Assessing the Suitability of Current Smartphone Platforms for Mobile Government

Thomas Zefferer, Sandra Kreuzhuber, and Peter Teufl

Secure Information Technology Center - Austria,
Inffeldgasse 16a, 8010 Graz, Austria
{thomas.zefferer,sandra.kreuzhuber,peter.teufl}@a-sit.at
http://www.a-sit.at

Abstract. Smartphones offer a great opportunity to improve governmental procedures and services in terms of efficiency and user acceptance. Unfortunately, the heterogeneity of current smartphone platforms such as Apple iOS, Google Android, or Microsoft Windows Phone 8 renders the integration of smartphones into such governmental procedures and services difficult. The choice of the most appropriate smartphone platform is crucial for the security and success of smartphone based procedures and services. Making the correct choice is a difficult task as smartphone platforms are continuously evolving. Furthermore, requirements that need to be fulfilled by the chosen platform heavily depend on the particular use case.
To overcome this problem, this paper identifies use cases, in which smartphones can be used to improve governmental procedures and services. From these use cases, relevant platform properties are derived. These properties are then analyzed on current versions of the three smartphone platforms Android, iOS, and Windows Phone 8. Based on the results of this analysis, the platforms' suitability for the identified use cases is assessed. This way, the paper provides responsible decision makers from governments and public administrations with a profound basis for choosing the correct smartphone platform for a given use case.

Keywords: Mobile government, Smartphones, Security, Android, iOS, Windows Phone 8

1 Introduction

During the past years, smartphones have emancipated from traditional end-user devices such as desktop computers and laptops. Nowadays, smartphones are an integral part of the typical western always-on society and frequently used to access information and services everywhere and at any time. For governments and public administrations, the recent emergence of smartphones offers new opportunities, but also raises new challenges. So far, the integration of information and communication technologies (ICT) in the context of e-government solutions has mainly focused on traditional end-user devices. With the recent emancipation of mobile end-user devices, governments and public administrations are

requested to take the step from electronic government (e-government) towards mobile government (m-government) and to integrate smartphones into governmental applications and solutions [1].

The need to open governmental applications and solutions to smartphones and similar mobile devices raises several problems. Most of these problems are related to the choice of appropriate smartphone platforms, for which governmental applications should be provided. During the past years, a rather heterogeneous ecosystem of different smartphone platforms has evolved. Currently, Google Android[1] and Apple iOS[2] represent the most popular smartphone platforms. However, also other platforms such as Microsoft Windows Phone 8[3] or BlackBerry[4] hold market shares and can be expected to gain relevance in future.

Unfortunately, current smartphone platforms differ significantly in terms of provided functionality and implemented security features. Hence, responsible decision makers must decide for each platform separately, for which applications this platform is suitable. This decision depends on the particular application's requirements regarding security and functionality, and on the particular platform's capability to meet these requirements. The choice of appropriate smartphone platforms is further complicated by their fast and continuous evolution. New versions of mobile operating systems and new features are introduced frequently and make it difficult to keep track of the current state of the art.

At the same time, taking wrong decisions can have severe consequences. This is for instance illustrated by an attack mounted in December 2012 on SMS based authentication mechanisms of European e-banking portals. By employing the capability to intercept SMS messages on Android, US$47.000.000 have been stolen from bank accounts [2]. This incident illustrates that detailed knowledge of application requirements and capabilities of smartphone platforms is crucial to make correct decisions regarding the choice of appropriate smartphone platforms. The comparison of different smartphone platforms has been the topic of several scientific publications [11]. The capabilities of different smartphone platforms for different fields of application have also been assessed in literature [12]. However, few publications have focused on the special field of e-government so far.

