Impact of the Security Requirements on Mobile Applications Usability

Catalin BOJA, Mihai DOINEA, Paul POCATILU
Department of Economic Informatics and Cybernetics
Bucharest University of Economic Studies
catalin.boja@ie.ase.ro, mihai.doinea@ie.ase.ro, ppaul@ase.ro

The use of mobile devices on such a large scale drives attention on their specific security issues like social engineering attacks, sensitive and personal data theft. Many studies show that the majority of users doesn't have a proper education or culture on securing their data kept on mobile devices. The paper analyses the relation between security and usability in mobile platforms, emphasizing the main security threats and the vulnerabilities that generate them. Also, best practices and metrics are proposed in order to improve the future studies related to this topic.
***Keywords**: Usability, Security, Mobile, Applications, Devices, Metrics, API*

1 Introduction

As more personal data is recoded and stored by electronic devices, the security of data and communication is an aspect that must be implemented by developers and must be correctly understood by users, [1]. Security has become an important aspect on mobile platforms in parallel with the rapid rate of smartphones and tablets adoption by mobile users. These devices are designed to be easily used, to be very functional and to provide a wide range of functions reserved not too long to notebooks or laptops. Usability is the *effectiveness, efficiency and satisfaction with which specified users achieve specified goals in particular environments* (ISO 9241) and is a key factor in defining the quality of mobile devices and applications from user perspective. And because user are the key players in the mobile market, the mobile industry, both software and hardware, are trying to maximize the usability level in order to gain a large market share. The mobile environment highlights the importance of usability because, despite its restrictions on display size, limited battery lifecycle, limited processing power and limited input possibilities has succeeded to surpass in terms of market penetration rate and incomes the more traditional markets of PCs, laptops or notebooks. Theoretically, the ICT security field has measures and techniques that can provide a high level of data and communication protection, if used correctly. Despite it, many studies, [2], [3], [4], [5], [6], [7], [8] and [9] have shown that from a user experience viewpoint this affects the usability of different processes.

The paper is organized as follows:

The section *Usability for Mobile Applications* deals with the usability concept and its characteristics; also with specific ways to achieve it on mobile applications.

Security Issues in Mobile Systems section presents and analyses the most important vulnerabilities for mobile devices with their impact on usability.

The section *Usability vs. Security Metrics* proposes two metrics that can be used to analyze the impact of security on usability for mobile applications.

The paper ends with conclusions and future work.

2 Usability for Mobile Applications

Usability is a primary characteristic for increasing the rate of success in completing different tasks in a system. In mobile computers usability is viewed as a feature that turns users from simple persons with no what so ever knowledge about mobiles, in standard or even professional users, heavily reliant on mobile devices. This characteristic is continuously dependent by the current evolution level of software technologies which change with each hardware breakthrough, [10].

Usability applies to several layers of a mobile system and acts differently, being highly dependent on a user education in terms of mobile systems. The layers to which usability applies are:

- user - mobile device interactions; how the buttons are positioned; what are the nearest functions that can be made with a single push of a button describing the ergonomic characteristic;
- operating system's usability; how well the OS manages applications, resources; what features can easily be of service when special functionalities are needed; how fast tends to respond to user-device interactions;
- user controls diversity; the power to cover as many requirements as needed by offering users controls that can implement not only basic functionalities but also combining between them in order to achieve complexity with high usability;
- data validation is another layer that is strictly dependent on the usability metric, that being closely related also with the general security level.

Usability belongs to a set of characteristics that directly influences the user experience and for this reason has the power to increase or decrease the user perception about a particular technology, a new feature or an entire infrastructure.

On mobile Web applications, as a consequence of the explosive HTML5 adoption and evolution, the user interface gets richer, thus allowing developers to keep the pages look and feel like native applications' user interface.

One way to improve usability in modern mobile operating systems is by providing access to standard tasks through APIs. Almost all modern mobile platforms allow developers to access built-in applications or windows to solve specific tasks in order to assure the best user experience.

Android platform uses intents (*Intent* class) that allow opening a dedicated application for a certain task (e.g. send emails, view pictures, web browsing etc.). For example, in order to select a contact, the following code can be used:

```
Intent intentPeople = new Intent(Intent.ACTION_PICK,
            android.provider.ContactsContract.Contacts.CONTENT_URI);
startActivityForResult(intentPeople, CONTACT);
```

By running this code, the user will have access to the standard application for contact selection, increasing the application's usability (Figure 1).

