Daniel Fischer, Bernd Markscheffel and Tobias Seyffarth

An overview of threats and security software solutions for smartphones.

Zuerst erschienen in:
International Journal for Information Security Research (IJISR) / Infonomics Society. - [S.l.] : Infonomics Society, ISSN 2042-4639, Vol. 3.2013, 3/4.
S. 427-431.

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", "Angriffs-vektor", "Schutz", "security", and "measure" combined with "mobile", "mobile device", "smart phone", 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 smart-phones. 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.

		Security Measures [1-57]				
		…	TM 2	TM 3	TM 4	…
Threats [1-101]	…			X		X
	20					
	21		X	X	X	
	22					
	…	X	X			

Figure 1. Excerpt from cross-reference table

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):

IBM	IDC	Juniper Research	TMR	Visiongain
Mobile Device Management	Security and Vulnerability Management	-	Mobile Device Management	Mobile Device Management
Mobile Data Protection	Other Security Solutions	Data and File Encryption	Mobile Data Security	Mobile Data Security
Mobile Identity and Access Management	Identity and Access Management	Identity and Access Management	Mobile Identity Management	Mobile Identity Management
Mobile Network Protection	Threat Management	-	Mobile Virtual Private Network	Mobile Virtual Private Network
Mobile Threat Management	Secure Content and Threat Management	Secure Content and Threat Management	Mobile Device Security	Mobile Device Security

Figure 2. Classification Approaches of Security Software Solutions

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).

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).

Classes	Products
Mobile Device Management	AirWatch Bring Your Own Device, AirWatch Verwaltung mobiler Geräte, Citrix Enterprise MDM, Fiberlink Maas360 Mobile Device Management, Fiberlink Maas360 Mobile Expense Management, Good Technology BoxTone for Good, McAfee Enterprise Mobility Management, MobileIron Mobile IT, MobileIron Atlas, SAP Afari, Symantec Mobile Management
Mobile Data Protection	AirWatch Verwaltung mobiler E-Mail, AirWatch Verwaltung mobiler Inhalte, Fiberlink Maas360 Secure Document Sharing, Fiberlink Maas360 Secure Mail, Good Technology Good for Enterprise, MobileIron Docs@work, Sophos Mobile Encryption, Symantec Data Loss Prevention for Mobile
Mobile Identity and Access Management	Good Technology Good Vault, Swifel Secure Mobile App Based Authentication, Vasco Data Security DIGIPASS
Mobile Network Protection	Check Point Software Technologies Mobile Access Software Blade, Good Technology Good Connect, Good Technology Good Share, MobileIron AppTunnel
Mobile Threat Management	Kaspersky Mobile Security, McAfee VirusScan Mobile, Sophos Mobile Security, Symantec Mobile Security
All-in-One-Solutions	AirWatch Mobile Sicherheit, Trend Micro Mobile Security 8.0, Fiberlink Maas360 Secure Productivity Suite

Figure 3. Classification of Security Software Solutions for Smartphones

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,

white papers). 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.

Security Measures	MDM	MDP	MIAM	MNP	MTM	AIO
…						
10: Encrypt smartphone memory		x				x
17: Use an anti-virus function / solution					x	
21: Install security updates regularly	x					x
29: Sandboxing		x				
40: Locking smartphone	x					x
41: Delete smartphone memory	x	x				x
…						

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.

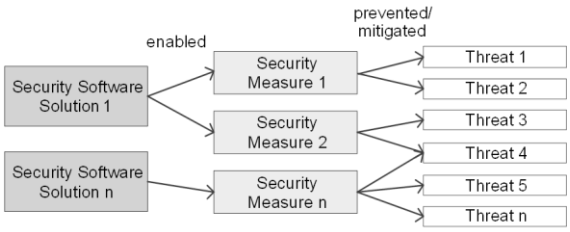

Figure 5. Security Software Solutions, Security Measures, and Threats

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

Threats	MDM	MDP	MIAM	MNP	MTM	AIO
…						
30: Exploiting wireless LAN vulnerabilities	x		x	x		x
32: Exploiting vulnerabilities of the operating system / apps	x	x				x
34: Tapping of the smartphone		x	x	x		x
37: Reading unencrypted data	x	x				x
58: Disabling security measures	x	x				x
59: Installing malware	x	x			x	x
…						

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

[1] P. Zheng and L. M. Ni, "The Rise of the Smart Phone," *IEEE Distributed Systems Online*, vol. 7, no. 3, 2006.

[2] IDC (ed.), *Android and iOS Combine for 91.1% of the Worldwide Smartphone OS Market in 4Q12 and 87.6% for the Year*. Framingham, 2013, http://www.idc.com/getdoc.jsp?containerId=prUS23946013#.UWvhI1ev1f0 (Accessed 2014-01-17).

[3] I. Kao, *Securing mobile devices inthe business environment*. IBM Press, October 2011, http://www-935.ibm.com/services/uk/en/attachments/pdf/Securing_mobile_devices_in_the_business_environment.pdf (Accessed 2014-01-17).

