Risk Catalogue for Mobile Business Applications

Basel Hasan[1], Patrick Schäfer[1], Jorge Marx Gómez[1] and Joachim Kurzhöfer[2]
[1]*Department of Computing Science, Oldenburg University, Oldenburg, Germany*
[2]*Lufthansa Industry Solutions, Norderstedt, Germany*

Keywords: Enterprise Mobility, Mobile Business Applications, Mobile Security, Mobile Threats, Risk Catalogues.

Abstract: Today mobile devices, namely smartphones and tablets, are the most popular and used devices. This reality makes companies willing to support mobile devices, which in turn increase the productivity of their employees by allowing them to perform several tasks and to be always updated on the move. However, in spite of the advance in mobile technologies, security is still the primary barrier to the adoption of mobile applications within the enterprise. Some companies avoid the use of mobile business applications due to the fear of security risks. Guidelines and risk catalogues give an overview on the potential risks when using particular applications. Typically, the existing guidelines and risk catalogues target IT-professionals, but not business users who mostly do not have the required technical knowledge to understand the risks. Thus, in this paper, potential risks to companies when adopting mobile business applications are presented in a risk catalogue including the potential mobile threats along with their likelihood of occurrence and possible malicious impact on business. This catalogue will help business users in reinforcing their awareness of possible mobile security risks.

1 INTRODUCTION

Mobile devices have become a more and more usual part of people's everyday life. According to Gartner, global sales of smartphones to end users totalled 403 million units in the fourth quarter of 2015, a 9.7 percent increase over the same period in 2014 (Gartner, 2016). Furthermore, global mobile data traffic is predicted to reach 173 million terabytes (TB) through 2018, an increase of over 300 percent from 2014 (Gartner, 2015).

Increasing advance of mobile technology and its usages, not only in private but in business sectors as well, triggered the enterprises to consider the mobility as inevitable success factors in their business. Enterprise mobility represents the next logical transition in mobile technology evolution which will continue to gain more prominence in enterprises not just to improve the return on investment, but also to improve operational efficiency of the mobile worker (Maan, 2012).

According to market research company IDC (International Data Corporation), the number of enterprise applications optimized for mobility will quadruple by year 2016 compared to year 2014, and IT organizations will dedicate at least 25 percent of their software budget to mobile applications by year 2017 (IDC, 2014). The key enablers of Enterprise Mobility are mobile devices that run mobile enterprise applications (MEAs), which enable quick access to corporate data. Companies gain many advantages when integrating mobile devices into their IT infrastructure. This integration enables business users to access critical business information while they are out of their offices. Consequently, they can make decisions in shorter time and meet their customers' needs.

The employment of MEAs can lead to higher productivity, higher employee satisfaction, and ubiquitous information access (Hoos et al., 2015). However, despite of many advantages of mobility, the adoption of mobile business applications is often slowed down not only because of classical factors like development costs and complexity of the systems, but also because of security concerns. According to a trend study by Luenendonk in year 2014, more than three-quarters of the interviewed companies rate security and privacy as the biggest hurdle when adopting mobile enterprise applications (Luenendonk, 2014). Furthermore, as mobile devices

Hasan, B., Schäfer, P., Gómez, J. and Kurzhöfer, J.
Risk Catalogue for Mobile Business Applications.
DOI: 10.5220/0005968900430053
In *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 2: ICE-B*, pages 43-53
ISBN: 978-989-758-196-0

become ubiquitous, new risks and challenges raise from this. They are increasingly dealing with personal and business data, and they are roaming in public networks with limited security and cryptographic protocols to protect the data (Kizza, 2015).

This paper focusses on determining the threats exist in mobile environments and their accompanying risk to business. Within this paper, mobile devices refer to smartphones and tablets. The rest of this Section is divided into two parts. The first part presents an overview of mobile business applications and the second part defines the security problems the companies face when they plan to adopt mobile business applications. Section 2 presents the related work. A mobile business scenario that describes a use case of MEAs is presented in section 3 along with business assets associated with usage of MEAs. After that, potential mobile threats and their accompanying risks are discussed in section 4 classified in five categories. Finally, the paper sums up with a conclusion and outlook in section 5.

1.1 Mobile Business Applications

In general, mobile applications are applications designed and implemented specifically for mobile devices. Nowadays, there are a huge variety of possible mobile business applications, which can be used in every department or field of functions in the enterprise, e.g. Customer Relationship Management (CRM), Business Intelligence (BI) or Human Resource (HR). Typically, mobile business applications are focused on the Business-to-Customer (B2C) and Business-to-Employee (B2E) domains.

Gröger et al. differentiated three main types of mobile business applications according to the target group of users (Gröger et al., 2013). These are depicted in Figure 1. In this paper, "apps" stands for mobile applications that run on smartphones and tablets. The first type of mobile business applications is mobile applications for costumers, e.g. apps for buying tickets. The second type is mobile applications for employees, e.g. mobile CRM (see section 3). The last type is mobile applications for business partners, which support inter-organizational interaction, e. g. in supply chains.

Mobile applications for employee are further classified into three categories (Gröger et al., 2013): a) standalone mobile applications that are not integrated with a server-side and data storage, b) groupware-connected mobile applications that are linked with standard enterprise groupware systems, e. g., Microsoft Exchange, c) back-end-integrated mobile applications are tightly integrated with the company's back-end, e.g. mobile ERP and mobile CRM.

