that there exists a huge amount of additional security controls, guidelines and checklists in addition to the ones reviewed in this study.

12.1.9. Summary of review of existing recommendations

The mitigation techniques found from the guidelines, checklists, and security controls can be categorised under the mitigation technique groups presented in Table 11. Mitigation mechanisms have been numbered with character M and a number. The main threats that it mitigates directly is listed in the end with T1-T11.

Table 11. Recommended or used mitigation techniques.

	Mitigation technique
M1.	Classifying data and data segregation. (T1, T10)
M2.	Not storing sensitive data locally but storing it to servers (and securing communications). Includes online access to sensitive data using a non-caching applications. (T1)
M3.	Encrypting the storage medias of the device. (T1, T3)
M4.	Common authentication mechanisms (PIN codes, passwords, patterns, etc.): User to device, device to service and user to service. (T1, T2)
M5.	Multi-factor authentication and extra authentication options. (T1, T2)
M6.	Handling and storing credentials securely in key-stores, crypto modules, secure elements, Trusted Platform Modules (TPMs), encrypted and/or hashed, and making sure they have enough entropy. (T2, T3)
M7.	Tracking the location of the device remotely. (T1, T2, T3)
M8.	Wiping the data from and/or locking the device remotely. (T1, T2, T3)
M9.	Disabling the phone from joining the networks by network service or phone providers. (T5, T7, T8, T11)
M10.	Secure recovery and backup procedures. (T4)
M11.	Training the user(s): security awareness, training and awareness programs, training incident response procedures and policies. (T1-T11)
M12.	Discovering vulnerabilities in the device and systems, e.g., with penetration testing to mitigate exploits. (T5, T6, T7)
M13.	Disabling unnecessary interfaces when they are not needed. Protecting external interfaces. (T5, T7, T9, T11)
M14.	VPN connection to secure communications. (T1, T7, T8, T11)
M15.	Automatic locking of devices. (T1, T2)
M16.	Updating and patching the device securely frequently or when needed, controlled software distribution, e.g., only from reliable sources. (T8)
M17.	Use well known, well tested and strong cryptographic algorithms and appropriate key lengths and enough entropy (randomness) and enforce the system to use them. (T3, T5, T2, T7)
M18.	Sandboxing , virtualisation and concealing to isolate software and data. (T5, T6)
M19.	Ensure secure distribution and provisioning of devices. (T8)
M20.	End-to-end encrypting communications (SMS, voice, video). (T1, T7, T10)
M21.	Scheduling of deletion of data such as sensitive personal data, periodic reloading and wiping of devices and reloading with specially prepared and tested disk image. (T5, T9)
M22.	Antivirus software. (T5)
M23.	Asset management, catalogues, MDM, Enterprise Mobility Management (EMM) and Mobile Application Management (MAM) solutions, and their features such as remote application removal. (T1, T2, T5, T8, T9)
M24.	Data loss prevention (DLP) including, e.g., implementing containers, scanning and monitoring to check for clear-text storage of confidential data and monitoring for the distribution of confidential data internally and to third parties. (T1, T10)
M25.	Avoiding malicious Wi-Fi access points by configuring individual laptops with the user's home Wi-Fi credentials, using 3G/4G dongles in laptops or providing new wireless access point connected by Ethernet cable to user's home access

	point. (T1, T5, T7, T8)
M26.	Application security by whitelisting and reputation checking. (T5, T6)
M27.	Event collection for enterprise analysis, including monitoring logs for attacks, security breaches and suspicious user behaviour. IDS, IPS, incident response, etc. (T1, T2, T5, T8, T9)
M28.	Considering alternative device ownership models (BYOD, COPE, something between?). (T1)
M29.	Forensics examinations. (T1, T2, T3, T5, T7)
M30.	Secure decommission, wiping, destroying, recycling, etc. (T1, T2, T3)
M31.	Disabling or removing unnecessary accounts, services and applications. (T1, T2, T5)
M32.	Risk assessment. Reviewing and updating policies. (T2, T4, T6)
M33.	Configuring non-executable stacks and heaps. (T2, T5)
M34.	Access control systems, such as capability-based access control models. (T2, T5)
M35.	Secure boot. (T1, T2, T3)
M36.	Encrypt (sensitive) data. (T1)

The following section presents existing countermeasures and security controls used in commercial products.

12.2. Existing countermeasures and security controls

Normal widely used consumer mobile and smartphones do not necessarily follow the guidelines or use the security controls presented in the section 12.1. 'Existing guidelines, checklists and lists of security controls'. In addition to this, they have not been designed with privacy in mind [131]. OS hardening, using additional frameworks for enforcing security policies or specific monitoring software might be done only after rooting of devices. Another possibility is to use a device that already has support for additional security controls. Such specialised smartphones or OSs targeted to security are available on a number of markets [132] [133] [134] [135] [136] [137] [138] [139] [140] [141] [142] [143] [144], as is specialised security software, e.g., to encrypt voice conversations [145], messaging [146], or to manage mobile devices, specialised secure laptops [147] and devices such as Solid State Drives (SSDs) [148] or memory cards [149] [150] [151] [152] to be attached to laptops and/or mobile phones.

The Internet is an insecure network and one effective solution to secure it is encryption. On the other hand its common knowledge that everything that's going on 'air' is not secure, and there will always be a way to decrypt data despite the strength of the algorithm. So why bother? Why do we need to encrypt data at all?

One simple answer to this question comes from the information value over time perspective. Even the most important information can be useless after a crucial moment. So although encryption will never be totally secure, it can delay the adversary for a period of time in which classified information is self-unclassified and become almost useless.

12.2.1. Secure storage and data encryption

Information or data at rest is an Information Technology (IT) term referring to inactive data which is stored physically in any digital form (e.g. databases, data warehouses, spread sheets, archives, tapes, off-site backups, mobile devices etc.). It is used as a complement to the terms Data in Use and Data in Motion.

Mobile devices store a huge amount of information. When taking these mobile devices outside the organisational perimeter, they become more vulnerable and the information stored within is likely to be stolen. Mobile devices are often subject to specific security protocols to protect Data at Rest from unauthorised access when lost or stolen and there is an increasing recognition that database management systems and file servers should also be considered as at risk. The longer data is left unused in storage, the more likely it might be retrieved by unauthorised individuals outside the network.

There are several ways to protect the information stored in devices. The most common are: 1) data encryption (M36), 2) restrict access to the device, and 3) MDM (M23).

There are several reasons to encrypt the data in devices, however you must encrypt sensitive data. As described in the section 12.1. 'Existing guidelines, checklists and lists of security controls', only well known, well tested and strong cryptographic algorithms should be used with appropriate key lengths and with enough entropy in the keys (M17). Mobile device encryption could be done by software or hardware.

Data encryption, which prevents data visibility in the event of unauthorised access or theft, is commonly used to protect Data in Motion and increasingly recognised as an optimal method for protecting Data at Rest.

But encryption is not a solution in itself. There are several issues to consider regarding encryption. First of all the most obvious things: what data should be encrypted? Maybe it is not necessary to encrypt every piece of data inside the device. So then how do we know what data should be encrypted? The use of a policy regarding the use and how data should be stored in the device could help in this matter. The second issue is what encryption method should be used? The encryption of data at rest should only include strong encryption algorithms and proper encryption modes. Encrypted data should remain encrypted when access controls such as usernames and passwords fail. Increasingly encryption on multiple levels is recommended.

The third issue is key management: How do you manage the keys? Keys should be managed properly to ensure that they are delivered to the right users, and to the right devices. A mechanism to change and renew the keys must be established.

Additional security controls have also been added to specific components used in laptops and/or in mobile phones. The first example is SSD drives that can self-destroy (M40) or be destroyed remotely by sending an SMS to the drive [148]. If the drive works as is described, if provides additional security controls but also introduces new threats such as the possibility to explode the drive if the laptop is neglected to be plugged into a charger. The second example is memory cards containing additional cryptographic modules (M6).

TrustChip [151] [153] is a microSD card which has an encryption engine with a crypto processor. It provides key management, encryption and authentication, and it is described as tamper resistant. This microSD has been used for securing VoIP calls, SMS messaging and encrypting files before storing them to clouds and decrypting encrypted files after downloading them from the cloud. Certgate's Protector memory cards provide similar functionality, however on BlackBerry devices they only encrypt emails [149]. Crypto AG's Crypto Mobile HC-9100 seems to work only with Samsung Galaxy S4 Mini and a number of Nokia (today Microsoft) phones [150]. SecuSmart and SecuSUITE [154] are microSD. There is a miniature computer integrated into the micro-SD card which contains the NXP SmartMX P5CT072 crypto-controller with a PKI coprocessor for authentication. An additional high-speed coprocessor encrypts emails, text messages, and voice communication using 128-bit AES, however the used mode of operation is not described. [152] SecuSUITE gives an additional security control when using the card in BlackBerries: It secures the keys used by the BlackBerry to encrypt the phone's business partition, and if the card is removed from the phone, the keys are no longer available. This also means that business partition with installed applications and existing documents can no longer be accessed [155].

Using this kind of memory card provides additional security especially for devices which do not have much computing power. In addition to hardware based encryption, decryption and integrity checking (M43), some of these products offer secure storage (M6). Separate memory cards with cryptographic functionalities have similarities to military products which are attached, e.g., to radio transmitters or mobile phones to enable secure communication only between devices having the similar product attached and configured properly.

It should be noted that hard disk (or storage media) encryption must be complete and Trusted Platform Module (TPM) must be used with a password [45].

12.2.2. Securing communication

Various types of cryptographic systems exist that have different strengths and weaknesses. Typically, they are divided into two classes; those that are strong, but slow to run and those that are quick, but less secure. Most

often a combination of the two approaches is used (such as SSL), whereby we establish the connection with a secure algorithm, and then if successful, encrypt the actual transmission with the weaker, but much faster algorithm [156].

We have the possibility to encrypt or otherwise protect data at different layers/levels, a) application, b) protocol and/or c) network. Choosing the right place for this to occur can involve looking at both security as well as resource requirements.

12.2.2.1. End-to-end encryption at the application layer

At the application layer, the actual application performs the encryption or other crypto function. This is the most desirable, but can place additional strain on resources and create unmanageable complexity. Encryption would be performed typically through an API such as the OpenSSL [157] toolkit or OS provided crypto functions.

An example would be an Secure/Multipurpose Internet Mail Extensions (S/MIME) encrypted email, which is transmitted as encoded text within a standard email. No changes to intermediate email hosts are necessary to transmit the message because we do not require a change to the protocol itself. Several applications for allowing end-to-end encryption of messages and VoIP call exist [146].

One application providing end-to-end encryption is Dencrypt [158] which secures mobile communication using dynamic encryption. The Dencrypt solution consists of a Communication Server located either at the customer site or hosted by Dencrypt. It is a turn-key solution and no additional configuration of the server or infrastructure is necessary.

The Communication Server's function is to establish a connection between two users. Users can be divided into groups for control and external partners can be invited into the Dencrypt system and their contacts can be fully controlled.

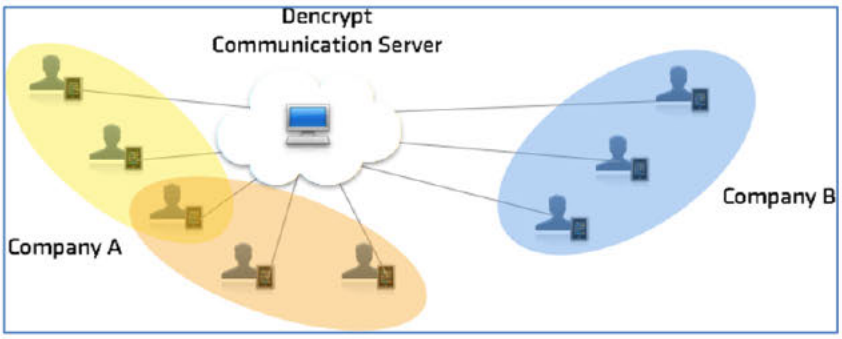


Figure 6. Overview of Dencrypt [158].

The Dencrypt solution is based on VoIP technology and applications for iOS, Android and Windows. Conversations are encrypted from smartphone to smartphone making it impossible for a third party to listen. No extra hardware is necessary because it works with the users private and company smartphone.

Dencrypt uses dynamic encryption developed in cooperation with Danish Technical University (DTU). Dynamic encryption utilises new encryption algorithms for each mobile call, adding an additional layer to the standard AES encryption scheme. After each mobile call both the randomly selected algorithm and encryption key are destroyed and the content of the call cannot be recreated.

12.2.2.2. Encryption at the protocol layer

At the protocol layer, the protocol provides the encryption service. Most commonly, this is seen in HTTP Secure (HTTPS), using SSL encryption to protect sensitive web traffic. The application no longer needs to implement secure connectivity. However, this does not mean the application has a free ride. SSL requires careful attention when used for mutual (client-side) authentication, as there are two different session keys, one for each direction. Each should be verified before transmitting sensitive data.

Adversaries and penetration testers use SSL to hide malicious requests (such as injection attacks for example). Content scanners are most likely unable to decode the SSL connection, letting it pass to the vulnerable web server.

12.2.2.3. Encryption at the network layer

Below the protocol layer it is possible to use technologies such as VPN to protect data. This has many incarnations, the most popular being Internet Protocol Security (IPsec), typically implemented as a protected 'tunnel' between two gateway routers. Neither the application nor the protocol needs to be crypto aware – all traffic is encrypted regardless. Possible issues at this level are computational and bandwidth overheads on network devices.

The only way to generate secure authentication tokens is to ensure there is no way to predict their sequence. In other words: true random numbers. It could be argued that computers can not generate true random numbers, but using new techniques such as reading mouse movements and key strokes, entropy has significantly increased the randomness of random number generators (RNGs) (M6). It is critical that you do not try to implement this on your own; use of existing, proven implementations is highly desirable [156].

Wi-Fi and 4th generation (4G) of the Global System for Mobile Communication (GSM)

Wi-Fi and GSM-4G are considered to be the weak link of the network chain and there many serious arguments that support this. By looking at the authentication and ciphering algorithms in 4G, such as Extensible Authentication Protocol for Authentication and Key Agreement (EAP-AKA), currently operating within the Long-Term Evolution (LTE) protocol, there are several vulnerabilities in LTE/ System Architecture Evolution (SAE) security architecture - specifically, insecure AKA key derivation procedures and the lack of fast re-authentication during handovers. [159] Even the hardest Wi-Fi Protected Access II (WPA2) encryption algorithm for Wi-Fi can break in 10 minutes by applying a dictionary attack with an open source tool, Aircrack [160].

Wireless intrusion prevention system (WIPS) is a level of defence for Wi-Fi. Commercial products can supply a holistic solution, such as the Cisco Wireless Intrusion Prevention System but this means building your own infrastructure and most likely needs to be done inside the borders of a small area, no more than hundreds of meters in extent.

It is possible to use active GSM-4G interceptor as IBIS-II. The IBIS-II is an advanced integrated active solution that includes all relevant subsystems in a single unit, allows the user to scan, analyse, intercept, monitor, record and track GSM mobiles, regardless of if they are encrypted by A5.1 or A5.2 encryption (monitoring is not done by forcing the mobile to use A5.0 or A5.2 but rather by an integrated deciphering capability) [161].

On the other hand this technique can also be used for protection. An economic and secure enough solution is a Private Mobile Network, especially vehicle based solutions which provide an efficient way to deploy a Private GSM network in minutes, ensuring that coverage can be provided when and where needed. [162]. This way we can avoid MitM attacks on GSM-4G but also keep logs and monitor the traffic for any malware application that has infected a smartphone or any mobile device.

Virtual Private Networks (VPNs)

The most common secure tunnelling protocol used in site-to-site VPNs (M14) is the IPsec Encapsulating Security Payload (ESP), an extension to the standard IP protocol used by the Internet and most corporate networks today. Most routers and firewalls now support IPsec and so can be used as a VPN gateway for the private network behind them [163].

Another option, 'mobile VPNs,' are gaining popularity because they are clientless and use standard browsers. These protect more than the login - they proxy data over an SSL / Transport Layer Security (TLS) tunnel. Mobile VPN products from vendors such as NetMotion and Columbitech are tuned for wireless, including optimization for low-speed cellular, WAN/LAN roaming and session persistence during brief network interruptions. [163]

VPN service providers should not keep logs, protect your anonymity, not discriminate against traffic or protocol types, offer exit servers to help you get around location-restricted content blocks, offer Anti-Malware/Anti-Spyware Features and all the above at a reasonable price. In no specific order here are some of the ones considered to be the best on the PC platform: Private Internet Access, TorGuard, IPVanish VPN, CyberGhost VPN [164].

Even though the same principles have to be followed by smartphones, there many deferent commercial products that need a lot of detailed research according to specific customer needs. On Android and Apple's platform there are VyprVPN, ExpressVPN, AirVPN, Mullvad, IPVanish, ibVPN, Private Internet Access. [165].

Last but not least, the final threat is 'DNS Leaking', which VPN providers and services have to be very cautious about. 'DNS Leaking' happens when your system, even after you've connected to a VPN or anonymity network like Tor, continues to query your ISP's DNS servers every time you visit a new website, connect to a new server, or fire up a new internet-connected application. Ultimately, it means that even though your traffic is encrypted, your ISP—or worse, anyone snooping on the 'last mile' of your internet connection (aka, the network between your computer and your ISP)—can clearly see everything you connect to on the internet and every site you visit on the web [166].

Over the past few years, many vendors have released secure remote access products that use SSL and ordinary web browsers as an alternative to IPsec/L2TP/PPTP VPNs. These 'SSL VPNs' are often referred to as 'clientless,' but it is more accurate to say that they use web browsers as VPN clients, usually in combination with dynamically-downloaded software (Java applet, ActiveX control, or temporary Win32 program that is removed when the session ends). Also, unlike PPTP, L2TP, and IPsec VPNs, which connect remote hosts to an entire private network, SSL VPNs tend to connect users to specific applications protected by the SSL VPN gateway [163]. There are SSL VPNs commercial products for all smartphones platform, such as Cisco AnyConnect and OpenVPN.

On the other hand there is an alternative and maybe even more secure solution, which is to build your own VPN. It is possible to use a built-in VPN client, found in the Settings on all smartphone platforms. You can select the type of VPN protocol to be used: PPTP, L2TP, L2TP/IPsec PSK, or L2TP/IPsec CRT. The last is most secure but requires a digital certificate. With L2TP/IPsec PSK, you can use a pre-shared key (a password). PPTP is the easiest type of VPN to set up, but it's also the least secure.

12.2.3. Mobile Device Management (MDM), Enterprise Mobility Management (EMM) and Mobile Application Management (MAM) solutions

The idea of BYOD is that instead of giving a corporate mobile device (smartphone or tablet mainly) to the members of an organisation, they can use their own devices in the professional environment. This way the employee only has to use and carry one device, instead of two (the personal and the professional). Obviously this increases tremendously the exposure to risk of corporate data. How can enterprises allow BYOD in the workplace while keeping information secure? This can be achieved, in part, with MDM.

MDM solutions (M23) are mobile policy and configuration management tools. They provide management across four different layers: 1) software management, 2) network service management, 3) hardware management and 4) security management [84]. Organisations are encouraged to consider MDM when planning mobile device deployment; however it should be understood that MDM doesn't add new security features to a platform but is a way to automate the configuration of the security features already provided by the platform [167].

The different solutions available to implement MDM include a central server and a client component running on each device under the control of the MDM. From the server, commands can be send to the all the devices or specifically to some of them. The range of commands or functions covered by the MDM depends on the solution or manufacturer, but in general all of them cover the items described in Figure 7.

Many MDM service vendors provide full EMM systems. EMM is a set of people, processes and technology focused on managing mobile devices, wireless networks and related services to enable use of mobile computing in a business context.

MAM differs from MDM by focusing on application management and providing lower degrees of control over the device but higher level control over applications. As described in [168], MAMs offer application wrapping, encrypting native applications and their data, and are used to insulate them from the rest of the OS, they are less onerous on the employee's personal device, but are less secure than MDM and proprietary sandboxes, as data is mixed together in a potentially hostile OS.

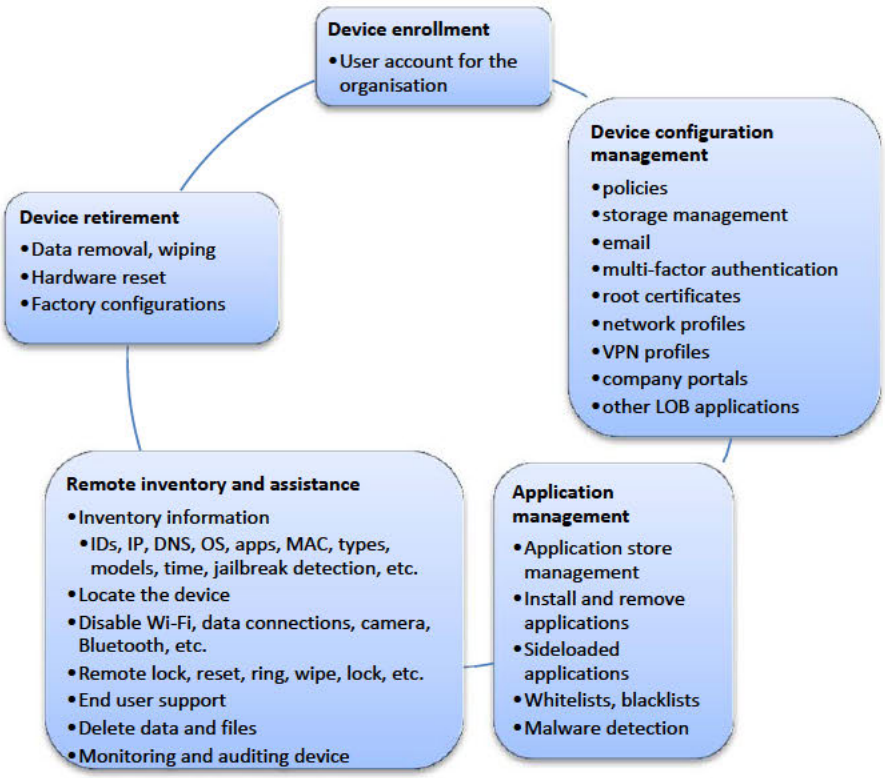


Figure 7. Features of MDM and/or EMM solutions.

Certain phone manufacturers have their own MDM solutions, and there are several commercial products on the market. Examples are AirWatch Enterprise Mobility Management, Amtel MDM, BlackBerry Enterprise Service, BoxTone, CA Technologies MDM, FiberLink, Good for Enterprise by Good Technology, IBM Endpoint

Manager for Mobile Devices, MaaS360 by FiberLink, MobiControl by Soti, MobileIron, SAP's software, Symantec Mobile Management Suite, Windows Phone MDM, XenMobile by Citrix, and Zenprise. Features and functions of certain MDMs have been compared e.g., in [169] [170]. Some MDMs use virtualisation techniques, see section 12.2.15. 'Virtualisation'.

It is not always possible to disseminate applications freely, because creators of the OS (e.g. Apple, Google and Microsoft) control the stores [39]. This is one reason for certain MDM solutions and secure smartphone models having their own application markets, and/or mechanisms for whitelisting installable applications. As described by Adam Ely [12], the number one concern of users with mobile security rollouts is privacy, and because of this employees are constantly pushing back on MDM implementations due to fear of employers seeing too much about their personal lives. This means that a good user experience is one of the most important features for successful BYOD and enforcement of policies.

12.2.3.1. AirWatch Mobile Security Management

AirWatch Mobile Security Management provides mechanisms for remote locking or wiping, multi-factor authentication, whitelists and blacklists for applications, location and time-based access control, FIPS 140 compliant document encryption via SSL, configuring policies to prevent copy/paste, and for email forwarding [171]. WidePoint Management Mobility Services provides formulating and enforcing security policies, employing encryption and access controls, remote access, device disposal and monitoring and regulating wireless usage [172].

12.2.3.2. Good for Enterprise

Good for Enterprise (GFE) is an application suite and a MDM which creates an enterprise-managed container that allows technical controls to be enforced in the absence of ones provided by the underlying platform. Good Dynamics (GD) includes a software development kit (SDK) and an application wrapping toolkit. When using GFE and/or GD, the following topics have to be thought about carefully: the underlying platform must be trusted, the Good Network Operations Centres (NOCs) must be trusted and it must be observed that there is no isolation between internal components such as email client and web browser [116].

12.2.3.3. Kaspersky Security for Mobile

Kaspersky Security for Mobile [173] integrates security and management for mobile devices. It combines mobile endpoint security capabilities and MDM functionality, effectively protecting mobile devices from various threats including phishing attacks, social engineering techniques, viruses, Trojans, and bots. Anti-theft functionality is provided along with corporate application containerisation and data encryption. [173]

Smartphones and tablets are supported including Android, iOS, Windows Phone 8, Windows Mobile, Symbian and BlackBerry and can be managed via one centralised management console. Plus, Over the Air (OTA) capabilities enable mobile access to corporate data and systems such as contacts, calendars and email systems so that mobile security is managed from a 'single pane of glass' [173].

Kaspersky Security for Mobile scans every file, application and email attachment using a combination of signature-based protection, heuristic analysis and cloud-assisted anti-malware technology. It works in the background with little or no effect on performance or productivity; and real-time updates from the cloud-based Kaspersky Security Network (KSN) delivers a fast response to new threats. Whilst the Anti-spam and Safe Browser filters out unwanted mobile calls and texts, and protects against phishing websites respectively [173].

12.2.3.4. Lacoon Mobile Threat Management Platform

Lacoon Mobile Security provides a Lacoon Mobile Threat Management Platform which is claimed to detect advanced mobile threats, mitigate risks and assess vulnerabilities and seamlessly integrate with MDMs and SIEM solutions [174]. Researchers from the same company have published guidelines on how MDMs can be bypassed [84].

12.2.3.5. MaaS360 MDM

The MaaS360 MDM [175] [176] solution can be quickly deployed and provides in depth visibility and control across mobile devices, applications, and documents. It supports most devices including Android, iPhone, iPad, Windows Phone, BlackBerry, and Kindle Fire.

Table 12. Highlights of Maas360 MDM [175]

Feature	Description
Enrolment	Convenient options to request device enrolment include over the air (OTA) using SMS, email, or a custom URL.
Integration	Mobile devices can be integrated with Enterprise Systems like Integrate with Microsoft Exchange, Lotus Notes, and Microsoft Office 365.
Unified console	A unified console for smartphones and tablets allows centralised policy and control across multiple platforms.
Monitoring	Continuously monitors devices through dynamic security and compliance features such as creating real-time compliance rules with automated actions, enforcing location-related compliance by using geo-fencing rules, and selectively wiping corporate data leaving personal data intact.
Diagnosis tools	User and application issues can be diagnosed and resolved in real time.
Graphical summaries	Dashboards deliver graphical, interactive summaries of the operation and compliance; creates detailed hardware and software inventory reports and applies privacy settings that block collection of personally identifiable information.

12.2.3.6. GlobalProtect by Palo Alto Networks

GlobalProtect [177] is a MDM solution that manages, protects devices and controls data through the integration of three components: GlobalProtect Gateway, GlobalProtect App and GlobalProtect Mobile Security Manager which are described in Table 13.

Table 13. Components of GlobalProtect [177].

Component	Description
GlobalProtect Gateway	Mobile threat prevention and policy enforcement based on apps, users, content, device and device state. A VPN tunnel is available via GlobalProtect App and it integrates with WildFire (malware signatures) for preventing new malware.
GlobalProtect App	App that provides device management, device state information, and secure connectivity. Connects to the GlobalProtect Gateway to access applications and data in accordance to policy. Device configuration and device state is exchanged with the GlobalProtect Mobile Security Manager; supported on Android, Apple iOS, Microsoft Windows, Apple Mac OS X and Linux.
GlobalProtect Mobile Security Manager	A device management tool to configure devices. Indentifies devices with infected apps by utilizing WildFire malware signatures; enforces security policies through shared information about the device and device state with GlobalProtect Gateway; hosts an enterprise application store for managing business applications.

