An Overview of Threats and Security Software Solutions for Smartphones

D. Fischer, B. Markscheffel, and T. Seyffarth
Ilmenau University of Technology
Germany

Abstract

The market of security software solutions for smartphones has grown considerably in the last years. A wide range of products is available. The objective of our paper is to develop an overview of security software solutions for smartphones. At first we identify typical threats and security measures for smartphones. Then we explore current security software solutions and describe how these can be classified. Furthermore, we analyse which security software solutions (respectively classes of security software solutions) can prevent or mitigate which threats.

1. Introduction

Smartphones are multifunctional mobile devices, which provide advanced capability and connectivity beyond typical cell phones [1]. One of its outstanding characteristics is the ability to enhance its functionality with the help of additional software applications (apps). This is one of the reasons for broadening the use cases of smartphones and its worldwide increasing diffusion in both every day’s private and professional life [2]. Moreover, smartphones are more and more integrated in mission critical processes and used to handle and to save permanently mission critical data [3].

Parallel to this development, one can observe an increasing amount of publication dealing with security incidents for smartphones [4]. Further authors describing threats and vulnerabilities for smartphones in detail and analysing possible attacking vectors [5, 6, 7]. This reflects the fact that already today a high potential of endangerment of smartphones exists. Moreover, researchers and practitioners are expecting a dramatic worsening of this situation [4].

In this area of conflict has a rapidly growing market for security software solutions for smartphones emerged, especially in the last few years. Enterprises like AirWatch, Citrix, Fiberlink, Kaspersky Lab, MobileIron, McAfee, Sophos or Symantec offering a whole range of products which are promising to make the use of smartphones safer.

Due to the variety of security software solutions some institutions recommend a classification of these products. IDC, for example, uses the following classes [8]: Secure Content Management, Threat Management, Security and Vulnerability Management, Identity and Access Management, and Other Security Solutions.

But a detailed description or definition of these classes is still missing or is too vague. Therefore a distinct mapping of security software solutions onto the classes is rather difficult or impossible. It is also not clearly recognisable which products respectively product classes with its security measures work against which threats, which vulnerabilities can be eliminated and which attacks can be prevented. This makes the selection of security software solutions for smartphones difficult and its use inefficient as well for enterprises and private users.

In this paper we develop a concise overview of threats and security software solutions for smartphones. In particular, we will discuss the following research questions:

(1) Which security software solutions for smartphones there are and how can they classified?

(2) What threats and security measures exists for smartphones?

(3) Which security software solutions for smartphones (respectively classes of security software solutions) by what security measures can prevent or mitigate which threats?

The paper is organised as follows: In the next section we define important terms we use throughout the paper. Thereafter we describe the findings of our predominantly empirical approach to answer the research questions, which were listed in the last preceding paragraph. In section three we identify and describe threats and security measures for smartphones and classify them (research question 2). In section four we propose current security software solutions for smartphones and different ways of classifications of them (research question 1). In section five we describe which security software solution and classes of them can prevent or mitigate which threat (research question 3). Finally, we
conclude the paper with a brief summary and outlook of future research.

2. Definitions

In this paper our focus lies on security of smartphones and data transmissions by smartphones.

A smartphone is a multifunctional and with the help of additional software applications (apps) extensible mobile device [1]. A mobile device is as starting point as well as an endpoint of mobile data transmission and can be considered as a system of hardware and software elements [9].

Security is a “condition in which risks existing as the result of threats [and vulnerabilities] during the use of [smartphones] are limited to an acceptable level by suitable security measures” [10]. Security objectives like confidentiality, availability, and integrity are used to describe the achieved level of security or to define a target state of security.

Vulnerabilities are defects or weaknesses of a smartphone hardware or software element, which can negatively affect the security.

Threats have a direct effect on vulnerabilities of a system so that it could be exploited for an attack. [10]. The consequences are loss of confidentiality, availability, and integrity.

Security measures (alias countermeasures or security safeguards) are actions, methods and tools that are appropriate to reduce or eliminate vulnerabilities [11]. Security measures counteract identified vulnerabilities and help to achieve security objectives.

A security software solution is a software product that is designed to provide security. Using such software, one or more security measures can be implemented [8].

3. Threats and Security Measures for Smartphones

In the first step of our research work we identify and describe threats for smartphones. Based on this, we develop a catalogue of security measures and consider which threats can be prevented or mitigated by these measures (to answer research question 2).

Therefore it is necessary to analyse existing catalogues of threats and security measures for mobile devices or smartphones, such as [4, 9, 12]. After that we conduct a literature review to extend these catalogues. We consider journal and conference papers from the last five years. To retrieve relevant papers we use the following keywords: “threat”, “attack”, “vulnerability”, “risk”, “Schwachstelle”, “Gefahr”, “Attacke”, “Angriffsvektor”, “Schutz”, “security”, and “measure” combined with “mobile”, “mobile device”, “smartphone”, and “smartphone”. In addition to the analysis of websites of selected national and international journals and conferences we also use Google Scholar, IEEE Xplore and the Web of Knowledge as search resources. We analyse relevant papers [11, 13, 14, 15, 16] which are dealing with new threats and security measures to expand in this way our catalogues of threats and security measures for smartphones [9].

