MOBILE BANKING SECURITY PRACTICES FOR ANDROID USERS

Bonimir Penchev

Abstract: *The widespread usage of mobile phones and smartphones in particular is related with the continuous expansion of their functionalities. Mobile banking is an option which gives users the possibility to perform various banking operations (such as account balance inquiry, account transactions, payments and other basic services available daily in banks) through a mobile device such as mobile phone, smartphone or tablet. A key factor for its wider usage is to increase the level of security, which in turn will increase user's confidence. In this paper, we investigate which of the security features for a safer mobile banking are included in 14 mobile antivirus and security applications for Android OS. In the final assessment are included three additional factors – license, usability and battery usage. On the other hand, based on the main channels for mobile banking (SMS, mobile websites and mobile applications) and the fact that the web browser can be a major source of malware applications, spoofing websites and targeted Trojans, we present how the existence of certain security indicators in mobile web browsers and their recognition would help the user to avoid security attacks. According to the results of our study, we can evaluate and select the combination mobile antivirus and security application - mobile web browser in order to increase user's confidence in mobile banking.*

Keywords: *Mobile security, Mobile banking, Mobile Antivirus and Security Applications, Mobile Web Browser.*

ACM Classification Keywords: *K.4.4 Electronic Commerce – Security*

Introduction

Mobile phones are an integral part of our daily lives. Their usage is not limited to operations like phone calls or text messaging. Technology progressed to such an extent that smartphones' functionalities can be compared to those of contemporary computers. In Smartphone's financial institutions explore an excellent opportunity to provide new type of services. Mobile banking is this type of service that allows the user to carry out various banking operations (such as account balance inquiry, account transactions, payments and other basic services available daily in banks) through a mobile device such as a mobile phone, smartphone or tablet.

Among the benefits that users can derive from mobile banking, there are also different restrictions. The most important of them is related to the security level of this service and it is one of the main user's concerns when deciding whether or not to use mobile banking. In this aspect it is necessary to examine the main critical points in the mobile banking process – bank system, transmission media, mobile device, and user. In our study we will focus on the mobile device.

According to a research conducted by Gartner [Gartner Inc., 2014] for 2013 the market share of smartphones reached 53.6% of overall sales of mobile phones. The same study states that there is an increase of 42.3% compared to 2012. Both these facts lead us to the conclusion that the proportion of the users currently using smartphones is constantly increasing. This is a good enough reason for us to focus our research on this type of mobile devices.

The main smartphone's security threats associated with mobile banking can be the following: banking malware, targeted Trojans, mobile spyware, mobile phishing, smishing, device lost and theft.

Unfortunately, Android OS keeps its leading position as well in terms of its usage – 66.4% [Gartner Inc., 2014], as in the number of developed malware applications – 97% of total mobile malware. [McAfee Company, 2013] These two facts are focusing us on researching mobile antivirus and security applications developed for Android platform.

There are different solutions for dealing with the security problems of smartphones in terms of mobile banking [AV-Comparatives Organization, 2014]:

- Anti-malware – on demand scan, automatic update, real time file protection, anti-phishing protection, USSD blocking, SMS/MMS scanner and filter, network protection, quarantine;
- Anti-theft – remote localization(GPS/network), remote wipe, remote lock, SMS or web interface for controlling anti-theft components, lock phone on SIM change, report thief's phone number, remote configuration, lock contacts and SMS/MMS, report thief's location on SIM changed, lock images and files;
- Authentication - lock screen with password protection, password policy (strength, length), maximum failure password attempts before wipe, inactivity timeout;
- Additional – data encryption, password protection for settings, no SIM activation, data network usage monitor, local wipe.

All these security features can be combined in a single application (antivirus and security application), which cares for smartphone's security.

On the other hand, based on the main channels for mobile banking (SMS, mobile websites and mobile applications) and the fact that the web browser can be a major source of malware applications,

spoofing websites (based on phishing) and targeted Trojans, we turn our attention to another aspect of security enhancement – mobile web browsers.

The goal of our work is to determine which of the existing mobile antivirus and security applications and mobile web browsers would help the users to increase the mobile banking security level in Android OS.

The main tasks we set are:

- To be made a comparative analysis of some of the existing mobile antivirus and security applications for Android smartphones;
- To be checked how the absence of mobile web browsers security indicators for Android smartphones is related to certain security attacks;
- To be determined which combination mobile antivirus and security application – mobile web browser hides the least risk for mobile banking security in the case of Android OS.