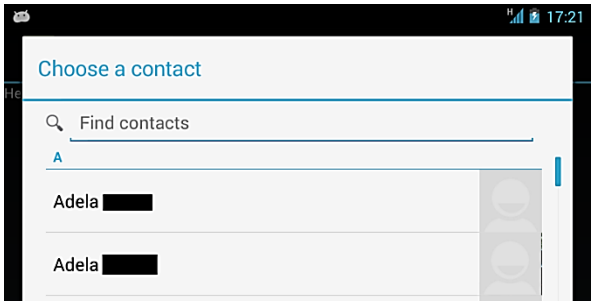

Fig. 1. Android contact picker launched by the application

This approach has at least two advantages:

- for developers: there are few lines of code and they do not have to recreate the user interface for this task;
- for users: they will benefit from a well know interface, with no need to learn something new.

Windows Phone API provides launcher and choosers for the same purpose (sending emails, SMSs, choosing pictures, playing media clips etc.).

The following code snippet is used to launch the built-in contact picker by using the *PhoneNumberChooserTask* class:

```
PhoneNumberChooserTask contactPicker = new PhoneNumberChooserTask();
contactPicker.Completed += contactPicker_Completed;
contactPicker.Show();
```

Figure 2 shows the same results for a Windows Phone device.

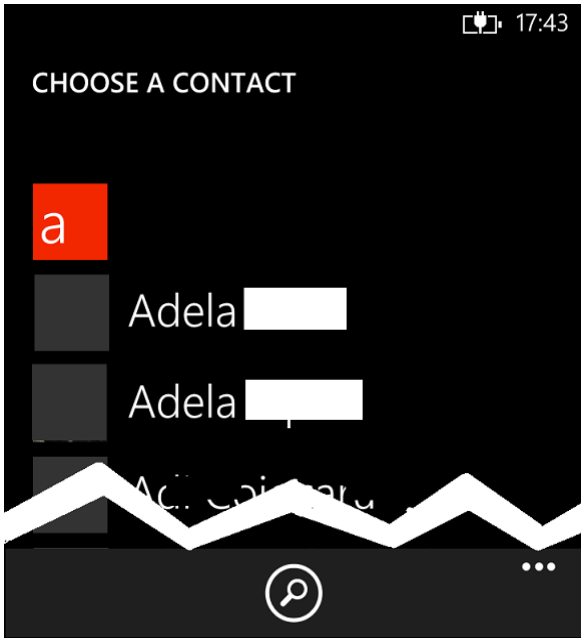

Fig. 2. Windows Phone number chooser launched by application

From both examples it can be seen that the user will get the full functionality of the built-in applications, with the option of selecting, browsing through or searching for the desired contact details.

iOS also makes available APIs to access built-in applications like Mail, Message, Camera, Contacts etc.

Usability is more user oriented than other characteristics and for this reason is very sensible to shifting's in user' behavior. Due to the an intrinsic characteristic of users, that of being heterogeneous, when talking about what they like to use and how, several characteristics, from which usability also, are viewed from a user strictly perspective in order to satisfy the designated target group to which they addresses:

- accessibility – is a general term used to describe the degree to which a mobile piece of software is accessible by as many people as possible, with as less of assistance or none, preferable;
- availability – is the characteristic which reflects the time in which mobile device is fully operational and users can access its resources without interference;
- usability – describes the extent to which a mobile system can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context without any kind of impediments;
- reliability – refers to the capacity of mobile systems to perform tasks, given a certain stressful setting without any unpredictable stops;
- efficiency – determines the relationship between the level of performance of a mobile system and the amount of resources used for generating results.

Usability is described as being an important link in the evolutionary chain of mobile systems because it represents the means through which users are consuming mobile devices resources, generating new requests and identifying new development possibilities which leads ultimately to the enlargement of mobile systems. Usability describes the user's intuitivism in using and accessing mobile resources without having a prior knowledge about how they can do that.