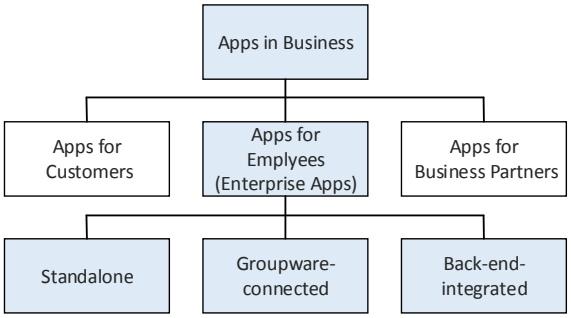

Figure 1: Classification of apps in business (Gröger et al., 2013).

In this paper, we focus on mobile applications for employees, which are also called MEAs. The scenario we defined in section 3 belongs the category "back-end-integrated" mobile applications.

Employees may use either corporate devices that are offered by the company or their own mobile devices for work purposes. Beside corporate mobile devices, the mobile technology Bring Your Own Device (BYOD) also offers advantages and opportunities for companies by reducing technology costs and increasing employees' productivity (Andriole and Bojanova, 2014). However, the companies need to know the potential risk associated with both cases, corporate devices or BYOD. More information about this point is in the next section.

1.2 Security Risk in Mobile Business Applications

Many organizations seem to procrastinate on adopting mobile solutions due to security fears. In other words, they doubt that the possible harm on business is bigger than their potential gain from using mobile business solutions. CISCO 2016 annual security report revealed that enterprises believe that mobility is at a high risk for security breach (CISCO, 2016).

Compared to traditional computing domains like Personal Computers (PCs), mobile devices have very different security principles. Daojing He et al. distinguished mobile security from traditional computer security according to three major factors (Daojing He et al., 2015). First, mobile devices have high mobility. Therefore, they can easily get stolen or lost. Second, mobile devices are strongly personalized, and they are normally operated by a unique user. Third, they have strong connectivity accessing various Internet services, and they are

connected to large number of interfaces (e.g. SD-cards, USB, Bluetooth ...etc.), and different types of communications (Wi-Fi, UMTS …etc.). This makes them more vulnerable to malware through a variety of channels. As stated by Hoos et al., "Security is one of the biggest barriers to introduce mobile technology in enterprises" (Hoos et al., 2015).

Although the number of mobile security threats is increasing almost exponentially, enterprises are not aware of threats arising from integrating mobile devices into their business process, furthermore, smartphone security is still in its infancy and improvements have to be made to provide adequate protection (v Do et al., 2015).

Our work tries to determine the potential threats in mobile environments to help enterprises get a better understanding of the potential risks. The idea behind the risk catalogue is to make the potential mobile threats and their accompanying risk more transparent to the enterprises. Knowing the potential mobile threats will help enterprises by defining the security requirements when adopting mobile business applications. This complies with the following statement: "Safe use of mobile devices arises from knowing the threats" (Markelj and Bernik, 2015).

The existing risk catalogues found in the literatures need a technical background in security. This make such catalogues very complex to be understood by business users. Such catalogues are included in the following section.

2 RELATED WORK

When it comes to threats catalogues, STRIDE Model and IT-Grundschutz Catalogue are often mentioned. STRIDE model is a threat modelling approach provided by Microsoft (Howard and Lipner, 2006). It defines six different categories of threats depending on the kind of attack that might be performed. Those categories are: Spoofing identities, Tampering with data, Repudiation, Information disclosure, Denial of services and Elevation of privileges. This approach is basically a classification scheme used to classify threats when conducting risk analysis, however it does not provide a detailed listing of potential threats. Moreover, it lacks a business context like the possible malicious impact on business, and it does not focus on mobile business applications.

In the second work, IT-Grundschutz Catalogue (BSI, 2013) is also used when conducting risk analysis. However, it is very generic and does not focus on mobile business applications. In general, risk catalogues are often divided by size and specialization into domain-general and domain-specific catalogues (Gramatica et al., 2015). In addition to IT-Grundschutz, ISO/IEC 27002 (ISO/IEC, 2013) and NIST 800-53 (NIST, 2013) are domain-general catalogues. Such catalogues are very complex for business users.

On the other hand, Domain-specific catalogues like PCI DSS (PCI DSS, 2012) for banking domain will help business users in such domain to better understand the potential risks. Furthermore, a threat catalogue specific for a Mobile Device Management (MDM) system has been presented by (Rhee et al., 2013). That catalogue focuses on mobile users, administrators, unauthorized entities and nature as threats sources. However, it is specific to MDM and not for mobile business applications in general. Moreover, it does not cover further threat sources, like mobile operating system, mobile networks and third-party mobile applications.

The risk catalogue presented in this paper provides a business view of the potential threats to mobile business applications along with estimation of the risks to business. An interesting empirical study was conducted to investigate whether existing threats catalogues facilitate the risk assessment process (Gramatica et al., 2015). The qualitative analysis in that study revealed that non-security experts are mostly worried about the difficulty of navigating through the catalogue (the larger and less specific the worse it was). Obviously, that result supports the idea behind our risk catalogue since it is specific for mobile business applications and targets business users, who are mostly non-security experts.

Specific risk catalogues for mobile business applications have not been presented so far.

3 MOBILE BUSINESS SCENARIO

In order to determine the potential threats to mobile business applications, business scenarios have been first defined to show the typical usage of mobile business applications. Those scenarios have been derived from praxis through discussion with business users from different enterprises who are using mobile devices for work purposes. After that, a set of possible business assets related to mobile business applications have been derived (see Section 3.1). Those assets help to estimate the possible impact on business when enabling mobile devices for work purposes.

Figure 2 shows the basic structure of a mobile environment. On the left side of the firewall, the mobile device is shown surrounded by possible

mobile techniques. These include Wi-Fi, cellular networks, Bluetooth, GPS, and others. The right side of the firewall shows the company's server-side, which includes all connected servers. The defined business scenarios focus on the side of the mobile device and its techniques.