In this paper, we provide decision makers from governments and public administrations a basis for correct decisions regarding the choice of appropriate smartphone platforms for security-critical governmental applications and solutions. We start by identifying general use cases that allow for an integration of smartphones into governmental applications and solutions. For each use case, we derive a set of research questions that potentially need to be answered by responsible decision makers. Furthermore, we discuss potential threats for the identified use cases and derive a set of platform properties that influence a smartphone platform's capability to fend off these threats. Subsequently, we analyze current versions of the three popular smartphone platforms Google Android, Ap-

[1] http://www.android.com/
[2] http://www.apple.com/ios/
[3] http://www.windowsphone.com
[4] http://www.blackberry.com

ple iOS, and Microsoft Windows Phone 8 according to the identified platform properties. Based on the obtained results of this analysis process, we finally assess the suitability of the three smartphone platforms for governmental use cases by answering the predefined research questions.

2 Use Cases

Smartphones have the potential to improve governmental processes in various ways. In general, two potential use cases can be distinguished. First, smartphones can be used by governments and public administrations to improve internal processes. Second, smartphones can be used by citizens to remotely access provided m-government services. These two general use cases are discussed in the following subsections in more detail. For each use case, research questions are derived that are potentially relevant for responsible decision makers.

2.1 Internal Usage

Efficiency has become one of the most important requirements for governments and public administrations [3]. During the past years, the integration of ICT and the application of e-government has significantly improved the efficiency of internal governmental processes. Nowadays, smartphones offer great opportunities to further improve efficiency by providing employees of governments and public administrations access to internal infrastructures and data anywhere and at any time. In most cases, smartphones are issued by the employer to its employees. However, recently a new trend called bring-your-own-device (BYOD) has emerged [5]. BYOD means that employees are allowed to use their own private smartphones to access corporate infrastructure and data. This saves costs for employers and is hence also interesting for public bodies that need to save money. However, BYOD also raises several security challenges as employers typically have no or only limited control over used smartphones.

In any case, the internal use of smartphones by employees raises several challenges for governments and public administrations. If responsible decision makers decide to allow employees to access internal infrastructures and data with smartphones, they need to find answers to the following questions.

- *Q1:* Which smartphone platforms should be chosen when equipping employees with smartphones?
- *Q2:* Which smartphone platforms should be supported in BYOD scenarios?
- *Q3:* Which smartphone platforms are in general beneficial in terms of security and functionality?

2.2 Citizen Applications

Smartphones are gradually replacing established end-user devices such as desktop computers or laptops and are evolving to the most preferred end-user devices

for accessing information and services. To react to this trend, governments and public administrations are requested to provide e-government services also for mobile end-user devices. Considering the current heterogeneous ecosystem of smartphone platforms, governments and public administrations have to decide for which platforms to provide mobile e-government applications. In particular, application providers need to find answers to the following research questions.

- *Q4:* Which smartphone platforms should be supported by provided m-government applications?
- *Q5:* Which level of security can be assumed for different smartphone platforms?
- *Q6:* Which smartphone platform provides most functionality for m-government applications?

3 Threat Analysis

To answer the above-defined research questions, different criteria can theoretically be taken into account. For instance, the choice of an appropriate smartphone platform can be based on platforms' current market shares or the price of respective end-user devices. However, for governmental applications, security is usually one of the most important criteria. In this section, we first elaborate on threats that potentially compromise the security of smartphones used in the above-mentioned use cases. From these threats we then derive a set of platform properties that are relevant for the security of a smartphone platform.

3.1 Assets and Threats

Data being stored and processed on smartphones represents the basic asset of smartphone based governmental applications. This applies to scenarios, in which employees of governments and public administrations access internal data with their smartphones, and also to scenarios, in which citizens use their smartphones to execute provided m-government applications and consume m-government services. The capability to protect data being processed and stored on mobile end-user devices is hence the main quality measure for smartphone platforms.

On current smartphone platforms, the security of the asset data is potentially compromised. Security issues on current smartphone platforms have been discussed in [4] and [6]. In general, an attacker can follow two strategies to gain access to data on the mobile device. These two strategies represent the main threats for confidential data on smartphones and are listed and discussed below.

- *Theft:* Due to their mobile nature, smartphones are more prone to loss and theft than stationary end-user devices such as desktop computers. By stealing the smartphone, attackers can potentially gain access to confidential data being stored on the device.