Mobile antivirus and security applications

The existing mobile antivirus and security applications, which can be used to enhance mobile banking security of Android smartphones, include a wide range of security features. Using the information from AV-Comparatives research [AV-Comparatives Organization, 2014], we have identified which security features are available as functionality in 14 mobile antivirus and security applications. The security features are those mentioned earlier in the introduction. For each existing feature the antivirus and security application earns 1 point. The features are grouped in four main categories. The maximum points that can be earned in each category are as follows: anti-malware (8 points), anti-theft (9 points), authentication (4 points) and additional (5 points). The results are presented in Table 1.

Table 1 clearly shows the leading mobile antivirus and security applications according to the existing security features: Avast! Mobile Security 3.0.7650, Tencent Mobile Manager 4.8.2 and Kaspersky Mobile Security 11.4.4.232.

Surely the presence of certain security features in mobile antivirus and security applications is not a guarantee for their optimum performance and risk reduction. To be more precise about the effectiveness of these applications is necessary to be conducted number of tests checking actual security features' operation. But this is not the subject of this report and could be only an outline for future work.

Table 1. Assessment on the presence of security features in mobile antivirus and security applications

Mobile Security Features Antivirus and Security Applications	Anti-malware (max 8 p.)	Anti-theft (max 9 p.)	Authentication (max 4 p.)	Additional (max 5 p.)	Total
AhnLab V3 Mobile 2.1.2.13	2.5	5.5	1	1	14.5
Avast! Mobile Security 3.0.7650	7	9	3	4	23
Bitdefender Mobile Security Premium 2.19.344	4	6	3	2	15
ESET Mobile Security 3.0.937.0-15	5.5	4.5	3	2	15
F-Secure Mobile Security 9.2.15183	3.5	6	4	2	15.5
Ikarus mobile.security 1.7.20	6	4.5	4	1	15.5
Kaspersky Mobile Security 11.4.4.232	8	6	3	4	21
Lookout Premium 8.17-8a39d3f	4.5	3.5	3	3	14
Qihoo 360 Antivirus 1.0.0	4.5	6	2	2	14.5
Quick Heal Total Security 2.00.021	5.5	6	1	4	16.5
Sophos Security and Antivirus 3.0.1154(7)	7	5.5	1	2	15.5
Tencent Mobile Manager 4.8.2	7	8	3	4	22
Trend Micro Mobile Security 5.0	3.5	3	3	2	11.5
Webroot SecureAnywhere Mobile Complete 3.6.0.6610	5.5	4.5	3	0	13

Another important problem in security implementation and in antivirus and security application's usage is the user requirement to receive reliable security without hardening in any way the operation of the smartphone. This defines three more factors that must be considered when choosing a mobile antivirus and security application:

- License – free or commercial;
- Usability – easiness and intuitive usage, since users tend to avoid the installation of such applications due to their complexity;
- Battery usage – the effect of constantly working mobile antivirus and security application on the battery life.

Table 2 presents the final assessment of mobile antivirus and security applications, based on three factors – security features, usability and battery usage. The maximum points that can be earned for each factor are as follows: security features (6 points), usability (6 points) and battery usage (6 points). The factor "license" is for information purpose. It is not graded and does not affect the final assessment. The data in column "Security features" is extracted from Table 1 and the values are converted on six point basis. The data in columns "Usability" and "Battery usage" are derived respectively from report of AV-TEST research [AV-TEST Institute, 2014] and report of AV-Comparatives research [AV-Comparatives Organization, 2014].

The results in Table 2 show that the overall score of the assessed mobile antivirus and security applications is moving in close range, i.e. any of them can be chosen and the level of security will be also in close range. Among the commercial applications Kaspersky Mobile Security 11.4.4.232 is going to be a wise choice. And with regard to free license applications Tencent Mobile Manager 4.8.2 and Avast! Mobile Security 3.0.7650 are at the forefront.