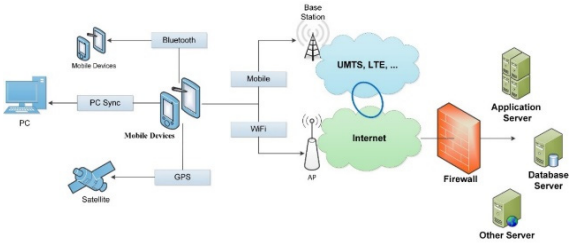

Figure 2: Mobile environment structure (adapted from (Jeon et al., 2011)).

The remainder of this Section describes an excerpt of a scenario on mobile CRM.

A sales representative, who is on a duty visit to a customer, runs a mobile CRM application on mobile device to access important financial information about the customer. The sales representative is also able to gain insight into present and past sales and returns belonging to the customer, and can access the needed sales data from his enterprise database server through the Internet. There are two ways: a) a wireless local area network (WLAN) connection, which is available in the customer's company, or b) mobile internet, which is provided by mobile service provider (MSP) of sales representative's company.

The sales representative is also able to present new products and marketing campaigns to the customer. The information about products and marketing campaigns can be stored directly on the hard drive of the representative's tablet, so access to it does not need an internet connection, but, such data should be synchronized from time to time.

During the duty visit, the sales representative connects his tablet with his enterprise's virtual private network (VPN). Now he can use a reporting tool to get some personal information about his customer. Here, personal data are seen as information that the customer gives about himself, his family, his coworkers or his business that are not directly related to some kind of monetary or service-related transactions. Such data are stored on an enterprise database server and can be accessed on mobile devices.

In the sales negotiations with the customer some difficulties appear. The customer did a supplier evaluation and concluded that there is a cheaper supplier than the sales representative's company. The sales representative now has to act quickly to retain the customer. He uses his tablet to get access to a reporting tool in order to get some information about the customer's possible frequency of orders, and the customer's willingness to pay. Such information helps the sales representative to estimates the customer's value to give him some kind of discount on the offered transaction conditions. After this meeting, the sales representative heads home. Once there, he uses his smartphone to connect to the internet via his own WLAN in order to create a report about his working time, feedback about extra hours and travelling distances using a mobile application adopted by his HR department.

3.1 Assets

After mobile business scenarios are defined, a set of assets are extracted from those scenarios. An asset represents an entity with a financial value for the enterprise (Rhee et al., 2013). It does not only represent a physical object and data, but also business processes. For example, if a mobile business application uses customer data to analyze the buying behavior of the customers and the process of analyzing is threatened, the company gets distorted results, which can lead to an adverse impact on the business.

The extracted assets are listed and categorized in Table 1. The first category is business data (B) that contains customer business data (e.g. name, address, company), customer personal data (e.g. notes about customers' behavior, like notes about hobbies from personal conversations), data about new products (product data), text messages, calls and business contacts. This category also includes campaign data (e.g. marketing campaign). In addition, corporate data, which should only be accessed by employees, can possibly be threatened. If these kinds of data are altered, deleted, or tracked by an attacker, it can cause severe damage to the business (e.g. misplaced or forgotten orders, deleted customer profiles). Therefore, an attack on this data can have an enormous direct or indirect negative financial impact on the company. Financial data, orders and returns are summarized as customer business data or corporate data.

The second category is personal data (P), which contains personal documents, videos, pictures, private authentication data, text messages, calls and contacts, which are stored on mobile devices. These data are typically stored on every smartphone or tablet.

Table 1: Assets associated to the usage of MEAs.

Business Data (B)	• Campaign Data (B1) • Contacts (B2) • Corporate Data (B3) • Customer Business Data (B4) • Customer Personal Data (B5) • Potential Customer Business Data (B6) • Messages (B7) • Product Data (B8) • Production Data (B9)
Personal Data (P)	• Authentication Data (P1) • Contacts (P2) • Documents (P3) • Messages (P4) • Media (P5)
Technical-related (T)	• Battery (T1) • Billing (T2) • Configuration Data (T3) • Hardware (T4) • OS (T5) • Services (T6) • Software (T7)

The third category includes the technical-related (T) assets like hardware, software and operating system of the mobile device. In larger companies, an attack on these assets could typically be worse, because the device itself just costs about a few hundred euros, while an attack on transactional or other business data can costs up to hundreds of thousands of euros. This category also contains the configuration data of the device, applications and the billing of used services.

4 RISK CATALOGUE

This section presents the threats and their accompanying risks that enterprises may face when they adopt mobile business applications. These have been summarized in a risk catalogue and classified in five categories based on the source of the potential threats. The structure of this catalogue is shown in Table 2 and an excerpt of this catalogue is shown in the appendix.

The estimation the likelihood of occurrence has been done based on the literature review and available reports taking into consideration two factors: a) the estimated frequency of threat appearance and b) the motivation and the capability of attacker.

Table 2: Risk Catalogue Structure.

Threats	Description & Risk Estimation	
Threat Name	Threats Short Description	
	Likelihood of Occurrence	Low, Medium or High
	Short Argumentation about the Likelihood of Occurrence	
	Possible Impact	Low, Medium or High
	Short Argumentation about the possible adverse impact on business Assets: List of possible affected assets (see section 3.1)	
	Risk Level	Low, Medium or High

In this work, the potential impact on business is rated based on the potential assets (see section 3.1) that can be affected by a threat. For instance, the impact is considered as high if the threat may enable access to personal customer data, publishing this information can damage the reputation of the enterprise severely, and lead to a huge loss of monetary resources. On the other hand, the potential impact is considered as medium if business user cannot carry out a business process for a short time because the service needed is unavailable. Table 3 describes how the risk is estimated.

