Annals of DAAAM for 2012 & Proceedings of the 23rd International DAAAM Symposium, Volume 23, No.1, ISSN 2304-1382
ISBN 978-3-901509-91-9, CDROM version, Ed. B. Katalinic, Published by DAAAM International, Vienna, Austria, EU, 2012
Make Harmony between Technology and Nature, and Your Mind will Fly Free as a Bird
Annals & Proceedings of DAAAM International 2012

RESEARCH OF SECURITY THREATS IN THE USE OF MODERN TERMINAL DEVICES

PERAKOVIC, D[ragan]; HUSNJAK, S[inisa] & REMENAR, V[ladimir]

Abstract: *Modern mobile terminal devices are multi-functional terminal devices with options such as: Internet access, using of applications, e-mail communication, messaging, data storage and using of multimedia files. The value of such data is often invaluable and vulnerability is often very high. Given the high use of smartphones and a variety of operating systems that they use (iOS, Android, Windows Phone ...), the logical is the fact that these devices are frequent targets of malicious attacks. Research of this paper will focus on defining forms of security threats and possible attacks on smartphones and a brief description of possibilities for protecting smartphones. There will be displayed features of operating systems and specified the security aspects and specifics which carry some of the modern operating systems of mobile terminal devices.*
Keywords: *Modern terminal device, security, threats, mobile operating systems*

1. INTRODUCTION

Modern mobile terminal devices because of their nature (variety of operating systems, confidential data, location data, multimedia files, etc.) represent a good target for potential attackers, who, because of financial, personal, political and other reasons, make attacks on these devices. Considering the increasing prevalence and use of modern mobile terminal devices (smartphones) at the global level, inevitable is the fact that there is a number of security threats that impact on those devices. Exploration of the possibilities of security attacks on smartphones influences global awareness of users about the problem, reducing the potential problems and improve the quality of life. User's awareness of current smartphone vulnerabilities, threats and dangers that exists is not in a sufficiently high level, so it is necessary to describe the possible threats and dangers to which users of smartphone devices can find. In this paper can be seen the segmentation and classification of sources of security threats of the modern terminal devices, a description of specific sources of threats and overview of currently dominating operating systems of mobile terminal devices.

2. FUNCTIONALITY AND USAGE OF MODERN TERMINAL DEVICES

Although there is no exact definition of what a smart terminal device (smartphone) is, it can be said that smartphone is a device that extends the capabilities of conventional mobile terminal device.

Key features of the smart terminal device are [10]:

a. operating system (OS)
b. applications
c. full QWERTY keyboard
d. permanent access to the Internet
e. ability to exchange messages

The functionality of mobile terminal devices depends not only on the hardware. Discussion about the features and capabilities of smartphones more and more takes the direction which operating system will run mobile device and which operating systems are available on the market. Mobile Operating System (MOS) represents system that manages the mobile terminal device [15].

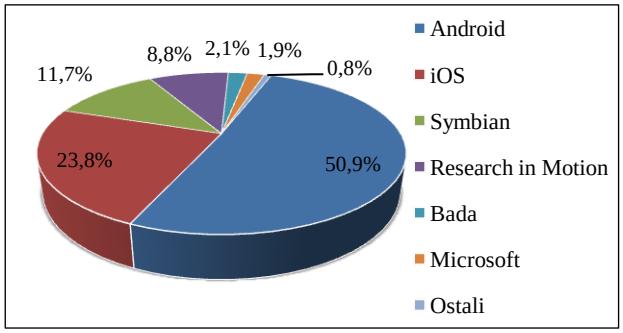

Fig. 1. Statistics of the use of operating systems of smart terminal devices [7]

In the third quarter of 2011, the 26% of all sold mobile devices were smart terminal devices. More interesting is the fact that this share is growing: in 2010 the part of sold smartphones was 19%, which is an increase of 72% compared to year 2009 [3].

Predictions indicate an almost linear increase in the use of smart terminal devices by the year 2015. According to their data, the average increase in the number of smart terminal devices is approximately 160 000 devices per year [11].

3. IDENTIFICATION OF SECURITY THREATS OF MODERN TERMINAL DEVICES

The impact of a threat can be determined by the assets of property that is affected by the threat.

List of possible affected assets:

a. Personal data
b. Corporate intellectual property
c. Classified information
d. Financial assets
e. Device and service availability and functionality

f. Personal and political reputation

Threats of modern terminal devices can be classified into the following categories: physically-based threats, application-based threats, network-based threats and web-based threats. In addition, there are also threats made of social engineering and BYOD (Bring Your Own Device), explained in detail below.

3.1 Device loss/theft

Given the size of the smartphone and the fact that their owners always carry them with themself, the chances of their loss are big. Loss/theft of smartphones means a lot more risks, not just financial.