Table 2. Final assessment of mobile antivirus and security applications

Factors Determining User's Choice and Security Applications / Mobile Antivirus	License	Security features (max 6 p.)	Usability (max 6 p.)	Battery usage (max 6 p.)	Total
AhnLab V3 Mobile 2.1.2.13	Free	3.3	6.0	6.0	15.3
Avast! Mobile Security 3.0.7650	Free/ Commercial	5.3	6.0	6.0	17.3
Bitdefender Mobile Security Premium 2.19.344	Commercial	3.5	6.0	6.0	15.5
ESET Mobile Security 3.0.937.0-15	Free/ Commercial	3.5	6.0	6.0	15.5
F-Secure Mobile Security 9.2.15183	Commercial	3.6	6.0	6.0	15.6
Ikarus mobile.security 1.7.20	Commercial	3.6	5.0	6.0	14.6
Kaspersky Mobile Security 11.4.4.232	Commercial	4.9	6.0	6.0	16.9
Lookout Premium 8.17-8a39d3f	Free/ Commercial	3.2	6.0	6.0	15.2
Qihoo 360 Antivirus 1.0.0	Free	3.3	6.0	6.0	15.3
Quick Heal Total Security 2.00.021	Commercial	3.8	5.5	6.0	15.3
Sophos Security and Antivirus 3.0.1154(7)	Free	3.6	6.0	6.0	15.6
Tencent Mobile Manager 4.8.2	Free	5.1	6.0	6.0	17.1
Trend Micro Mobile Security 5.0	Commercial	2.7	6.0	6.0	14.7
Webroot SecureAnywhere Mobile Complete 3.6.0.6610	Commercial	3.0	6.0	6.0	15

Mobile Web Browsers

Our main guideline for mobile web browser security will be directed to check if it is in compliance with The World Wide Web Consortium (W3C) user interface requirements and security indicators in particular [W3C, 2010]. If these requirements are not met and if some of the security indicators are missing, users can more easily be misled about the identity of the website or the security of the connection. This in turn is directly related to the mobile banking security, which may be compromised and exposed to attacks such as: phishing, malicious web sites, espionage, eavesdropping. The presence of the security indicators on a given web browser would not completely eliminate the risk, but users aware with the security indicators would make informed decisions about the websites that they visit.

User interface security indicators in web browsers are divided in two categories [Amrutkar, Traynor and Oorschot, 2011]:

- Primary user interface indicators – padlock icon, address bar, https URL prefix, favicon, site-identity button or URL coloring (signifying the presence of EV-SSL and SSL certificates);
- Secondary user interface indicators – security properties dialog, domain name, owner information, verifier information, information on why a certificate is trusted, validity period of manually accepted certificates (self-signed) and cipher details of an SSL connection.

Table 3 presents the results of a previously conducted research [Amrutkar, Traynor and Oorschot, 2012], which identifies how the absence of certain security indicators in particular mobile web browsers (for our study we have chosen only Android web browsers - Android 2.3.3, Chrome Beta 0.16.4130.199, Firefox Mobile 4 Beta 3, Opera Mini 6.0.24556, Opera Mobile 11.00) may lead to potential attacks such as phishing without SSL, phishing with SSL, phishing using a compromised CA (Certificate Authority) and industrial espionage/eavesdropping. Sign “+” implies that the corresponding attack is possible on the browser, while sign “-” implies that it is not possible.

Table 3. Potential attacks to mobile web browsers

Mobile Attacks / Browsers	Phishing without SSL	Phishing with SSL	Phishing using a compromised CA	Industrial espionage/ Eavesdropping
Android 2.3.3	+	-	-	+
Chrome Beta 0.16.4130.199	-	-	-	+
Firefox Mobile 4 Beta 3	-	-	-	+
Opera Mini 6.0.24556	-	+	+	+
Opera Mobile 11.00	-	+	+	+

Phishing without SSL. If users accidentally enter a malicious website and have difficulties in viewing the entire website's URL due to the constrained screen size of the smartphone, they can be deceived by a domain name slightly different from the original one. Such website containing spoofed padlock icon and closely imitating legitimate website's content can easily provide an illusion of strong encryption. But if such website is rendered in a browser that offers identity information such as owner's name, it will be easier for the user to identify the phishing attack.

Phishing with SSL. If the attacker have decide not just to spoof padlock icon, but to buy a legitimate inexpensive SSL certificate for the website, the browser is going to display SSL security indicators such as https URL prefix and URL coloring site identity button in addition to the padlock icon providing illusion of security. In this case if the browser does not offer identity information the phishing attack will be successful.