Table 3: Risk Levels Estimation Matrix.

Threat		Adverse Impact		
		Low	Medium	High
Likelihood of Occurrence	High	Medium Risk	High Risk	High Risk
	Medium	Medium Risk	Medium Risk	High Risk
	Low	Low Risk	Medium Risk	Medium Risk

In the following subsections, the potential threats in mobile environments are described in a way that helps business users to understand them without need of high technical knowledge in security.

4.1 Mobile Device

Mobile devices themselves can be attacked in several ways. They can be harmed physically, but also the data stored locally on the them and business processes can be threatened as well.

First, the **physical damage** of mobile devices is considered as a threat. Every piece of the hardware (e.g. battery, network adapter, hard drive…etc.) can break at any time, because of defects in the

production process or because of mishandling through the user. If we take the business scenario, the sales representative can unintentionally drop his mobile device due to its small size. The direct financial loss is the mobile device itself, however, the sale representative cannot look up or place a customer's order because of a broken mobile device. This can result in an indirect financial loss. Moreover, the productivity of the sales representative will consequently decrease. If the mobile device's hard drive is broken, important data can be lost. However, most business data are not only stored on the device, but they are synchronized with the company system. The impact on business is therefore low. Moreover, as physical damage of mobile devices is unintentional and the motivation and capability to threaten the business through broken mobile devices is very low, the likelihood of occurrence of such threats is estimated as low.

The second threat in this category is the **loss of mobile devices**. Back to the business scenario: the sales representative may lose his tablet, while in a hurry on the way to the customer. Then he would not be able to perform business processes such as placing orders for the customer. In addition, if business data are stored locally on the mobile device, the impact on business can be high, since corporate or customer data can be exposed and sold to competitors or other potential buyers. On the other hand, if the business data is not directly stored on the mobile device, the confidentiality and integrity of these data are not affected. However, the device could still be used to access business data or perform business processes through mobile business applications installed on it, which are not secured enough or whose login data is stored on the device. This leads to loss of authenticity of certain performed actions and processes. Therefore, potential impact on business through the loss of a mobile device is rated as medium. According to the Kaspersky survey in 2013, one in every six users has experienced loss, theft or catastrophic damage to a mobile device (such as laptop, smartphone or tablet) in the last 12 months (Kaspersky, 2013). According to the same survey, 32% of smartphones and 28% of tablets had work emails, 20% of smartphones and 29% of tablets had business documents. Furthermore, Srinivasan and Wu differentiated between device theft and data theft (Srinivasan and Wu, 2012). According to them, the theft of mobile device is random in nature and the adversary is not interested in the data stored on the device, but motivated by the financial gains from reselling of stolen mobile device, however the third-party who buys the device may be interested in the data on the device.

Another kind of loss of mobile devices is **unattended mobile devices** that are left temporary unsupervised and picked up later by the user. In the business scenario for example the sales representative leaves his tablet unattended in order to make a call. An unattended device for a short time is not such a great threat, because of the limited time and probable lack of intention of the unauthorized user to cause severe damage to the business. In addition, the capability of accessing the smartphone or tablet of such a person is often not good enough to use critical applications or access essential data. Therefore, the associated risk to business from temporary loss of mobile devices is estimated as low.

4.2 Third Party Mobile Applications

Mobile applications can be threatened through other mobile applications that unintentionally exploit errors or use unneeded access rights to perform their tasks. However, malicious software or so called **malware** can threaten mobile applications. Malware come in many different forms. Viruses contain every type of malicious code that is mostly unintentional downloaded by the user of the mobile device. This can happen, for example, through drive-by-downloads. The first malware aimed at smartphones hit in 2004 and the first virus for mobile phones was written by a group known as 29A in June 2004 (Ramu, 2012).

Malware (e.g. Trojans, worms, spyware, Ransomware and Grayware) can be distributed through different channels like peer-to-peer networks or through mobile applications stores from the operating system vendor. **Trojans** typically come with applications that look useful, and then deliberately perform harmful actions once installed, their real intention is a malicious action targeting mobile device and its data (v Do et al., 2015). For example, ZitMo, is a mobile version of the Trojan Zeus, which works in conjunction with the Zeus banking Trojan to steal login information or money from user's bank account (Pu et al., 2014). **Worms** can typically self-reproduce and propagate themselves to mobile devices via mobile technologies like SMS, MMs or Bluetooth. For instance, a Symbian OS worm that targets mobile phones through Bluetooth, so that the infected mobile becomes a portal for further propagation of this malware to all its Bluetooth neighbours. This can cause massive consequences like increased network throughput, battery depletion and causing mobile

failure by corruption of system binaries (Adeel and Tokarchuk, 2011). Another threat in this category is **spyware**, which typically focuses on collecting data from the user's mobile device without the user's knowledge or approval and sending it to an attacking entity (Lookout, 2011). The collected data can range from personal data like locations, contacts and messages to critical business data used by mobile business applications.

The other type of threats in this category is **grayware** that is often downloaded and installed with free software or applications, for example adware. What makes adware dangerous is that the proposed advertisements can lead to scamming websites or websites with more downloadable malware, which can carry out many unintended activities without the user being even aware of them (Rao and Nayak, 2014).