12.2.4. Securing mobile data and data loss prevention (DLP) solutions

12.2.4.1. Bluebox Mobile Data Security

Bluebox Mobile Data Security runs on iOS and Android. As described in [178], it concentrates on securing data, and not devices by using a data and employee centric approach. It uses cloud based mobile data security solution that respects employee privacy and allows freedom of choice to use any application without compromising security. The data-centric approach employs the technology innovations described in Table 14:

Table 14. Technologies used in BlueBox Mobile Data Security [178].

Technology	Description
Data wrapping	Provides document level encryption and context-aware configurable policies of data at rest, in applications and in transit; data security policies can be enforced on any app; end-to-end security for corporate data from mobile device to source at device level or application-specific VPNs as well as site-to-site connectivity for internal applications.
Instantaneous Application Protection	Secures and deploys any internal or public application without SDKs or coding and employees can use their public apps, without compromising mobile data security. Data leakage is controlled by context aware policies between apps and over the network to cloud storage locations.
Data Awareness Engine	Corporate data is separated from personal data via context-aware mechanisms and policies.
Invisible Workspace	Produces a transparent, secure workspace for mobile apps delivered from the application catalog; passcode-protected access to all apps are managed centrally in the invisible workspace while updates are delivered dynamically to mobile application security policies without requiring restarts.
Mobile device and application integrity	Incorporates defence mechanism against platform level vulnerabilities such as application tampering or jailbreaking/rooting.

The employee-centric approaches allows for [178]:

- Easy enrolment via the Apple App Store or Google Play.
- Mobile employees to use any public apps, anytime, from Apple App Store or Google Play without sacrificing corporate data security or the native application experience.
- Transparent privacy dashboard provides employees full visibility into what IT is and isn't tracking.
- Personal mode preserves the BYOD employee's right to reclaim their mobile device at will and temporarily suspend access to corporate data, for ultimate BYOD empowerment.

12.2.4.2. MaaS360 Secure Productivity Suite

MaaS360 Secure Productivity Suite [176] is an enterprise data loss prevention solution incorporating consistent and seamless workflows. It is a cloud-based solution for iOS, Android and Windows Phone enabling employees to securely access corporate data without affecting the mobile experience on their personal devices. MaaS360 is available as a standalone solution without enroling devices in MDM.

Some benefits of MaaS360 include separate personal and corporate data, sensitive data leakage risk reduction, ability to leverage single sign-on for authentication, policies can be set at the user-level, online and offline compliance checks, and granular administrative controls.

Table 15. Highlights of MaaS360 Secure Productivity Suite [176].

Tool	Description
MaaS360 Secure Mail	An office productivity application with email, calendar and contacts; includes FIPS 140-2 compliant, AES-256 encryption for iOS, Android and Windows Phone, restricts forwarding, moving to other applications, and screen captures; cut and paste restrictions.
MaaS360 Mobile Application Security	A mobile application container to prevent data leaks; compliance violations alerts in real-time and automated enforcement actions; No device VPN needed as tunneling is available at the App-level for secure access to corporate data.
MaaS360 Secure Browser	A web browser for iOS and Android devices enabling secure access to corporate intranet sites and enforcing compliance of security and HR policies; no device VPN required to access to corporate intranet sites and network; detailed reporting of policy violations with audit trail of blocked domains accessed; URL filters and security policies defined based on categories.

12.2.4.3. TITUS Classification for Mobile

TITUS Classification for Mobile [179] can be used to protect against data spills, and to secure corporate email on mobile devices. It employs color-coded classifications alerting users to data sensitivity, prompting users to stop, think, and identify the business value of the information they are sharing. TITUS Classification for Mobile security policies catches data leaks before they happen. Policy tips encourage and enforce proper handling and sharing of business information, preventing disclosure to unintended recipients [179].

Table 16. Highlights of TITUS Classification for Mobile [179].

	Extends support for Microsoft Active Directory and Azure Rights Management Services (RMS) to mobile devices.
Enforcing	Enforces persistent data protection policies that remain with both email and documents — no matter where or with whom they are shared.
Data loss prevention (DLP)	Mobile device DLP
Mobile container	TITUS Classification for Mobile container secures and encrypts business email and documents; enables secure SharePoint Collaboration.
Policies	Policies leverage classification for fine-grained control over the ability to email, print, copy, and open files into third party applications.

TITUS Classification for Mobile can automatically apply persistent Microsoft RMS protection to files uploaded to the Cloud without user intervention.

12.2.5. Secure smartphones and their security controls

All of the reviewed secure smartphones include or are able to run MAM, MDM and/or EMM solutions (M23).

12.2.5.1. BlackBerry

BlackBerry Balance and BlackBerry Enterprise Service 10 (BES10) have additional security controls compared to 'normal' mobile devices. Both of them separate work and personal information and classify data based on the source of the data. Personal and Work spaces (M18) can have different security rules, e.g., for installing applications and network routing. BES10 uses tunneling techniques which incorporates multiple layers of encryption between devices, BES10 and the wireless resources. BES10 is presented in Figure 8. The white paper [134] does not describe which mode of Wi-Fi encryption is used, how the system enforces the mobile phone and wireless access point to use it, which algorithms are used in VPN connections, which modes of operation and ciphersuites do AES encryption and SSL/TLS encryption use or are preferred to be used. BlackBerry has FIPS 140-2 certification, however the level of certification (from 1 to 4) is unknown. Based on Reuters [180], The Pentagon has cleared Blackberry devices for use on U.S. Defense Department networks.

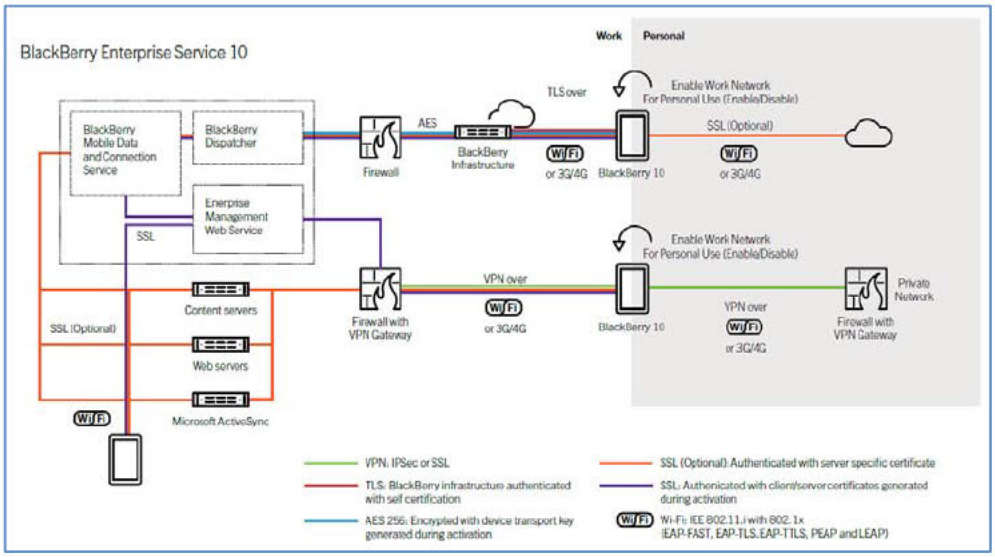


Figure 8. Overview of Secure Enterprise Connectivity of BES10 [134].

Other interesting special security controls in BES10 are, e.g., 1) wiping the Work space if certain events occur or specific conditions are met, 2) specifying whether user can add third-party accounts for services such as social networks, to the device, and 3) specifying if the device can use certain internal services such as Bluetooth, SMS/MMS or camera.

CESG [181] describes the differences between EMM modes in Blackberry 10. They have been presented in Table 17.

Table 17. Enterprise Mobility Management (EMM) modes of BlackBerry 10 [181].

Mode	Activation type	Description
EMM-Corporate	Work and Personal - Corporate	This option activates a BlackBerry Balance device that separates work and personal data. Your organisation only has control over the work space.
EMM-Regulated	Work Space Only	This option activates a device that only has a work space.
EMM-Regulated with Balance	Work and Personal - Regulated	This option activates a regulated BlackBerry Balance device that separates work and personal data and gives your organization additional control over device features.

This study is interested in modes similar to EMM-Regulated with Balance. For such, CESG recommends the network architecture presented in Figure 9 [182].

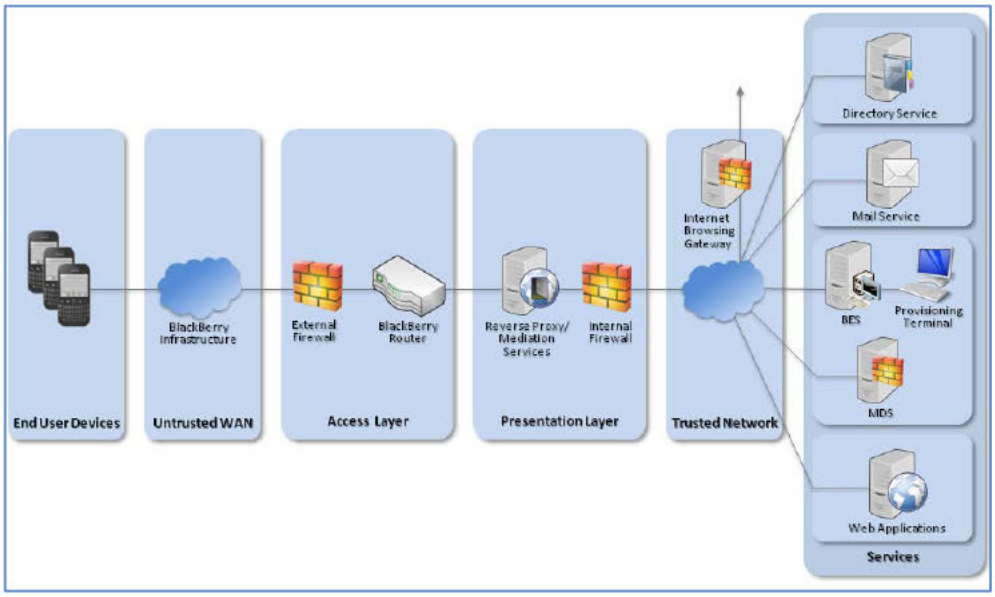


Figure 9. Recommended network architecture for BlackBerry 10 deployments [182].

Information and guidance for BlackBerry Secure Work Space can be found from [183].

12.2.5.2. Microsoft Windows Phone

Microsoft's Windows Phone 8.1 has support for an enterprise device management protocol, which can be used for device enrolment, device configuration management, application management, remote inventory and assistance and device retirement. Device configuration includes disabling resources such as certain sensors, wireless interfaces, screen capture, Microsoft accounts, certain programs or Microsoft's application store. List of supported policies can be found in [184].

More information about MDM used in Lumia phones is gathered under Nokia Expert Centre's page in [185].

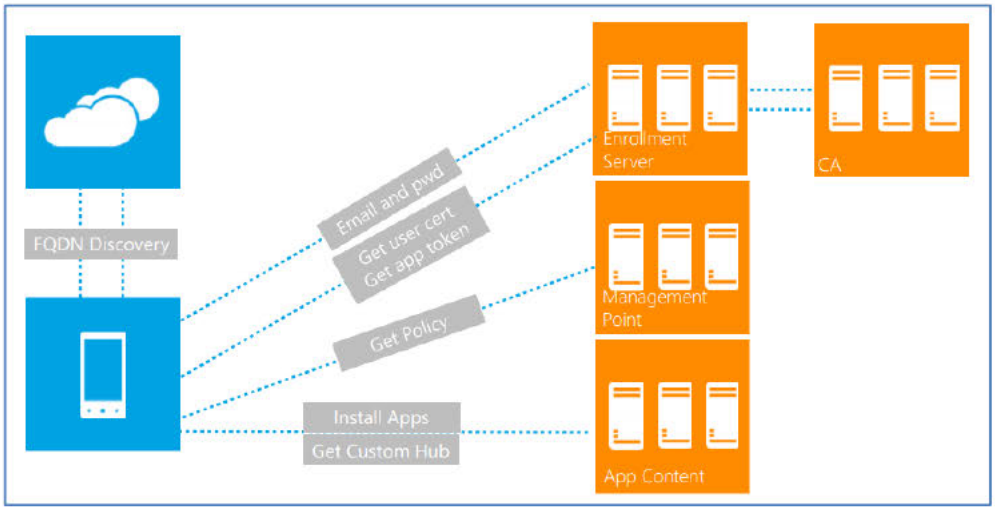


Figure 10. Windows Phone 8.1 Enterprise Device Management Architecture [78].

Windows Phone supports the following cryptographic algorithms: AES, HMACSHA1, HMACSHA256, Rfc2898DeriveBytes, RSA, SHA1, and SHA256.

Windows Phone supports usage of TPMs. TPM is a standards-based crypto-processor capable of creating and protecting cryptographic keys and hashes. In addition, a TPM can digitally sign data using a private key that software cannot access. Essentially, a TPM is a crypto-processor and secure storage place that both UEFI and the OS can use to store integrity data, meaning hashes (which verify that firmware and critical files have not been changed) and keys (which verify that a digital signature is genuine).

Among other functions, Windows Phone uses the TPM (M6) for cryptographic calculations and to protect the keys for BitLocker storage encryption, virtual smart cards, and certificates. All Windows Phone 8.1 devices include a TPM.

Windows Phone 8.1 performs device encryption, which is based on BitLocker technology, to encrypt the internal storage of devices with 128-bit AES encryption. The encryption key is protected by the TPM to ensure that the data cannot be accessed by unauthorised users, even if the internal storage media is physically removed from the device.

The Require Device Encryption policy prevents users from disabling device encryption and forces encryption of internal storage. Additional security can be included when the Device wipe threshold policy has been implemented to wipe the device when a brute-force attack on the PIN lock is detected.

Windows Phone stores the apps on an encrypted Secure Digital (SD) card partition that is specifically designated for applications. This feature is always enabled, so there is no need to explicitly set a policy to have this level of protection. The use of SD cards can be disabled if needed to increase security due to the fact that personal content (like photos or videos) is stored in an unencrypted partition so the user can access this information on other devices.

12.2.5.3. Apple iOS

Apple's iOS includes a built-in MDM solution (M23). It has differences between the management features of personal and corporate-owned iOS devices. Apple's iOS provides common MDM functionalities for personal devices such as controlling corporate managed accounts, applications, documents, and data, as well as integrated security features such as password enforcement and remote lock or wipe of lost or stolen devices. In addition to these, iOS MDM enables separation of enterprise settings, accounts, and applications installed by MDM from installations performed by the user. It is claimed that personal data is not accessible to the organization. In corporate-owned devices it is possible to filter content, setup devices directly to have some wanted configurations after getting them from Apple (by using Apple's Device Enrollment Program (DEP), supervise if the devices are shared by several people, remote wipe the device, and use an always-on VPN and/or a global proxy [186] [187] [188] [189] [190]. Third-party MDM solutions can be built on the native MDM provided by iOS. It is possible to flag email addresses to ensure that only trusted contacts receive sensitive messages [191]. As described in [192], iOS has strong security features in some very specific areas such as code-signing and DEP, to help prevent jail-breaking and copying of applications from the Apple App store.

Devices with iOS always use enabled hardware-based encryption using 256-bit AES to protect all data on the device [193]. It is mentioned in [189] that the cryptographic modules in iOS 8 are undergoing validation for compliance with U.S. Federal Information Processing Standards (FIPS) 140-2 Level 1. Strangely, it is claimed in Apple's developer pages [193], that the cryptographic modules in iOS 6 or later have been validated to comply with U.S. Federal Information Processing Standard (FIPS) 140-2 Level 1.

The device's unique ID (UID) and a device group ID (GID) are AES 256-bit keys fused (UID) or compiled (GID) into the application processor during manufacturing.

Apart from the UID and GID, all other cryptographic keys are created by the system's RNG using an algorithm based on CTR_DRBG. System entropy is generated from timing variations during boot, and additionally from

interrupt timing once the device has booted. Keys generated inside the Secure Enclave use its true hardware RNG based on multiple ring oscillators post processed with CTR_DRBG.

Every Apple device since the iPhone 3GS has had an encrypted file system. When your iPhone or iPad is locked, data and applications remain encrypted until your passcode is entered, after which anything you access is auto-decrypted for use or display, until the device relocks itself due to inactivity. Recently Apple has updated its privacy policy with iOS8, and now devices with this version of the OS cannot be accessed by the company itself. Now everything stored in the devices are under the protection of the user passcode. The specific technical changes are outlined in [194].

An overview of the security architecture iOS is presented in Figure 11. It should be noted that the security architecture presented in [194] is missing the Secure Element at the Kernel layer.

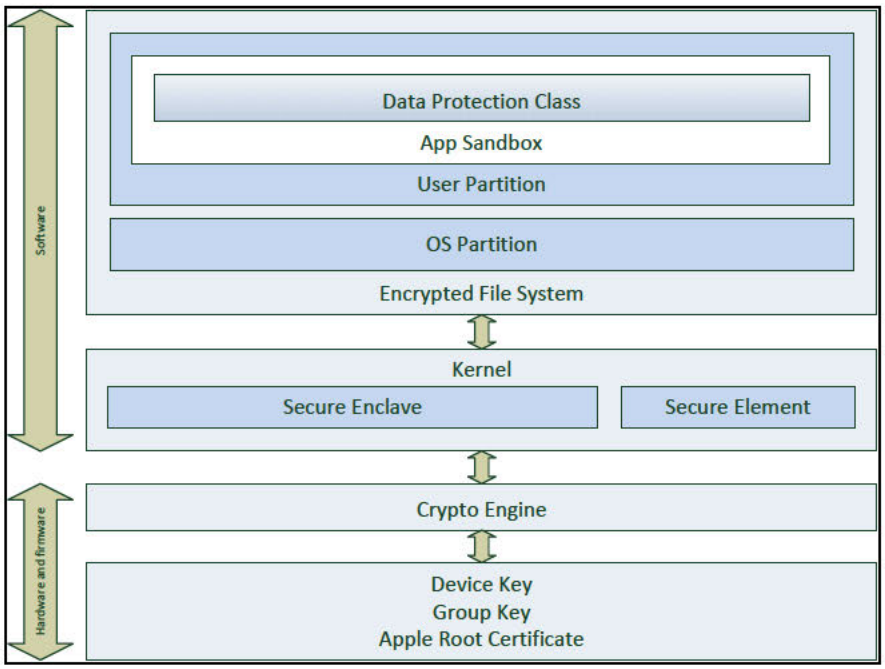


Figure 11. Overview of security architecture of iOS [189].

Strangely enough, Apple's official documentation places Secure Enclave in the software layer, to describe it as a Hardware unit (coprocessor). The following paragraphs are extracted from [194]:

'Secure Enclave: is a coprocessor (Apple A7 or later A-series) that uses its own secure boot and software update separate from the application processor. It provides all cryptographic operations for Data Protection key management. During fabrication is provisioned with a UID that is not accessible to the rest of the system and not know to Apple. When the device starts up the UID is used to create an ephemeral key that is used to encrypt the device's memory used by the Secure Enclave. [194]'

Apple uses a technology called Data Protection to protect data stored in flash memory on the device. Key system apps, such as Messages, Mail, Calendar, Contacts, and Photos use Data Protection by default, and third-party apps installed on iOS 7 or later receive this protection automatically. Data Protection is implemented by constructing and managing a hierarchy of keys, and builds on the hardware encryption technologies built into each iOS device. Data Protection is controlled on a per-file basis by assigning each file to a class; accessibility is determined by whether the class keys have been unlocked.

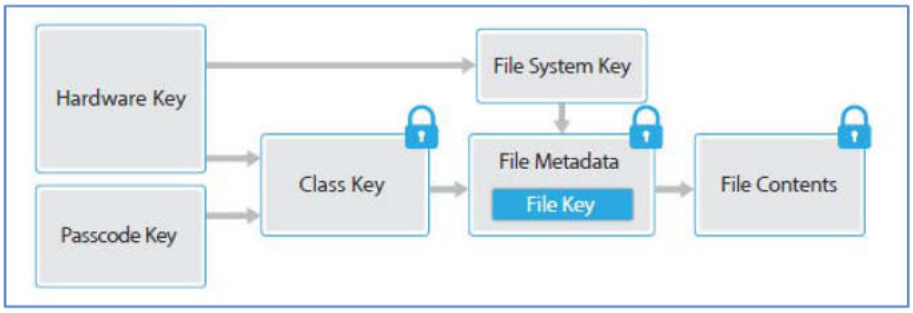


Figure 12. iOS key management [194].

The content of a file is encrypted with a per-file key, which is wrapped with a class key and stored in a file's metadata, which is in turn encrypted with the file system key. The class key is protected with the hardware UID and, for some classes, the user's passcode. This hierarchy provides both flexibility and performance. For example, changing a file's class only requires rewrapping its per-file key, and a change of passcode just rewraps the class key.

By setting up a device passcode, the user automatically enables Data Protection. iOS supports four-digit and arbitrary-length alphanumeric passcodes. In addition to unlocking the device, a passcode provides entropy for certain encryption keys. On a device with an A7 or later A-series processor, the Secure Enclave also enforces a 5-second delay between repeated failed unlocking requests. This provides a governor against brute-force attacks in addition to safeguards enforced by iOS.

When a new file is created on an iOS device, it's assigned a class by the application that creates it. Each class uses different policies to determine when the data is accessible. The basic classes are 1) complete protection, 2) protected unless open, 3) protected until first user authentication and 4) no protection.

One very interesting solution provided by Apple is Touch ID, the fingerprint sensing system (M5) to provide a new way to access to the device. This technology reads fingerprint data from any angle and learns more about a user's fingerprint over time. When the device is set up to use Touch ID the fingerprint of the user is scanned and enrolled. The device is unlocked by the simple recognition of the user's fingerprint without asking a passcode.

Touch ID can be trained to recognise up to five different fingers. With one finger enrolled, the chance of a random match with someone else is 1 in 50,000.

The fingerprint sensor is active only when the capacitive steel ring that surrounds the Home button detects the touch of a finger. The 88-by-88-pixel, 500-ppi raster scan is temporarily stored in encrypted memory within the Secure Enclave while being vectorised for analysis. The resulting map of nodes is stored without any identity information in an encrypted format that can only be read by the Secure Enclave.

With Touch ID enabled, when a device is locked, the keys for Data Protection class Complete are wrapped with a key that is given to the Touch ID subsystem inside the Secure Enclave. When a user attempts to unlock the device, if Touch ID recognises the user's fingerprint, it provides the key for unwrapping the Data Protection keys, and the device is unlocked. The keys needed for Touch ID to unlock the device are lost if the device reboots and are discarded by the Secure Enclave after 48 hours or five failed Touch ID recognition attempts.

12.2.5.4. Android operating system (OS)

Android OS is an open source platform based on Linux and its documentation is more focused on helping developers create applications than explaining how it is designed or works. However useful information can still be extracted.

The main Android platform building blocks are a processor-agnostic OS built on top of the Linux kernel and Java applications running in the Android runtime (ART).

There are two types or sources of applications: Pre-installed and User-installed.

Android OS can be configured to verify a user-supplied password prior to providing access to a device. In addition to preventing unauthorised use of the device, this password protects the cryptographic key for full file system encryption [195].

Applications running in Android OS that need to share user information can use Android OS permission checks to protect this data.

'*During installation, a third-party application may request permission to access these resources. If permission is granted, the application can be installed and will have access to the data requested at any time when it is installed.* [196]'

'*Any applications which collect personal information will, by default, have that data restricted only to the specific application. If an application chooses to make the data available to other applications though IPC, the application granting access can apply permissions to the IPC mechanism that are enforced by the operating system.* [196]'

Third-party applications that want to access data input devices, such as camera, microphone or GPS, must have been explicitly granted access by the user through the use of Android OS Permissions [196].

Android OS provides a set of cryptographic APIs including implementations of standards such as AES, RSA, DSA, and SHA. Android 4.0 introduced the KeyChain class to allow applications to use the system credential storage for private keys and certificate chains [195]. Applications accessing the KeyChain normally go through the steps described in Table 18 [197].

Table 18. Steps of application accessing the KeyChain in Android OS [197].

Step	Description
1.	Receive a callback from an X509KeyManager that a private key is requested.
2.	Call choosePrivateKeyAlias to allow the user to select from a list of currently available private keys and corresponding certificate chains. The chosen alias will be returned by the callback alias (String), or null if no private key is available or the user cancels the request.
3.	Call getPrivateKey(Context, String) and getCertificateChain(Context, String) to retrieve the credentials to return to the corresponding X509KeyManager callbacks.

The following paragraphs are extracted from [197]:

'*An application may remember the value of a selected alias to avoid prompting the user with choosePrivateKeyAlias on subsequent connections. If the alias is no longer valid, null will be returned on lookups using that value. An application can request the installation of private keys and certificates or check Certificate Authority (CA) certificates using different methods of this class.* [197]'

Android 3.0 and later provides full filesystem encryption using AES128 with CBC and ESSIV:SHA256 [195].

Android 5.0, called Lollipop, includes, e.g., the following improvements: a) faster encryption which encrypts only used blocks on the data partition to make the first boot faster, b) encryption of the first boot, c) support for patterns and encryption without a password, and d) hardware-backed storage of the encryption key. Currently only ext4 and f2fs filesystems support fast encryption. [198]

In the Android 5.0 release, there are four encryption states: default, PIN, password and pattern [198]. Upon first boot, the device generates a 128-bit key. This key is then encrypted with a default password, and the encrypted key is stored in the crypto metadata. The 128-bit key generated is valid until the next factory reset. Upon factory reset, a new 128-bit key is generated. [198]

The following paragraphs are extracted from [198]:

'When the user sets the PIN/pass or password on the device, only the 128-bit key is re-encrypted and stored. (i.e. user PIN/pass/pattern changes do NOT cause re-encryption of userdata.) [198]'

'In order to encrypt, decrypt or wipe /data, /data must not be mounted. However, in order to show any user interface (UI), the framework must start and the framework requires /data to run. To resolve this conundrum, a temporary filesystem is mounted on /data. This allows Android to prompt for passwords, show progress, or suggest a data wipe as needed. It does impose the limitation that in order to switch from the temporary filesystem to the true /data filesystem, the system must stop every process with open files on the temporary filesystem and restart those processes on the real /data filesystem. [198]'

To do this, all services must be in one of three groups: core, main, and late_start, as described in Table 19.

Table 19. Service groups of Android OS [198].

Service	Description
core	Never shut down after starting.
main	Shut down and then restart after the disk password is entered.
late_start	Does not start until after /data has been decrypted and mounted.

There are four flows presented in Table 20 for an encrypted device. A device is encrypted just once and then follows a normal boot flow. In addition to these flows, the device can fail to encrypt /data [198].

Table 20. Flows for an encrypted device [198].

Flow categories	Flows
Encrypt a previously unencrypted device	Encrypt a new device with forceencrypt: Mandatory encryption at first boot (starting in Android L).
	Encrypt an existing device: User-initiated encryption (Android K and earlier).
Boot an encrypted device	Start an encrypted device with no password: Boot an encrypted device that has no set password (relevant for devices running Android 5.0 and later)
	Start an encrypted device with a password: Boot an encrypted device that has a set password.

To give an idea of how it works, the sequence of steps to perform the operation 'Starting an encrypted device without default encryption' (with password), can be seen in the Table 21.

Table 21. Process of starting an encrypted device without default encryption [198].

Step	Operation
1.	Detect encrypted device with a password
2.	Mount tmpfs (temporal file system)
3.	Start framework to prompt for password
4.	Decrypt data with password
5.	Stop framework
6.	Mount /data
7.	Start full framework. Now the framework boots all its services using the decrypted /data filesystem, and the system is ready for use.

'The encrypted key is stored in the crypto metadata. Hardware backing is implemented by using Trusted Execution Environment's (TEE) signing capability. The master key is encrypted with a key generated from the user's password and the stored salt, and signed with a stored TEE key. [198]'

The process proceeds as shown in the Table 22.

Table 22. Process of TEE signing [198].

Step	Operation
1.	Generate random 16-byte disk encryption key (DEK) and 16-byte salt.
2.	Apply scrypt to the user password and the salt to produce 32-byte intermediate key 1 (IK1).
3.	Pad IK1 with zero bytes to the size of the hardware-bound private key (HBK). Specifically, we pad as: 00 || IK1 || 00..00; one zero byte, 32 IK1 bytes, 223 zero bytes.
4.	Sign padded IK1 with HBK to produce 256-byte IK2.
5.	Apply scrypt to IK2 and salt (same salt as step 2) to produce 32-byte IK3.
6.	Use the first 16 bytes of IK3 as KEK and the last 16 bytes as IV.
7.	Encrypt DEK with AES CBC, with key KEK, and initialization vector IV.