– *Malware:* Compared to traditional mobile phones, smartphones allow users to install additional software. Attackers can use this feature and make users to install malware on smartphones in order to gain access to stored data. Recent reports show that smartphone malware is indeed a growing issue [7].

3.2 Security-relevant Platform Properties

The security of confidential data stored or processed on smartphones is potentially compromised by the threats theft and malware. A smartphone platform's capability to fend off these threats depends on several properties of the particular platform. Security-relevant platform properties are identified and discussed in the following subsections. We will later use these properties to analyze and assess the security of current smartphone platforms and their appropriateness to be used in the context of governmental use cases.

Data Protection: The capability to reliably protect data even if the device gets lost or stolen is a key criterion for the assessment of a smartphone platform's suitability for governmental use cases. The capability to reliably protect data in the case of loss or theft depends on the following aspects.

– *Access protection:* This aspect covers the platform's support for access-protection features. These features assure that only legitimate users are able to access the smartphone's GUI and data stored on the device. Typical implementations of access-protection mechanisms on smartphones rely on password based authentication schemes. When assessing the security of a smartphone platform, the set of supported access-protection methods and their resistance against known attacks need to be considered.
– *Encryption:* Encryption is a cryptographic method that assures the confidentiality of data. Current smartphone platforms typically support different types and methods of encryption. An important aspect of encryption systems is the secure derivation and storage of encryption keys that are used to encrypt confidential data. The set of supported encryption methods and implemented key-derivation functions are hence main aspects that need to be considered when assessing the security of smartphone platforms.
– *Secure storage of credentials:* PINs, passwords, or cryptographic keys that grant access to protected data or services are usually subsumed under the term credentials. Credentials represent highly confidential data that need to be appropriately protected when being stored on smartphones. Some smartphone platforms provide especially protected storage locations for credentials. The availability of such storage locations and their capability to protect credentials are important aspects that need to be considered when assessing the security of smartphone platforms.
– *Mobile device management:* Supported security features such as access protection or encryption are typically optional and need to be manually enabled by the user. Experience has shown that users often refrain from activating

these features for convenience reasons. Mobile device management (MDM) has recently evolved as a potential solution to this problem, as it allows for a central management and configuration of smartphones. Furthermore, MDM allows for remote execution of tasks and routines on smartphones. This way, data stored on smartphones can for instance be remotely deleted (remote wipe) when the device gets lost or stolen. MDM is mainly applied in professional environments, where smartphones are for instance issued by an employer to its employees. In these scenarios, the employer being the owner of the issued smartphones has the legal and organizational power to centrally control and configure these devices. For scenarios, in which users use their own private smartphones, MDM is usually not an option. Still, the support for MDM solutions is a relevant aspect that needs to be considered when assessing the security of smartphone platforms.

Malware Resistance: The resistance against malware is another key criterion for the assessment of a smartphone platform's suitability for security-critical governmental use cases. The resistance against malware mainly depends on the following aspects.

- *API and IPC:* Basically, malware has access to the same application programming interfaces (APIs) and capabilities for inter-process communication (IPC) as ordinary smartphone applications. IPC capabilities and the provided API are hence important aspects for an assessment of the platform's security. If a platform provides fewer capabilities to access system functionality through provided APIs, also malware on this platform is less powerful as it simply has no access to system functionality. The same basically applies for IPC and similar capabilities provided by the smartphone platform.
- *Resistance against rooting:* To improve the capabilities of malware on targeted smartphones, attackers often try to exploit known security flaws of smartphone platforms in order to gain root access to the smartphone's operating system. This is a major threat as attackers with root access to a smartphone can potentially circumvent implemented security measures. The resistance against rooting is hence an important aspect that needs to be considered when assessing the security of smartphone platforms.
- *Integrated security features:* Smartphone platforms implement various features to improve the security of smartphones and to fight malware. These features range from restrictions of potential application sources, over security measures on operating-system level, to sophisticated permission systems that restrict capabilities and access rights of installed applications. The availability of such security features and their implementation are hence also relevant aspects that need to be considered when assessing the security of smartphone platforms.
- *Availability of updates:* Frequent security updates are an important mechanism to fix discovered security flaws and to keep systems up to date. Outdated and unfixed versions of operating systems typically contain more known security flaws and are hence more prone to malware based attacks.