Another type of malware that prevents the user from accessing some functionalities or files, requiring a payment in order to unblock the access to them, is **ransomware** (Lacerda et al., 2015). For instance, Lockdroid.E is a Trojan for Android devices and it functions like typical ransomware that locks the victim's screen; the victim may then be asked to pay a ransom to unlock their mobile device (Venkatesan, 2016).

To sum up, malware can have a severe impact on business. They can hinder the normal usage of mobile devices and applications, bother the user with unwanted advertisements, destroy all data stored locally on mobile device (e.g. sensitive customer data). Moreover, spying on data can provide critical business data to an unauthorised third party.

4.3 Mobile Operating System

The mobile operating system (mOS) can serve as a source for possible threats to mobile business applications. Two main misconfigurations are considered as threat sources under this category. The first one is the **rooting of mOS**. Rooting itself is not a threat. However, it compromises the integrity of the operating system and can make security technologies that depend on operating system, such as containers, vulnerable to attack (Lookout, 2015). Rooting describes an action from the user to gain root permissions of the respective device and operating system. This process is generally referred to as root on Android OS and jailbreak on iPhone OS (iOS) (Damopoulos et al., 2013). Rooting of mOS is usually used to remove preinstalled, unwanted applications, customize the theme and functions of the mOS or so that the user can install unofficial applications. However, not only the user of the rooted mobile device is able to use these gained permissions, but also malware or attackers can use them to perform even more severe adverse actions. This makes the mobile operating system more vulnerable.

Gartner predicted that by 2017, 75 percent of mobile security breaches will be the result of mobile application misconfigurations like jailbreaking or rooting (Gartner, 2014). According to the same report, Gartner recommends that IT security leaders enforce "no jailbreaking/no rooting" rule, and devices in violation should be disconnected from sources of business data, and potentially wiped, depending on policy choices. If an attacker gains root access to the mOS, the attacker may also get access to the MEAs intercepting data streams to prohibit remote IT commands, or access to data stored locally on a mobile device (Michaelis, 2012). Usually enterprises apply a mandatory enterprise device management with jailbreak & rooting detection (Michaelis, 2012). This will decrease the opportunity of having a rooted mobile device enrolled into an enterprise device management. Therefore, the possible malicious impact on business is estimated as medium.

The second misconfiguration in this category is that of **missing updates** of the mOS. Missing updates can cause risk because they always include patches and security updates. However, the impact depends on how critical the missing updates are.

4.4 Mobile Networks

Different mobile networks can be used to launch attacks against mobile devices. These attacks can have severe consequences and differ in their likelihood of occurrence and possible adverse impacts on business.

This category includes threats like Denial of Service (**DoS**) that denies performing a certain service or running a certain software or application. DoS-attacks not only focus on the denial of services, they can reduce the ability of valid users to access resources (Suvda Myagmar et al., 2005) or they can induce incorrect operation (Rhee et al., 2013). Most commonly known are Distributed Denial of Service (DDoS) attacks, which use a huge amount of malware-infected devices and PCs to disrupt the correct working of a server. Denial of Service-attacks can be launched through wired and wireless network connections like Wi-Fi or internet connections from mobile service providers. Typically, such networks are attacked via a DDoS attack, which is launched using botnets. A botnet is a network of internet-connected devices, which were infected with

malicious software without the knowledge of their users. It is capable of executing computationally demanding tasks in feasible time (v Do et al., 2015). DDoS is one of the adverse actions that can be performed by using botnets, although their users are unaware of that. Moreover, an attack on the cellular internet of a MSP can have adverse consequences for businesses. If such an attack is launched, the use of services like Long Term Evolution (LTE) can be limited or completely denied (Jermyn et al., 2014).

A look at the business scenario (see section 3) reveals that MEAs often need a functioning Internet connection to company's server. If the sales representative wants to place an order, he needs an Internet connection to the server. If the server or the mobile internet connection of the MSP is attacked through a Denial of Service-attack, he cannot place the orders. This might cause an indirect financial loss. Therefore, the impact level is estimated as medium. Furthermore, DoS-attacks can also target mobile ad-hoc networks (MANETs) like direct Peer-to-Peer Wi-Fi or Bluetooth-connections.

Another kind of denial of service, which particularly targets mobile devices, is the **sleep deprivation** or battery exhaustion. It is used to drain the battery of a mobile device by preventing the mobile device from saving battery in sleep modes or similar through constant service requests (Martin et al., 2004). In addition, sleep deprivation can also be applied in form of flooding attack in MANETs where either a specific node or a group of nodes is targeted by forcing them to use their vital resources (e.g. Battery) (Jain, 2014). However, the impact level of this type of DoS is estimated as low.

The second type of mobile network threats is Man-in-the-Middle attacks (**MitM**), that intercept communications in networks to eavesdrop, alter, or delete the exchanged data. The attacker is placed in the middle between the client/server communication flows. (Moonsamy and Batten, 2014) described three popular MitM attacks (SSL Hijacking, SSL Stripping, DNS Spoofing) targeted at smartphone applications. Two scenarios of MitM attacks were simulated in (Kennedy and Sulaiman, 2015). The first scenario is an unencrypted Wi-Fi networks, that do not provide encryption of network traffic. A type of such networks is captive portals, that typically use encryption to secure user's credentials when authenticating to the network, but the network traffic is not encrypted and can be sniffed over the air (Godber and Dasgupta, 2002). In the second scenario, an active malicious actor can control the wireless access points and can launch attacks against mobile applications. For instance, the evil twin attack can be used to deceive users into connecting to a rogue access point (Nikbakhsh et al., 2012). Back to the business scenario, the sales representative may use an available open WLAN when meeting with customer unaware that this network is unsecured. This open WLAN may be provided by an adverse entity, not from the customer' company.