If the user elects to change or remove their password in settings, the UI triggers the appropriate commands and the disk master key is re-encrypted with the new password [198].

Examples of Android based secure smartphones are Blackphone [135], Elektrobit [136], LG Gate [137], Samsung KNOX [141], Bull Hoox m2 [199], and GSMK CryptoPhone 500 [143].

12.2.5.5. Blackphone

Blackphone uses a security-enhanced Android OS build [135]. Its specific security controls are disabling Wi-Fi except at trusted wireless access points (M13), and using encrypted calls and messaging (M20) via Silent Circle [200], VPN service of Disconnect [201], and the private cloud of SpiderOak [202]. Silent Circle uses Zimmermann Real-Time Transport Protocol (ZRTP) published in RFC 6189 [203]. Disconnect would also provide services other than VPN, such as private browsing and searching, and anti-theft services [204]. Silent Text from Silent Circle is based on XMPP [205]. Blackphone was hacked in Black Hat DEF CON 2014 [206] [207].

12.2.5.6. Elektrobit

Elektrobit's specialised Android based device platform includes a TPM to provide integrity and to store keys, secure data storage, tamper detection mechanisms and optional 3rd party solutions for secure communications [136]. Details of the TPM are not described.

12.2.5.7. LG GATE

As with certain BlackBerry devices, LG GATE includes a FIPS 140-2 certified crypto module to encrypt data in the device, and to enable IPsec and SSL VPN. In LG GATE, email can be secured, e.g., so that only certain emails can be forwarded or the device can be remotely wiped and locked. LG GATE [137] is compatible with MDM like AirWatch [171], SAP, SOTI and FiberLink. Level of the FIPS 140-2 certification (from 1 to 4) is unknown.

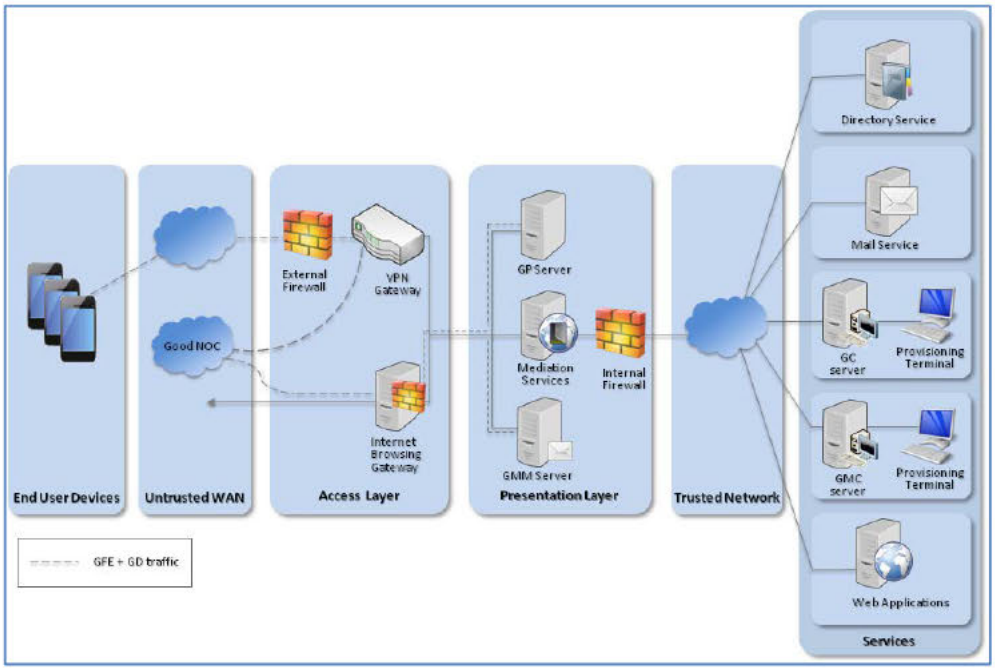


Figure 13. Recommended network architecture for GFE and GD deployments with a device VPN [208].

12.2.5.8. Samsung KNOX

Samsung KNOX has specific security controls such as continuous integrity monitoring of the Linux kernel, Secure Enhancement (SE) for Android [209], e.g., to enforce Mandatory Access Control (MAC) policies, isolation of wanted applications and data from the rest of the device, and two-factor biometric authentication (via a fingerprint scanner [138] [139]). Device has FIPS 104-2 level 1 certification, ARM TrustZone [210] based data encryption and storage for keys and client certificates, and it supports at least AirWatch [171] and SAP MDMs.

Finnish Communications Regulatory Authority's National Cyber Security Centre Finland (NCSA-FI) has approved the Samsung Knox to be used in Finland in security level IV [211] [212] [213]. This means that Samsung KNOX has KATAKRI II certificate which means that the phone fulfills the security requirements of Finland's government and is suitable for restricted use by authorities. KATAKRI II certification is the newest security level used at Finland's government level, started in 2011 [214]. According to Reuters [180], the Pentagon has cleared Samsung KNOX devices for use on U.S. Defense Department networks. Based on TechWeekEurope, usage of Samsung KNOX-enabled mobile devices have been approved within the NSA under the agency's Commercial Solutions for Classified Program [215] and it has been cleared for use by the US Department of Defence [216]. This list of classified devices can be found in [217]. KNOX has been approved by the CESG [218].

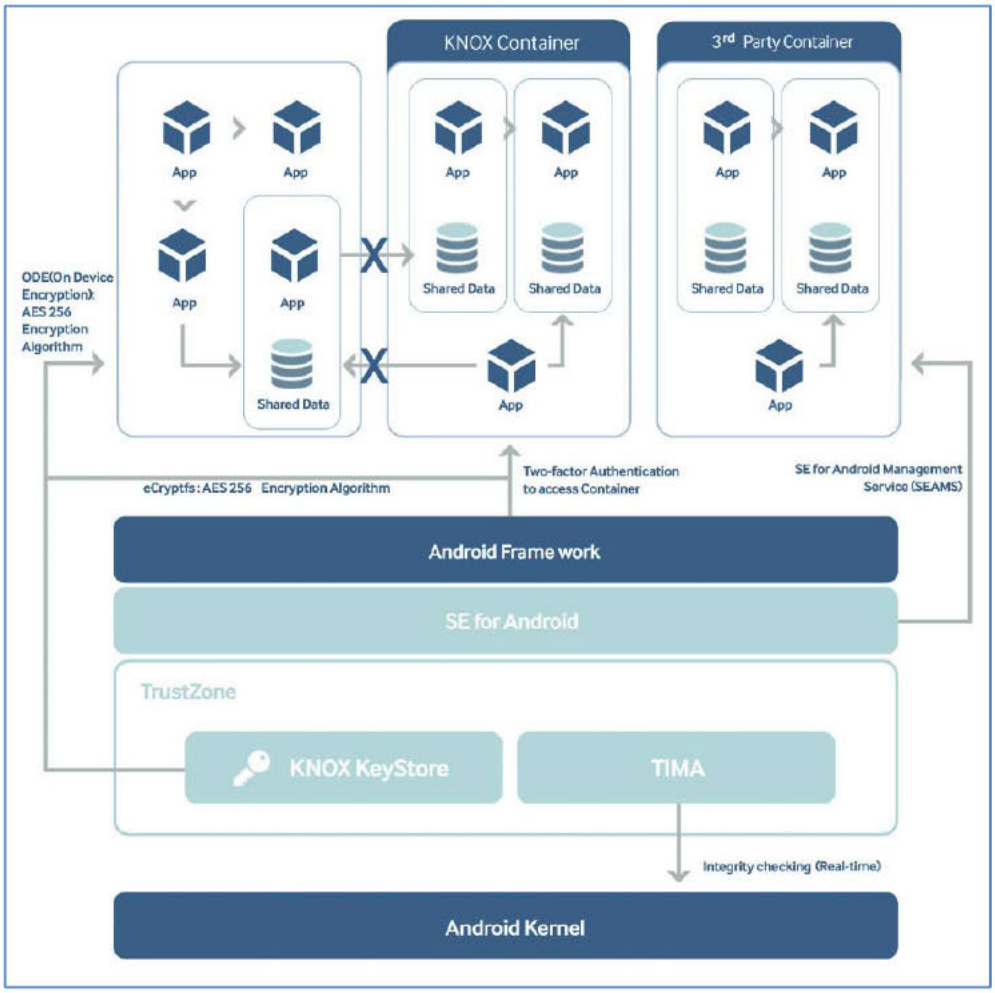


Figure 14. Diagram of Samsung KNOX features [140].

TrustZone architecture can secure peripherals such as interrupt controllers, timers and user I/O devices [219]. It can be used as a system-wide Trusted Execution Environment (TEE) [220].

CESG's 'End User Devices Security Guidance: Samsung devices with KNOX' [221] recommends that all remote or mobile working scenarios use a typical remote access architecture based on the Walled Garden Architectural Pattern presented in Figure 15.

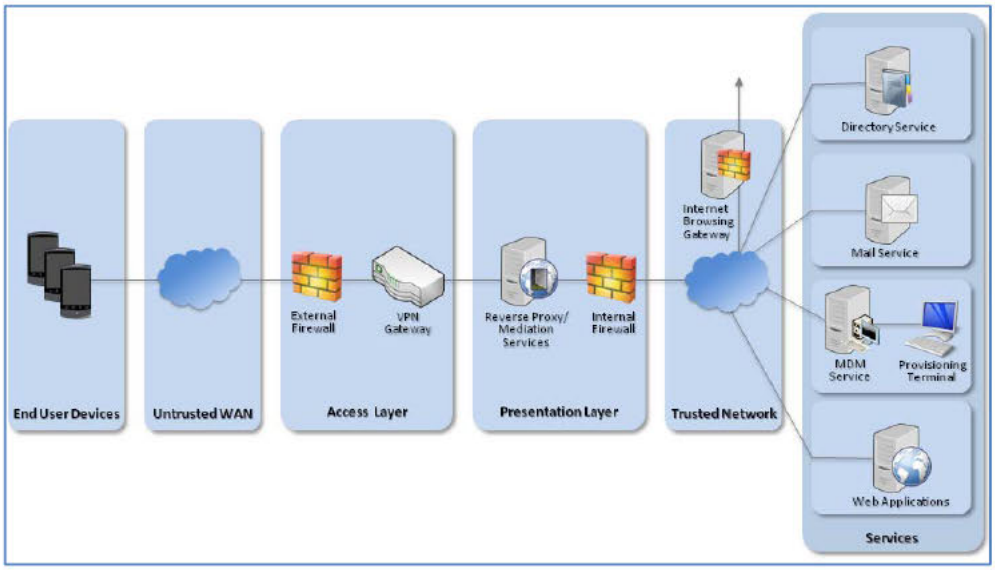


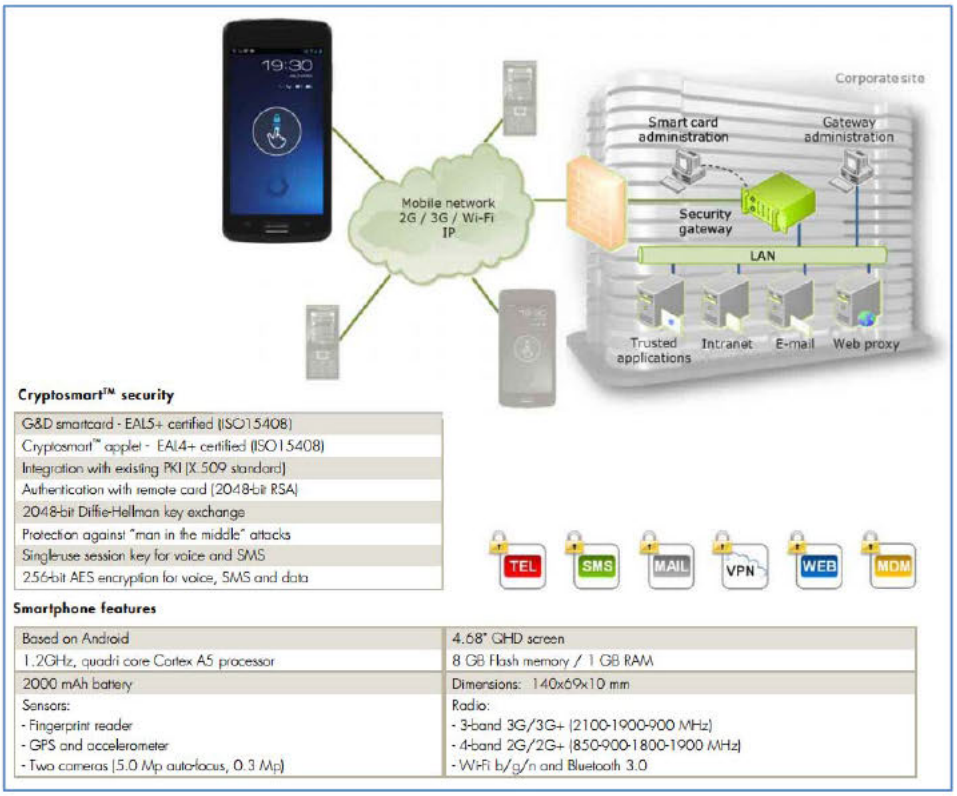
Figure 15. Recommended network architecture for deployments of Samsung devices with KNOX [221].

In October 2014, an unnamed researcher claimed that a PIN chosen by a user during setup of the KNOX App is stored in clear text on the device [222]. TechWeekEurope [223] wrote that Samsung has denied this, as it did [224]. In December 2013 it was reported by Ben-Gurion University of the Negev that their security researcher Mordechai Guri discovered a critical vulnerability from KNOX [225]. It could be possible to install an application to the non-secure container and use that to capture and expose all communication from the phone.

12.2.5.9. Bull Hoox m2 and Hoox m1

Bull [142] has two phone models for sensitive data usage and sharing, Hoox m2 [199] which is a smartphone based on Android OS and Hoox m1 [226] which which has a hardened proprietary OS. As described in [199] and [226], both models use ISO 15408 certified smartcards and applets, Diffie-Hellman based key exchange, and have 256-bit AES encryption of voice, SMS messages and data. As described in [199], Hoox m2 includes a fingerprint reader. Hoox m1 has a feature not present in models of any other phone manufacturers: undetectable secure communication. What is meant by this is unclear. It uses also local encryption of data and has a firewall inside the phone. [226]

Bull's Hoox m2's features are presented in Figure 16and m1's in Figure 17.



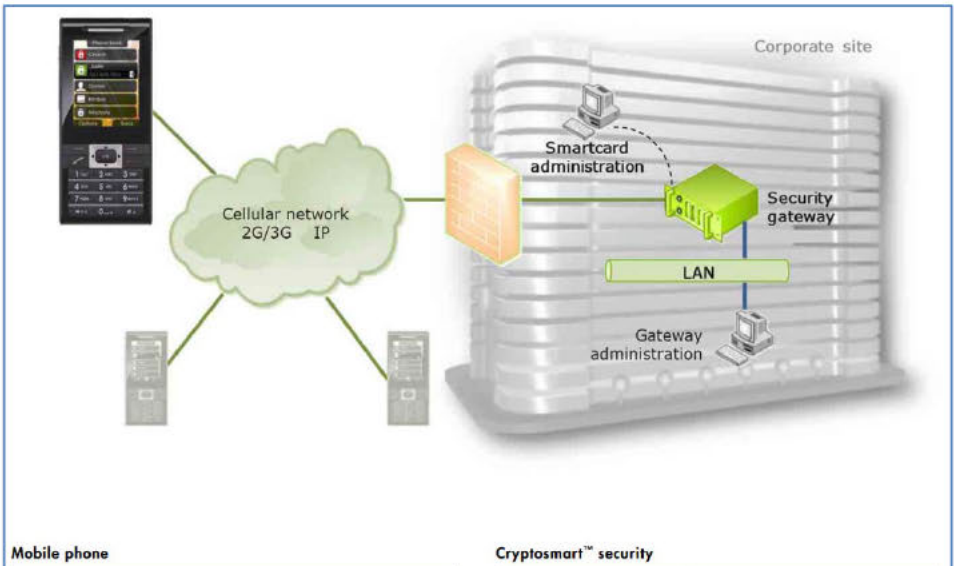
Cryptosmart™ security

G&D smartcard - EAL5+ certified (ISO15408)
Cryptosmart™ applet - EAL4+ certified (ISO15408)
Integration with existing PKI (X.509 standard)
Authentication with remote card (2048-bit RSA)
2048-bit Diffie-Hellman key exchange
Protection against "man in the middle" attacks
Single-use session key for voice and SMS
256-bit AES encryption for voice, SMS and data

Smartphone features

Based on Android	4.68" QHD screen
1.2GHz, quadri core Cortex A5 processor	8 GB Flash memory / 1 GB RAM
2000 mAh battery	Dimensions: 140x69x10 mm
Sensors: - Fingerprint reader - GPS and accelerometer - Two cameras (5.0 Mp auto-focus, 0.3 Mp)	Radio: - 3-band 3G/3G+ (2100-1900-900 MHz) - 4-band 2G/2G+ (850-900-1800-1900 MHz) - Wi-Fi b/g/n and Bluetooth 3.0

Figure 16. Overview of Bull's Hoox m2 features [199].



Mobile phone

Hardened proprietary operating system - RTOS
HSPA - 900/2100 3G, quad-band EDGE 2G
Terminal with native security
Music, FM radio and video players
1.3 Mp camera, 2.2" 240x320 screen
112 x 49 x 13 mm, 95 g
Local encryption of user data
Firewall (TCP filter, physical and logical port control)

Cryptosmart™ security

G&D smartcard - EAL5+ certified (ISO15408)
Cryptosmart™ applet - EAL4+ certified (ISO15408)
Integration with existing PKI (X.509 standard)
Authentication with remote card (2048-bit RSA)
2048-bit Diffie-Hellman key exchange
Protection against "man in the middle" attacks
Single-use session key for voice and SMS
256-bit AES encryption for voice, SMS and data

Figure 17. Overview of Bull's Hoox m1 features [226].

12.2.5.10. GSMK CryptoPhone

GSMK CryptoPhone differs from all previously described secure phone models in the following areas: 1) GSMK allows anyone to review the source code used in the GSMK Cryptophone (M37), 2) it has models for mobile, landline and satellite communication but also software for Windows and Windows Mobile, and 3) special self-destroying messages (M39). Security controls available in other phones are voice and SMS message encryption [143].

GSMK CryptoPhone has smartphone models based on Android, Microsoft Windows Mobile, but also normal GSM quad-band mobile phones. It is strange is that some leaflets [227] describe that a heavily modified and stripped-down Windows Mobile version 6.5 has been used in some models. It should be noted that version 6.5 is historic, it is not updated in few years, and it is not open source.

CryptoPhone was used to analyse communications in the baseband processor and discover suspicious activity indicating the presence of fake base stations nearby [228].

12.2.5.11. Jolla's Sailfish operating system (OS)

Jolla [144] has similar approach as GSMK CryptoPhone in its openness; anyone can review the source code of the OS, as well as open source software installed to the phone (M37). In an optimal situation, this approach stops malicious software before it can be distributed. It is able to run Android software in Jolla. The Dalvik runtime is isolated, so it is possible to turn certain permissions off from certain Android software (M18).

12.2.5.12. Sectra Tiger 7401

Sectra Tiger 7401 [229] provides a mobile encryption solution at security level SECRET. It is approved by the Dutch security agency for national SECRET and it is pending approval by the European Union (EU) at security level SECRET.

The Sectra Tiger 7401 is a secure mobile phone that is designed for ease of use. It is developed for people with strict security requirements that also need to be able to communicate securely when not at the office or when travelling. This phone meets their high demands of flexibility and mobility. It is easy for new users to adapt to, and can be used for secure voice communication and sending secure SMS and data. Sectra Tiger 7401 a) operates on 2nd (2G) and 3rd (3G) generation GSM as well as satellite communication and IP-networks, b) enables non-encrypted and end-to-end encryption in a single device and c) is interoperable and SCIP-compatible: it operates on the SECRET security level and provides transparent interoperability between national, EU and NATO domains.

12.2.6. Multiple user accounts

Multiple user accounts have been in Android since version 4.2 and usable in tablet devices, and since Android 5.0 [230] also in smartphones. Multiple user account (M42) allows users to maintain their own screen locks, separate home screens, contacts, wallpapers and general settings, however there are several differences compared to user accounts in OSs used in laptops and desktop computers. Uninstalling an application on one account uninstalls it on all accounts, and accepting new permissions for an application on one account accepts them across all accounts. The owner of the phone can remove secondary accounts at any time. Using multiple accounts is useful, e.g., if parents want to let their children to use the same device without giving them too much permission (guest mode). Multiple user accounts are used in organisations laptops but as far as we know, not yet in smartphones.

12.2.7. Multi-factor authentication products

Multi-factor authentication (MFS) is authentication mechanism (M4, M5) which includes at least two of the three existing authentication factors: 1) knowledge (something you know), 2) possession (something you have),

and 3) inherence (something you are). As described in [231], these factors are not unique to mobile devices; however, there are mobile device-specific issues to consider for all three factors.

Fido Alliance has currently two specifications for user authentication, to enable authentication without passwords and to use the second authentication factor in authentication [232].

12.2.7.1. Something you know

As described in [231], the knowledge factor is currently the most commonly used authentication factor for user authentication. A user presents a user ID or a username and then provides a secret value, the password that only the user knows. The authentication scheme relies on the strength of the secret value: how difficult the password is to guess [231].

As described in [231], strong passwords are needed to protect user accounts from various types of brute force attacks; this means that password policies have to be followed. How good and bad passwords can be distinguished has been described in [233]. As described in [15] and [231], passwords that conform to such security policies can be difficult to enter on mobile devices. Requiring users to enter such passwords repeatedly creates usability problems [231]. Many guidelines presented in section 12.1. 'Existing guidelines, checklists and lists of security controls' mention the importance of good passwords.

The knowledge factor is often combined with the possession factor, e.g., when the user has to answer (type or enter) a correct code to a call, to be able to authenticate [231].

12.2.7.2. Something you have

Simplest examples of possession factors from real life are physical keys used to open physical locks. Common choices for proving possession are: a) Hardware tokens that generate one-time passwords (OTPs) such as RSA SecurID, VASCO, SafeNet SafeWord, Authenex A-Key, SecureMetric SecureOTP, and ActivIdentity OTP Token, b) hardware tokens that perform cryptographic operations and connect directly to the device authenticating the user, to transmit the result of a cryptographic operation to the server, c) access to an email address is often used to authenticate users, especially for password reset operations, and d) the mobile device itself can be 'registered' with an application, and then, possession of the device can be used as a 'something you have' authentication facto. [231]

It is possible to use these methods also with mobile applications. Some vendors have started producing specialised hardware such as smartcard readers that can be connected to the headphone jacks on mobile devices [231].

Commercial software based security tokens such as [234] [235] [236] [237] exist. They enable usage of the mobile phone as an authentication factor. In addition to software based tokens, commercial hardware authenticators [236] and OTP tokens [238] exist.

In addition to guidelines for securing mobile devices described in the sections 12.1.5. 'Communications-Electronics Security Group (CESG)' and 12.1.6. 'Centre for the Protection of National Infrastructure (CPNI)', CESG and CPNI provide guidelines for using Excitor G/On OS with end user mobile devices [239]. A recommended architecture for the platform is described in Figure 18.

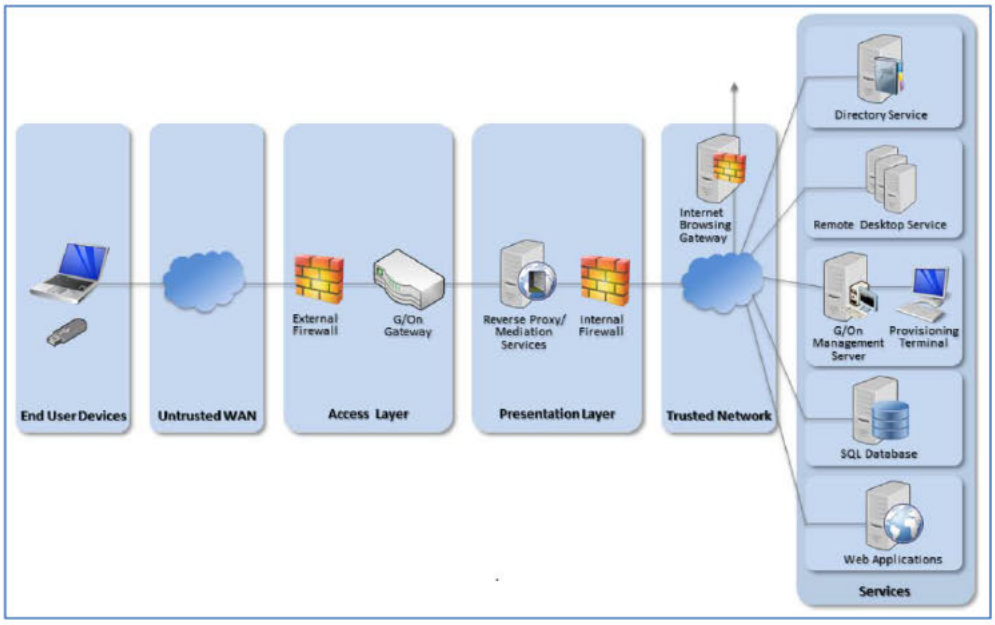


Figure 18. Recommended architecture for deployments of Excitor G/On OS [239].

Choices for these factors that require a user carry an additional device are less convenient for the user especially since one of the reasons for the popularity of mobile devices is convenience [231].

SecurEnvoy SecureAccess Tokenless 2FA [237] is a mobile phone based tokenless two-step verification for remote access. It allows users to authenticate on any device, anywhere via voice call passcodes, real time SMS Passcodes, reusable passcodes that change each day or multiple days, passcodes that can be sent by secure email and more. All methods are available for online or offline authentication and users can be automatically deployed via Lightweight Directory Access Protocol (LDAP) group membership.

Benefits to users and businesses are the following:

- There is no need to remember an additional secret piece of information as they can reuse the Microsoft or LDAP password; only need to enter one thing they know rather than two pieces of information.
- Only requirement for the user is to read an industry standard 6 digit passcode from their phone.
- Eliminates need to carry additional authentication devices.

Benefits to businesses are the following:

- Meets or exceeds regulatory compliance requirements.
- Any mobile phone that can receive an SMS message is supported without any SMS delivery delay issues affecting performance.
- No token deployment replacement costs, resynchronisation or PIN resets which reduces the cost of help desk administration.

12.2.7.3. Something you are

The inherence factor is described in [231] as follows: '*This authentication factor uses biometrics to authenticate users, and is starting to become popular with mobile devices. Some mobile devices come equipped with fingerprint readers, facial recognition software, etc. However, most devices only allow the biometric verification hardware/software to be used by the operating system for unlocking the devices. Currently, most mobile*

devices do not allow applications to utilize specialized hardware/software to authenticate users using biometrics. [231]'

Authors of [231] describe the main problem of the inherence factor: '*The main problem with using biometrics on mobile devices is that most devices do not support a standard interface using which biometric information can be collected. Eventually, this problem may be resolved; once applications can rely on devices to gather biometric information, usability issues associated with authentication on mobile devices will be virtually eliminated. However, the typical concerns with biometrics such as tuning false accept / false reject rates will still need to be addressed.* [231]'

Typical biometrics used to authenticate users (not just on mobile devices) include facial features, speech patterns, fingerprints, iris patterns, etc. Some of these are easier to bypass than others [231].

12.2.8. Tracking of devices

All current smartphones and tablets and also some laptops include chips for location tracking (M7), enabling geolocation of the device when it is turned on and connected to the Internet. Some manufacturers provide this at the OS level, and specific software is also available. To make tracking of devices possible even if they are not turned on, an additional tracking device could be used and attached to the mobile device (M49). Examples of such are Bravo [240] which uses crowdsourcing to locate devices, RuuviTracker [241], and ThingSee [242]. With laptops the integration would be easier, because usually there is some free space inside them, however with smartphones this might be too difficult.