3 Security Issues in Mobile Systems

Mobile security covers a wide range of vulnerabilities or attack that target users' data, financial and credit card information or the control of different phone services. In [11] there are emphasized top vulnerabilities and attack methods of the two most used mobile platforms, Apple iOS and Google Android. Also, Microsoft's Windows Phone platform can be added here [12]. The main security issues for these platforms are briefly presented further.

Recover lost data in case of mobile theft or destruction is very important for security. All mentioned operating systems provide internal services designed to automatically backup user data, encrypt or wipe off user data remotely and to locate a specific device. The users have to be aware of these capabilities and to enable them. All these can be or are disabled by default, because of privacy issues,. These facilities require access to

network/ data services and/ or location access. All platforms include hardware support for data encryption.

Another important security issue is related to device protection by using passwords, PIN codes, biometric data, drawings or specific procedures. According to several studies, such as [13] and [14], about half of the users do not lock their devices using any of the above methods. Also, there were identified several situation that could lead to security vulnerabilities for the users:

- the passcode is shared with other peoples;
- the passcode is kept on a device or is written on paper;
- the passcode is reused;
- the same passcode is used for more devices or applications.

The *passcode* represent the most used device unlocking approach. In order to increase the usability of the authentication process, mobile devices have implemented lately procedures based on finger swiping actions [15]. These methods convince more users to use a password locking mechanism but the swipe-lock patterns are less secure than a PIN like password or other third-party mechanisms, [16], [17]. Also, face recognition and fingerprint authentication tend to be used more and more, they having a high impact on usability. The login/ sign in process usually influences the applications usability, so that users prefer to store the passwords or credentials in order to skip this step when the applications are launched again. This represents a vulnerability that has a higher impact on mobile devices than on desktop computers, especially because many user use only unsecured screen locks (without passcode or other security method).

Mobile applications request on installation user access permissions to different local services and data repositories. There are many market available applications that require more permissions than required. Without a proper security culture, common users accept without reading or understanding the security risk to which are exposed when granting those rights. For many users this very important security installation step has become a default accept action, like the classic terms and conditions acceptance. This could be an issue especially if the permission are not shown like a warning before the installation process and the user has to be aware of the fact that he or she has to look for these.

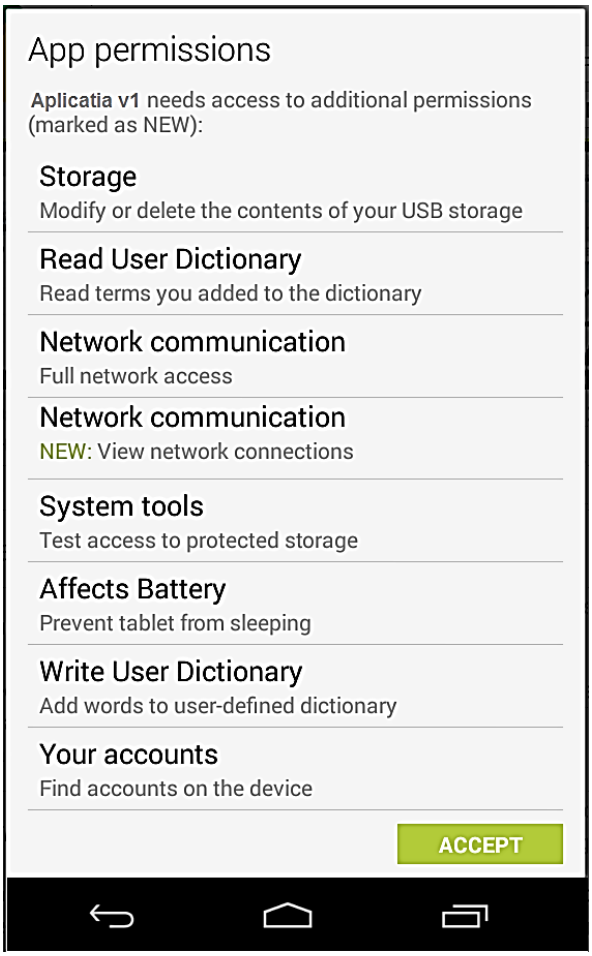

Fig. 3. Android permissions acceptance screen

Depending on the platform and operating system a mobile applications may require permissions or not for tasks like:

- read and write contacts;
- read and write calendar entries (appointments, tasks);
- read or monitor text or multimedia messages;
- send e-mail, text or multimedia messages;
- make phone calls;
- get user location (GPS, network, data mobile phone network);

- access the Internet;
- read and write on file system.