Phishing using a compromised CA. When the attacker compromises CA, rogue certificates for legitimate website can be obtained. And if the CA is trusted by the browser, all certificates will be accepted and no warnings will be shown to the user. But if the browser offers user interface to enable certificate viewing, the user would not be so easily misled.

Industrial espionage/Eavesdropping. Such attacks can be achieved in browsers that do not show constantly https URL prefix, do not offer cipher details of an SSL connection, or are showing SSL

indicators for websites with mixed content (for example the attacker can change website's code with a code injection).

Based on the data, presented in Table 3, we can make a conclusion that the users should be directed to the usage of either Chrome Beta 0.16.4130.199 or Firefox Mobile 4 Beta 3. Although they do not provide the maximum level of security, their usage is more appropriate than that of the other tested browsers.

Conclusion

The widespread usage of mobile phones and smartphones in particular leads to diversification of their functionalities. Mobile banking is a kind of additional feature, which provides many facilities to the users. One of the problems of its wider uptake is the question about security. In this study we attempt to facilitate users by representing them a comparison by certain criteria and offering them choices of mobile antivirus and security application and suitable mobile web browser. The focus was on Android OS, as it is first in the list of used mobile operating systems. According to the results, we can conclude that a very good option for consumers would be the usage of free Tencent Mobile Manager 4.8.2 or Avast! Mobile Security 3.0.7650 or commercial Kaspersky Mobile Security 11.4.4.232 in combination with mobile web browser Chrome Beta 0.16.4130.199 or Firefox Mobile 4 Beta 3. For sure it would not completely eliminate the risk to mobile banking security, but at least it would be a step in its enhancement and along with that would increase user's confidence in this type of service.

Bibliography

[Amrutkar, Traynor and Oorschot, 2011] C. Amrutkar, P. Traynor and P.C. Oorschot. An Empirical Evaluation of Security Indicators in Mobile Web Browsers, Georgia Institute of Technology, 2011

[Amrutkar, Traynor and Oorschot, 2012] C. Amrutkar, P. Traynor and P.C. Oorschot. Measuring SSL Indicators on Mobile Browsers: Extended Life, or End of the Road?, Information Security, 15th International Conference, ISC 2012, Passau, Germany, September 19-21, 2012. Proceedings, Springer Berlin Heidelberg, Berlin, ISBN: 978-3-642-33382-8

[AV-Comparatives Organization, 2014] AV-Comparatives Organization Web Site. Mobile Security Review, www.av-comparatives.org/wp-content/uploads/2014/09/avc_mob_201407_en.pdf, (Accessed 12 December 2014)

[AV-TEST Institute, 2012] AV-TEST Institute Web Site. Mobile Security Apps, www.av-test.org/fileadmin/pdf/publications/droidcon_2012_avtest_presentation_mobile_security_apps.pdf, (Accessed 12 December 2014)

[AV-TEST Institute, 2013] AV-TEST Institute Web Site. AV-TEST Examines 22 Antivirus Apps for Android Smartphones and Tablets, www.av-test.org/fileadmin/pdf/avtest_2013-01_android_testreport_english.pdf, (Accessed 12 December 2014)

[AV-TEST Institute, 2014] AV-TEST Institute Web Site. 32 Protection Apps for Android Put to the Test, www.av-test.org/en/news/news-single-view/32-protection-apps-for-android-put-to-the-test/?=, (Accessed 12 December 2014)

[Gartner Inc., 2014] Gartner Inc. Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013, www.gartner.com/newsroom/id/2665715, (Accessed 12 December 2014)

[McAfee Company, 2013] McAfee Company Web Site. Mobile Malware Growth Continuing in 2013, www.mcafee.com/us/security-awareness/articles/mobile-malware-growth-continuing-2013.aspx, (Accessed 12 December 2014)

[W3C, 2010] W3C Web site. Web Security Context: User Interface Guidelines, www.w3.org/TR/2010/WD-wsc-ui-20100309/, (Accessed 12 December 2014)

Authors' Information

Bonimir Penchev *– University of Economics – Varna, Assist. Prof., Varna, Bulgaria, Institute of Mathematics and Informatics - Bulgarian Academy of Sciences, PhD Student, Sofia, Bulgaria;*
e-mail: bonimir@gmail.com

Major Fields of Scientific Research: Information Systems Security, Mobile Banking