12.2.9. Intrusion Detection and Prevention Systems (IDS/IPS)

An intrusion detection system is a device or software application that monitors network or information system activities for malicious activities or policy violations and automatically alerts administrators when a compromise is detected.

The IDS works by monitoring system activity and examining vulnerabilities in the system, file integrity and conducting an analysis of patterns based on already known attacks or network or system anomalies. An IDS is a passive system where its sensor detects a potential security breach, logs the information and then triggers an alert. In contrast, a reactive system or IPS, prevents attacks by resetting the connection, dropping a malicious packet or blocking all further traffic from the source IP address or port.

IPSs are prevalent these days and commonly detect as well as prevent attacks.

Intrusion Detection Systems use one of two detection techniques, anomaly-based and signature-based.

Anomaly-based IDS

An anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is 'normal' for that network such as the bandwidth that is normally utilised, types of protocols used, port and device connections and alert the administrator or user when traffic is detected which is anomalous, or significantly different, from the baseline. Anomaly based IDSs may generate false positive alerts for legitimate use if the baselines are not intelligently configured.

Signature-based IDS

A signature based IDS monitors packets on the network and compares them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. Signature based IDSs may not detect a zero-day threat.

Types of IDSs include the Network Intrusion Detection System (NIDS), Host Based Intrusion Detection Systems (HIDS) and Wireless Intrusion Detection System (WIDS).

Other IDSs include the Application protocol-based intrusion detection system (APIDS), Protocol-based intrusion detection system (PIDS), and Intrusion Detection Message Exchange Format (IDMEF) but will not be discussed here as they are outside the scope of this study.

12.2.9.1. Network intrusion detection systems (NIDS)

Network intrusion detection systems are positioned at a strategic point or points within a network to monitor traffic to and from all devices. An analysis is performed on passing traffic on the entire subnet that works in promiscuous mode, and matches the traffic that passes through the subnets against a library of known attacks. If an attack is identified, or abnormal behaviour is sensed, an alert will be sent to the administrator. Most modern intrusion detection systems are IPS and companies are developing next generation technology to keep pace with the changing threat landscape.

According to Greg Young of Gartner Research, '*Gartner uses the term 'next-generation network IPS' to indicate the necessary evolution of network IPS to deal with changes in network communications and applications and changes in the threat landscape. As a minimum, a next-gen IPS will have standard first-generation IPS capabilities plus application awareness, context awareness, content awareness especially providing full stack inspection.*'

Cisco FirePOWER Next-Generation IPS (NGIPS)

Cisco FirePOWER NGIPS [243] solution integrates real-time contextual awareness, network intrusion prevention and intelligent security automation. It allows you to tackle the entire attack field providing more visibility into the environment.

Highlights

- Real-time contextual awareness that correlate extensive amounts of event data related to IT environments like applications, users, devices, OSs, vulnerabilities, services, processes, network behaviours, files, and threats.
- Advanced threat protection validated by independent third-party testing.
- Intelligent security automation such as event impact assessment, IPS policy tuning, policy management, network behaviour analysis, and user identification.
- Low-latency, single-pass design of appliances that promote high performance and scalability.
- Application control options including URL filtering and advanced malware protection (AMP) discover, track, and block suspect files and malware preventing the spread of outbreaks and reinfection.

McAfee Network Security Platform (NSP)

The McAfee NSP [244] is an IPS solution that discovers and blocks advanced threats in the network using multiple, signature-less detection techniques such as Advanced Threat Defence, real-time emulation, and endpoint integration. The next-generation hardware platform scales to speeds of over 40 Gbps, so that performance meets the needs of demanding networks.

McAfee NSP uses behavioural heuristics with real-time McAfee Global Threat Intelligence feeds to accurately identify and prevent malicious attacks for which no signature exists. It does this by organising multiple security technologies to handle elusive and evasive attacks that are missed when only one approach is used in an IDS.

Highlights

- Streamlines security operations with beyond layer-7 visibility to expose hidden attack patterns for fast, accurate response to network-borne attacks.

- Identifies both the known and unknown attack by leveraging multiple signature-less intrusion detection engines as well as vulnerability-based signature detection to defend against malware and zero day attacks.
- Reliable, high-performance multi-gigabit throughput even when next-generation features, enabled with stateful fail-over, are available.

Checkpoint Intrusion Prevention System (IPS) Software Blade

The Check Point IPS [245] is a Next-generation IPS plus firewall and also features application control, URL filtering, Data Loss Prevention (DLP) and multi-Gigabit performance - up to 15 Gbps of IPS and 30 Gbps of firewall throughput. In addition, stateful inspection and SecureXL technology deliver multi-tier IPS inspection and accelerated IPS throughput.

Highlights

- One-click activation of IPS and firewall protection on any Check Point gateway.
- Protects against malware, DDoS/DoS attacks, application and server vulnerabilities, unwanted traffic (IM/P2P), and insider threats.
- Geo protection policies - traffic can be monitored based on source or destination country.
- Real-Time protections - constantly updated with new defences against emerging threats.
- Microsoft vulnerability coverage provides preemptive protections against emerging vulnerabilities and exploits.

Sourcefire Next-Generation IPS

The Sourcefire Next-Generation IPS [246] integrates real-time contextual awareness, full-stack visibility and intelligent security automation to deliver effective security, performance and low total cost of ownership. The passive IDS mode notifies of suspicious network traffic and behaviour while inline IPS mode blocks threats. Optional subscription licenses can be purchased to add Application Control, URL Filtering and Advanced Malware Protection. The Sourcefire FireSIGHT Management Center allows administrators to centrally manage hundreds of appliances.

Highlights

- Application Control solutions do not require new hardware, detection or management points within the network.
- Granular control of over 1,800 applications detected and classified by risk and business relevance.
- URL Filtering subscription adds the ability to filter more than 280 million top level domains by risk level and over 82 categories

Open Source IDS

There are quite a few open source IDSs available with Snort being one of the most popular. Other NIDS include Suricata (IDS/IPS), Bro-IDS, and Kismet (WIDS).

Open Source IDS	Description	Highlights
Snort IDS snort.org	Snort is a network intrusion prevention system that performs real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis, content searching/matching, and detects a variety of attacks and probes.	Packet sniffer (i.e. tcpdump) Packet logger (useful for network traffic debugging, etc)
Suricata IDS/IPS suricata-ids.org	Suricata implements a complete signature language to match on known threats, policy violations and malicious behaviour. It also detects	Highly scalable - multithreaded and load balancing. Automatic protocol identification – allows for writing a

	many anomalies in the traffic it inspects.	rule to the protocol, not to the port expected. File Identification, MD5 Checksums, and File Extraction. NSM – Network Security Monitoring.
Bro-IDS bro.org	Bro provides a comprehensive platform for network traffic analysis, focusing on semantic security monitoring at scale. It provides users with a flexible framework that facilitates customised, in-depth monitoring exceeding the capabilities of traditional systems.	Adaptable - domain-specific scripting language enables site-specific monitoring policies. Flexible - is not restricted to any particular detection approach and does not rely on traditional signatures. Forensics - logs what it sees and provides a high-level archive of a network's activity. In-depth Analysis – has analysers for many protocols, enabling high-level semantic analysis at the application layer.
Kismet WIDS kismetwireless.net/	Kismet is a wireless IDS, providing a stateless and stateful IDS for layer 2 and layer 3 wireless attacks. It alerts on fingerprints (specific single-packet attacks) and trends (unusual probes, disassociation floods, etc).	Wireless network detector. Sniffer. Works with wireless cards that supports raw monitoring (rfmon) mode. Identifies networks by passively collecting packets and detecting standard named networks.

12.2.9.2. Host intrusion detection systems (HIDS)

A HIDS runs on individual hosts or devices on the network. It monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. A snapshot is taken of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to take action.

Some well-known commercially available HIDS include McAfee Host Intrusion Prevention, Trend Micro EPS w/ Mobile Security, Symantec Endpoint Protection and Checkpoint.

McAfee Complete Endpoint Protection — Enterprise

McAfee Complete Endpoint - Protection [247] is a tool that provides protection for all endpoints including Windows, Mac and Linux systems; plus smartphones, tablets, and virtual machines. It simplifies management and reduces costs while effectively protecting endpoints from threats including rootkits and advanced persistent threats (APTs). It employs a Security Connected approach consisting of dynamic whitelisting, smart scanning, advanced anti-malware, mobile protection, etc.

Highlights

- Behaviour and reputation protection integrated with cloud-based McAfee Global Threat Intelligence to protect against cyber threats across files, the web, messages, and network.
- Real Time for McAfee ePO brings immediate visibility into the security posture and security software configurations to fix problems quickly
- Easy installation, only takes 20 minutes to get started

Trend Micro End Point Security and Mobile Security

Trend Micro Enterprise Security for Endpoints [248] delivers protection including antimalware, web reputation technology to block access to malicious websites, and HIPS protection. With Trend Micro's cloud-based security, pattern files are managed in the cloud and not on endpoints, thus freeing computing resources and optimizing performance.

Trend Micro Enterprise Security for Endpoints provides protection for file servers, desktops, and laptops with faster scans, support for virtual desktop infrastructure (VDI) and virtual patching. Add on Trend Micro Enterprise Data Protection for mobile security, integrated data loss prevention (DLP), and data encryption.

Highlights

Mobile Device Security add-on:

- Detects and blocks malicious applications and data files
- Anti-malware and web reputation blocks malware and malicious websites
- Capable of detecting attacks that enter via network applications, ports and services, using the firewall and IDS
- User policies can be configured to monitor, block, and logs calls, SMS and MMS sent to and from devices

Symantec Endpoint Protection

Symantec Endpoint Protection [249] combines traditional antivirus, Network Threat Protection analysis, firewall and IPS to deliver full protection on physical and virtual systems.

Highlights

- Replaced traditional scanning of every file with scan elimination and de-duplication through Virtual Image Exception and Shared Insight Cache, reducing scan times and providing the fastest performance available. Known good files can be skipped.
- Provides layered protection across Windows, Mac, Linux and Virtual machines
- Enhanced remote deployment
- Granular policy settings that enable system lockdown, host integrity and application and device control

Check Point Capsule Cloud

Check Point Capsule [250] enables organizations to extend their corporate security policy to mobile devices, providing real-time protection against web threats for mobile users outside of the enterprise security perimeter. Check Point Capsule offers the protection of the Check Point Software Blades as a cloud-based service, and ensures that corporate policy is always enforced and corporate data and devices are protected.

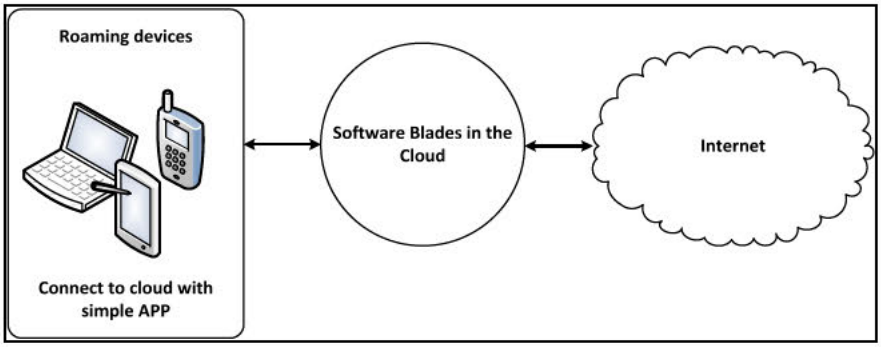


Figure 19. Overview of CheckPoint Capsule Cloud [250]

Highlights

- Protects laptops, iOS / Android tablets and smartphones or laptops.
- All traffic from any roaming device is directed to the cloud service using a secure tunnel; data is not sent in the clear and packets are scanned for both inbound and outbound traffic.
- Remote offices can leverage the security service by connecting their local appliance to the cloud, thus extending corporate security without deploying additional hardware.
- Logs can be viewed and polices managed via the Check Point Security Management web interface.
- Client installation supports Group Policy Object (GPO) distribution and Single Sign-On (SSO); the client configures itself.
- Integrates with Active Directory.
- Newly discovered threats are sent to ThreatCloud; each newly discovered threat signature is distributed to other Check Point connected gateways and the cloud to block the threat before it spreads.

Open Source HIDS

Open Source SECurity (OSSEC)
Open Source SECurity (OSSEC) [251] is a free, Host-based Intrusion Detection System that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting and active response. It runs on most OSs, including Linux, Solaris, Advanced Interactive eXecutive (AIX), HP-UX, Berkeley Software Distribution (BSD), Windows, Mac and VMware ESX. OSSEC also includes log monitoring and SIEM functionality. Other benefits of note are compliance, central management, real-time and configurable Alerts, agent and agentless monitoring.

Advanced Intrusion Detection Environment (AIDE)
Advanced Intrusion Detection Environment (AIDE) [252] is a file and directory integrity checker. It runs on Linux and works by creating a database from the regular expression rules that it finds from the config file(s). Once this database is initialised it can be used to verify the integrity of the files. Several message digest algorithms are used to check the integrity of the file and usual file attributes can also be checked for inconsistencies.

Tripwire
Open Source Tripwire [253] software is a security and data integrity tool that monitors and alerts on specific file changes. It scans the file system and stores information on each file scanned in a database. Subsequently, the same files are scanned and the results compared against the stored values in the database and changes are

reported. Cryptographic hashes are employed to detect changes in a file without storing the entire contents of the file in the database.

Open Source Tripwire also serve many other purposes, such as integrity assurance, change management, and policy compliance.

Mobile IDS/IPS

Although there are many host-based IDS/IPS available, solutions for mobile devices are not as prevalent. Two companies that have brought IDS/IPS to mobile devices arena are Zimperium Mobile Security and Skycure.

Skycure

Skycure's [254] technology offers a complete device-level approach to securing mobile devices from internal and external threats. Its mobile apps are seamless, running in the background and do not affect usability, performance, or battery consumption. The apps alert the user in real-time when the device's security is compromised. The apps also provide the user with mitigation steps and educational content to help better secure the mobile device.

Highlights

- iOS and Android devices supported
- Active honeypot where detection sensors identify when the device is under attack and trigger protection
- Continuous detection - continuous behavioural analysis of device and wireless network activity
- Selective Protection - protects mobile devices selectively in accordance with specific IT policies
- Cloud-based enabling management
- Secure communications to prevent Wi-Fi MitM attacks
- Cloud-based and/or on premise deployment

Zimperium Enterprise Mobile Security

Zimperium Enterprise Mobile Security [255] has several products to secure mobile devices. zIPS is a mobile intrusion prevention system application for iOS and Android devices that defends against both network and host-based cyber-attacks, and can detect both known and unknown threats by analyzing the behaviour of a mobile device. By monitoring small deviations in the mobile device's statistics, processes, memory, CPU and other parameters, z9 technology can accurately identify the specific type of malicious attack, and the forensics that indicate the circumstances of how the attack occurred. The z9 engine does not use application sandboxing or tunnel traffic through the cloud, but sits directly on the mobile devices within the zIPS application.

Product named z9 monitors the whole device for malicious behaviour and dynamically detects known and unknown threats in real-time thereby preventing compromised mobile devices from gaining access to the corporate network by isolating the device or disabling it from the Wi-Fi access point. It can detect the following host based attacks: a) spearphishing attacks via malicious URLS and PDF files, b) malicious applications such as time bombs and self-modifying applications, c) OS exploits and d) kernel exploits. From the network attacks it can detect the following: a) reconnaissance scans, b) network traffic redirection, i.e., MitM attacks, c) SSL stripping techniques, d) rogue access points, e) rogue basestation/femtocell.

To complement zIPS, Zimperium also offers zConsole, an enterprise mobile threat management dashboard that provides visibility into each security incident on zIPS-protected mobile devices with forensic detail. zAnti, is an

enterprise mobile risk assessment penetration testing tool for performing security audits. It is a mobile penetration testing toolkit that lets security managers assess the risk level of a network and gives administrators the ability to simulate an advanced adversary in order to identify the malicious techniques they use to compromise the network. Using the available customizable network reconnaissance scans, security administrators can also discover authentication, backdoor, brute-force attacks, DNS and protocol-specific attacks and rogue access points.

12.2.9.3. Wireless intrusion detection systems (WIDS) and prevention systems (WIPS)

Wireless Intrusion Detection Systems helps protect wireless LANs (WLAN) by monitoring the radio spectrum for the presence of unauthorised rogue access points and the use of wireless attack tools. When a rogue access point is detected, an alert is sent. Rogue access points are discovered by comparing the MAC address of the participating wireless devices or fingerprinting.

Wireless Intrusion Prevention Systems prevent attacks perpetrated through exploits conducted via the infiltration of rogue access points. WIPS sensors analyse the traffic in the air and then send the information to WIPS server. The WIPS server then compares and validates the information against the defined policies and assigns a threat classification. If a threat is discovered the administrator is sent an alert and the WIPS takes automatic protection measures.

Motorola* AirDefense *Wireless IDPS

AirDefense's Security & Compliance commercial solution [256] is an advanced continuous wireless monitoring tool that identifies network attacks, vulnerabilities and can terminate connections to any rogue device. It is meant for both intrusion detection and prevention. The system uses collaborative intelligence, with access points and dedicated sensors that work with a server appliance to monitor all 802.11 (a/b/g/n) wireless traffic. In addition to protection against threats the solution also offers policy and compliance monitoring.

Kismet

Kismet [257] is a free and open source wireless network detector, sniffer, and intrusion detection system. It works with any wireless card that supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet also supports plugins that extends sniffing to other media such as DECT.

Kismet passively collects packets, detecting standard named and hidden networks, and inferring the presence of non-beaconing networks via data traffic. It includes IDS functionality, providing both stateless and stateful IDS for layer 2 and layer 3 wireless attacks. Kismet can alert on fingerprints (specific single-packet attacks) and trends such as unusual probes, disassociation floods, etc.

Snort IDS

As described in the section 12.2.9.1. 'Network intrusion detection systems (NIDS)', Snort IDS is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS). [258] It can also be configured via rule sets as a WIDS.

12.2.10. Security Information & Event Management (SIEM)

As described by Algis Kibirkstis in [259] A SIEM system is defined as a hybrid solution coming from two distinct security-related products: Security Information Management (SIM) systems, technologies focused upon policy and standards compliance through the consolidation of logs, the analysis of data and the reporting of findings; and Security Event Management (SEM) systems, which provide technical support in the management of threats, events and security incidents in real time [259].

In a nutshell, SIEM systems identify, monitor, record and analyse security events or incidents; they also usually employ log management.

12.2.10.1. HP's ArcSight ESM

ArcSight Enterprise Security Management (ESM) [260] software is a comprehensive SIEM solution that provides real-time event correlation and security analytics to identify and prioritise threats and remediate incidents. Data is automatically collected from devices and applications from within a user and environmental context, and Big Data analytics capability is offered for high volume organizations (up to 100TB per node).

Security auditors benefit from ArcSight's ability to collect, store, and analyse any log or event data from any system and can purchase add-on compliance packs with built in reporting that supports PCI, SOX, and IT governance.

In addition, ArcSight can instantly detect activities on the network including insider or zero-day attacks, as it is able to collect and categorise up to 100,000 events per second.

With an agent in a smart phone, it is possible to get logs from there and integrate them to ArcSight as connectors. This enables usage of the information of MDM systems in ArcSight's event correlation. It is also possible to use logs of email (or similar) servers to get information about the used device (such as browser). This enables easily, e.g. identifying type of devices, identifying if the user has multiple devices and tracking users as they use devices from different locations, and generating alerts based on policies.

12.2.10.2. McAfee SIEM

The McAfee SIEM [261] combines event, threat, and risk data together to provide security intelligence, rapid incident response, seamless log management, and extended compliance reporting. The Enterprise Security Manager consolidates, correlates, assesses, and prioritises security events for both third-party and McAfee solutions. The McAfee SIEM solution is made up of the components described in Table 23.

Table 23. Main components of McAfee SIEM.

Component	Description
McAfee Enterprise Security Manager	Identifies critical threats and satisfies compliance audit requirements. The continuous global threat and enterprise risk feeds expedites remediation of threats and compliance reporting is done quickly and efficiently.
McAfee Enterprise Log Manager	Automates log management and analysis. Logs are signed and validated, to ensure authenticity and integrity necessary for regulatory compliance and forensics. It includes ready-made compliance rule sets and reports.
McAfee Database Event Monitor for SIEM	Monitors access to database configurations and data; non-intrusive security logging of database transactions. It consolidates database activity into a central audit repository; integrates with McAfee Enterprise Security Manager to analyse and detect suspect activity.
McAfee Advanced Correlation Engine	Monitors data in real-time thereby allowing for use of both rule-based and rule-less correlation engines at the same time to detect risks and threats before they occur; can be deployed in either real-time or historical modes.

Other components include the McAfee Global Threat Intelligence for Enterprise Security Manager, McAfee Application Data Monitor and the McAfee Event Receiver.

12.2.10.3. Splunk Enterprise (w/ App for Enterprise Security)

Splunk Enterprise [262] is an affordable, Operational Intelligence Platform that monitors and analyses machine data from IT systems and technology infrastructure. It collects and indexes any machine-generated data from just about any source or location in real-time. This includes data streaming from packaged and custom applications, application servers, web servers, databases, wire data from networks, virtual machines, telecoms equipment, OSs, sensors, mobile devices and more.

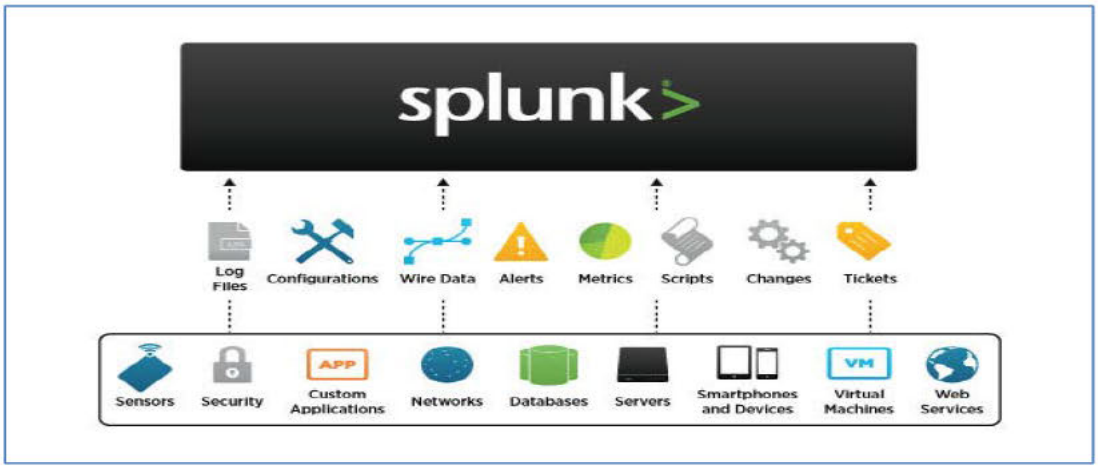


Figure 20. Splunk [262].

The Splunk App for Enterprise Security add-on adds ability to uncover APTs, conduct Incidence Response, perform compliance audits and run comprehensive risk analytics.

12.2.10.4. LogRhythm SIEM 2.0

LogRhythm [263] integrates log management and SIEM capabilities with file integrity monitoring and machine analytics along with with Host and Network Forensics. This next generation SIEM analyses all available log and machine data and combines it with forensic data capture at the host and network levels. Additionally, the AI Engine, LogRhythm's patented Machine Analytics technology, delivers automated, continuous analysis of all activity observed within the environment.

LogRhythm's Next Gen SIEM platform delivers real-time threat and breach detection and alerting, advanced correlation and pattern recognition, anomaly detection for users, hosts and network, forensic and log analysis, integrated case management and continuous compliance assurance with automation suites with no additional setup or configuration required.

12.2.10.5. IBM Security QRadar SIEM

IBM QRadar [264] combines log source event data from device endpoints and applications located throughout a network. Normalization and correlation activities are performed on raw data to distinguish real threats from false positives and the system can also correlate system vulnerabilities with event and network data, to foster prioritisation of security incidents.

With add-ons IBM Security QRadar QFlow or VFlow Collector appliance, QRadar SIEM can monitor the use of applications such as ERP, databases, Skype, VoIP and social media from within the network. Another option, IBM Security X-ForceThreat Intelligence, supplies a list of potentially malicious IP addresses including malware hosts, spam sources, etc.

IBM QRadar also features detailed data access and user activity reports to manage compliance and security intelligence in cloud environments.

12.2.10.6. AlienVault (all-in-one) SIEM+

AlienVault's Unified Security Management (USM) [265] platform includes five capabilities in a single console: SIEM, Behavioural Monitoring (netflow analysis, log collection, full packet capture), Threat Detection (IDS,

HIDS, WIDS, file integrity), Asset Discovery and Vulnerability Assessment (testing, continuous monitoring). Both threats and compliance can be managed to include host-based, passive and active technologies.

This SIEM includes industry standard functionality and collects event logs and audit data come from OSs, network equipment, security devices like firewalls and IDS, vulnerability assessment tools, etc. Additionally, the USM built-in log management provides the raw logs needed for forensic analysis.

AlienVault's Network Intrusion Detection (NIDS) solution utilises Snort and Suricata, providing both signature-based anomaly detection and protocol analysis technologies.

12.2.10.7. Prelude OSS

Prelude [266] is an agentless SIEM that collects, normalises, sorts, aggregates, correlates and reports all security-related events independently of the product brand or license.

Prelude OSS is an Open Source version of Prelude published under the GPL V2. It implements the event management part of Prelude (SEM) and provides the basic functionality to manage a small network consisting of less than 10 systems.

12.2.11. Vulnerability Assessment Scanner (VAS)

A vulnerability assessment scanner is a software program that assesses computer information systems, networks or applications for weaknesses. Current VAS solutions include Tenable Network Security [267], Rapid 7 Nexpose [268], Retina CS Enterprise [269] and Retina CS for mobile [270] of Beyondtrust, Saint 8 [271], GFI Languard [272], SecurityMetrics Mobile Scan [273], OpenVAS [274] and Retina CS Community [275].

12.2.11.1. Tenable Network Security

Tenable's VAS solution includes Nessus, Passive Vulnerability Scanner (PVS) and Security Center [267]. They provide continuous network monitoring, identify vulnerabilities, reduce risk, and ensure compliance. Their properties are described in Table 24.

Table 24. Features of Tenable VAS solutions.

Solution	Description
Nessus Vulnerability Scanner	Tight integration with malware defences, patch management tools, SIEM, BYOD, firewalls, cloud infrastructure and virtualised systems. More supported technologies than any other vendor: OSs, network devices, hypervisors, databases, tablets, phones, web servers and critical infrastructure. Mobile devices plugin including BB, IOS, Windows Phone and Android MDM Mobile Device reporting
Passive Vulnerability Scanner	Identifies server and client-side vulnerabilities in new or transient assets Provides deep packet inspection to continuously discover and track users, applications, cloud infrastructure, trust relationships and vulnerabilities Automatically discovers users, infrastructure and vulnerabilities across various technologies to include OSs, network devices, hypervisors, databases, tablets, phones, web servers, cloud applications, and critical infrastructure.
Security Center Continuous View	Continuous Monitoring Platform that provides a special combination of detection, reporting and pattern recognition utilizing industry recognised algorithms and models. Vulnerability Management Log Collection Mobile, virtual & cloud coverage Compliance and patch monitoring Network Behaviour Analysis Malware detection Forensic analysis Incident Response

12.2.11.2. Rapid 7 Nexpose

Nexpose [268] is a vulnerability management solution that analyses vulnerabilities, controls, and configurations. To prioritise and drive risk reduction, it uses RealContext™ and RealRisk™ technologies, and simulates the adversary's mindset.

Mobilisafe is Nexpose's cloud based solution for continuous monitoring of vulnerabilities on mobile devices without requiring agents being installed on them. It allows for the automatic risk assessment of all the mobile devices (tablets, smartphones) and provides simple tools to eliminate those risks. Risks can be mitigated quickly and employees can easily update their devices to the latest available firmware to eliminate vulnerabilities, or those devices can be blocked from accessing the company network.