[4] M. Becher, F.C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices," *Proceedings of the 2011 IEEE Symposium on Security and Privacy*, Washington, 2011, pp. 96–111.

[5] McAfee Labs (ed.), *McAfee Threats Report: First Quarter 2013*. McAffe Press, 2013, http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2013-summary.pdf (Accessed 2014-01-09).

[6] F-Secure Labs (ed.), *Mobile Threat Report January-March 2013*. Helsinki, 05/2013, http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2013.pdf (Accessed 2014-01-08).

[7] I. Muttik, *Securing Mobile Devices: Present and Future*. McAfee Labs, 2011, http://www.mcafee.com/us/resources/reports/rp-securing-mobile-devices.pdf (Accessed 2013-07-14).

[8] S. Hudson, B.E. Burke, C.A. Christiansen, D. Kusnetzky, S. D. Drake, and K. Burden, *Worldwide Mobile Security Software 2004-2008 Forecast*. IDC Doc No. 32590, Framingham, IDC, 2004.

[9] D. Fischer, B. Markscheffel, S. Frosch, and D. Büttner, "A Survey of Threats and Security Measures for Data Transmission over GSM/UMTS Networks," *Proceedings of the 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012)*, London, 2012, pp. 477–482.

[10] Federal Office for Information Security BSI, *IT-Grundschutz-Catalogues*, Bonn, 2005, https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html (Accessed 2014-01-10).

[11] B. Schneier, *Secrets and lies - Digital security in a networked world*, John Wiley & Sons, Indianapolis, 2004.

[12] L. Liu, X. Zhang, G. Yan, and S. Chen, "Exploitation and Threat Analysis of Open Mobile Devices," *Proceedings of the 5th ACM/IEEE Symposium on Architectures for Networking and Communications Systems*, New York, 2009, pp. 20–29.

[13] Federal Office for Information Security BSI, *Mobile Endgeräte und mobile Applikationen – Sicherheitsgefährdungen und Schutzmaßnahmen*, Bonn, 2006, https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html (Accessed 2014-03-10).

[14] A. Alkassar, S. Schulz, C. Stüble, "Sicherheitskern(e) für Smartphones: Ansätze und Lösungen - Vom Mikrokern bis zu Capabilities – Verschiedene Lösungsansätze für die App-Trennung und –Kontrolle," *Datenschutz und Datensicherheit*, No. 3, 2012, pp. 175–179.

[15] T. Hemker, "Ich brauche das! - Mobile Geräte im Unternehmenseinsatz," *Datenschutz und Datensicherheit*, No. 3, 2012, pp. 165–168.

[16] F. Weiß, "Consumerization," *Wirtschaftsinformatik*, No. 6, 2012, pp. 351–354.

[17] T. Peltier, *Information Security Risk Analysis*, RC Press, Boca Raton, Fla., Auerbach, 2001.

[18] P. Redman, J. Girard, T. Cosgrove, M. Basso, *Magic Quadrant for Mobile Device Management Software*, http://www.gartner.com/technology/reprints.do?id=1-1FRG59X&ct=130523&st=sb, 2013 (Accessed 2014-01-18).

[19] P. Firstbrook, J. Girard, N. MacDonald, *Magic Quadrant for Endpoint Protection Platforms*, https://www.gartner.com/doc/2292216/magic-quadrant-endpoint-protection-platforms, 2013 (Accessed 2014-01-18).

[20] A. Allan, *Magic Quadrant for User Authentication*, http://de.security.westcon.com/documents/47462/Vasco_Magic_Quadrant_for_User_Authentication_March_2013.pdf, 2013 (Accessed 2014-01-28).

[21] V. Dheap, *Enterprise Mobile Security - Solutions Landscape*, http://instituteforadvancedsecurity.com/ias-blogs/community-blogs/b/vijay_dheap/archive/2012/02/24/enterprise-mobile-security-solutions-landscape.aspx, 2013 (Accessed 2014-02-11).

[22] S. Hudson, B.E. Burke, C.A. Christiansen, C.J. Kolodgy, S.D. Drake, K. Burden, *Market analysis - Worldwide Mobile Security Software 2004-2008 Forecast*, IDC #31131, Vol. 1, Tab: Markets, 2004.

[23] Juniper Research (Ed.), *Mobile Data Security*, http://www.juniperresearch.com/reports.php?id=37, 2006, (Accessed 2014-02-27).

[24] Transparency Market Research (Ed.), *Mobile Security Software Market - Global industry size, market share, trends, analysis, and forecasts 2012 – 2018*, http://www.transparencymarketresearch.com/mobile-security-software-market.html (Accessed 2014-01-04).

[25] Visiongain (Ed.), *Global Mobile Security (mSecurity) Market 2013-2018*, http://www.visiongain.com/Report/1000/Global-Mobile-Security-%28mSecurity%29-Market-2013-2018, 2013 (Accessed 2014-01-04).