We compile a catalogue of 101 typical threats for smartphones. We divided these threats into following classes:

- reconnaissance attacks,
- eavesdropping attacks,
- availability attacks,
- manipulation attacks,
- user behaviour.

Our security measures catalogue covers nine organisational and 48 technical measures for smartphones. Additionally we subdivided the technical security measures into measures for communication security, measures for the security of smartphone, and other technical security measures. Measures for communication security protect the communication channels and data transmissions by smartphones whereas measures for the security of smartphones, e.g. antivirus software, sandboxing. As other technical security measures we classified all measures that could not be assigned to one of the above-mentioned groups. The organisational security measures contain rules on the handling of smartphones and on stored sensitive data. Which security measure can prevent or mitigate which threat we explain with the help of a cross-reference table [17]. Figure 1 illustrates a sample part of our cross-reference table. A field filled with an “X” indicates that a security measure takes effective action against the appropriate threat.

![Figure 1. Excerpt from cross-reference table](image)

The complete cross-reference table shows that the majority of the 101 threats can be prevented or at least weakened with the help of one or more security measures. We could not find any adequate security measures for 33 threats.
4. Classification of Security Software Solutions

In our second research phase we identify security software solutions for smartphones and classes of these software solutions (to answer research question 1).

We perform a further literature review. The focus here is to analyse publications of market research institutes, such as Gartner, IDC, Juniper Research. For the selection of relevant publications we use the following keywords: “security”, “security product”, “security software”, and “security solution” combined with “market”, “mobile”, “mobile device”, “smart phone”, and “smartphone”. All identified security software solutions together with their important facts were summarised in a table. We also describe the identified classifications of security software solution for smartphones and try to unify these classifications. Finally, we check if all security software solutions can be categorised into our unified classifications. To identify security software solutions we considered the manufactures of mobile security software solutions that are named in the “Magic Quadrant for Endpoint Protection Platforms”, “Magic Quadrant for Mobile Device Management Software” and „Magic Quadrant for User Authentication” of Gartner Inc. [18, 19, 20].

As a result of our literature review we could identity five classification approaches of security software solutions [21, 22, 23, 24, 25] (see Figure 2):

- Mobile Device Management (MDM),
- Mobile Network Protection (MNP),
- Mobile Threat Management (MTM), and
- All-in-One-Solutions (AIO).

MDM solutions enable functionalities to secure and manage smartphones centralised. MDP solutions protect data on smartphone using encryption as well as separating corporate data from a user’s personal data. MIAM solutions ensure authentication of the smartphone user and authentication of the device during data transmissions [18]. MNP solutions contain security measures that allow a secure connection from smartphones to back-end services [21]. MTM solutions offer anti-virus, firewall, anti-spam, and anti-phishing functions [21]. AIO solutions offer functionalities of two or more classes which are named above.

We are able to categorise 33 security software solutions for smartphones into our unified classification (see Figure 3).

![Figure 2. Classification Approaches of Security Software Solutions](image)

Based on the categorisation of IBM [21] we suggest a ‘universal’ classification approach with following six classes of security software solutions:

- Mobile Device Management (MDM),
- Mobile Data Protection (MDP),
- Mobile Identity and Access Management (MIAM),
- Mobile Network Protection (MNP),
- Mobile Threat Management (MTM), and
- All-in-One-Solutions (AIO).

5. Analyse of the Impact of Security Software Solutions

In the third phase, we explore which security software solutions for smartphones (or classes of security software solutions) can prevent or mitigate which threats (to answer research question 3).

We analyse which security measures (contained in our catalogue) are enabled by which security software solution. For this mapping we primarily took into account publications by manufacturers of security software solutions (e.g. documentation,
To find out which security measures are enabled by which class of security software solutions we count the number of measures provided by the security software solutions in each class. If more than half of the security software solutions in one class contain a security measure we assign these measures to this class. Figure 4 shows a small cut-out of our mapping that documented which product classes enable which security measures.

**Figure 4. Product Classes and their Security Measures**

With the help of our cross-reference table (cp. section 3), we can describe which threats can be prevented or mitigated by which security software solutions respectively classes of security software solutions. Error! Reference source not found.5 illustrates the cause-effect relationship between security software solutions, security measures, and threats that we have supposed.

**Figure 5. Security Software Solutions, Security Measures, and Threats**

Figure 6 shows a sample part of our mapping that documented which product classes enable which security measures.

**Figure 6. Product Classes and their Impact of Threats**

### 6. Conclusion and Future Research

Considering the results of our literature reviews we were able to describe 101 threats and 51 security measures for smartphone. For every threat we analysed which security measures can prevent or mitigate the threat. Finally, we were able to outline that adequate security measures are not available for every threat.

Based on the classification approaches of five market research institutes we could distinguish six classes of security software solutions. Also we were able to classify 33 security software solutions into these unified classification.

Furthermore we can describe in detail which security software solutions respectively classes of security software solutions prevent or mitigate which threats. This will enable an easier and more accurate selection of security software solutions for smartphones for both business and private users.

Future research could target a further analysis and more detailed description of impacts of the specific security measures whereby it is of particular interest to what extent a security measure can mitigate threats. This would enable more accurate statements about the security of smartphones and the value of security software solutions for smartphones. We also consider a further evaluation of our classification.

### 7. References