4.5 Mobile User

This category includes potential threats that can be caused by the mobile user as a potential threat source, through unintentional actions without being aware of the security risks while using the mobile device. The major problem is the use or access to untrusted content in the form of websites, which are accessed by users. This is often used for **phishing** activities or the distribution of malware through hostile entities. Typically, business users are unaware of such risks and threats, which they are exposed to by simply browsing the internet and looking up things like shops, online travel agencies and others (Marble et al., 2015).

Phishing websites try to steal login and personal data from the user, e.g. phishing mails or advertisements. Both are used to trick the user into entering private information and login data in replica websites of commonly known websites or through the offering of free downloads or low price shopping. Phishing is a serious threat for business in areas like auction sites, payment services, retail and social networking sites (Symantec, 2014). In addition to the direct costs of phishing, company can also lose trust of customers if the customer data is compromised. Furthermore, if the attacker succeeds in obtaining the login credentials (username, password und PIN, etc.), then the attacker can perform all actions authorized to the mobile device's owner. As result, the impact of risk to business is considered as high.

McAfee Labs Threats Report in 2014 revealed that phishing continues to be an effective tactic for infiltrating enterprise networks (McAfee Labs, 2014). According to the same report, 80% of test takers in a McAfee phishing quiz have fallen for at least one in seven phishing emails. Furthermore, results showed that finance and HR departments, those holding the most sensitive corporate data, performed the worst at detecting fraud, falling behind other departments by a margin of 4% to 9%. Attackers are motivated to target mobile devices due to several different reasons, one of which is the mobile device's display constraints that could be used to hide the URL bar (Abura'ed et al., 2014).

Beside phishing, **downloading of untrusted mobile application** is another type of threat that takes place due to the fact that the user is unaware of the associated risks of such applications. The most known form of threat is called drive-by download, that works by exploiting vulnerabilities in web browsers, plug-ins or other components that work within browsers (Levinson, 2012). Those kind of threats try to prompt users through advertisements or adverse websites to take an action that downloads malware on their mobile devices. An Area of concern for mobile devices is also the Quick Response (QR) codes that can be scanned with a mobile device' camera as input into QR reader's app, then malicious attackers can use these codes to redirect users to malicious websites to download malicious apps (Marble et al., 2015). As the drive-by download can install and launch a malware, the impact to business is estimated as high (see section 4.2). Another threat under this category is **social engineering**, which is based on human behavior. For instance, phishing is solely based on social engineering by exploiting human vulnerability in order to trick the victim into providing sensitive credentials (Abura'ed et al., 2014).

Finally, **unaware privilege granting** to the third-party mobile applications can be done without the knowledge of the mobile user. For example, Android and iOS inform the user about the access rights required while installing a mobile application. Although users are warned or informed about that, they tend to overlook this information and just grant the access privileges to the mobile application. Potential risk to business can arise if the installed third-party application gets the privilege to access contacts list that includes business contacts.

5 CONCLUSION AND OUTLOOK

In this paper, a risk catalogue, which includes a list of potential mobile threats classified in five categories has been presented. First, mobile business scenarios have been defined to get insight in the typical usage of mobile business applications. Then, a set of business assets have been determined considering the defined scenarios. An estimation of the potential impact on business has been made by mapping between potential threats and assets. This catalogue gives a business view on the mobile threats. Generally, there are existing risk catalogues, but they show a generic and not business-context view, which makes them complex for business users.

The resulted artifact (the risk catalogue) was evaluated through discussion with experts from the business domain. They found that the threats overview in the risk catalogue is detailed enough and would allow a reader to access important information quickly. Moreover, they found that mapping the assets with potential threats is meaningful for business users especially for those who do not know which assets can be threatened when using mobile devices for work purposes. Based on their feedback, a good improvement can be made by assigning a value for each asset and considering that value in the risk estimation.

Defining security requirements for mobile business applications requires a knowledge about the potential security threats and risk in mobile business environments. Therefore, the risk catalogue presented will be extended further to determine mobile security measures and mapping them to the potential threats to mitigate the potential risk. Furthermore, the risk catalogue and the mapping between security threats and measures will be implemented as an online wiki system, which will facilitate quick access to the information about security threats and measures. It is intended to provide the implemented catalogue with important functions (e.g. based on roles, an administrator can add, delete, modify the threats, measures as well as the mapping between them) making it extendable to include further threats. Finally, as the security requirements can be different for each enterprise depending on its size and domain, it is also intended to give the possibility that each enterprise can manage its own catalogue.

REFERENCES

Abura'ed, N., Otrok, H., Mizouni, R. and Bentahar, J. (2014). Mobile phishing attack for Android platform. In *10th International Conference on Innovations in Information Technology*, Al Ain, United Arab Emirates, pages 18-23.

Adeel, M. and Tokarchuk, L. N. (2011). Analysis of Mobile P2P Malware Detection Framework through Cabir & Commwarrior Families. In *IEEE Third International Conference on Privacy, Security, Risk and Trust*. Boston, MA, USA, pages 1335-1343.

Andriole, S. J. and Bojanova, I. (2014). Optimizing Operational and Strategic IT. *IT Professional*, 16 (5):12–15.

BSI (2013). IT-Grundschutz-Catalogues. Available at: *https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html*, checked on May 2016.

CISCO (2016). Cisco 2016 Annual Security Report. Available at: *http://www.cisco.com/c/en/us/products*

/security/annual_security_report.html, checked on May 2016.

Damopoulos, D., Kambourakis, G., Anagnostopoulos, M., Gritzalis, S. and Park, J. H. (2013). User privacy and modern mobile services. Are they on the same path?. *Personal and Ubiquitous Computing*, 17(7):1437–1448.