12.2.11.3. Retina CS Enterprise

Retina CS Enterprise [269] provides context-aware vulnerability assessment and risk analysis. Retina's architecture works with users to proactively identify security exposures, analyse business impact, and plan and conduct remediation across a disparate and heterogeneous infrastructure.

Highlights

- Discovers network, web, mobile, cloud and virtual infrastructure
- Profiles asset configuration and risk potential
- Pinpoints vulnerabilities, malware and attacks
- Analyses threat potential and return on remediation
- Remediates vulnerabilities via integrated patch management
- Reports on vulnerabilities, compliance, benchmarks, etc.
- Protects endpoints against client-side attacks

12.2.11.4. Retina CS for Mobile

Retina CS for Mobile [270] integrates mobile device assessment and vulnerability management thereby reducing risks for Android, Blackberry and devices managed via ActiveSync by implementing a proactive approach for discover, prioritise and fix smartphone security weaknesses.

Retina CS for Mobile supports compliance requirements with in-depth mobile vulnerability management audit trails as well as ability to audit mobile device hardware, applications and configurations. Automatic vulnerability audit updates are available via BeyondSaaS, a cloud-based, vulnerability assessment solution.

Other notable features include mobile device vulnerability profiles and severity based remediation.

12.2.11.5. Saint 8

Saint 8 [271] is an integrated security tool suite incorporating Vulnerability Assessment, Penetration Testing, Configuration Assessment and Regulatory Compliance (NIST SCAP, IAVA, PCI etc.). It is supported on the MacOS, Windows and Linux platforms and does not assess mobile devices except for laptops running the aforementioned OSs.

12.2.11.6. GFI Languard

GFI Languard [272] is a VAS that scans for vulnerabilities on Windows, Linux, MacOS, Android, and Apple iOS. It is also a network security scanner and performs remediation or patch management for Linux, Windows and MAC OS. Other capabilities include network and software auditing.

12.2.11.7. SecurityMetrics Mobile Scan

MobileScan [273] is a mobile defence application that identifies and reports mobile device vulnerabilities to secure mobile transactions on Android and iOS devices.

Highlights

- Scanning technology based on Payment Card Industry (PCI) mobile processing best practices
- Easy to use interface that directs users through each step of the scanning process
- Scanning schedule can be customised
- Award-winning customer support to educate and assist merchants with questions regarding
- Clear Threat Reporting - the report assigns a total risk score, summarises discovered vulnerabilities, and provides recommendations on threat resolution.
- Online compliance – centralised reporting to manage and track the security of all devices

12.2.11.8. Open Source VAS

Open Vulnerability Assessment System (OpenVAS)

OpenVAS [274] consists of several services and tools. Its main component is the OpenVAS Scanner, an SSL-secured service-oriented architecture. The scanner executes Network Vulnerability Tests (NVTs) which are updated daily via the OpenVAS NVT Feed or by a commercial feed service.

The OpenVAS Manager controls the scanner and provides the intelligence and the OpenVAS CLI provides a command-line interface, with the ability to act as a full service daemon, thus providing user and feed management.

The Greenbone Security Assistant (GSA) offers a web-based GUI called the Greenbone Security Desktop (GSD); it is a Qt-based desktop client that runs on Linux and Windows.

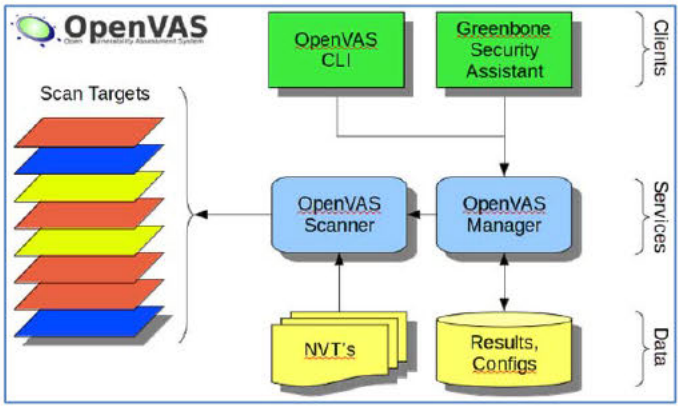


Figure 21. OpenVAS [274].

Retina CS Community

Retina Community [275] is a free VAS that identifies network vulnerabilities (including zero-day), configuration issues, and missing patches across OSs, applications, devices, and virtual environments. Up to 256 IPs are allotted for the free edition.

Retina Community features user profiles based on job function, full support for VMWare and integration with vCenter and exploit identification.

Other VAS systems with far less functionality and features include Microsoft Baseline Security Analyzer (MBSA) [276], Nexpose Community Edition, and SecureCheq.

12.2.12. Mobile Internet Security Suites

Internet security suites for personal mobile devices are becoming increasingly popular and are just as susceptible to the same attacks as desktop computers. The 2013 Norton Report showed that 57 percent of adults were unaware that security solutions existed for mobile devices, emphasizing the lack of awareness of mobile threats. Although Android has less vulnerability than iOS or Windows, it is attacked more because there are more devices with it installed on the market.

Mobile Internet Suite capabilities basically mirror those offered for desktops, except that the solutions are mostly cloud based, to reduce load on the processor, save space and preserve battery life.

Some companies offering mobile security apps include Kaspersky, Norton, McAfee, Network Intercept and Qihoo 360. Some free mobile security options are Avast Free Mobile Security, AVG Mobilation Anti-Virus Free, and Lookout Mobile Security.

Mobile Security Suite	Description	Highlights
Kaspersky Internet Security for Android	Secures tablets and smartphones with real-time protection against spam, viruses and spyware; blocks malicious sites; remote management; theft protection/ lost/stolen phone locator; automatic scanning of apps downloaded;	Two way firewall; Safe Money feature protects online transactions; privacy protection
Norton Mobile Security	Protects against malware, greyware and phishing; blocks unwanted calls/texts (spam); identifies apps that have privacy risks. Most features for Android phones and tablets; limited features for iOS and no BB support; No IDS/IPS.	Auto scans downloaded apps and able to scan SD cards; backs up contacts across devices;
360 Security (for Android phones only) **Qihoo 360**	Defends against malware; scans for and fixes vulnerabilities; blocks unwanted calls and SMS;	Data usage monitor; mobile data firewall; accelerator and power saver; cleans trash files, private usage history and useless APKs. Free.
McAfee Mobile Security – Android	Real-time antivirus protection - scans for malicious code in apps, SD cards and files; call and SMS filter; remote wipe and backup/restore capability.	Password protected uninstall feature; multiuser application profiles; CaptureCam silently takes a snapshot of thief and emails it to owner; ARP spoofing protection
McAfee Mobile Security for iPhone and iPad	Data backup and restore; PIN protect your photos and devices with Secure Media vault; lost / stolen locator service	CaptureCam; Remote Scream - activates an alarm to locate a lost or stolen device.
Network Intercept – SecureMe for Mobile Phones	AV Scanning as a Service; 128 bit web traffic encryption; Anti-Phishing and Anti-Malware Service	Anonymous web browsing; MitM Protection; compression
Open Whisper Systems	**Open Source** security for mobile devices offering secure phone and text communication; licensed GPLv3 and free.	Red Phone delivers end-to-end encryption for calls; TextSecure encrypts text and chat messages over the air and on the phone (Curve25519, AES-256, and HMAC-SHA256). Messages are encrypted locally.

12.2.13. Mobile firewalls

One example of a firewall running on a smartphone is Mobiwal [277]. It is an Android Firewall that monitors and controls the data connections initiated by a user's applications. Mobiwal prevents data leakage, manages

data limits and increases battery uptime. It doesn't need root permission, and can be run directly on any Android device, whether it is rooted or not.

Highlights

- Data permissions can be customised to Allow/Block individual applications. Mobiwol allows freedom to decide which apps access the web and how, with the option to block all background activity for an app, allowing it to connect to the outside world only when it's active in the foreground (saving battery).
- The Data Usage Reporting feature replaces the Android built-in Data Usage screens to show exactly how much data apps on your device use collectively as well as individually, and also lets you set limits on data usage.
- Mobiwol tracks and logs the activity initiated by your device; each application that accesses a data connection is logged, along with the IP address of the server for which it is intending to connect.
- Real-time notifications - notifies you when an application tries to connect to the Internet by sending a notification to the notification bar

12.2.14. Proxifiers

A proxifier is software which can make other programs pass through a proxy server by intercepting and modifying their network requests (M38). There is a lot of different software for different platforms, with some platforms having none. For example, ProxyCap is under a proprietary (Shareware) license (but not with the code available) for MacOSX, Windows and Windows Mobile and supports SOCKS5 and SSH1 and SSH2. On the other hand for Linux and Android there are open-source applications that supports SOCKS5 but not SSH1 and SSH2. Proxifiers have been compared in Wikipedia [278].

As described in [279], there are several problems with proxies, such as slow performance.

12.2.15. Virtualisation

Virtualisation (M18) is used in several system components to improve security.

Mobile virtualisation is hardware virtualisation on a smartphone, enabling secure separation between the underlying hardware and the software that runs on top of it. Mobile virtualisation could be used in smartphones to make them cheaper [280] [281], but also in enterprise phones to support multiple domains and OSs on the same hardware [282] [283] [284] [285]. As described in [286], VMware's Mobile Virtualization Platform (MVP) solution had to be preloaded into the phone by the manufacturer, and the approach of having two phones in one didn't catch on in general for users or IT managers.

Virtual Desktop Infrastructure (VDI) is a service hosting user's desktops on remove servers, and allowing users to access these desktops over a network from almost any device, including desktops, laptops, tablets and smartphones. This means that users can access their desktop from any location, without having to use only single client device or OS. Because resources are centralised, users moving between locations can still access the same desktop environment with their applications and data. Vendors such as Citrix [287], HP [288] and VMware [289] are offering VDI solutions. It is claimed that VDIs provide IT administrators with centralised delivery, management, control of virtual desktops and more efficiency [290].

One example product using the VDI approach is Hypori (originally DroidCloud) [168]. It is claimed that it is possible to integrate Hypori platform with existing EMM, MDM and MAM solutions as also application stores, LDAP, multifactor authentication solutions, monitoring, DevOps deployments and auditing [168].

Jolla smartphones [144] run Alien Dalvik [291] on top of the Sailfish OS as a virtual machine. Alien Dalvik lacks some features of Google's DalvikVM on Android and some device specific information, features and memory, but it provides running Android applications in a virtual machine. RIM is offering BlackBerry PlayBook support

for Android applications, but it allows running only Android applications that have been packaged and added correctly to the Blackberry World.

All virtualisation techniques use the resources of the device, and thus can result in battery exhaustion.

12.2.16. Summary of the review of existing products

All of the described secure phone models, secure OSs, MDMs, and monitoring products used in them give plenty of mechanisms for administrators to track devices and their usage, authenticate users with multi-factor mechanism, as well as manage security policies. Still, there are several possible improvements for the systems, as described in the following sections.

There are many monitoring tools available to keep networks, information systems and increasingly, mobile devices, secure from attacks including SIEM systems, IDS, HIDS, WIDS and VAS.

Table 25. Existing monitoring solutions

	Monitoring solution	Description
SIEM	Security Information & Event Management	Manages threats, events and security incidents in real time.
NIDS	Intrusion Detection System	Network based tool that monitors network traffic and sends alerts when a compromise is detected.
HIDS	Host Intrusion Detection System	Host based tool that monitors file integrity on systems and sends alerts when a compromise is detected.
WIDS	Wireless Intrusion Detection System	Monitors wireless traffic to detect and prevent attacks such as DoS or rogue access points.
VAS	Vulnerability Assessment Scanner	Software application that assesses security vulnerabilities in networks or host systems

Existing commercial and free products are lacking some of mitigating techniques listed in Table 6, however they are using some additional mitigation techniques, which have not yet been recommended in guidelines, checklists, or other documents presented in the section 12.1. 'Existing guidelines, checklists and lists of security controls'. Such mitigation techniques can be categorised under the groups listed in Table 26.

Table 26. Additional mitigation techniques in commercial products.

	Mitigation technique
M37.	Reviewing the source code of the OS and the applications. (T2, T5, T8)
M38.	Host-based / mobile firewalls, IDS and IPS. (T11, T5, T1)
M39.	Self-destroying messages. (T1)
M40.	Destroying the data by destroying the storage media remotely (T3, T1, T2)
M41.	Security labeling of contacts and data to prevent information leaking by email (T1)
M42.	Multiple user accounts with different permissions (T1, T2)
M43.	Hardware accelerated encryption and/or RNG (T3, T1)

The following section describes related ideas presented by researchers.

12.3. Countermeasures presented by researchers

This section describes research papers including mechanisms and frameworks for enforcing security policies, and security controls to be used, e.g., in mobile devices, but which have not (yet) been widely deployed in commercial products.

12.3.1. Malware and rootkit detection

As described in [292], static analysis, dynamic analysis, monitoring and virtualisation have been used for securing Android. Several AV products for smart phones are available, and many guidelines mention AV software as one of security controls (M22).

As discussed in [46], rootkit detection tools must be isolated from the OS that is being monitored: In normal desktop computers rootkit detectors are executed on a secure co-processor or isolated using virtualisation, however they were not suitable for smartphones when the article was written. Virtualisation, TPM and MTM can be used to detect rootkits.

12.3.2. Enforcing security policies

Proposals of ways for enforcing policies (M46) in mobile devices have been presented in [293] [294] [292] [295] [296] [297] [14].

The authors of [295] present a Context-Related Policy Enforcing for Android (CRêPE) architecture, which runs on Android OS and enables user to change the behaviour of the phone according to contextual situations. Context-related policies can be set by the user and authorised third parties at run-time or remotely via SMS, MMS, Bluetooth or QR-code.

In [294], a digital rights management (DRM) based policy enforcement architecture is proposed. The research is focused on applications that delivered content via SMS, MMS, or email. It is mentioned that unintended exposure can leak business secrets or compromise the access control system. Unauthorised exposure of commands could reveal the application behaviour, and indirectly the user's intent and tampering of the commands could lead applications to misbehave.

The approach presented in [297] is to edit the Android boot script to make software called FireDroid the parent process of Zygote which is responsible for launching all new processes on Android. This way, FireDroid is able to monitor all processes on Android. Policies can allow or deny actions, kill applications, or prompt the user for one of those choices. To edit the Android boot script, rooting of the device is required.

Aurasium [292] allows full control of execution of applications. This is done by repackaging and signing the application. This approach does not require rooting or re-flashing Android devices.

RetroSkeleton presented in [296] does not require rooting of the device. The proposed approach is to modify existing applications with wanted policies. The system diagram of RetroSkeleton is presented in Figure 22.

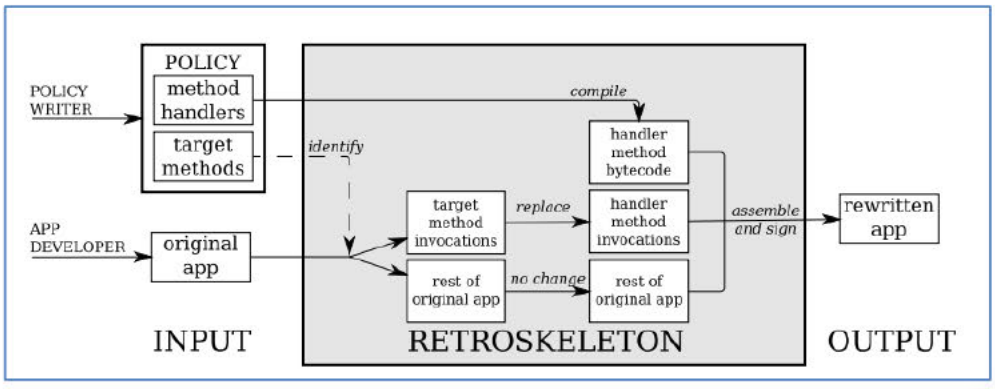


Figure 22. RetroSkeleton System Diagram [296].

A short presentation of FireDroid and RetroSkeleton can be watched from [298].

In [14] a security policy enforcement framework called MobileGuardian is proposed. Security policy enforcement is divided into 1) sensitive data isolation, 2) security policy formulation, 3) security policy testing and 3) security policy execution.

12.3.3. Multi-factor authentication

As described in previous sections, commercial mobile devices already use multi-factor authentication, e.g., by combining passwords, fingerprint readers, location information, contactless and connected software and hardware tokens, and smart cards. Researchers have proposed additional techniques such as face [299] [300] [301], iris data [302] [299], finger-vein [303], voice [299] [300], hand geometry, handwriting, gait/walking pattern [304] [299], and keystroke pattern [305] [306] recognition. Many of these recognition mechanisms require additional hardware and software, which increases the price (and usually also the size) of the product, and thus are not yet widely used. Biometric recognition techniques have several challenges [307], such as problems in face recognition under different lightning conditions [308].

Authentication can also be improved, by hardening keypads as presented in [309].

As described in [24], passwords are one of the most challenging topics to communicate, and one of the most difficult behaviours to be changed. They are also expensive, e.g., for Espoo city, it costs 200,000 euros a year to change forgotten passwords of the city's workers [310]. OWASP gives the following security control [122]: '*Instead of passwords consider using longer term authorization tokens that can be securely stored on the device (as per the OAuth model). Encrypt the tokens in transit (using SSL/TLS). Tokens can be issued by the backend service after verifying Smartphones secure development guidelines for application developers the user credentials initially. The tokens should be time bounded to the specific service as well as revocable (if possible server side), thereby minimizing the damage in loss scenarios. Use the latest versions of the authorization standards (such as OAuth 2.0). Make sure that these tokens expire as frequently as practicable.*'

The following examples are presented as ideas to change user behaviour: 1) People should be ensured to create strong passwords or passphrases, and 2) people should be taught how to use passwords securely.

There are mechanisms for preventing the use of weak passwords [311], and to analyse the security of passwords [233]. Because passwords are ubiquitous, and people tend to have tens of accounts, there is a risk that people use the same (otherwise good) password in multiple accounts, use almost the same password in multiple accounts but change only the last characters of the password, or enrol a list of passwords in different accounts. This risk exists even if people use mechanisms, such as presented in [312] to remember their passwords. Mechanisms to discover if the same passwords have been used in different accounts are very limited if not impossible. Using passwords, especially in mobile devices, presents additional challenges. Typing passwords with a mobile device takes a long time with the constrained keyboards [313], and is error-prone [15] Reports about hacked websites where passwords have been stolen and published abound. These passwords were not stored safely or were so weak that they were easy to decipher [39].

The authors of [24] give an example: if a user is using the same password for multiple accounts, they most likely cannot remember many passwords, and thus password management tools should be considered along with tuition on how to use them. An even better solution would be disabling passwords totally. As described in the section 12.3. 'Countermeasures presented by researchers', new types of passwords, based, e.g., on patterns, figures or questions have been researched. With a combination of new types of passwords, graphical CAPTCHAs, certificates, and multifactor, implicit and/or adaptive authentication, the usage of passwords could be decreased or even be disabled and system usability improved without decreasing its security (M48).

When the amount of required separate devices in the multi-factor authentication procedure increases, the risk of losing one of them increases. Because of this, there should be backup mechanisms, e.g., to select any of the available corresponding factors.

12.3.4. Context-based and implicit authentication

As described in [314], multi-factor authentication is costly to implement, it disrupts legitimate user activity and can be bypassed. Bypassing examples have been presented in [315] [316]. With context-based authentication, organisations can create rules that determine, pre-authentication, whether and how a given authentication process should proceed based on context. Context can include information such as a) device registration and fingerprinting, b) source IP reputation data, c) comparing user's current information with the corresponding information kept in a directory or user store, d) geo-location, e) geo-fencing, f) geo-velocity, and g) behavioural analysis [314]. Context-aware authentication mechanisms have been proposed in [317] [318] [319].

Implicit authentication (M44) is an ability to authenticate mobile users based on actions they would carry out anyway. It has similarities to context-based authentication, e.g., if location is used for the authentication. Jacobson et al. [320] use this in a scoring algorithm where combination of time of day, location of the user and time elapsed since the last good call, and inter-arrival time between bad calls are used to calculate an authentication score. Positive and negative events must be identified. Positive events are common habits and they increase the authentication score. Negative events are not commonly seen for a user or are associated with attacks, and they decrease the authentication score. When the authentication score falls below a specific threshold, the user must explicitly authenticate themselves, e.g., by providing a password.

Implicit authentication provides additional security controls and most likely improves usefulness of the device, if it is implemented properly. Possibilities of context-aware systems in providing more secure user authentication, e.g., by applying the context itself as an authentication factor have been discussed in [321].

12.3.5. Adaptive security

Adaptive information security (M45) enables changes and modification of security mechanisms at runtime [322]. Adaptive security has some similar features to implicit authentication. In fact, implicit authentication can be seen as one part of adaptive security: it could be used only if the security level of the system is between certain thresholds, otherwise explicit authentication mechanisms, e.g., based on passwords or biometric recognition would be used.

One use case for adaptive security is selecting encryption mechanisms for transmitted data, video and VoIP calls, or for text messages. If the security level in the environment is good, the system may rely only on encryption of communication protocols such as Wi-Fi, 3G and 4G. When the security level deteriorates, the system starts to use additional encryption layers, e.g., by using VPN tunnels, IPsec, TLS/SSL, and/or PGP, with ciphersuites that have been previously or during the runtime selected suitable for certain security levels. Adaptive security could be used to improve user experience, and also decrease bad user experience, e.g. as caused by VPN.

Even at the lowest security level, the used ciphersuites should be secure. For example, when using TLS or DTLS, version 1.2 should be used with ciphersuites that 1) use keys suitable for mobile devices (RSA and DSA take much more memory space than ECDSA and PSK), 2) provide perfect forward secrecy by using exchange mechanisms with ephemeral functionality such as ECDHE and DHE, 3) use at least 128-bit AES keys, 4) use block-cipher modes that provide AE, such as GCM, CCM or EAX, 5) do not provide anonym authentication, does not provide NULL-encryption and 6) uses 8 octet bit MAC if MAC is used. Examples of ciphersuites providing these features are TLS_DHE_PSK_WITH_AES_256_GCM_SHA384, TLS_PSK_DHE_WITH_AES_256_CCM_8, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 and TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8.

12.3.6. Securing communication without CAs

Security systems using certification authority (CA) based public key infrastructure (PKI) have several problems [323] [324] [325] [326], which can be caused, e.g., because of compromise of CA organisations [327] [328] [329] [330]. Many TLS/SSL implementations have and have had serious vulnerabilities [331] [332] [333] [334], and many of the supported protocols or algorithms used in implementations are obsolete and insecure [335].

Protocols such as Pretty Good Privacy (PGP) and OpenPGP [336], Off-the-Record (OTR) messaging [337], okTurtles [326] and hardware based one-time pads (OTP) [128] have been proposed and used instead of systems based on CAs and PKI (M47).

DNSChain is used to authenticate webpages and okTurtles individuals with DNSChain. PKI and CA based authentication is replaced with a NameCoin (NMC) based on, and asynchronous Off-the-record (OTR) is used to provide end-to-end encryption and perfect forward secrecy (PFS) [326] [338].

Tinfoil Chat (TFC) described in [128] uses information to theoretically secure encryption and authentication, hardware RNGs, and data diodes to prevent exfiltration of plaintext and encryption keys.

OTR is used mostly for IM, and it provides encryption, authentication, deniability, and PFS [337].

12.3.7. Summary of review of research publications

Research papers are proposing using some additional mitigation techniques, which have not been recommended in guidelines, checklists, or other documents presented in the section 12.1. 'Existing guidelines, checklists and lists of security controls' or haven't been used in commercial products presented in section 12.2. 'Existing countermeasures and security controls'. Such mitigation techniques can be categorised under the groups described in Table 27.

Table 27. Additional mitigation techniques presented in research publications.

	Mitigation technique
M44.	Context-aware and/or implicit authentication. (T2, T5)
M45.	Adaptive security. (T1, T2, T5, T6, T7, T11)
M46.	Security policy enforcement frameworks. (T1, T6)
M47.	Not CA based secure communication. (T5, T6, T8)

It should be noted that there has also been research done in other areas to improve the security of smartphones.

13. Results

This section analyses which of the risks described in the sections 9. ‘Usage scenarios, actors and assets to be protected‘, 10. ‘Threats‘ and 11. ‘Risk analysis‘ can and which cannot be mitigated by using guidelines, security controls, checklists, research proposals, or the commercial products presented in the ‘Literature Review‘. Several security controls exists, however not all of them are widely used.

It was discovered that authentication mechanisms need improvements. For example, the user has to be authenticated also during the usage of the device, not just when she/he is logging into the device or to the services. The reason for this is that an unauthorised user might gain the device after the login and use it maliciously before the next required login.

Sensitive data should be protected better; there should be mechanisms for finding out where, by who and how the data is stored and transmitted, and that the data is destroyed properly.

There should be mechanisms for safe use of mobile devices that provide secure access to the Internet even if the nearest mobile cell tower could be down or discovered to be malicious.

There should be mechanisms to let adversaries to access devices under blackmailing and torturing without giving them access to sensitive information.

Several guidelines recommend teaching (security awareness). It was mentioned also by several companies such as MDM providers.

New countermeasures, recommendations and security controls are described and analysed in the next section.

14. New countermeasures, security controls and recommendations

It was discovered, that there are organisations which do not handle SECRET or TOP SECRET (at GSC level) information in mobile devices at all, but let people access such information, e.g., only in physically protected offices. This is a good practice; however apparently there sometimes needs to be access to such information outside offices. As can be seen from the section 13. 'Results', there are no good enough mitigation mechanisms for all existing risks, and thus new mitigation mechanisms are required. This section describes such new countermeasures, recommendations, and security controls.

14.1. Protecting sensitive data

It is possible to make SecureDrives [148] to explode when the battery of the SSD drive runs out or when it does not access a GSM signal. Current computer motherboards support waking up the system when a previously paired Bluetooth device (such as a mobile phone) comes near enough, and to hibernate or standby when this device goes away from the motherboard. The same approaches could be used in situation when the user goes too far from the device. For example, an approach presented in SALT card [339] uses the following mechanism: When the user is near the phone with the SALT card, the device is unlocked but when they leave the phone locks itself.

The device could end all sensitive connections, logout from corporate networks, unmount corporate disk partitions and network drives, or just shut down properly (not only hibernate or standby but really shut the device and wipe the RAM). If there was an additional OS, GPS module and a place for a SIM card, it would be possible to still send location information to preconfigured phone numbers or via email. Reading the distance between the user and the device, or device and the working location should not rely only on one technique. If using two or more techniques and interfaces are combined, the likelihood of having risk of single point of failure decreases.

With adaptive security (M45), it would be possible to deny access to certain sensitive data when the security level becomes too low, e.g., in certain locations, or even to remove certain data from the device but still let the user use the device (M48).

In data protection, it could be possible to use ideas from BlueBox Security [178] described in the section 12.2.4.1. 'Bluebox Mobile Data Security'.

14.2. Protecting against theft and unauthorised borrowing

It would be possible to add additional movement sensors to mobile devices, or use the sensors already inside the device. If the device is moved 'wrongly' when it is locked, it could, e.g., raise alarms.

In addition to movement sensors, location based keys [339] and extra location trackers [241] [240] [242] could be integrated into devices or used with them.

14.3. Protecting communication channels

LTE Direct [340] allows wireless access up to 500 meters and connecting directly between cell phones without using cellular towers. It has been experimented with e.g., by Qualcomm and Facebook, and it can be used for chatting or for advertising by offering customised deals [341].

LTE Direct uses approaches used in P2P, mesh and mobile ad-hoc networks. There are several research papers about routing in ad-hoc networks using WLAN and Bluetooth [342] [343]. They have been used around the world, e.g., the One Laptop per Child project [344] uses WLAN and mesh-networks and FireChat [345] uses Bluetooth and P2P. Ad hoc networks have certain security challenges [346], and thus they could also affect LTE Direct. Additional threats are malicious cell towers [228] [87] [347] [348] , and IMSI catchers [349], but also power-loss or other failures in cell towers, causing infrastructure to become unavailable. In LTE Direct (or in WLAN), it could be possible to route data traffic only via trusted devices. For securing routing and for trusting the devices, the following approaches have been proposed; a) cryptographic approaches [350], b) trust based methods [351] [352], c) statistical methods and combinations of them [353]. Ideas from all of them could be combined into LTE Direct. In [350] trust for devices is gained using a preconfigured list of public keys or hash lists calculated from these trusted public keys. In [353] a scheme using both trust based methods and statistical methods is presented. One possible approach for routing traffic securely is described in Figure 23.