There are some differences on applications' installation process between Android and Windows Phone. On Android devices after the user chooses to install an application, the application permission window will pop up (Figure 3).

The user can choose to continue or not. The users has to analyze the required permissions and to correlate them with the application functionality.

On Windows Phone devices, the application's required permission are displayed on the installation page among other application information, and the user has to scroll down to see the required permissions (Figure 4). In this case the user has to know where to look for these permissions before installing the application.

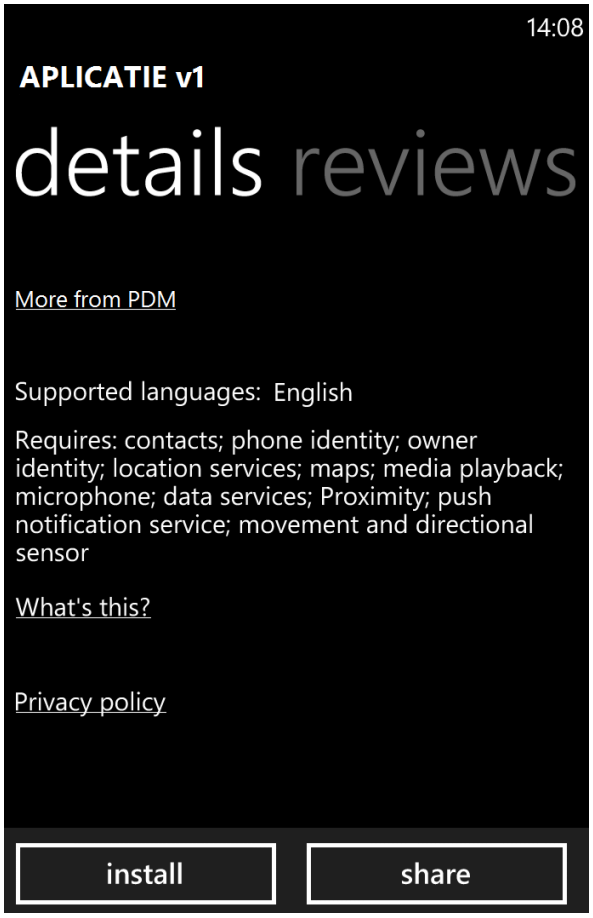

Fig. 4. Windows Phone installation screen with application's required permissions

If a Windows Phone application requires access to user's location, a dedicated window will ask the user to accept this or not.

By *SMShing*, the mobile phone phishing, the users are spamming with short text messages that are intended to trick them into accessing websites or to download malicious software. The messages seem to come from a trusted source and they ask users to:

- send personal information (credit or debit cards, PINs, passwords etc.)
- call a given phone number;
- send a text message to a given phone number;
- send a URL to a malicious Web site or application.

Mobile malware applications represent the most significant security threat in the last year. A security report released by Kaspersky [18] has showed that in 2013 the most common Android malwares are Backdoor Trojans, followed by Trojans and on the third place SMS-Trojans. Once installed the applications deliver routines that:

- initiate background calls or text messages to premium or royalty numbers;
- block the user's access to the phone;
- steal users' data (contacts, messages, pictures);
- record conversations;
- take pictures using mobile devices cameras;
- display ad messages and install ad-software.

Android is the most targeted platform by malware (over 75% of malware is directed to Android). This is related to market share that exceeds 75%, but also because the Android application could be delivered also by third party marketplaces, not only by Google Play. Also, the applications can be installed by using several sources (Web pages, internal or external storage etc.). Moreover, the applications publishing process is easier than for iOS or Windows Phone applications.

Users' role is very important to reduce the security threats. The users should use passcodes or other authentication methods, to backup and encrypt sensitive data. Also, they have to be aware about the risks they expose when installing application from unknown or unsafe sources, or when read the emails, text

or multimedia messages or when they navigate on Web.