Daojing He, Chan, S. and Guizani, M. (2015). Mobile application security: malware threats and defenses. *Wireless Communications*, IEEE, 22(1):138–144.

Gartner (2014). Gartner Says 75 Percent of Mobile Security Breaches Will Be the Result of Mobile Application Misconfiguration. Available at: *http://www.gartner.com/newsroom/id/2753017*, checked on May 2016.

Gartner (2015). Gartner Forecasts 59 Percent Mobile Data Growth Worldwide in 2015. Available at: *http://www.gartner.com/newsroom/id/3098617*, checked on May 2016.

Gartner (2016). Gartner Says Worldwide Smartphone Sales Grew 9.7 Percent in Fourth Quarter of 2015. Available at: *http://www.gartner.com/newsroom/id/3215217*, checked on May 2016.

Godber, A. and Dasgupta, P. (2002). Secure wireless gateway. In *The ACM workshop. Atlanta*, GA, USA, pages 41-46.

Gramatica, M. de, Labunets, K., Massacci, F., Paci, F. and Tedeschi, A. (2015). The Role of Catalogues of Threats and Security Controls in Security Risk Assessment: An Empirical Study with ATM Professionals. In *Requirements Engineering: Foundation for Software Quality,* vol. 9013, Lecture Notes in Computer Science, Cham: Springer International Publishing, pages 98–114.

Gröger, C., Silcher, S., Westkämper, E. and Mitschang, B. (2013). Leveraging Apps in Manufacturing. A Framework for App Technology in the Enterprise. *Procedia CIRP*, 7:664–669.

Hoos, E., Gröger, C., Kramer, S. and Mitschang, B. (2015). ValueApping: An Analysis Method to Identify Value-Adding Mobile Enterprise Apps in Business Processes. In *Enterprise Information Systems*, Lecture Notes in Business Information Processing, vol. 227, Cham: Springer International Publishing, pages 222–243.

Howard, M. and Lipner, S. (2006). The security development lifecycle: SDL, a process for developing demonstrably more secure software, Secure software development series, Microsoft Press, Redmond.

IDC (2014). IDC Reveals Worldwide Mobile Enterprise Applications and Solutions Predictions for 2015. Available at: *http://www.idc.com/getdoc.jsp?containerId=prUS25350514*, checked on May 2016.

ISO/IEC (2013). ISO/IEC 27002, Information technology-Security techniques-Code of practice for information security controls.

Jain, S. (2014). Security Threats in Manets. A Review. I*nternational Journal on Information Theory*, 3(2):37–50.

Jeon, W., Kim, J., Lee, Y. and Won, D. (2011). A Practical Analysis of Smartphone Security. In *Human Interface and the Management of Information. Interacting with Information*, Lecture Notes in Computer Science, vol. 6771, Springer Berlin Heidelberg, Berlin, Heidelberg, pages 311–320.

Jermyn, J., Salles-Loustau, G. and Zonouz, S. (2014). An Analysis of DoS Attack Strategies Against the LTE RAN. *Journal of Cyber Security and Mobility*, 3(2):159–180.

Kaspersky (2013). One in Every Six users suffer loss or theft of mobile devices. Available at: *http://www.kaspersky.com/about/news/press/2013/one-in-every-six-users-suffer-loss-or-theft-of-mobile-devices*, checked on May 2016.

Kennedy, M. and Sulaiman, R. (2015). Following the Wi-Fi breadcrumbs: Network based mobile application privacy threats. In *International Conference on Electrical Engineering and Informatics (ICEEI)*, Denpasar, Bali, Indonesia, pages 265-270.

Kizza, J. M. (2015). Mobile Systems and Corresponding Intractable Security Issues. In *Guide to Computer Network Security, Computer Communications and Networks*, Springer London, London, pages 491–507.

Lacerda, A., Queiroz, R. de and Barbosa, M. (2015). A systematic mapping on security threats in mobile devices. In *Internet Technologies and Applications (ITA)*, Wrexham, United Kingdom, pages 286-291.

Levinson, M. (2012). 6 Ways to Defend Against Drive-by Downloads. Available at: *http://www.cio.com/article/2448967/security0/6-ways-to-defend-against-drive-by-downloads.html*, checked on May 2016.

Lookout (2011). Lookout Mobile Threat Report. Available at: *https://www.lookout.com/img/images/lookout-mobile-threat-report-2011.pdf*, checked on May 2016.

Lookout (2015). Enterprise Mobile Threat Report. The State of iOS and Android Security Threats to Enterprise Mobility [Whitepaper]. Available at: *https://info.lookout.com/rs/051-ESQ-475/images/Enterprise_MTR.pdf*, checked on May 2016.

Luenendonk (2014). Mobile Enterprise Review. Mehr Strategie wagen. Available at: *luenendonk-shop.de/out/pictures/0/mc_mobileenterprisereview_studie_f210214(1)_fl.pdf*, checked on May 2016.

Maan, J. (2012). Enterprise Mobility – A Future Transformation Strategy for Organizations. In *Advances in Computer Science, Engineering & Applications, Advances in Intelligent Systems and Computing*, vol. 167, Springer Berlin Heidelberg, Berlin, Heidelberg, pages 559–567.

Marble, J. L., Lawless, W. F., Mittu, R., Coyne, J., Abramson, M. and Sibley, C. (2015). The Human Factor in Cybersecurity: Robust & Intelligent Defense. In *Cyber Warfare, Advances in Information Security*, vol. 56, Springer International Publishing, Cham, pages 173–206.