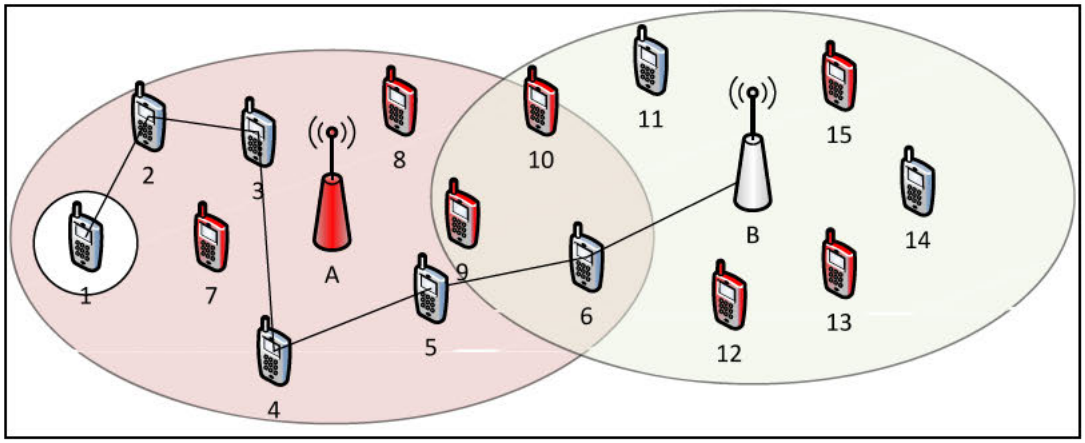


Figure 23. Example of secure routing.

In Figure 23 the device of the high level decision maker is phone number 1. Phones 2, 3, 4, 5, 6, 11 and 14 are trusted, as is cell tower B. Devices 7, 8, 9, 10, 12, 13, and 15 and cell tower A are not trusted and thus they should not be used to route traffic or to connect to.

If the high level official is visiting (semi-)hostile countries or locations, but there is a need to access home organizations' services without exposing information about the user, VPN alone is not an option. When using VPN without additional services such as open or random VPNs or proxies, it is possible to analyse the traffic and see if someone is connecting, e.g., from a hotel to certain VPN services which can be mapped to certain organizations (such as NATO). In some situations this information might cause physical risk to the user. In such cases, anonymization networks such as Tor could be used to protect privacy of the users. If using Tor, risks of malicious exit nodes and traffic analysis [354] can be mitigated by owning hidden services, so exit nodes would not be used, and the traffic would go from the mobile device to the service fully via Tor. Hidden services have been enabled, e.g., by Facebook [355]. It should be noted, that usage of Tor might be useful only in very few cases due to lack of speed.

In addition to these, it would be possible to have personal bodyguards carrying private antennas or repeaters, or such devices could be inserted into user's car or home.

14.4. Protection mechanisms against blackmailing and torturing

The system could have fake passwords that the user knows can be given to an adversary, e.g., if tortured or blackmailed. The system would let the adversary in, but not to access any sensitive information. The fake part

of the system could still look correct, and have several files looking correct and sensitive, and allow access to fake remote services such as email (M52).

14.5. Frequent swapping and wiping devices

As described in the section 12. 'Literature Review', scheduling of deletion of data such as sensitive personal data, periodic reloading and wiping of devices and reloading with specially prepared and tested disk images have been proposed. These should be done always after security incidents such as finding malware from the device. It would be possible to do this also, e.g., every day. The user would have one device in use and the rest of similar devices would be under monitoring, wiping, reloading, or testing. The user could change the device when coming to work or leaving the workplace. In addition, forensics tools could be used easily after possible incidents.

Frequent swapping of devices (M53) would give protection also against hardware tampering, e.g., in scenarios where the adversary has modified the smartphone battery or other parts.

14.6. Information dynamic storage, information location randomisation

In general the location of information can be subdivided into three main categories: 1) in the local system memory (e.g. information creation and editing), 2) in transit between systems (e.g. information exchange over network), and 3) at rest (e.g. saved on data storage). When considering the information protection and trust, at least confidentiality, integrity and availability (CIA triad) have to be taken into account. For information in system memory, the main focus is put on integrity (e.g. ensure correct information processing by the local system); information in transit considers all three aspects (e.g. secure and trusted information access); while information at rest is concerned mainly about implementing strong encryption algorithms.

Information at rest can be considered to be the most vulnerable if access to it is gained under certain conditions, as at that point it is only as secure as encryption algorithm implemented. In this case the location of stored information can be predetermined as it is statically located within a physical device (e.g. hard disk drive) or a cluster of devices (e.g. network attached storage).

To make unauthorised access to the information harder upon breach of physical security and implemented safeguards, the idea of developing information dynamic storage could be developed where information is always on the move within the predefines system boundaries instead of being static. Information dynamic storage in principle should maintain the process of constant information dynamic allocation and randomisation in a way that is transparent and easily usable for authorised user, but make it hard and unpredictable to the adversary. A conceptual prototype would consider the following basic principles: information location randomisation approach development (the storage systems involved, information dynamic location method and its management); specific hardware requirements (including storage technologies and power supply needs); filesystem and memory allocation independence (should be platform independent and support popular OSs); performance penalties (evaluating and optimising the performance of such an approach); fault tolerance and resilience (information defragmentation and recovery in case of system failure).

As an abstract example, the similar address space layout randomization (ASLR) method could be considered as a good concept example for information dynamic allocation and segmenting within the computer memory. However, information dynamic storage takes information location randomization to a whole new level, by using novel research and technological models.

14.7. Policy enforcement

'Understanding how the individual is using the data on their device is essential to successfully protecting data in the mobile world.' –Adam Ely [12]

An effective awareness program requires identifying which human behaviours pose the greatest risk to the organisation, the government, etc., and then establishing an engaging training program that changes those behaviours. [24] A gap analysis must be performed beforehand [356]. All common threats and attacks apply also to high-level decision-makers, however because of the value of information they are holding, there might be much more sophisticated attacks against them. In practice this means that more training should be done and it should not only include common threats but give real examples of results and punishments of, e.g., sensitive data leakage.

'About 2/3 of companies report putting enterprise needs above the user needs. As a result, users simply ignore security policies and simply chose to 'go around' IT.' –Adam Ely [12]

Organisations should do active assessment such as vulnerability scans and penetration testing of mobile devices [11]. Target vulnerability validation techniques include password cracking, penetration testing, social engineering, and application security testing [357]. In addition to these, false attacks could be used to increase awareness by disconcerting the user.

One new policy could be having additional user profiles (M42), e.g., for family members of high-level officials or decision-makers. This way the user could lend the device easily, e.g., to his/her children, however they would have their own user profiles with less permissions. This could be done already when giving the device to the user; the administrator could ask from the user if there is a need for additional accounts.

14.8. Monitoring

One problem is that user might want to be able to visit any web page. When proxy servers and firewalls are used, they usually prevent visiting illegal and malicious ones, however sometimes also some required web pages. One possibility to enable the visiting of every possible web page is to combine ideas from adaptive security, proxifiers, proxy servers and VDI solutions. All the traffic would go through a proxifier and a proxy server and the proxy server would transmit the request (e.g., a HTTP GET) to the destination without checking any whitelists or blacklists. When the proxy server received the reply (e.g., a web page), it would parse it (automatically or manually by trusted individuals) and translate it to a format that is suitable for a mobile device. It would be possible, e.g., to show only the plain text from web pages the user wants to visit. The proxy server would adapt and modify its behaviour based on the security level of the system.

This would enable similar security features as when using VDI viewers, however with the added possibility for monitoring and result modification in the proxy server. The end user could visit any web page, click any link, etc. In such an approach the proxy server (and a real person using it) must be trusted, because end-to-end encryption between the mobile device and the accessed service could not be provided.

14.9. Buying extra security

It is described in [358] that Germany's Federal Intelligence Service, the Bundesnachrichtendienst (BND) has asked for money to buy 0-day vulnerabilities on the open market. By doing so, it would be possible to gain information about security vulnerabilities in their own systems, and if there are not yet patches or updates against them, to design other ways to protect against them.

Similar results could be gained by offering high prices to people for hacking and finding vulnerabilities from wanted systems or from certain parts from systems. There have been competitions, e.g., to hack smartphones [359] [360] and to bug bounties with prizes to find vulnerabilities from different phones [361], software [362] [363] and systems.

14.10. Summary of new countermeasures

New mitigation techniques have been described in Table 28.

Table 28. Recommended or used mitigation techniques.

	Mitigation technique
M48.	Improved authentication and access control by combining multifactor authentication, context-awareness, implicit authentication and adaptive security. (T1, T2, T5)
M49.	Protecting sensitive data, e.g., by locking the device when the user is not near, or by denying access to sensitive data if the security level of the environment is not good enough. (T1)
M50.	Protecting against theft and unauthorised access using location trackers and movement sensors. (T4)
M51.	Protecting communication over 4G by using ideas from secure routing protocols and mesh networks. (T7, T8, T11)
M52.	Protecting against blackmailing and torturing. (T2, T4)
M53.	Swapping and wiping devices every day. (T5, T9)
M54.	Improved monitoring solutions. (T5, T2, T11)
M55.	Buying additional security (0-days, penetration testing, hacking competitions) (T10, T5, T6, T7, T8, T11)
M56.	Continuous security training for the users. (T10, T6, T5, T8, T9, T1, T2)
M57.	Securing data, not devices. (T1)

The ongoing research related to these topics should be followed.

15. Conclusion

As described in this paper, there are several security controls that can be used in advanced mobile devices to enforce security policies and to improve security of such devices. To make them usable, policies must be in a line with the usage of these devices, and technical security controls must not be too difficult. Current widely used security controls such as using usernames and passwords for authentication can be changed to more usable ones without decreasing the level of security in authentication.

Rather than starting from the scratch, organisations should start from publicly developed, vetted, and supported security benchmarks, security guides, or checklists related to technical security controls and security policies.

As can be seen, there are still many technical opportunities to make mobile devices more secure. They cost money and thus make the devices more expensive; however in some use cases it might be necessary. Usage of technical security mechanisms, secure hardened mobile devices and technical enforcing mechanisms are required but not enough; users need to be security aware, which requires user training but also penetration testing. Awareness can be increased also by alarming the user. Training must not only include security awareness but also descriptions of security policies, why they exist, why they should be followed, etc. Security training must be frequent, because people tend to change their behaviour. In many cases, training might also be a cheaper way to improve security than adding all possible technical features to the systems.

Bibliography

[1] US-CERT, “Technical Information Paper-TIP-10-105-01 - Cyber Threats to Mobile Devices,” 2010. [Online]. Available: https://www.us-cert.gov/sites/default/files/publications/TIP10-105-01.pdf. [Accessed 03 October 2014].

[2] P. Ruggiero and J. Foote, “Cyber Threats to Mobile Phones,” 2011. [Online]. Available: https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf. [Accessed 03 October 2014].

[3] Fortinet, “2014 Threat Landscape Report,” Fortinet, 2014.

[4] F-Secure, “Mobile Threat Report Q1 2014,” F-Secure, 2014.

[5] Webroot, “Mobile Threat Report 2014,” Webroot, 2014.

[6] Trend Micro, “Mobile Threat Information Hub,” [Online]. Available: http://about-threats.trendmicro.com/us/mobile. [Accessed 03 October 2014].

[7] Norton, “Analysis of Mobile Threats,” [Online]. Available: http://www.symantec.com/threatreport/topic.jsp?id=threat_activity_trends&aid=analysis_of_mobile_threats. [Accessed 03 October 2014].

[8] V. Svajcer, “Sophos Mobile Security Threat Report,” 2014. [Online]. Available: http://www.sophos.com/en-us/medialibrary/PDFs/other/sophos-mobile-security-threat-report.pdf. [Accessed 03 October 2014].

[9] Info Security Magazine, “Mobile Security Experts: Worst is Yet to Come,” 07 October 2014. [Online]. Available: http://www.infosecurity-magazine.com/news/mobile-security-experts-worst-is/. [Accessed 08 October 2014].

[10] ENISA, “ENISA Threat Landscape 2013,” ENISA, 2013.

[11] M. Souppaya and K. Scarfone, “Guidelines for Managing the Security of Mobile Phones in the Enterprice,” NIST Special Publications, 2013.

[12] M. Zorz, “Exploring the mobile security landscape,” 07 July 2014. [Online]. Available: http://www.net-security.org/article.php?id=2068. [Accessed 11 November 2014].

[13] A. Ely, "Mobile Security Myth 3: You Know Where Your Mobile Data Is," 25 July 2013. [Online]. Available: https://bluebox.com/business/mobile-security-myth-3-you-know-where-your-mobile-data-is/. [Accessed 26 November 2014].

[14] Y. Wang, K. Vangury and J. Nikolai, “Mobile Guardian: A Security Policy Enforcement Framework for Mobile Devices,” 2014.

[15] M. Jakobsson, “Why Mobile Security is not Like Traditional Security,” 2011.

[16] Burson-Marsteller, “Twiplomacy Study 2014,” 25 June 2014. [Online]. Available: http://twiplomacy.com/blog/twiplomacy-study-2014/. [Accessed 30 September 2014].

[17] ENISA, “Smartphones: Information security risks, opportunities and recommendations for users,” ENISA, 2010.

[18] SANS, “Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers,” [Online]. Available: https://www.sans.org/critical-security-controls/control/3. [Accessed 08 October 2014].

[19] SANS Institute, “SANS SCORE Mobile Device Checklist version 1.3,” SANS.

[20] SANS Institute, “Security Policy for the use of handheld devices in corporate environments”.

[21] ENISA, “Smartphone Secure Development Guidelines for App Developers,” ENISA, 2011.

[22] OWASP, “Projects/OWASP Mobile Security Project - Top Ten Mobile Controls,” 05 March 2014. [Online]. Available: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Top_Ten_Mobile_Controls. [Accessed 21 October 2014].

[23] CESG and Centre for the Protection of National Infrastructure, “Collection: Bring Your Own Device Guidance,” 06 October 2014. [Online]. Available: https://www.gov.uk/government/collections/bring-your-own-device-guidance. [Accessed 27 October 2014].

[24] M. Merkow, T. Dudley, D. M. Vaughn, V. Gernand, T. P. Quade, R. Maughan, J. Pescatore and A. Merola, “Hardening The HumanOS,” The SANS Institute, 2013.

[25] Cabinet Office and Efficiency and Reform Group, “End User Device Strategy: Security Framework & Controls,” 25 March 2013. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/261980/EUD_Security.pdf. [Accessed 27 October 2014].

[26] Ministry of Defence, “Subject: Government Security Classification Scheme,” 2014. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/300970/20140217-Industry_Security_Notice-ISN-2014-01-updated-April-2014-U.pdf. [Accessed 27 October 2014].

[27] Panda Security, “How secure are the world's leaders' cell phones?,” 7 July 2014. [Online]. Available: http://www.pandasecurity.com/mediacenter/security/secure-worlds-leaders-cell-phones/. [Accessed 30 September 2014].

[28] M. Holehouse, “iPads banned from Cabinet meetings over surveillance fears,” 03 November 2013. [Online]. Available: http://www.telegraph.co.uk/news/politics/10423514/iPads-banned-from-Cabinet-meetings-over-surveillance-fears.html. [Accessed 30 September 2014].

[29] The Telegraph, “Ex-MI5 boss Dame Stella Rimington 'loses laptop at airport',” 01 June 2012. [Online]. Available: http://www.telegraph.co.uk/news/uknews/crime/9305060/Ex-MI5-boss-Dame-Stella-Rimington-loses-laptop-at-airport.html. [Accessed 03 October 2014].

[30] E. Whinnett, “Foreign Minister Julie Bishop's phone was hacked at the height of the MH17 crisis,” 16 August 2014. [Online]. Available: http://www.heraldsun.com.au/news/foreign-minister-julie-bishops-phone-was-hacked-at-the-height-of-the-mh17-crisis/story-fni0fiyv-1227026241325?nk=a0c5b415138032326ad45bbbb07f430a. [Accessed 30 September 2014].

[31] Australian Associated Press, “Tony Abbott says phone hack did not compromise talks with Julie Bishop,” 16 August 2014. [Online]. Available: http://www.theguardian.com/world/2014/aug/16/tony-abbott-phone-hack-not-compromise-julie-bishop. [Accessed 30 September 2014].

[32] Europe Online, “Report: Belgian permier's car robbed, document stolen, while in gym,” 08 August 2014. [Online]. Available: http://en.europeonline-magazine.eu/report-belgian-premiers-car-robbed-document-stolen-while-in-gym_351473.html?wpf_eol_country=11. [Accessed 01 October 2014].

[33] The News Tribe, “Pubjab law minister's mobile phone stolen from his car,” 25 June 2014. [Online]. Available: http://www.thenewstribe.com/2014/06/25/punjab-law-ministers-mobile-phone-stolen-from-his-car/. [Accessed 01 October 2014].

[34] Geekaphone, “Is someone listening to your phone calls? How secure is your mobile phone?,” 12 July 2011. [Online]. Available: http://geekaphone.com/blog/mobile-security-infographic/. [Accessed 30 September 2014].

[35] The Cryptzone Group 2012, “Perceptions of security awareness study by Cryptzone,” 2012. [Online]. Available: http://www.cryptzone.com/_download/articles/Cryptzone_Study_Perceptions_Security_Awareness.pdf. [Accessed 30 September 2014].

[36] Nasuni Corporation, “Shadow IT in the Enterprice,” [Online]. Available: http://www6.nasuni.com/rs/nasuni/images/White_Paper-Shadow_IT_in_the_Enterprise.pdf. [Accessed 30 September 2014].

[37] T. Wilson, “10 Ways to Get Users to Follow Security Policy,” 01 November 2007. [Online]. Available: http://www.darkreading.com/vulnerabilities---threats/10-ways-to-get-users-to-follow-security-policy/d/d-id/1128525. [Accessed 01 October 2014].

[38] K. Beaver, “Security Awareness Training is a Critical Component to Changing Employee Behavior,” [Online]. Available: https://www.tnwinc.com/products-services/ethics-compliance-elearning/security-awareness-training/. [Accessed 01 October 2014].

[39] National Cyber Security Centre (NCSC), “Cyber Security Assessment Netherlands - CSAN-4,” NCSC, 2014.

[40] D. Cappelli, A. Moore and R. Trzeciak, The CERT Guide to Insider Threats - How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud), Pearson Education, Inc., 2012.

[41] ENISA, “Top Ten Smartphone Risks,” [Online]. Available: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks. [Accessed 14 October 2014].

[42] OWASP, "Top 10 Mobile Risks," [Online]. Available: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Risks. [Accessed 24 November 2014].

[43] A. Kesäniemi, “Mobile Application Threat Analysis,” [Online]. Available: https://www.owasp.org/images/c/c9/Mobile-threat-analysis-short-presentation_owasp.pdf. [Accessed 22 October 2014].

[44] Y. Amit and A. Sharabani, "Mobile Security Attacks - A Glimpse From the Trenches," 2014. [Online]. Available: https://www.owasp.org/images/a/ab/AppSecIL_2014_Mobile_Security_Attacks_-_A_Glimpse_From_the_Trenches_-_Yair_Amit_-_Adi_Sharabani_-_Skycure.pdf. [Accessed 03 November 2014].

[45] CPNI, “Mobile Devices - Guide for Implementers,” February 2013. [Online]. Available: https://www.cpni.gov.uk/documents/publications/non-cpni_pubs/2013-02-22-mobile_devices_guide_for_implementers.pdf. [Accessed 24 November 2014].

[46] J. Bickford, R. O'Hare, A. Baliga, V. Ganapathy and L. Iftode, “Rootkits on Smart Phones: Attacks and Implications,” 2009.

[47] H. Kärkkäinen, ”Apple myy Suomessa vaarallisia puhelimia - ja sulkee kauppiaiden suut,” 30 October 2014. [Online]. Available: http://www.digitoday.fi/tietoturva/2014/10/30/apple-myy-suomessa-vaarallisia-puhelimia--ja-sulkee-kauppiaiden-suut/201415103/66. [Haettu 30 October 2014].

[48] Viestintävirasto, ”iPhone 4 - puhelimien mobiiliselain vaarassa,” 24 September 2014. [Online]. Available: https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/09/ttn201409241655.html. [Haettu 30 October 2014].

[49] R. Savola, T. Väisänen, A. Evesti, P. Savolainen, J. Kemppainen and M. Kokemäki, “Toward risk-driven security measurement for Android smartphone platforms,” in *Information Security for South Africa*, Johannesburg, 2013.

[50] CPNI, “Mobile Devices - Executive Briefing Paper,” February 2013. [Online]. Available: http://www.cpni.gov.uk/documents/publications/non-cpni_pubs/2013-02-22-mobile_devices-executive_briefing_paper.pdf. [Accessed 27 October 2014].

[51] R. Shirey, “Internet Security Glossary, Version 2,” IETF, 2007.

[52] M. Guri, G. Kedma, A. Kachlon and Y. Elovici, “AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies,” in *MALCOM 2014*, 2014.

[53] Ben Gurion University, “How to leak sensitive data from an isolated computer (air-gap) to near by mobile phone - AirHopper,” 28 October 2014. [Online]. Available: https://www.youtube.com/watch?v=2OzTWiGl1rM. [Accessed 24 November 2014].

[54] Innovations report, “Georgia Tech Turns iPhone Into spiPhone,” 19 October 2011. [Online]. Available: http://www.innovations-report.com/html/reports/information_technology/georgia_tech_turns_iphone_spiphone_184116.html. [Accessed 25 November 2014].

[55] Y. Michalevsky, D. Boneh and G. Nakibly, “Gyrophone: Recognizing Speech From Gyroscope Signa,” in *23rd USENIX Security Symposium (SEC’14)*, 2014.

[56] D. Graziano, "Galaxy Note II vulnerability allows hackers to bypass lock screen [video]," 04 March 2013. [Online]. Available:

http://bgr.com/2013/03/04/galaxy-note-ii-vulnerability-android-359267/. [Accessed 29 October 2014].

[57] Rambus Inc., "Side Channel Analysis Demo: Mobile Device," 25 June 2013. [Online]. Available: http://www.youtube.com/watch?v=cPDDNVKo43w. [Accessed 29 October 2014].

[58] Cryptography Reseach , "cptwg.org," 16 October 2013. [Online]. Available: http://www.cptwg.org/assets/2013/2013-1016_cptwg_cri-dpa_present.pdf. [Accessed 29 October 2014].

[59] D. Genkin, A. Shamir and E. Tromer, "RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis," [Online]. Available: http://www.tau.ac.il/~tromer/acoustic/. [Accessed 29 October 2014].

[60] "FROST: Forensic Recovery Of Scrambled Telephones," [Online]. Available: https://www1.informatik.uni-erlangen.de/frost. [Accessed 29 October 2014].

[61] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze and J. M. Smith, "Smudge Attacks on Smartphone Touch Screens," in *WOOT 10*, 2010.

[62] M. Kumar, T. Garfinkel, D. Boneh and T. Winograd, "Reducing Shoulder-surfing by Using Gaze-based Password Entry," in *Proceedings of the 3rd symposium on Usable privacy and security*, 2007.

[63] G. Ollmann, "The Phishing Guide - Understanding & Preventing Phishing Attacks," IBM Security Systems.

[64] APEC, "CAPEC-163: Spear Phishing," [Online]. Available: https://capec.mitre.org/data/definitions/163.html. [Accessed 29 October 2014].

[65] Kaspersky, "The Darkhotel APT - A story of unusual hospitality," Kaspersky lab, 2014.

[66] G. Rydstedt, B. Gourdin, E. Burztein and D. Boneh, "Framing Attacks on Smart Phones and Dumb Routers: Tap-Jacking and Geo-localization attacks," in *Usenix Worshop on Offensive Technology (wOOt 2010)*, 2010.

[67] APEC, "CAPEC-407: Social Information Gathering via Pretexting," [Online]. Available: https://capec.mitre.org/data/definitions/407.html. [Accessed 29 October 2014].

[68] APEC, "CAPEC-413: Pretexting via Tech Support," [Online]. Available: https://capec.mitre.org/data/definitions/413.html. [Accessed 29 October 2014].

[69] L. Kharouni, F. Hacquebord, N. Huq, J. Gogolinski, F. Merces, A. Remorin and D. Otis, "Operation Pawn Storm - Using Decoys to Evade Detection," Trend Micro, 2014.

[70] H. Solomon, "Sophisticated attacks uses fake Web sites as bait," 27 October 2014. [Online]. Available: http://www.itworldcanada.com/article/sophisticated-attack-uses-fake-web-sites-as-bait/98566. [Accessed 29 October 2014].

[71] R. Cellan-Jones, "Government calls for action on mobile phone crime," 11 February 2010. [Online]. Available: http://news.bbc.co.uk/2/hi/technology/8509299.stm. [Accessed 20 October 2014].

[72] Consumer Reports, "Smart phone thefts rose to 3.1 million last year, Consumer Reports finds," 28 May 2014. [Online]. Available: http://www.consumerreports.org/cro/news/2014/04/smart-phone-thefts-rose-to-3-1-million-last-year/index.htm. [Accessed 20 October 2014].

[73] SANS, "OUCH! Losing Your Mobile Device," 10 2012. [Online]. Available: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201210_en.pdf. [Accessed 21 October 2014].

[74] Technische Fakultät, "FROST: Forensic Recovery Of Scrambled Telephones," [Online]. Available: https://www1.informatik.uni-erlangen.de/frost. [Accessed 20 October 2014].

[75] T. Müller, M. Spreitzenbarth and F. C. Freiling, "Forensic Recovery of Scrambled Telephones," 2012.

[76] B. X. Chen, "Hacker Says iPhone 3GS Encryption Is 'Useless' for Businesses," 23 July 2009. [Online]. Available: http://www.wired.com/2009/07/iphone-encryption/. [Accessed 04 November 2014].

[77] Microsoft, “Windows Phone 8.1 Enterprise Device Management Protocol,” October 2014. [Online]. Available: http://www.microsoft.com/en-us/download/confirmation.aspx?id=36831. [Accessed 03 November 2014].

[78] R. Lemos, “Pop-up program reads keystrokes, steals passwords,” 29 June 2004. [Online]. Available: http://news.cnet.com/2100-7349_3-5251981.html. [Accessed 02 October 2014].

[79] M. Nohlberg, Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks, Stockholm: University of Skövde, 2008.

[80] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze and J. M. Smith, “Smudge Attacks on Smartphone Touch Screens,” in *TOOT 10*, 2010.

[81] C. Guo, H. J. Wang and W. Zhu, “Smart-Phone Attacks and Defences,” in *HotNets III*, 2004.

[82] N. J. Percoco and S. Schulte, "Adventures in BouncerLand - Failures of Automated Malware Detection within Mobile Application Markets," in *Black Hat USA 2012*, 2012.

[83] D. Brodie, "Practical Attacks against Mobile Device Management (MDM)," 2013. [Online]. Available: https://media.blackhat.com/eu-13/briefings/Brodie/bh-eu-13-lacoon-attacks-mdm-brodie-wp.pdf. [Accessed 31 October 2014].

[84] M. Kumar, “Sony Xperia Devices Secretly Sending User Data to Servers in China,” 28 October 2014. [Online]. Available: http://thehackernews.com/2014/10/sony-xperia-devices-secretly-sending.html. [Accessed 30 October 2014].

[85] T. J. Hold, O. Smirnova and Y.-T. Chua, “Stolen Data Markets: An Economic and Organizational Assessment,” August 2014. [Online]. Available: http://defcon.org/images/defcon-22/dc-22-presentations/Holt-Smirnova-Chua/DEFCON-22-Holt-Smirnova-Chua-Stolen-Data-Markets-Updated.pdf. [Accessed 01 December 2014].

[86] Symantec, "Regin: Top-tier espionage tool enables stealthy surveillance," Symantec, 2014.