The availability of frequent updates is hence an important aspect that needs to be considered when assessing the security of smartphone platforms.

4 Platform Analysis

Based on the identified relevant system properties, we analyse current versions of the three popular smartphone platforms Apple iOS, Google Android, and Microsoft Windows Phone 8 in this section. BlackBerry has not been considered in detail, as this platform is currently less popular in private and non-corporate scenarios. The conducted analysis has been based on literature research, Web research, and on information provided by the platform vendors.

4.1 Apple iOS

Apple smartphones (iPhone) and the mobile operating system Apple iOS have significantly contributed to the development and current popularity of smartphones. In this section, we analyze the platform's capabilities to protect security-critical data and to resist malware.

Data Protection: Access protection, encryption, secure storage of credentials, and mobile device management have been identifed as relevant aspects regarding the protection of confidential data on smartphones. These aspects are investigated on Apple iOS in the following in more detail.

- *Access protection:* Access to iOS devices can be protected by means of numeric PINs or more complex passphrases that contain also alphanumerical and special characters. However, access protection is disabled by default and needs to be enabled either by the user or by an MDM solution in place.
- *Encryption:* Apple iOS supports a comprehensive and powerful encryption system. Actually, this encryption system consists of two separate subsystems. The first subsystem allows for the encryption of the entire file system. The second subsystem can be used by smartphone applications to encrypt files individually. For each file, a protection class needs to be selected that defines the encryption method, the used key, and the underlying key derivation method. Depending on the chosen protection class, a secure element is integrated into the key-derivation process, which significantly improves the resistance against brute-force attacks. In general, it can be stated that iOS provides application developers with a powerful encryption system to protect confidential data. However, it is in the responsibility of the application developer to appropriately use and employ the provided encryption mechanisms.
- *Secure storage of credentials:* A so-called KeyChain is available on iOS smartphones. The KeyChain is an especially protected container that can be used by application developers to store security-critical credentials on the mobile device. Similar to the encryption system, developers are responsible to correctly use functionality provided by the KeyChain.

– *Mobile device management:* Apple iOS provides broad support for MDM. An appropriate MDM client is integrated directly into the mobile operating system. From a technical point of view, iOS is well suited for the deployment of appropriate MDM solutions, as it allows for a central configuration (e.g. enable file encryption and access protection) and control (e.g. remote wipe) of iOS devices.

Malware Resistance: Aspects of the Apple iOS platform that are relevant for the platform's resistance against malware are discussed in the following in more detail.

– *API and IPC:* Compared to Google Android, iOS provides only a reduced API for the implementation of third-party applications. The provided API does not support access security-critical system functionality such as SMS processing. Additionally, iOS does not provide broad support for background services and multitasking. While this reduces the power of applications, it also limits the capabilities of malware residing on the smartphone.
– *Resistance against rooting:* Rooting or jailbreaking has become very common on iOS devices. Users typically jailbreak their smartphones in order to allow for the installation of more powerful applications that circumvent restrictions of the original operating systems. There are several tools available, that ease the jailbreaking of iOS devices and that facilitate the rooting of smartphones also for technically inexperienced users.
– *Integrated security features:* Apple iOS follows a sandboxing based approach to separate different applications from each other and to avoid that installed applications negatively influence each other. Additionally, iOS implements a permission system that restricts applications' capabilities to access system functionality. Access to certain functionality has to be requested by the application and granted by the user. Furthermore, iOS allows the download and installation of applications from the official Apple AppStore only. Applications offered through this AppStore are subject to reviews and quality-assurance mechanisms. This complicates the distribution of malware for the iOS platform and can hence be seen as a security feature.
– *Availability of updates:* Updates are available for iOS based devices frequently. At this point, iOS is clearly advantageous compared to Google Android. Main reason for the satisfactory situation regarding updates is the fact that there is only one vendor for hardware and software. The limited number of different devices and operating-system versions facilitates the provision of updates on a regular basis.