4 Usability vs. Security Metrics

For describing usability a special metric has been proposed, *UM*, to reflect the degree in which a user tends to complete different tasks in a mobile system without the help or assistance of a third party, by using the following relation:

$$UM(\%) = \frac{1}{nop}\sum_{i=1}^{nop} q_i$$

where:

- *nop* – number of total working sessions recorded in the system;
- q_i – percentage of a current working session i completed by a user without any kind of assistance.
- The values for UM metric are found between 0 and 1 ($UM\epsilon[0;1]$). If all the working sessions on a mobile device are successfully completed without any kind of assistance, $q_i = 1, \forall i = \overline{1, nop}$, then the maximum value of metric UM is reached, that being *UM = 1*. Otherwise if no working sessions can be completed successfully and need all the hard time assistance who's possible in order to achieve a result then *UM = 0*.

The results of the *UM* metric are of type:

$$[UM] = \frac{[\sum_{i=1}^{nop} q_i]}{[nop]} = \frac{[q_i]}{[number\ of\ working\ sessions]}$$

How the number of working sessions and q_i are with no dimension, also UM has no dimension.

Another proposed metric is the impact of a security feature on usability. The metric is based on the required effort to complete a given task with and without the security feature enabled. As seen in practice, the effort required to do a task with a security feature enabled is higher than with that security feature disabled. For example, the user has to enter the username and password to access his or her account for a secured application. For this reason the credentials are store for the next sessions.

The impact of a security feature metrics (I_{SF}) is calculated as:

$$I_{SF} = \frac{E_1}{E_0}$$

where:

- E_1 – the effort required to do a specific task with the security feature, SF, enabled;
- E_0 – the effort required to do a specific task (the same) with the security feature, SF, disabled;

Usually, the effort is represented by the number of tasks or by duration.

The I_{SF} metric has values greater than zero with the following meanings:

- if the value is less than 1 or equal, the impact of the security feature is very weak;
- values greater than 1 show the degree of security feature negative influences the usability.

Security is one of the characteristics that tend to balance usability in the opposite direction. So a very fragile bound is developing between one and another, as one get to increase, the other one tends to lose its strength. If the number of security controls is higher than usability has a much smaller positive impact upon users.

In figure 5 is depicted the equilibrium achieved between the number of total limitations of a mobile systems in terms of security controls and the usability factor perceived by the user.

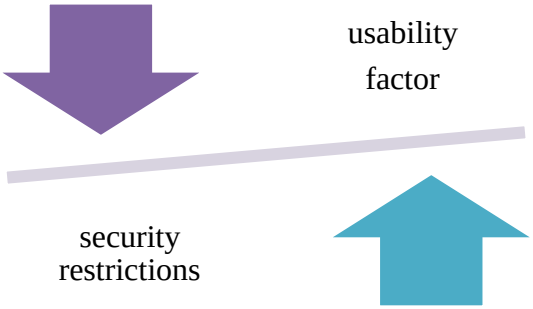

Fig. 5. Security vs. Usability

Besides the advantages brought by this characteristic, usability is impacted by several other mobile devices key aspects that not always are to let go, such as:

- impact of input limitations;
- impact of low resolution;
- impact of slow computer hardware;
- impact of download speed.

Security must be correctly approached in mobile systems in order to obtain a good degree of usability. Such approach is still limited by some characteristics of mobile devices that are not yet overpassed.

5. Conclusions

As referenced studies have shown, users prefer usability over strong security measures. In public environments, where users are choosing the solution based on their satisfaction, developers are forced to choose the usability factor and to provide less secure measures. The solution is to automatize or to implement background security processes that will require less effort from users.

The next steps for this research are:

- data gathering for the proposed metrics, in order to calculate them for a large number of mobile applications
- metrics validation, based on previous step with their application on new mobile software.

The process of data gathering requires a large amount of work that can be overpassed by developing and using tools to automate some tasks.

Acknowledgment

Parts of this research have been published in the Proceedings of the 12th International Conference on Informatics in Economy, IE 2013 [19].

References

[1] B. Schneier, Secrets and lies: digital security in a networked world, New York: Wiley, 2000.

[2] A. Adams and A. Sasse, "Users are not the enemy," *Communication of the ACM*, vol. 42, no. 12, pp. 41-46, 1999.

[3] Kaspersky, "Usability and security: the endless pursuit of perfection," Kaspersky, 2012.

[4] M. A. Sasse and I. Flechais, "Usable Security. Why do we need it ? How do we get it ?," in *Security and Usability: Designing secure systems that people can use*, Sebastopol, O'Reilly, 2005, pp. 13-30.