[87] M. Shaulov and D. Brodie, "Practical Attacks against Mobile Device Management Solutions," 2013. [Online]. Available: https://media.blackhat.com/us-13/US-13-Brodie-A-Practical-Attack-against-MDM-Solutions-Slides.pdf. [Accessed 31 October 2014].

[88] M. Shaulov and D. Brodie, "Practical Attacks against Mobile Device Management Solutions," 30 September 2013. [Online]. Available: https://www.youtube.com/watch?v=PWOe1Pj_cUE. [Accessed 31 October 2014].

[89] M. Marquis-Boire, B. Marczak, C. Guarnieri and J. Scott-Railton, “You Only Click Twice: FinFisher's Global Proliferation,” March 2013. [Online]. Available: https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/. [Accessed 07 November 2014].

[90] FireEye, "Sidewinder targeted attack against Android in the golden age of ad libraries," 2014.

[91] J. Forristal, "Android Master Key Exploit – Uncovering Android Master Key That Makes 99% of Devices Vulnerable," 03 July 2013. [Online]. Available: https://bluebox.com/technical/uncovering-android-master-key-that-makes-99-of-devices-vulnerable/. [Accessed 26 November 2014].

[92] J. Forristal, "Android Fake ID Vulnerability Lets Malware Impersonate Trusted Applications, Puts All Android Users Since January 2010 At Risk," 29 July 2014. [Online]. Available: https://bluebox.com/technical/android-fake-id-vulnerability/. [Accessed 26 November 2014].

[93] G. Weidman, 14 01 2014. [Online]. Available: http://www.bulbsecurity.com/pivoting-a-shell-through-android-with-sms/.

[94] OpenSignal, "Android Fragmentation Visualized (August 2012) - The many faces of a little green robot," August 2012. [Online]. Available: http://opensignal.com/reports/fragmentation.php. [Accessed 31 October 2014].

[95] OpenSignal, "Android Fragmentation Visualized (August 2014)," August 2014. [Online]. Available: http://opensignal.com/reports/2014/android-fragmentation/. [Accessed 2014 October 2014].

[96] Arxan, “State of Mobile App Security - Apps Under Attack - volume 3,” November 2014. [Online]. Available:

https://www.arxan.com/assets/1/7/State_of_Mobile_App_Security_2014_final.pdf. [Accessed 25 November 2014].

[97] Google, "Dashboard," November 2014. [Online]. Available: https://developer.android.com/about/dashboards/index.html. [Accessed 06 November 2014].

[98] "OWASP Mobile Security Project - Dangers of Jailbreaking and Rooting Mobile Devices," [Online]. Available: https://www.owasp.org/index.php/Projects/OWASP_Mobile_Security_Project_-_Dangers_of_Jailbreaking_and_Rooting_Mobile_Devices.

[99] K.-J. Karlsson, "Android Anti-forensics: Modifying CyanogenMod," in *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, 2014.

[100] U. Tupakula and V. Varadharajan, "Securing Mobile Devices from DoS Attacks," in *16th International Conference on Computational Science and Engineering*, 2013.

[101] Wikipedia, "Denial-of-service attack," Wikipedia, [Online]. Available: http://en.wikipedia.org/wiki/Denial-of-service_attack. [Accessed 09 December 2014].

[102] B. R. Moyers, J. P. Dunning, R. C. Marchany and J. G. Tront, "Effects on Wi-Fi and Bluetooth Battery Exhaustion Attacks on Mobile Devices," in *43rd Hawaii International Conference on System Sciences*, 2010.

[103] US-CERT, "Alert (TA14-017A)," US-CERT, 17 January 2014. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA14-017A. [Accessed 09 December 2014].

[104] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defence mechanisms: classification and state-of-the art," *Computer Networks,* vol. 44, pp. 643-666, 2004.

[105] ISO/IEC, *ISO/IEC 27005, Information technology — Security techniques — Information security risk management,* ISO/IEC, 2011.

[106] SANS, "Critical Security Controls Version 5," [Online]. Available: https://www.sans.org/critical-security-controls/controls. [Accessed 08 October 2014].

[107] The Center for Internet Security Benchmark Program, "CIS Security Benchmarks," [Online]. Available: http://benchmarks.cisecurity.org/. [Accessed 08 October 2014].

[108] National Institute of Standards and Technology (NIST), "National Checklist Program Repository," [Online]. Available: http://web.nvd.nist.gov/view/ncp/repository. [Accessed 08 October 2014].

[109] SANS, "Data Protection," [Online]. Available: https://www.sans.org/critical-security-controls/control/17. [Accessed 08 October 2014].

[110] Viestintävirasto, "[Teema] Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön, osa 1/3," 20 October 2014. [Online]. Available: https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/10/ttn201410201101.html. [Haettu 21 October 2014].

[111] Viestintävirasto, "[Teema] Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön, osa 2/3," 22 October 2014. [Online]. Available: https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/10/ttn201410221239.html. [Haettu 23 October 2014].

[112] Viestintävirasto, "[Teema] Tietoturvavinkkejä matkapuhelimen turvalliseen käyttöön, osa 3/3," 24 October 2014. [Online]. Available: https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/10/ttn201410241327.html. [Haettu 24 October 2014].

[113] CESG, "End User Devices Security and Configuration Guidance," 06 October 2014. [Online]. Available: https://www.gov.uk/government/collections/end-user-devices-security-guidance. [Accessed 27 October 2014].

[114] CESG, "End User Devices Security Guidance: Enterprice Considerations," 23 January 2014. [Online]. Available: https://www.gov.uk/government/publications/end-user-devices-security-guidance-enterprise-considerations/end-user-devices-security-guidance-enterprise-considerations. [Accessed 27 October 2014].

[115] CESG, "Good for Enterprise and Good Dynamics: Security Guidance," 18 October 2013. [Online]. Available: https://www.gov.uk/government/publications/good-for-enterprise-and-good-dynamics-security-guidance/good-for-enterprise-

and-good-dynamics-security-guidance. [Accessed 27 October 2014].

[116] S. Bourne, "Sophos Mobile Device Management and CESG Guidelines," February 2013. [Online]. Available: http://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/UK%20public%20sector/sophos-police-security-procedures-ios-wpuk.pdf?la=en. [Accessed 24 November 2014].

[117] CESG and CPNI, "BYOD Guidance: Device Security Considerations," [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360960/BYOD_Guidance_-_Device_Security_Considerations.pdf. [Accessed 24 November 2014].

[118] CPNI, “Mobile Devices,” [Online]. Available: https://www.cpni.gov.uk/advice/cyber/mobile-devices/. [Accessed 24 November 2014].

[119] CPNI, “Mobile Devices - Guide for Managers,” February 2013. [Online]. Available: https://www.cpni.gov.uk/documents/publications/non-cpni_pubs/2013-02-22-mobile_devides_guide_for_managers.pdf. [Accessed 24 November 2014].

[120] CPNI, “Mobile Devices - Executive Briefing Paper,” February 2013. [Online]. Available: http://www.cpni.gov.uk/documents/publications/non-cpni_pubs/2013-02-22-mobile_devices-executive_briefing_paper.pdf. [Accessed 24 November 2014].

[121] OWASP, "Top 10 Mobile Controls," [Online]. Available: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#tab=Top_10_Mobile_Controls. [Accessed 24 November 2014].

[122] “Cryptographic_Storage_Cheat_Sheet,” [Online]. Available: https://www.owasp.org/index.php/Cryptographic_Storage_Cheat_Sheet#Rule_-_Only_use_strong_cryptographic_algorithms.

[123] NIST, "Cryptographic Algorithm Validation Program (CAVP)," [Online]. Available: http://csrc.nist.gov/groups/STM/cavp/index.html. [Accessed 24 November 2014].

[124] Wikipedia, “CCM mode,” [Online]. Available: http://en.wikipedia.org/wiki/CCM_mode. [Accessed 05 February 2015].

[125] Wikipedia, “Galois/Counter Mode,” [Online]. Available: http://en.wikipedia.org/wiki/Galois/Counter_Mode. [Accessed 05 February 2015].

[126] Wikipedia, “OCB mode,” [Online]. Available: http://en.wikipedia.org/wiki/OCB_mode. [Accessed 05 February 2015].

[127] M. Ottela, “Tinfoil Chat - Messaging platform immune against mass surveillance,” 2014. [Online]. Available: https://www.cs.helsinki.fi/u/oottela/tfc.pdf. [Accessed 04 December 2014].

[128] WebRoot, “Survey: Mobile Threats are Real and Costly,” November 2012. [Online]. Available: http://www.webroot.com/shared/pdf/byod-mobile-security-study.pdf. [Accessed 25 November 2014].

[129] Palo Alto Networks, “10 Things Your Next Firewall Must Do,” Palo Alto Networks, 2014.

[130] M. Perry, "Mission Impossible: Hardening Android for Security and Privacy," 2 April 2014. [Online]. Available: https://blog.torproject.org/blog/mission-impossible-hardening-android-security-and-privacy. [Accessed 27 October 2014].

[131] T. Simonite, “For $3,500, a Spy-Resistant Smartphone,” 18 March 2014. [Online]. Available: http://www.technologyreview.com/news/525556/for-3500-a-spy-resistant-smartphone/. [Accessed 01 October 2014].

[132] BlackBerry, “Security you can trust,” [Online]. Available: http://uk.blackberry.com/business/enterprise-mobility/mobile-security.html. [Accessed 30 September 2014].

[133] BlackBerry, “There's good security and then there's national security - BlackBerry 10 and BES10 - The perfect balance of protection and productivity,” 2013. [Online]. Available: http://uk.blackberry.com/content/dam/blackBerry/pdf/business/english/BlackBerry-Security-Brochure.pdf. [Accessed 30 September 2014].

[134] Blackphone, “Secure by Design - A 21st - century smartphone,” 2014. [Online]. Available: https://www.blackphone.ch/#introduction. [Accessed 30 September 2014].

[135] Elektrobit, “Android Based EB Specialized Device Platform - Custom made LTE Smartphones and Tablets,” [Online]. Available: http://www.elektrobit.com/what_we_deliver/wireless/offering/specialized_device_platform. [Accessed 30 September 2014].

[136] LG, “LG GATE - Guarded access to enterprise,” [Online]. Available: http://www.lg.com/us/mobile-phones/lggate/welcome. [Accessed 30 September 2014].

[137] Samsung, “Samsung KNOX 2.0: The evolution of enterprice mobility,” [Online]. Available: https://www.samsung.com/global/business/mobile/platform/mobile-platform/knox/. [Accessed 01 October 2014].

[138] Samsung, “KNOX 2.0: The evolution of enterprice mobility,” 21 May 2014. [Online]. Available: https://www.samsung.com/global/business/mobile/platform/mobile-platform/knox/downloadFile/KNOX2.0_Brochure_21.May.2014.pdf. [Accessed 01 October 2014].

[139] Samsung, “Meet evolving enterprice mobility challenges with Samsung KNOX,” 27 February 2014. [Online]. Available: https://www.samsung.com/global/business/mobile/platform/mobile-platform/knox/downloadFile/Samsung-KNOX_Whitepaper_web_Feb.27.2014-0.pdf. [Accessed 01 October 2014].

[140] Samsung, “Samsung KNOX,” [Online]. Available: https://www.samsungknox.com/en. [Accessed 01 October 2014].

[141] Bull, “Hoox,” [Online]. Available: http://www.bull.com/hoox/secure-mobile-smartphone. [Accessed 01 October 2014].

[142] GSMK, “GSMK CryptoPhone,” [Online]. Available: http://www.cryptophone.de/en. [Accessed 01 October 2014].

[143] Jolla, "Jolla," [Online]. Available: http://jolla.com/. [Accessed 24 Nobember 2014].

[144] Nabishi Systems, “Nabishi Secure Voice 3G for (iOS) iPhone & Apple devices. (BlackBerry & Android APPs will be available shortly),” [Online]. Available: http://ww2.nabishi.com/nab-admin/index.php/secure-iphone-app/. [Accessed 06 October 2014].

[145] EFF, "Secure Messaging Scorecard," [Online]. Available: https://www.eff.org/secure-messaging-scorecard. [Accessed 06 November 2014].

[146] General Dynamics C4 Systems, “TACLANE - Multibook Secure Laptop,” [Online]. Available: http://www.gdc4s.com/taclane-multibook.html. [Accessed 06 October 2014].

[147] SecureDrives, “SecureDrives,” [Online]. Available: http://securedrives.co.uk/index.php?route=information/information&information_id=13. [Accessed 03 October 2014].

[148] J. Kirk, “Certgate Unveils Encryption SD Cards for Mobiles,” 04 March 2009. [Online]. Available: http://www.pcworld.com/article/160669/article.html. [Accessed 06 October 2014].

[149] Crypto AG, “Crypto Mobile HC-9100,” [Online]. Available: http://www.crypto.ch/en/products-and-services/products/crypto-mobile-hc-9100. [Accessed 06 October 2014].

[150] Ultra Electronics AEP, “Ultra Communicate TrustChip,” [Online]. Available: http://www.ultra-aep.com/trustchip-mobile-phone-encryption-enging. [Accessed 06 October 2014].

[151] SecuSmart, “At the Heart of all Secusmart Solutions,” [Online]. Available: https://www.secusmart.com/en/for-public-authorities/secusmart-security-card/. [Accessed 03 November 2014].

[152] Ultra Electronics AEP, “TrustChip,” [Online]. Available: http://www.ultra-aep.com/trustcall-1/196-trustchip-1/file. [Accessed 06 October 2014].

[153] SecuSmart, "SecuSmart home page," [Online]. Available: https://www.secusmart.com/en/. [Accessed 2014 November 2014].

[154] P. Sayer, “With SecuSmart chip, German officials free to talk and type securely on BlackBerry Z10,” 08 March 2013. [Online].

Available:
http://www.pcworld.idg.com.au/article/455886/secusmart_chip_german_officials_free_talk_type_securely_blackberry_z10/. [Accessed 03 November 2014].

[155] OWASP, “Guide to Cryptography,” owasp.org, 2014. [Online]. Available: https://www.owasp.org/index.php/Guide_to_Cryptography. [Accessed 02 December 2014].

[156] OpenSSL Project, "OpenSSL Project Homepage," [Online]. Available: http://www.openssl.org/. [Accessed 24 November 2014].

[157] Dencrypt, “Dencrypt homepage,” Dencrypt, [Online]. Available: http://dencrypt.eu/?gclid=CLig26ChtMICFWSWtAodKGAAmg. [Accessed 09 December 2014].

[158] A. Bikos and N. Sklavos, “LTE/SAE Security Issues on 4G Wireless Networks,” *Security & Privacy, IEEE ,* 2014.

[159] V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta and S. Shrawne, “Vulnerabilities of Wireless Security protocols,” 2012.

[160] Ability, “Active-GSM-Interceptor,” interceptors.com, [Online]. Available: http://www.interceptors.com/intercept-solutions/Active-GSM-Interceptor.html. [Accessed 02 December 2014].

[161] Private Mobile Networks, "4G / LTE - PMN have now released their 4G LTE EPC software and its agnostic eNodeB capability.," Private Mobile Networks, [Online]. Available: http://www.privatemobilenetworks.com/solutions/4g/. [Accessed 02 December 2014].

[162] L. Phifer, "VPN, Remote access security best practices," searchenterprisewan.techtarget.com/, June 2009. [Online]. Available: http://searchenterprisewan.techtarget.com/tip/VPN-remote-access-security-best-practices. [Accessed 02 December 2014].

[163] A. Henry, "Five Best VPN Service Providers," lifehacker.com, 14 March 2014. [Online]. Available: http://lifehacker.com/5935863/five-best-vpn-service-providers. [Accessed 02 December 2014].

[164] P. Selmeczy, "5 Best VPNs for Android 2014," bestvpn.com, 11 April 2014. [Online]. Available: https://www.bestvpn.com/blog/9276/best-vpns-for-android/. [Accessed 02 December 2014].

[165] A. Henry, “How to Boost Your Internet Security with DNSCrypt,” lifehacker.com, 30 May 2014. [Online]. Available: http://lifehacker.com/how-to-boost-your-internet-security-with-dnscrypt-510386189. [Accessed 02 December 2014].

[166] NSA, "Mobile Device Management: A Risk Discussion for IT Decision Makers," August 2012. [Online]. Available: https://www.nsa.gov/ia/_files/factsheets/mdm_decision_makers.pdf. [Accessed 25 November 2014].

[167] Hypori, "BYOD (Bring Your Own Device)," [Online]. Available: http://www.hypori.com/byod.php. [Accessed 26 November 2014].

[168] R. L. Mitchell, "MDM tools: Features and functions compared," 15 January 2014. [Online]. Available: http://www.computerworld.com/article/2497055/mobile-device-management/mdm-tools-features-and-functions-compared.html. [Accessed 03 November 2014].

[169] K. Hess, "5 Mobile Device Management Features That Matter," 5 June 2014. [Online]. Available: http://www.tomsitpro.com/articles/mdm-solutions-comparison,2-745.html. [Accessed 03 November 2014].

[170] AirWatch, “Mobile Security,” [Online]. Available: http://www.air-watch.com/solutions/mobile-security. [Accessed 30 September 2014].

[171] WidePoint, “Managed Mobility Services,” [Online]. Available: https://www.widepoint.com/managed-mobility-services/. [Accessed 30 September 2014].

[172] Kaspersky, “Kaspersky Security for Mobile,” Kaspersky, [Online]. Available: http://www.kaspersky.com/business-security/mobile. [Accessed 08 December 2014].

[173] Marketwire, "Lacoon Mobile Threat Management Platform Enables Enterprises to Comprehensively Detect, Assess and Mitigate Mobile Cyber Threats," 29 July 2014. [Online]. Available: http://cloudcomputing.ulitzer.com/node/3129270. [Accessed 04

November 2014].

[174] Fiberlink, “Mobile Device Management (MDM),” Fiberlink, [Online]. Available: http://www.maas360.com/products/mobile-device-management/. [Accessed 08 December 2014].

[175] Fiberlink, “MaaS360 - Security Productivity Suite,” Fiberlink, [Online]. Available: http://www.maas360.com/products/secure-productivity-suite/?s=home. [Accessed 08 December 2014].

[176] Palo Alto Networks, “GlobalProtect: Safely enable mobile devices,” Palo Alto Networks, [Online]. Available: https://www.paloaltonetworks.com/products/technologies/globalprotect.html. [Accessed 08 December 2014].

[177] Bluebox, “Bluebox homesite,” Bluebox, [Online]. Available: https://bluebox.com/. [Accessed 08 December 2014].

[178] TITUS, “TITUS homepage,” TITUS, [Online]. Available: http://www.titus.com. [Accessed 08 December 2014].

[179] D. Alexander, “Samsung, BlackBerry devices cleared for use on U.S. defence networks,” 03 May 2013. [Online]. Available: http://uk.reuters.com/article/2013/05/03/us-usa-defense-smartphones-idUKBRE94204E20130503. [Accessed 27 October 2014].

[180] CESG, “End User Devices Security Guidance: BlackBerry 10.2,” 10 June 2014. [Online]. Available: https://www.gov.uk/government/publications/end-user-devices-security-guidance-blackberry-102. [Accessed 27 October 2014].

[181] CESG, “BlackBerry 10.2 - EMM-Regulated with Balance,” 10 June 2014. [Online]. Available: https://www.gov.uk/government/publications/end-user-devices-security-guidance-blackberry-102/blackberry-102-emm-regulated-with-balance--2. [Accessed 27 October 2014].

[182] CESG and CPNI, “BYOD Guidance: BlackBerry Secure Work Space,” [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360970/BYOD_Guidance_-_BlackBerry_Secure_Work_Space.pdf. [Accessed 24 November 2014].

[183] Microsoft, "Windows Phone 8.1 Mobile Device Management Overview," April 2014. [Online]. Available: https://thelumiablog.files.wordpress.com/2014/08/windows-phone-8-1-mdm-overview.pdf. [Accessed 03 November 2014].

[184] Nokia, "Mobile device management resource hub," [Online]. Available: https://expertcentre.nokia.com/en/articles/kbarticles/Pages/Mobile-device-management-resource-hub.aspx. [Accessed 03 November 2014].

[185] Apple, "iPhone in Business," [Online]. Available: https://www.apple.com/iphone/business/. [Accessed 10 November 2014].

[186] Apple, “iOS and the new IT,” [Online]. Available: https://www.apple.com/ipad/business/it/management.html. [Accessed 10 November 2014].

[187] Apple, "iOS Enterprise Deployment Overview," [Online]. Available: https://www.apple.com/ipad/business/docs/iOS_Enterprise_Deployment_Overview_EN_Sep14.pdf. [Accessed 11 November 2014].

[188] Apple, "iOS Security - October 2014," October 2014. [Online]. Available: https://www.apple.com/business/docs/iOS_Security_Guide_Oct_2014.pdf. [Accessed 10 November 2014].

[189] Apple, “Reinvent your enterprise with iOS,” [Online]. Available: https://developer.apple.com/enterprise/. [Accessed 10 November 2014].

[190] Apple, "iOS and the new IT," [Online]. Available: https://www.apple.com/iphone/business/it/. [Accessed 10 November 2014].

[191] MWR InfoSecurity, "Securethought: Mobile Working - An MWR InfoSecurity Briefing Paper," March 2012. [Online]. Available: https://www.mwrinfosecurity.com/system/assets/433/original/mwri_mobile-working-white-paper_2012-03-05.pdf. [Accessed 24 November 2014].

[192] Apple, "Device and data security," [Online]. Available: https://help.apple.com/deployment/ios/#/apdd6c4ce271. [Accessed 10

November 2014].

[193] Apple, "iOS Security - September 2014," September 2014. [Online]. Available: https://s3.amazonaws.com/s3.documentcloud.org/documents/1302613/ios-security-guide-sept-2014.pdf. [Accessed 01 December 2014].

[194] Android, “System and kernel security,” source.android.com, [Online]. Available: https://source.android.com/devices/tech/security/overview/kernel-security.html. [Accessed 19 December 2014].

[195] Android, “Application Security,” source.android.com, [Online]. Available: https://source.android.com/devices/tech/security/overview/app-security.html. [Accessed 19 December 2014].

[196] Android, “KeyChain,” developer.android.com, [Online]. Available: http://developer.android.com/reference/android/security/KeyChain.html. [Accessed 19 December 2014].

[197] Android, “Encryption,” source.android.com, [Online]. Available: https://source.android.com/devices/tech/security/encryption/index.html. [Accessed 19 December 2014].

[198] Bull, “Secure you mobile workday - Hoox m2 Smartphone,” [Online]. Available: http://www.bull.com/download/security/S-Hoox_m2-enWeb.pdf. [Accessed 01 October 2014].

[199] Silent Circle, “Silent Circle,” 2014. [Online]. Available: https://silentcircle.com/. [Accessed 30 September 2014].

[200] Disconnect, “Disconnect Secure Wireless,” [Online]. Available: https://disconnect.me/mobile/secure-wireless. [Accessed 30 September 2014].

[201] SpiderOak, “The Power of Privacy,” [Online]. Available: https://spideroak.com/features/. [Accessed 30 September 2014].

[202] A. J. a. J. C. P. Zimmermann, “ZRTP: Media Path Key Agreement for Unicast Secure RTP,” April 2011. [Online]. Available: https://tools.ietf.org/html/rfc6189. [Accessed 30 September 2014].

[203] Disconnect, “Disconnect Mobile,” [Online]. Available: https://disconnect.me/mobile/disconnect-mobile. [Accessed 30 September 2014].

[204] S. Gallagher, "Exclusive: A review of the Blackphone, the Android for the paranoid," 30 June 2014. [Online]. Available: http://arstechnica.com/security/2014/06/exclusive-a-review-of-the-blackphone-the-android-for-the-paranoid/. [Accessed 04 November 2014].

[205] D. Ford, “Blackphone rooted at Defcon - Part 2,” 11 August 2014. [Online]. Available: https://blog.blackphone.ch/2014/08/11/blackphone-rooted-at-defcon%E2%80%8A-%E2%80%8Apart-2/#more-140. [Accessed 08 October 2014].

[206] J. Case, “Justin Case @ TeamAndIRC,” 9 August 2014. [Online]. Available: https://twitter.com/TeamAndIRC/status/498269471002226688. [Accessed 30 September 2014].

[207] CESG, “Good for Enterprise and Good Dynamics: Security Guidance,” 18 November 2013. [Online]. Available: https://www.gov.uk/government/publications/good-for-enterprise-and-good-dynamics-security-guidance/good-for-enterprise-and-good-dynamics-security-guidance. [Accessed 27 October 2014].

[208] NSA, “Security Enhancements (SE) for Android,” [Online]. Available: http://seandroid.bitbucket.org/. [Accessed 01 October 2014].

[209] ARM, “ARM TrustZone,” [Online]. Available: http://www.arm.com/products/processors/technologies/trustzone/index.php. [Accessed 01 October 2014].

[210] Viestintävirasto, ”Kyberturvallisuuskeskus suojaa luokiteltua tietoa,” 30 September 2014. [Online]. Available: https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/09/ttn201409301451.html. [Haettu 16 October 2014].

[211] Viestintävirasto - Kyberturvallisuuskeskus, ”Viestintäviraston NCSA-toiminnon hyväksymät salausratkaisut,” 01 October 2014. [Online]. Available: https://www.viestintavirasto.fi/attachments/Viestintaviraston_NCSA-

toiminnon_hyvaksymat_salausratkaisut.pdf. [Haettu 16 October 2014].

[212] Samsung Electronic Nordic, ”Viestintävirasto myönsi Samsung KNOXille tietoturvasertifioinnin,” 25 September 2014. [Online]. Available: http://www.epressi.com/tiedotteet/turvallisuus/viestintavirasto-myonsi-samsung-knoxille-tietoturvasertifioinnin.html. [Haettu 16 October 2014].

[213] Puolustusministeriö, ”KATAKRI - Kansallinen turvallisuusauditointikriteeristö versio II,” Puolustusministeriö, 2011.

[214] S. McCaskill, "Samsung Knox Approved For Classified Information By US Government," 23 October 2014. [Online]. Available: http://www.techweekeurope.co.uk/news/samsung-knox-government-approval-154074. [Accessed 27 October 2014].

[215] S. McCaskill, "Samsung Knox Gets US Military Approval," 16 May 2014. [Online]. Available: http://www.techweekeurope.co.uk/news/samsung-knox-military-use-145688. [Accessed 27 October 2014].

[216] NSA, "Commercial Solutions for Classified Program Components List," [Online]. Available: https://www.nsa.gov/ia/programs/csfc_program/component_list.shtml. [Accessed 27 October 2014].

[217] CESG, “Configuration guidance for the use of Samsung devices with KNOX for remote working at OFFICIAL,” 14 May 2014. [Online]. Available: https://www.gov.uk/government/publications/end-user-devices-security-guidance-samsung-devices-with-knox. [Accessed 27 October 2014].

[218] ARM, “ARM Security Technology - Building a Secure System using TrustZone Technology,” April 2009. [Online]. Available: http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf. [Accessed 01 October 2014].

[219] C. Marforio, N. Karapanos and C. Soriente, “Smartphones as Practical and Secure Location Verification Tokens for Payment,” 2014.

[220] CESG, “Guidance - End User Devices Security Guidance: Samsung devices with KNOX,” 14 May 2014. [Online]. Available: https://www.gov.uk/government/publications/end-user-devices-security-guidance-samsung-devices-with-knox/end-user-devices-security-guidance-samsung-devices-with-knox. [Accessed 27 October 2014].

[221] "Why Samsung Knox isn't really a Fort Knox ***UPDATE***," 23 October 2014. [Online]. Available: http://mobilesecurityares.blogspot.co.uk/2014/10/why-samsung-knox-isnt-really-fort-knox.html. [Accessed 27 October 2014].

[222] D. Macrae, "Samsung Denies That KNOX Security For Android Is 'Completely Compromised'," 26 October 2014. [Online]. Available: http://www.techweekeurope.co.uk/news/samsung-denies-knox-security-android-completely-compromised-154150. [Accessed 27 October 2014].

[223] Samsung KNOX News, "In response to a blog post on Samsung KNOX," 24 October 2014. [Online]. Available: https://www.samsungknox.com/en/blog/response-blog-post-samsung-knox. [Accessed 27 October 2014].