4.2 Google Android

During the past years, Android has evolved to the most popular smartphone platform in terms of market share. We analyze Android's capabilities to protect confidential data and to resist malware in this section.

Data Protection: Compared to Apple iOS, Android follows slightly different approaches to protect confidential data. Details of supported methods and mechanisms are discussed in the following.

- *Access protection:* Android support various different access-protection methods. Users can define simple PINs or more complex alphanumerical passwords to protect access to their device. Alternatively, access to Android smartphones can also be protected by means of a secret pattern. However, this approach has turned out to be less secure due to reduced entropy compared to password based access-protection methods. Current versions of Android also support biometric access-protection methods based on photos of legitimate users (face unlock). Also this method has recently turned out to be insecure. All access-protection methods are disabled by default and need to be enabled by the user or an MDM solution in place. Hence, the user (or a MDM solution) is in charge of selecting appropriate methods and of choosing secure passcodes.
- *Encryption:* Encryption is supported on Android since version 3.0 (Honeycomb). Similar to access-protection methods, encryption is disabled by default and needs to be manually enabled. In contrast to Apple iOS, Android does not support file based encryption. If encryption is enabled, the entire file system is encrypted using AES. The encryption key is derived from a passcode defined by the user. A secure element is not involved in the key derivation. Hence, brute force attacks on the passcode (and hence on the encryption key) can also be carried out off the smartphone.
- *Secure storage of credentials:* Current versions of Android provide application developers with an API to a special data structure in order to securely store credentials. Similar to Apple iOS, this data structure is called KeyChain. The Android KeyChain encrypts stored credentials using AES and an encryption key derived from the user's access-protection passcode. A passcode based access-protection method is hence a mandatory prerequisite of the Android KeyChain. Again, the derived key does not depend on a secret stored in a secure element, which eases the implementation of brute-force attacks.
- *Mobile device management:* Compared to Apple iOS, Android supports only very limited MDM capabilities. Only few system properties can actually be defined by MDM solutions. Several smartphone vendors tackle this problem by enhancing Android with proprietary MDM capabilities. This has led to a significant fragmentation, which in turn complicates the deployment of MDM solutions and the support of different Android devices. Another limitation of the Android platform regarding the use of MDM is the lack of integrated MDM clients. Using MDM on a smartphone requires the installation of a separate app that acts as MDM client and enforces defined MDM policies. As this app is subject to the same potential security flaws as any other app on the smartphone, this approach raises additional security issues.

Malware Resistance Recent reports show that Android is more prone to malware than other smartphone platforms. Reasons for this vulnerability are discussed in more detail below.

- *API and IPC:* Compared to other platforms, Android offers application developers a much richer API that allows third-party applications access to various system features. Additionally, Android provides a wider support for inter-process communication and allows the implementation of arbitrary background services. While a rich API and wide support for IPC is beneficial for the implementation of powerful applications, it also allows for the development of more powerful malware. On Android, malware is able to implement functionality that would require root access to the operating system on other smartphone platforms.
- *Resistance against rooting:* The rooting of Android devices is quite common nowadays. Several tools exist that allow even technically inexperienced users to easily and quickly gain root access to the operating system of their mobile phone. Similarly, various malware exists that employs known security flaws to gain root access to the attacked smartphone's operating system. In general, Android's resistance against rooting must be rated as rather poor.
- *Integrated security features:* Similar to other smartphone platforms, Android follows and implements a sandboxing approach to separate third-party applications from each other. This assures that one application cannot access data that belongs to another application installed on the same smartphone. The probably most relevant security feature of Android is its permission system [9]. Access to resources and functionality of a smartphone (e.g. access to stored contacts, access to GPS functionality, etc.) requires appropriate permissions. For instance, if an application wants to make use of e.g. GPS functionality, it has to request assignment of the respective permission. Requested permissions have to be granted by the user upon installation of the application. Hence, the user is responsible for assigning requested permissions and for defining access rights and capabilities of installed applications. This is also the main problem of Android's permission system. Users are often not aware of implications of granted permissions and often do not understand this security feature [10].
- *Availability of updates:* Android suffers from fragmentation. Several smartphone vendors supply their devices with modified versions of the Android operating system. In these cases, vendors are responsible to supply customers with appropriate system updates. As the provision of system updates causes effort but does not directly produce profit, updates are often provided on an irregular basis only.