Markelj, B. and Bernik, I. (2015). Safe use of mobile devices arises from knowing the threats. *Journal of Information Security and Applications*, 20:84–89.

Martin, T., Hsiao, M., Ha, D. and Krishnaswami, J. (2004). Denial-of-Service Attacks on Battery-powered Mobile Computers. In *Proceedings of the Second IEEE International Conference on Pervasive Computing and*

Communications (PerCom'04), IEEE Computer Society, Washington, DC, USA, pages 309-318.

McAfee Labs (2014). McAfee Labs Threats Report. Available at: *http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2014.pdf*, checked on May 2016.

Michaelis, P. (2012). Enterprise Mobility – A Balancing Act between Security and Usability. In *ISSE 2012 Securing Electronic Business Processes*, Springer Fachmedien Wiesbaden, Wiesbaden, pages 75–79.

Moonsamy, V. and Batten, L. (2014). Mitigating man-in-the-middle attacks on smartphones - a discussion of SSL Pinning and DNSSec. In *The 12th Australian Information Security Management Conference*, pages 5–13.

Nikbakhsh, S., Manaf, A. B. A., Zamani, M. and Janbeglou, M. (2012). A Novel Approach for Rogue Access Point Detection on the Client-Side. In *2012 IEEE Workshops of International Conference on Advanced Information Networking and Applications (WAINA)*, Fukuoka, Japan, pages 684-687.

NIST (2013). Recommended Security Controls for Federal Information Systems, SP. 800-53.

PCI DSS (2012). PCI DSS Risk Assessment Guidelines.

Pu, S., Chen, Z., Huang, C., Liu, Y. and Zen, B. (2014). Threat analysis of smart mobile device. In *General Assembly and Scientific Symposium (URSI GASS)*, 2014 XXXIth URSI. Beijing, China, pages 1-3.

Ramu, S. (2012). Mobile Malware Evolution, Detection and Defense. In *EECE 571B*, Term Survey Paper.

Rao, U. H. and Nayak, U. (2014). Malicious Software and Anti-Virus Software. In *The InfoSec Handbook*, Apress, Berkeley, CA, pages 141–161.

Rhee, K., Won, D., Jang, S.-W., Chae, S. and Park, S. (2013). Threat modeling of a mobile device management system for secure smart work. *Electronic Commerce Research*, 13(3):243–256.

Srinivasan, A. and Wu, J. (2012). SafeCode – Safeguarding Security and Privacy of User Data on Stolen iOS Devices. In *Cyberspace Safety and Security*, Lecture Notes in Computer Science, vol. 7672, Springer Berlin Heidelberg, Berlin, Heidelberg, pages 11–20.

Suvda Myagmar, Adam J Lee and William Yurcik (2005). Threat Modeling as a Basis for Security Requirements. In *Symposium on Requirements Engineering for Information Security (SREIS)*, pages 1-8.

Symantec (2014). Fraud Alert: Phishing — The Latest Fraud Alert: Phishing — The Latest Tactics and Potential Business Impacts – Phishing [White Paper]. Available at: *http://www.symantec.com/content/en/us/enterprise/white_papers/b-fraud-alert-phishing-wp.pdf*, checked on May 2016.

v Do, T., Lyche, F. B., Lytskjold, J. H. and van Thuan, D. (2015). Threat Assessment Model for Mobile Malware. In *Information Science and Applications*, Lecture Notes in Electrical Engineering, vol. 339, Springer Berlin Heidelberg, Berlin, Heidelberg, pages 467–474.

Venkatesan, D. (2016). Android ransomware variants created directly on mobile devices. Available at: *http://www.symantec.com/connect/blogs/android-ransomware-variants-created-directly-mobile-devices*, checked on May 2016.

APPENDIX

An excerpt of the risk catalogue is briefly depicted in Table 4.

Table 4: Excerpt of the risk catalogue.

Threats	Description & Risk Estimation	
MitM attack on mobile ad hoc networks	Man-in-the-Middle attack (MitM) intercepts communications in mobile ad hoc networks (MANETs) (primarily Bluetooth and peer-to-peer Wi-Fi) to eavesdrop, alter or delete the data being exchanged between two mobile devices.	
	Likelihood of Occurrence	**Low**
	Motivation, capability and frequency of MitM attacks on ad-hoc networks are rated as low, because ad-hoc networks like Bluetooth are set up mostly for a short period and very irregularly.	
	Possible Impact	**Medium**
	Messages can be spied on and altered while being exchanged between two mobile devices in a mobile ad-hoc network. Assets: B 7, P 4	
	Risk Level	**Medium**
Spyware	Spyware is a software secretly installed on mobile device. It typically focuses on gathering information on individuals or organisations without their knowledge or approval, and sending it to an adverse entity.	
	Likelihood of Occurrence	**Medium**
	A capable and motivated attacker. According to the statistics, the likelihood of a user encountering malware is rated as medium.	
	Possible Impact	**High**
	Spying on personal data is the main purpose of spyware, such data can be also used to advertise pop-up products. However, business data can be spied on. Assets: B [1-9], P [1-5]	
	Risk Level	**High**
Rooting / Jailbreaking	Gaining root access and rights of mobile operating system. It is not a threat itself, but increases the system vulnerability.	
	Likelihood of Occurrence	**Low**
	Motivation of business users to perform adverse actions on enterprises is low. Usually enterprises apply a mandatory enterprise device management with jailbreak & rooting detection.	
	Possible Impact	**Medium**
	If an attacker gains root access to mobile operating system, the attacker may also get access to the MEAs intercepting data streams to prohibit remote IT commands, or access to data stored locally on a mobile device. Assets: T5	
	Risk Level	**Medium**