[5] A. Whitten and J. D. Tygar, "Usability of Security: A Case Study," Carnegie Mellon, 1998.

[6] B. Lampson, "Privacy and security. How to get it.," *Communications of the ACM*, vol. 52, no. 11, pp. 25-27, 2009.

[7] A. Whitten, "Making Security Usable," Carnegie Mellon University, 2004.

[8] L. F. Cranor and S. Garfinkel, "Secure or Usable?," *IEEE Security & Privacy*, no. September 2004, pp. 16-18, 2004.

[9] D. Norman, "When Security Gets in the Way," *Interactions, ACM*, vol. 16, no. 6, 2010.

[10] I. Ivan, C. Ciurea, B. Vintila and G. Nosca, "Particularities of Verification Processes for Distributed Informatics

Applications," *Informatica Economica*, vol. 17, no. 1, 2013.

[11] L. Phifer , "Top 10 Android Security Risks," eSecurity planet, 2011.

[12] Microsoft, "Windows Phone 8 Security Overview," September 2013. [Online]. Available: http://go.microsoft.com/fwlink/?LinkId=266838.

[13] M. Weber, "BYOD Survey 2013: Employees and Companies Remain Lax with BYOD Security," September 2013. [Online]. Available: http://www.coalfire.com/The-Coalfire-Blog/September-2013/BYOD-Survey-2013-Employees-and-Companies-Remain-La. [Accessed September 2013].

[14] McAfee, "McAfee Reveals Consumers Fail To Protect Their Mobile Devices," February 2013. [Online]. Available: http://www.mcafee.com/us/about/news/2013/q1/20130224-01.aspx. [Accessed September 2013].

[15] C. Braz and J. M. Robert, "Security and Usability: The Case of the User Authentication Methods".

[16] U. Jendricke and D. Gerd tom Markotten, "Usability meets Security – The Identity-Manager as your Personal Security Assistant for the Internet," in *ACSAC '00. 16th Annual Conference*, 2000.

[17] I. M. a. D. S. M. Bogicevic, "Identity Management - A survey," in *Proceedegins of the XIII International Symposium SymOrg 2012: Innovative Management & Business Performance*, Zlatibor, 2012.

[18] Kaspersky Lab, "Kaspersky Lab IT Threat Evolution: Q2 2013," 15 August 2013. [Online]. Available: http://www.kaspersky.com/about/news/virus/2013/Kaspersky_Lab_IT_Threat_Evolution_Q2_2013. [Accessed September 2013].

[19] C. Boja and M. Doinea, "Usability vs. Security in mobile applications," *Proc. of the IE 2013 International Conference*, pp. 138-142, 2013.

Catalin BOJA is associate professor at the Economic Informatics and Cybernetics Department at the Academy of Economic Studies in Bucharest, Romania. In June 2004 he has graduated the Faculty of Cybernetics, Statistics and Economic Informatics at the Academy of Economic Studies in Bucharest. He is a team member in various undergoing university research projects where he applied most of his project management knowledge. His work currently focuses on the analysis of mobile computing, information security and cryptography. He is currently holding a PhD degree on software optimization and on improvement of software applications performance.

Mihai DOINEA is a PhD, assistant professor, within Bucharest University of Economic Studies. His PhD thesis approaches the field of Informatics Security with clear objectives in finding security optimization methods for distributed applications. His research is also backed up by a master diploma in Informatics Security (2006). He is assistant professor, teaching Data Structures, Advanced Programming Languages, and Mobile Application Programming. He published more than 30 articles in collaboration or as

single author and his research interests are directed to areas such as security, distributed applications, artificial intelligence and optimization algorithms.

Paul POCATILU graduated the Faculty of Cybernetics, Statistics and Economic Informatics in 1998. He achieved the PhD in Economics in 2003 with thesis on Software Testing Cost Assessment Models. He has published as author and co-author over 45 articles in journals and over 40 articles on national and international conferences. He is author and co-author of 10 books, (Mobile Devices Programming and Software Testing Costs are two of them). He is professor at the Department of Economic Informatics and Cybernetics within the Bucharest University of Economic Studies, Bucharest. His current research areas are software testing, software quality, project management, and mobile application development.