4.3 Microsoft Windows Phone 8

Microsoft has launched its new smartphone platform Windows Phone 8 (WP8) in late 2012 with the aim to catch up with the currently leading platforms Google

Android and Apple iOS. In order to analyze its security and suitability for governmental use cases, this section discusses identified security-relevant properties of Windows Phone 8 devices.

Data Protection: Relevant properties that influence WP8's capability to protect confidential data are discussed in the following in more detail.

- *Access protection:* Windows Phone 8 supports the definition of 4 to 16 digit numeric PINs to protect access to the device. Interestingly, a first analysis shows that alphanumeric passphrases can only be used in conjunction with an MDM solution being in place.
- *Encryption:* According to the official documentation, the Windows Phone 8 platform uses the BitLocker technology for full file-system encryption [8]. The used encryption keys are stored in a trusted platform module (TPM) that is mandatory for each Windows Phone 8 device. Integration of the TPM into the encryption system assures that only trusted boot components verified by an UEFI Secure Boot environment are able to decrypt the file system. Interestingly, file-system encryption can only be activated by MDM policies but not by individual end users.
- *Secure storage of credentials:* To securely store confidential data as well as credentials in the application's isolated storage, data can be encrypted using WP8's data protection API. The used decryption keys are unique for each application and generated at the first start of an application. The keys are derived using the TPM, the user's credentials, and an application identifier.
- *Mobile device management:* WP8 supports basic MDM policies to centrally define access protection mechanism, enable disk encryption, and to apply a remote wipe of the device. MDM is fully integrated in the operating system. Thus, when configuring devices using Microsoft Exchange ActiveSync or Windows Intune, no additional MDM client is required.

Malware Resistance: We have also analyzed WP8's capabilities to resist malware. Results of this analysis are discussed in the following.

- *API and IPC:* Compared to Android, the WP8 platform provides a restricted API and very limited IPC capabilities for third-party applications only and is hence basically comparable to Apple iOS. Also, WP8 provides no wide support for the definition of background tasks. For instance, voice recording and the use of the smartphone camera are not possible in background tasks. This avoids the feasibility of spyware.
- *Resistance against rooting:* WP8 devices include UEFI Secure Boot for verifying the integrity of the operating system. Each software component loaded at boot time is verified and checked for a valid signature. As each component has to be signed by Microsoft, modified versions of the operating system or alternative boot components, which grant root access to the device, cannot be executed in theory. In practice, the situation with WP8 appears to be

advantageous compared to Android or iOS. However, WP8 is still a quite new platform and time will show if it is indeed more resistant against rooting than other platforms.
- *Integrated security features:* Similar to Android and iOS, WP8 follows a sandboxing approach (so-called chambers) to avoid that applications influence each other negatively. WP8 also implements a permission system (so called capabilities) that allows users to define the available functionality for an application. As an additional security feature, WP8 does not allow applications to share data. Each application can only access its own isolated storage. Similar to iOS, applications for Windows Phone 8 can only be installed from the Windows Phone Store or being distributed via a company account to employees. Thus, users cannot install applications from e.g. e-mails or untrustworthy download locations. To prevent malware, Microsoft applies a rather strict review process for third-party applications distributed through the Windows Phone Store.
- *Availability of updates:* Although Windows Phone 8 devices are distributed by multiple hardware vendors, Microsoft is in full control of the Windows Phone 8 platform. Except for some small extensions on Nokia devices, all WP8 handsets run the original version of the operating system. Feature updates, bug fixes, and firmware updates from hardware vendors are distributed directly by Microsoft and should be available frequently.