[224] Ben-Gurion University of the Negev, “BGU Security Researchers discover Vulnerability in Samsung's Secure Software on the Company's Flagship Device Galaxy S4,” 24 December 2013. [Online]. Available: http://in.bgu.ac.il/en/Pages/news/samsung_breach.aspx. [Accessed 27 October 2014].

[225] Bull, “Secure you mobile workday - Hoox m1 mobile,” [Online]. Available: http://www.bull.com/download/security/S-Hoox_m1-enWeb.pdf. [Accessed 01 October 2014].

[226] GSMK, “GSMK CryptoPhone 400,” [Online]. Available: http://www.cryptophone.de/upload/files/28/original/CP400-Brochure.pdf. [Accessed 02 December 2014].

[227] A. B. Foss, “Secret surveillance of Norway’s leaders detected,” Aften Posten, 16 December 2014. [Online]. Available: http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html. [Accessed 05 January 2015].

[228] Sectra, “Sectra Tiger 7401,” Sectra, [Online]. Available: http://communications.sectra.com/security-solutions/tiger-7401. [Accessed 08 December 2014].

[229] Android, "Android 5.0, Lollipop," [Online]. Available: http://www.android.com/versions/lollipop-5-0/. [Accessed 21 November 2014].

[230] A. Sethi, O. Manzoor and T. Sethi, “User Authentication on Mobile Devices,” Citigal.

[231] Fido Alliance, “Specifications Overview,” Fido Alliance, [Online]. Available: https://fidoalliance.org/specifications. [Accessed 05 January 2015].

[232] M. Jacobsson and M. Dhiman, “The Benefits of Understanding Passwords,” in *USENIX HotSec*, 2012.

[233] Entrust, “Enterprice Authentication - Securing Identities in an Evolving Environment,” August 2014. [Online]. Available: http://www.entrust.com/wp-content/uploads/2012/07/DS_EnterpriseAuth_web_Aug2014.pdf. [Accessed 28 October 2014].

[234] SafeNet, “Mobile Phone & Software Authentication Tokens - Secure remote network access and digital signing with no hardware authenticator required,” [Online]. Available: http://www.safenet-inc.com/multi-factor-authentication/authenticators/software-authentication/. [Accessed 28 October 2014].

[235] EMC^2, "RSA Authentication Manager - Authenticators," [Online]. Available: http://www.emc.com/collateral/data-sheet/h9061-sid-ds.pdf. [Accessed 28 October 2014].

[236] SecurEnvoy, “SecurAccess,” SecurEnvoy, [Online]. Available: https://www.securenvoy.com/products/securaccess/overview.shtm. [Accessed 08 December 2014].

[237] Gemalto, “Mobile Security - Security solutions for mobile as an endpoint,” August 2012. [Online]. Available: http://www.gemalto.com/dwnld/6835_ent_wp_Mobile_Enterprise_Security.pdf. [Accessed 28 October 2014].

[238] CESG and CPNI, “BYOD Guidance: Excitor G/On OS,” 06 October 2014. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360991/BYOD_Guidance_-_Excitor_G_On.pdf. [Accessed 24 November 2014].

[239] TrackR bravo, "TrackR bravo - The Thinnest Tracking Device. Ever.," 2014. [Online]. Available: https://www.indiegogo.com/projects/trackr-bravo-the-thinnest-tracking-device-ever--2. [Accessed 25 November 2014].

[240] RuuviTracker, “RuuviTracker,” [Online]. Available: http://ruuvitracker.fi/. [Accessed 25 November 2014].

[241] Haltia, "ThingSee," 2014. [Online]. Available: http://www.thingsee.com/. [Accessed 25 November 2014].

[242] CISCO, “Next-Generation Intrusion Prevention System (NGIPS),” CISCO, [Online]. Available: http://www.cisco.com/c/en/us/products/security/ngips/index.html. [Accessed 11 12 2014].

[243] McAfee, “McAfee Network Security Platform,” McAfee, [Online]. Available: http://www.mcafee.com/us/products/network-security-platform.aspx. [Accessed 11 12 2014].

[244] Checkpoint, “IPS Software Blade,” Checkpoint, [Online]. Available: http://www.checkpoint.com/products/ips-software-blade/. [Accessed 11 12 2014].

[245] Sourcefire, “Next-Generation Network Security,” Sourcefire, [Online]. Available: http://www.sourcefire.com/products/next-generation-network-security. [Accessed 11 12 2014].

[246] Intel Security, “McAfee Complete Endpoint Protection - Enterprise,” McAfee for Business, [Online]. Available: http://www.mcafee.com/au/products/complete-endpoint-protection-enterprise.aspx#vt=vtab-Overview. [Accessed 09 December 2014].

[247] Trend Micro, “Enterprise Security for Endpoints,” Trend Micro, [Online]. Available: http://www.trendmicro.com/us/enterprise/security-suite-solutions/esea-endpoint-advanced/index.html. [Accessed 09 December 2014].

[248] Symantec, “Symantec Endpoint Protection,” Symantec, [Online]. Available: http://www.symantec.com/endpoint-protection.

[Accessed 09 December 2014].

[249] Check Point Software Technologies Ltd., “Check Point Capsule Cloud,” Check Point Software Technologies Ltd., [Online]. Available: https://www.checkpoint.com/products/capsule-cloud/index.html. [Accessed 09 December 2014].

[250] Open Source SECurity, “OSSEC homepage,” ossec.net, [Online]. Available: http://www.ossec.net/. [Accessed 09 December 2014].

[251] AIDE, “AIDE homepage,” sourceforge.net, [Online]. Available: http://aide.sourceforge.net/. [Accessed 09 December 2014].

[252] Open Source Tripwire, “Open Source Tripwire,” sourceforge.net, [Online]. Available: http://sourceforge.net/projects/tripwire/. [Accessed 09 December 2014].

[253] Skycure, “Smart Protection for Smart Devices,” skycure.com, [Online]. Available: https://www.skycure.com/. [Accessed 09 December 2014].

[254] Zimperium Enterprise Mobile Security, “Zimperium Enterprise Mobile Security homepage,” zimperium.com, [Online]. Available: https://www.zimperium.com/. [Accessed 09 December 2014].

[255] Motorola Solutions, “Airdefense Wireless Intrusion Detection and Prevention,” Motorola Solutions, [Online]. Available: http://www.motorolasolutions.com/US-EN/Business+Product+and+Services/Software+and+Applications/WLAN+Management+and+Security+Software/AirDefense%20WIDS%20WIPS. [Accessed 09 December 2014].

[256] Kismet, “Kismet homepage,” kismetwireless.net, [Online]. Available: https://www.kismetwireless.net/. [Accessed 09 December 2014].

[257] Snort, “Snort homepage,” snort.org, [Online]. Available: https://www.snort.org/. [Accessed 09 December 2014].

[258] A. Kibirkstis, “What is the Role of a SIEM in Detecting Event of Interest?,” SANS, November 2009. [Online]. Available: http://www.sans.org/security-resources/idfaq/siem.php. [Accessed 09 December 2014].

[259] HP, “Arcsight ESM,” HP, [Online]. Available: http://www8.hp.com/us/en/software-solutions/arcsight-esm-enterprise-security-management/index.html. [Accessed 09 December 2014].

[260] Intel Security, “Security Information and Event Management (SIEM),” McAfee for Business, [Online]. Available: http://www.mcafee.com/au/products/siem/index.aspx. [Accessed 09 December 2014].

[261] Splunk, “What is Splunk Enterprise?,” Splunk, [Online]. Available: http://www.splunk.com/view/splunk/SP-CAAAG57. [Accessed 09 December 2014].

[262] LogRhythm, “One Integrated Solution,” LogRhythm, [Online]. Available: http://www.logrhythm.com/siem-2.0/one-integrated-solution.aspx. [Accessed 12 December 2014].

[263] IBM, “IBM Security QRadar SIEM,” IBM, [Online]. Available: http://www-03.ibm.com/software/products/en/qradar-siem. [Accessed 11 12 2014].

[264] AlienVault, “Security That’s Unified, Simple, & Affordable.,” AlienVault, [Online]. Available: https://www.alienvault.com/products. [Accessed 11 12 2014].

[265] CS, “Prelude Presentation,” CS, [Online]. Available: http://www.prelude-siem.com/index.php/uk/. [Accessed 11 12 2014].

[266] Tenable Network Security, “Tenable Network Security homepage,” Tenable Network Security, [Online]. Available: http://www.tenable.com/. [Accessed 09 December 2014].

[267] Rapid 7, “Nexpose: Vulnerability Management Capabilities,” Rapid 7, [Online]. Available: http://www.rapid7.com/products/nexpose/capabilities.jsp. [Accessed 09 December 2014].

[268] BeyondTrust, “Retina CS Enterprise Vulnerability Management,” BeyondTrust, [Online]. Available:

http://www.beyondtrust.com/Products/RetinaCSThreatManagementConsole/. [Accessed 09 December 2014].

[269] BeyondTrust, “Retina CS for Mobile,” BeyondTrust, [Online]. Available: http://www.beyondtrust.com/Products/RetinaCSMobile/. [Accessed 09 December 2014].

[270] SAINT Corporation, “SAINT homepage,” SAINT Corporation, [Online]. Available: http://www.saintcorporation.com/index.html. [Accessed 09 December 2014].

[271] GFI, “GFI LanGuard,” gfi.com, [Online]. Available: http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard/specifications. [Accessed 09 December 2014].

[272] SecurityMetrics, “SecurityMetrics MobileScan,” SecurityMetrics, [Online]. Available: https://www.securitymetrics.com/mobilescan. [Accessed 09 December 2014].

[273] OpenVAS, “OpenVAS homepage,” openvas.com, [Online]. Available: http://www.openvas.com/. [Accessed 09 December 2014].

[274] BeyondTrust, “Free Security Management Console that Includes Third-Party Patching, Mobile Device Scanning and Virtual App Scanning,” BeyondTrust, [Online]. Available: http://go.beyondtrust.com/cscommunity. [Accessed 11 12 2014].

[275] T. Rains, “Microsoft Free Security Tools – Microsoft Baseline Security Analyzer,” Microsoft, 22 October 2012. [Online]. Available: http://blogs.microsoft.com/cybertrust/2012/10/22/microsoft-free-security-tools-microsoft-baseline-security-analyzer/. [Accessed 05 January 2015].

[276] Mobiwal, “About Mobiwal,” Mobiwal, [Online]. Available: http://www.mobiwol.com/index.html. [Accessed 11 12 2014].

[277] Wikipedia, "Comparison of proxifiers," [Online]. Available: http://en.wikipedia.org/wiki/Comparison_of_proxifiers. [Accessed 27 November 2014].

[278] Palo Alto Networks, "Still Using Proxies for URL Filtering? There's a Better Way," Palo Alto Networks, 2013.

[279] B. Hookway, "Low cost Android: Crossing the $100 barrier," 07 February 2010. [Online]. Available: http://www.visionmobile.com/blog/2010/02/low-cost-android-crossing-the-100-barrier/. [Accessed 26 November 2014].

[280] A. Singh, "VirtualLogix VLX Virtualization Software Selected by ST-Ericsson for Low-Cost Android-Ready Smartphone Platform," 18 February 2010. [Online]. Available: http://technews.tmcnet.com/fixed-mobile-convergence/topics/mobile-communications/articles/76086-virtuallogix-vlx-virtualization-software-selected-st-ericsson-low.htm. [Accessed 26 November 2014].

[281] VMware, "VMware to Bring Virtualization to Mobile Phones, Enabling a Host of Benefits for Handset Vendors, Corporations and Mobile Phone Users," 10 November 2008. [Online]. Available: http://www.vmware.com/company/news/releases/mvp.html. [Accessed 26 November 2014].

[282] S. Whittle, "VMware foresees mobile virtualization in 2010," 21 May 2009. [Online]. Available: http://www.cnet.com/news/vmware-foresees-mobile-virtualization-in-2010/. [Accessed 26 November 2014].

[283] D. Marshall, "VMware's virtualization of Android smartphones makes two-phones-in-one possible," 08 December 2010. [Online]. Available: http://www.infoworld.com/article/2625025/virtualization/vmware-s-virtualization-of-android-smartphones-makes-two-phones-in-one-possible.html. [Accessed 26 November 2014].

[284] N. Gohring, "VMware shows off mobile virtualization on Android," 15 February 2011. [Online]. Available: http://www.infoworld.com/article/2623217/smartphones/vmware-shows-off-mobile-virtualization-on-android.html. [Accessed 26 November 2014].

[285] InfoWorld, "Beyond virtualization: Why VMware bought AirWatch," 23 January 2014. [Online]. Available: http://www.infoworld.com/article/2610377/mobile-device-management/beyond-virtualization--why-vmware-bought-airwatch.html. [Accessed 26 November 2014].

[286] Citrix, "XenDesktop," [Online]. Available: http://www.citrix.com/products/xendesktop/overview.html. [Accessed 26 November

2014].

[287] HP, "ConvergedSystem for Client Virtualization," [Online]. Available: http://www8.hp.com/us/en/products/converged-systems/client-virtualization/vdi-in-a-box.html. [Accessed 26 November 2014].

[288] VMware, "Horizon (with View)," [Online]. Available: http://www.vmware.com/products/horizon-view. [Accessed 26 November 2014].

[289] Netrepid, “CITRIX HOSTED VIRTUAL DESKTOPS,” [Online]. Available: http://www.netrepid.com/virtual-desktop-vdi/citrix/. [Accessed 26 November 2014].

[290] Myriad Group, "Alien Dalvik (inc Alien Vue)," [Online]. Available: http://www.myriadgroup.com/products/device-solutions/mobile-software/alien-dalvik/. [Accessed 26 November 2014].

[291] R. Xu, M. Park and R. Anderson, “Aurasium: Practical Policy Enforcement for Android Applications,” in *USENIX Security 12*, 2012.

[292] M. Nauman, S. Khan and X. Zhang, “Apex : Extending Android Permission Model and Enforcement with User-defined Runtime Constraints,” in *Inf. Syst. J.* , 2010.

[293] M. Ongtang, K. Butler and P. McDaniel, “Porscha: Policy oriented secure content handling in android,” in *Proceedings Annual Computer Security Applications Conference ACSAC*, 2010.

[294] M. Conti, B. Crispo, E. Fernandes and Y. Zhauniarovich, “CRêPE: A system for enforcing fine-grained context-related policies on android,” *IEEE Transactions on Information Forensics and Security,* pp. 1426-1438, 2012.

[295] B. Davis and H. Chen, “RetroSkeleton: Retrofitting Android Apps,” in *MobiSys '13*, Taipei, Taiwan, 2013.

[296] G. Russello, A. B. Jimenez, H. Naderi and W. v. d. Mark, “FireDroid: hardening security in almost-stock Android,” in *Proceeding ACSAC '13 Proceedings of the 29th Annual Computer Security Applications Conference*, 2013.

[297] P. Landers, "FireDroid - Hardening security in almost-stock Android," 03 February 2014. [Online]. Available: https://www.youtube.com/watch?v=dSqIP6s1M3A. [Accessed 25 November 2014].

[298] K. Sirlantzis, G. Howells, F. Deravi, S. Hoque, P. Radu, G. McConnon, X. Savatier, J.-Y. Ertaud, N. Ragot, Y. Dupuis and A. Iraqui, “Nomad Biometric Authentication: Towards Mobile and Ubiquitous Person Identification,” in *2010 International Conference on Emerging Security Technologies (EST)*, 2010.

[299] Y.-S. Jeong, J. S. Park and J. H. Park, “An efficient authentication system of smart device using multi factors in mobile cloud service architecture,” *International Journal of Communication Systems,* 2014.

[300] E. Hayashi, O. Riva, K. Strauss, A. J. B. Brush and S. Schechter, "Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications," in *Proceedings of the Eighth Symposium on Usable Privacy and Security*, 2012.

[301] S. Kurkovsky, T. Carpenter and C. MacDonald, “Experiments with Simple Iris Regocnition for Mobile Devices,” in *2010 Seventh International Conference on Information Technology: New Generations (ITNG)*, 2010.

[302] Z. Liu and S. Song, “An embedded real-time finger-vein recognition system for mobile devices,” in *IEEE Transactions on Consumer Electronics, vol.58, no.2*, 2012.

[303] J. Mäntyjärvi, M. Lindholm, E. Vildjiounaite, S.-M. Mäkelä and H. Ailisto, “Identifying users of portable devices from gait pattern with accelerometers,” in *Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP 05). IEEE International Conference on*, 2005.

[304] M. Trojahn and F. Ortmeier, “Toward Mobile Authentication with Keystroke Dynamics on Mobile Phones and Tablets,” in *2013 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2013.

[305] DARPA, “Active Authentication,” [Online]. Available: http://www.darpa.mil/Our_Work/I2O/Programs/Active_Authentication.aspx. [Accessed 07 October 2014].

[306] N. Mastali and J. I. Agbinya, “Authentication of subjects and devices using biometrics and identity management systems for persuasive mobile computing: A survey paper,” in *2010 Fifth International Conference on Broadband and Biomedical Communications (IB2Com)*, 2010.

[307] C. Zhen and Y. Su, “Research about human face recognition technology,” in *International conference on Test and Measurement (ICTM 09)*, 2009.

[308] K. I, "Keypad against brute force attacks on smartphones," in *Information Security, IET , vol.6, no.2*, 2012.

[309] K. Moilanen, “Salasanojen unohtelu maksaa Espoon kaupungille vuosittain 200 000 euroa,” 29 October 2014. [Online]. Available: http://www.metro.fi/uutiset/a1387807844890. [Accessed 26 November 2014].

[310] S. Komanduri, R. Shay, L. F. Cranor, C. Herley and S. Schechter, “Telepathwords: preventing weak passwords by reading users' minds,” in *USENIX Security*, 2014.

[311] B. Schneier, “Choosing Secure Passwords,” 03 March 2014. [Online]. Available: https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html. [Accessed 07 October 2014].

[312] M. Jakobsson and R. Akavipat, “Rethinking Passwords to Adapt to Constrained Keyboards,” in *IEEE MoST*, 2012.

[313] K. Graham, “Moving Beyond 2-Factor Authentication With 'Context',” darkreading.com, 05 December 2014. [Online]. Available: http://www.darkreading.com/endpoint/authentication/moving-beyond-2-factor-authentication-with-context/a/d-id/1317911. [Accessed 05 December 2014].

[314] S. Shah, “How I bypassed 2-Factor-Authentication on Google, Facebook, Yahoo, LinkedIn, and many others.,” 03 May 2014. [Online]. Available: https://shubh.am/how-i-bypassed-2-factor-authentication-on-google-yahoo-linkedin-and-many-others/. [Accessed 08 December 2014].

[315] D. Sancho, F. Hacquebord and R. Link, “Finding Holes - Operation Emmental,” 2014. [Online]. Available: 2014. [Accessed 05 December 2014].

[316] L.-C. F. Q. W. Chun-Dong Wang, “Zero-Knowledge-Based User Authentication Technique in Context-aware,” in *Multimedia and Ubiquitous Engineering, 2007. MUE 07. International Conference on*, 2007.

[317] J. C. D. Lima, C. C. Rocha, I. Augustin and M. A. R. Dantas, “A Context-Aware Recommendation System to Behavioral Based Authentication in Mobile and Pervasive Environments,” in *Embedded and Ubiquitous Computing (EUC), 2011 IFIP 9th International Conference on*, 2011.

[318] H. Witte, C. Rathgeb and C. Busch, “Context-Aware Mobile Biometric Authentication based on Support Vector Machines,” in *Emerging Security Technologies (EST), 2013 Fourth International Conference on*, 2013.

[319] M. Jakobsson, E. Shi, P. Golle and R. Chow, “Implicit Authentication for Mobile Devices,” in *HotSec 09 Proceedings of the 4th USENIX conference on Hot topics in security*, 2009.

[320] K. Halunen and A. Evesti, “Context-Aware Systems and Adaptive User Authentication,” in *Evolving Ambient Intelligence*, 2013.

[321] A. Evesti and E. Ovaska, “Comparison of Adaptive Information Security Approaches,” *ISRN Artificial Intelligence 2013,* 2013.

[322] C. Ellison and B. Schneier, “Ten Risks of PKI: What You're not Being Told about Public Key Infrastucture,” *Computer Security Journal,* vol. XVI, no. 1, pp. 1-8, 2000.

[323] N. Bar-Yosef, “Examining Threats Facing Public Key Infrastucture (PKI) and Secure Socket Layer (SSL),” securityweek.com, 12 February 2012. [Online]. Available: http://www.securityweek.com/examining-threats-facing-public-key-infrastructure-pki-and-secure-socket-layer-ssl. [Accessed 04 December 2014].

[324] P. Eckersley, “How secure is HTTPS today? How often is it attacked?,” EFF, 25 October 2011. [Online]. Available: https://www.eff.org/deeplinks/2011/10/how-secure-https-today. [Accessed 04 December 2014].

[325] G. Slepak, “DNSChain + okTurtles (version 1.1.1),” [Online]. Available: http://okturtles.com/other/dnschain_okturtles_overview.pdf. [Accessed 04 December 2014].

[326] M. Lennon, “GlobalSign Acknowledges System Breach,” securityweek.com, 10 September 2011. [Online]. Available: http://www.securityweek.com/globalsign-acknowledges-system-breach. [Accessed 04 December 2014].

[327] M. Lennon, “Hacker Forces DigiNotar Into Bankrupty,” securityweek.com, 20 September 2011. [Online]. Available: http://www.securityweek.com/hacker-forces-diginotar-bankruptcy. [Accessed 04 December 2014].

[328] B. Prince, “VeriSign Attackers Swiped Data from Servers, Management Left in the Dark,” securityweek.com, 02 February 2012. [Online]. Available: http://www.securityweek.com/verisign-attackers-swiped-data-servers-management-left-dark. [Accessed 04 December 2014].

[329] P. Eckersley, “Iranian hackers obtain fraudulent HTTPS certificates: How close to a Web security meltdown did we get?,” EFF, 23 March 2011. [Online]. Available: https://www.eff.org/deeplinks/2011/03/iranian-hackers-obtain-fraudulent-https. [Accessed 04 December 2014].

[330] P. Ducklin, “Anatomy of a "goto fail" - Apple's SSL bug explained, plus an unofficial patch for OS X,” Sophos, 24 February 2014. [Online]. Available: https://nakedsecurity.sophos.com/2014/02/24/anatomy-of-a-goto-fail-apples-ssl-bug-explained-plus-an-unofficial-patch/. [Accessed 04 December 2014].

[331] SANS, “Common issues in PKI implementations - climbing the "Slope of Enlightenment",” SANS Institute, 2003.

[332] OpenSSL, “OpenSSL vulnerabilities,” openssl.org, [Online]. Available: https://www.openssl.org/news/vulnerabilities.html. [Accessed 04 December 2014].

[333] Codenomicon, “Heartbleed,” heartbleed.com, April 2014. [Online]. Available: http://heartbleed.com/. [Accessed 04 December 2014].

[334] B. Möller, T. Duong and K. Kotowich, “This POODLE Bites: Exploiting The SSL 3.0 Fallback,” September 2014. [Online]. Available: https://www.openssl.org/~bodo/ssl-poodle.pdf. [Accessed 04 December 2014].

[335] J. Callas, L. Donnerhacke, H. Finney and D. Shaw, “OpenPGP Message Format,” November 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4880.txt. [Accessed 04 December 2014].

[336] N. Borisov, I. Goldberg and E. Brewer, “Off-the-Record Communication, or, Why Not To Use PGP,” in *WPES'04*, 2004.

[337] okTurtles, “okTurtles,” okturtles.com, [Online]. Available: http://okturtles.com/. [Accessed 04 December 2014].

[338] SALT LLC, "SALT - Keyless entry for your phone," 2014. [Online]. Available: https://www.kickstarter.com/projects/2018413691/salt-keyless-entry-for-your-phone. [Accessed 25 November 2014].

[339] Qualcomm, “An autonomous, "always on" proximal discovery solution,” [Online]. Available: https://www.qualcomm.com/invention/research/projects/lte-direct. [Accessed 01 October 2014].

[340] T. Simonite, “Future Smartphones Won't Need Cell Towers to Connect,” 29 September 2014. [Online]. Available: http://www.technologyreview.com/news/530996/future-smartphones-wont-need-cell-towers-to-connect/. [Accessed 01 October 2014].

[341] J. Välimäki, “Bluetooth and Ad Hoc Networking,” [Online]. Available: http://www.netlab.tkk.fi/opetus/s38030/k02/Papers/16-Jari.pdf. [Accessed 21 November 2014].

[342] P. Suri and S. Rani, "Bluetooth network-the adhoc network concept," in *SoutheastCon, 2007*, 2007.

[343] One Laptop per Child, "One Laptop per Child," [Online]. Available: http://one.laptop.org/. [Accessed 21 November 2014].

[344] OpenGarden, "FireChat," [Online]. Available: https://opengarden.com/firechat. [Accessed 21 November 2014].

[345] K. Karppinen, Security Measurements based on Attack Trees in a Mobile Ad Hoc Network Environment, Espoo: VTT Publications, 2005.

[346] B. Levine, “Who is putting up 'interceptor' cell towers? The mystery deepens,” 02 September 2014. [Online]. Available: http://venturebeat.com/2014/09/02/who-is-putting-up-interceptor-cell-towers-the-mystery-deepens/. [Accessed 01 October 2014].

[347] B. Schneier, “Fake Cell Phone Towers Across the US,” 19 September 2014. [Online]. Available: https://www.schneier.com/blog/archives/2014/09/fake_cell_phone.html. [Accessed 04 November 2014].

[348] Septier, “Septier IMSI Catcher,” [Online]. Available: http://www.septier.com/368.html. [Accessed 01 October 2014].

[349] J. Latvakoski and T. Väisänen.Finland/EU Patent EP 1983715 A1, 2007.

[350] P. Chatterjee, I. Sengupta and S. Ghosh, "A Distributed Trust Model for Securing Mobile Ad Hoc Networks," in *IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC)*, 2010.

[351] J.-H. Cho, A. Swami and I.-R. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks," in *Communications Surveys & Tutorials*, 2011.

[352] S. Jain and J. S. Baras, "Distributed Trust Based Routing in Mobile Ad-Hoc Networks," in *proceedings of the 2013 Military Communications Conference (MILCOM 2013)*, San Diego, California, 2013.

[353] S. Chakravarty, M. V. Barbera and G. Portokalidis, "On the Effectiveness of Traffic Analysis Against Anonymity Networks Using Flow Records," *Passive and Active Measurements,* pp. 247-257, 2014.

[354] Facebook, "Facebook's onion address," [Online]. Available: https://facebookcorewwwi.onion/. [Accessed 06 November 2014].

[355] SANS, “Security Skill Assessment and Appropriate Training to Fill Gaps,” [Online]. Available: https://www.sans.org/critical-security-controls/control/9. [Accessed 08 October 2014].

[356] K. Scarfone, M. Soppaya, A. Cody and A. Orebaugh, “NIST Special Publication 800-115: Technical Guide to Information Testing and Assessment,” NIST.

[357] Z. Zorz, "German spy agency wants to buy and use 0-day bugs," 11 November 2014. [Online]. Available: http://www.net-security.org/secworld.php?id=17622. [Accessed 27 November 2014].

[358] Z. Zorz, "Mobile Pwn2Own 2014: Windows Phone's sandbox resists attack," 14 November 2014. [Online]. Available: http://www.net-security.org/secworld.php?id=17640. [Accessed 27 November 2014].

[359] S. Sabens, "Mobile Pwn20wn 2014: The day two recap," 12 November 2014. [Online]. Available: http://h30499.www3.hp.com/t5/HP-Security-Research-Blog/Mobile-Pwn2Own-2014-The-day-two-recap/ba-p/6670234#.VHbwVvmSygZ. [Accessed 27 November 2014].

[360] BlackPhone, “BlackPhone's Bugcrowd,” [Online]. Available: https://bugcrowd.com/blackphone. [Accessed 27 November 2014].

[361] Telegram, “Security Contest Winter 2013-2014 FAQ,” [Online]. Available: https://core.telegram.org/contestfaq. [Accessed 27 November 2014].

[362] Telegram, “$300,000 for Cracking Telegram Encryption,” [Online]. Available: https://telegram.org/blog/cryptocontest. [Accessed 27 November 2014].