5 Assessment

The results obtained from the conducted platform analysis build the basis for a concrete assessment of the investigated smartphone platforms' suitability for m-government related use cases. In particular, we assess the two previously defined concrete use cases by answering the research questions that have been defined in Section 2. We finally use the results of this assessment to rank the investigated platforms according to their suitability for mobile government.

5.1 Internal Usage

This use case covers scenarios, in which governments and public administrations allow their employees to use smartphones in order to improve the efficiency of internal processes. Either these smartphones are issued by the employer, or employees are allowed to use their own private smartphones following the BYOD approach. The integration of smartphones into internal processes raises several challenges for governments and public administrations. These challenges are reflected by the research questions *Q1* to *Q3* defined in Section 2.

Considering the results of the conducted platform analysis, research question *Q1* can be answered as follows. As for all analyzed platforms access protection and encryption is optional and needs to be manually enabled, the availability of appropriate MDM solutions is obviously an important requirement. The conducted platform analysis has shown that MDM is rather difficult to implement

and use on Android. Main reasons are the need for additional client software and the increasing fragmentation of this platform. Another important point is Android's weak resistance against malware compared to other platforms. Summarizing, in order to answer research question *Q1*, we can state that Android should not be chosen when supplying employees with smartphones. Apple iOS and WP8 appear to provide a similar level of security and suitability for this use case. However, while much experience is already available for the iOS platform, WP8 is still a rather new platform and still has to prove its practicability.

Similar considerations apply to research question *Q2*. However, if employees are asked and allowed to bring their own devices, slightly different requirements need to be considered. The most important aspect in this case is fragmentation, as employees usually own and use a broad spectrum of different end-user devices. Again, the conducted analysis has shown that Android is disadvantageous in this context as it shows the highest degree of fragmentation of all evaluated smartphone platforms. To answer research question *Q2*, we can hence state that the support of Android cannot be recommended in BYOD programs. Again, WP8 and iOS are more suitable to meet given requirements and are thus more suitable when following BYOD approaches.

Considering research question *Q3*, the conducted platform analysis has revealed that Android provides definitely more functionality than the rather restrictive platforms iOS and WP8. However, the drawback of this increased functionality is a higher vulnerability against malware and attacks. The selection of an appropriate platform hence has to be made subject to security and functionality requirements of the given scenario. In any case, decision makers need to be well aware of the given trade-off between security and functionality.

In summary, reliance on the smartphone platforms iOS and WP8 is suggested for this use case. The use of Android cannot be recommended due to the platform's security vulnerabilities and its increasing fragmentation. If decision makers still decide to rely on Android due to its improved functionality, they need to be well aware of potential security-reducing consequences.

5.2 Citizen Applications

This use case describes scenarios, in which public administrations provide citizens with smartphone applications for a more efficient and convenient conduction of governmental procedures. This use case raises several challenges that are reflected by research questions *Q4* to *Q6* defined in Section 2. Although these research questions cover different aspects, they can be condensed to one central question: Which is the most suitable smartphone platform for this use case?

Considering the demand to reach as many citizens as possible, Google Android and Apple iOS definitely need to be considered as potential target platforms. However, market share is not the only criterion that needs to be considered. The choice of an appropriate target platform also depends on the context and on the requirements of the smartphone application that is to be provided to citizens. If functionality is the most important criterion, Google Android is definitely a good choice as it allows for more powerful applications than iOS

or WP8. However, in many cases, m-government applications process security- and privacy-critical data. Hence, security is often a key requirement that needs to be met. For such applications, Android is often not the best choice due to the platform's vulnerability to malware. For security-critical applications, Apple iOS and Microsoft WP8 should be chosen as target platform instead.

5.3 Platform Ranking

We have used the obtained results of the conducted platform assessment to rank the investigated smartphone platforms according to their capabilities to meet requirements of e-government use cases. For each defined research question, we have ranked the three platforms accordingly.

	Google Android	Apple iOS	Microsoft WP8
Q1	3	1	2
Q2	3	1	2
Q3 – Security	3	2	1
Q3 – Functionality	1	2	3
Q4 – Security-critical applications	3	1	2
Q4 – Non-critical applications	1	2	3
Q5	3	2	1
Q6	1	2	3

Fig. 1. Ranking of the assessed smartphone platforms according to identified research questions.

As shown in Figure 1, Apple iOS turns out to be the overall winner when directly comparing all rankings of all platforms. Google Android is successful especially in use cases and scenarios, in which functionality is more important than security. For security-critical scenarios, Android is not an option. After a first analysis, Microsoft Windows Phone 8 can be assumed to be closer to iOS than to Android in terms of functionality and security. However, being a relatively new platform, WP8 still has to prove its capabilities to provide an appropriate level of security and functionality in practice.

6 Conclusions

In this paper, we have assessed the capabilities of the three popular smartphone platforms Google Android, Apple iOS, and Microsoft Windows Phone 8 to be used in different use cases related to e-government and mobile government. For this purpose, we have identified relevant security properties of smartphone platforms. We have then analyzed the above-mentioned platforms according to these security properties. Based on the results of this analysis process, we have finally assessed the platforms' suitability for m-government use cases.

Results show that there is a trade-off between the provided functionality of a smartphone platform and its security. Considering the fact that m-government use cases very often define strict security requirements, especially the platforms Apple iOS and Microsoft WP8 have turned out to be suitable for m-government use cases. Although Google Android can be an option in special cases, the use of Android can in general not be recommended due to various unsolved security issues of this platform.

By identifying strengths and weaknesses of different smartphone platforms, this work supports responsible decision makers of governments and public administrations to make the correct decisions and to choose appropriate target platforms when deploying smartphone based solutions. This way, this work enhances the development of secure and useful m-government applications at an early stage and helps to employ the potential of smartphones to further improve governmental services.

References

1. Zefferer, T. and Teufl, P.: Opportunities and Forthcoming Challenges of Smartphone-based m-Government Services. Megatrends in eGovernment - European Journal of ePractice, (2011).
2. Schwartz, M.: Zeus Botnet Eurograbber Steals $47 Million. InformationWeekSecurity, http://www.informationweek.com/security/attacks/zeus-botnet-eurograbber-steals-47-millio/240143837, (2012).
3. Yanqing, G.: E-Government: Definition, Goals, Benefits and Risks. Management and Service Science MASS 2010 International Conference, pp. 9–12, (2010).
4. Enck, W., Ongtang, M., and McDaniel, P.: Understanding Android Security. IEEE Security Privacy Magazine, vol. 7, pp. 50–57, (2009).
5. Woods, S.: Bring Your Own Device (BYOD) Increasingly Important to Small Business Budgets. Technorati, http://technorati.com/business/small-business/article/bring-your-own-device-byod-increasingly, (2013).
6. Enck, W., Octeau, D., Mcdaniel, P., and Chaudhuri, S.: A Study of Android Application Security. USENIX Security, August, pp. 935–936, (2011).
7. Lookout Mobile Security: 2011 Mobile Threat Report. https://www.lookout.com/resources/reports/mobile-threat-report, (2011).
8. Microsoft: Windows Phone 8 security and encryption. http://www.windowsphone.com/en-US/business/security, (2013).
9. Barrera, D., Kayacik, H., Mcdaniel, P., van Oorschot, P. and Somayaji, A.: A methodology for empirical analysis of permission-based security models and its application to android. In Proceedings of the 17th ACM conference on Computer and communications security, pp. 73–84, (2010).
10. Felt, A.: Android Permissions: User Attention, Comprehension, and Behavior. In Science And Technology, pp. 1–16, (2012).
11. Rogers, M. and Goadrich, M.: A hands-on comparison of iOS vs. android. In Proceedings of the 43rd ACM technical symposium on Computer Science Education (SIGCSE '12). ACM, New York, NY, USA, 663-663 (2012).
12. Renner, R., Moran, M., Hemani, Z., Thomas, E., Pio, H.S., and Vargas, A.: A comparison of mobile GIS development options on smart phone platforms. In Proceedings of the 2nd International Conference on Computing for Geospatial Research & Applications (COM.Geo '11). ACM, New York, NY, USA (2011).