A lost or stolen device, especially those without security settings like passwords, can present a significant risk to enterprises and consumers, including: [2]

a. Data breach
b. Loss of intellectual property and trade secrets
c. Loss of personal information

3.2 Attacks on smartphone devices intended for recycling

Due to a growing awareness of identity theft many people and organizations now destroy or wipe computer hard drives before decommissioning. However, the same thing is not yet happening with smartphones. At the same time, more and more devices are being recycled.

The number of recycled handsets is expected to exceed 100 million units in 2012. Shorter handset replacement periods, growing demand for low-cost handsets in emerging markets, regulatory requirements, and growing consumer awareness are key factors driving the market for recycled handsets [14].

3.3 Malware Attacks

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. It can include viruses, worms, spyware, adware and trojans.

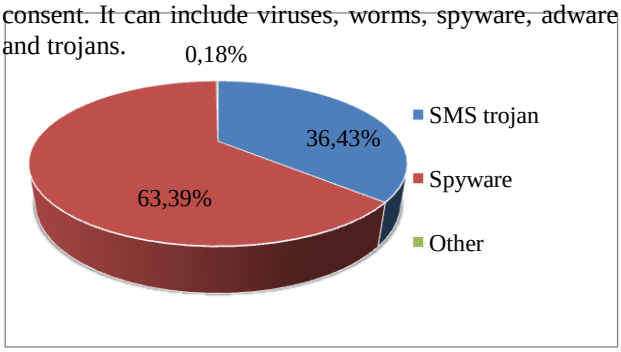

Fig. 2. Types and percentages of malware attacks on smartphones [2]

The vast majority of malware infecting smartphones and tablets can be classified into two categories: spyware and SMS Trojans (Fig. 2.). Profit is the major motive for both types of attacks.

3.3 Inadvertent disclosure of information

Users are not always aware of all the functionality of smartphone apps. Even if they have given explicit consent, users may be unaware that an app collects and publishes personal data. Location data, for example, is often used in social networks – in messages or uploaded photo metadata, in augmented reality apps, micro-blogging posts, etc. Most apps have privacy settings for controlling how and when location data is transmitted, but many users are unaware (or do not recall) that the data is being transmitted, let alone know of the existence of the privacy setting to prevent this [1].

3.4 Surveillance attacks

Smartphones can be used to keep a targeted individual under surveillance. Smartphones contain sensors such as camera, accelerometer, microphone and GPS. This, combined with the possibility of installing thirdparty software and the fact that a smartphone is closely associated with an individual, makes it a useful spying tool.

3.5 Phishing attacks

Phishing attacks represent a phenomenon in which an attacker collects user credentials (such as passwords and credit card numbers) by means of fake apps or (SMS, email) messages that seem genuine.

Phishing represents an illegitimate way of extracting confidential information from smartphone devices, like a bank account number, online transaction password and your social networking account passwords etc. In phishing process, smartphone users are lured in such a way that they end up giving information on their own. Applications intended for phishing attacks are designed specifically for smartphones, and they try to get access to restricted information on the device [9].

3.6 Web browser exploits

Applications that use web browser exploits are designed to take advantage of vulnerabilities in a web browser or software that can be launched via a web browser such as a Adobe Flash player. Simply by visiting a web page, an unsuspecting user can trigger a browser exploit that can install malware or perform other actions on a device [16].

3.7 Automatically download the application

The threat, which is manifested through automatically begin downloading an application when a user visits a web page. In some cases, the user must take action to open the downloaded application, while in other cases the application can start automatically.

3.8 Network spoofing attacks

Network spoofing attacks happened when an attacker pretends to be someone else in order gain access to restricted resources or steal information [8].

An attacker deploys a rogue network access point (WiFi or GSM) and users connect to it. The attacker subsequently intercepts (or tampers with) the user communication to carry out further attacks such as phishing [1].

3.9 Network exploits

Network exploits uses advantage of software flaws in the mobile operating system or other software that operates on local (e.g., Bluetooth, Wi-Fi) or cellular (e.g.,

SMS, MMS) networks. Network exploits often do not require any user intervention, making them especially dangerous when they are used to automatically propagate malware.

3.10 Social Engineering

These types of attacks on smartphones include the techniques of modern terminal device users install malicious applications on your device or allow the visibility of their information without being aware of it.

Attacks using social engineering include [16]:

a. Apps repackaging - a malware writer takes a legitimate application, modifies it to include malicious code, then sets as available for download.
b. Attacks using a newer version of a software - creator of the malicious software sets a newer version of a software application that is infected with malware.

3.11 BYOD (Bring Your Own Device)

BYOD is a phrase that has become widely adopted to refer to employees who bring their own computing devices - such as smartphones, laptops and PDAs – to the workplace for use and connectivity on the corporate network [17].

BYOD is one of the newer causes of data vulnerability. Employees are accessing sensitive corporate information from their home computers, smartphones and tablets [4].

Consumer technology is generally not as secure and manageable as required by the enterprise.

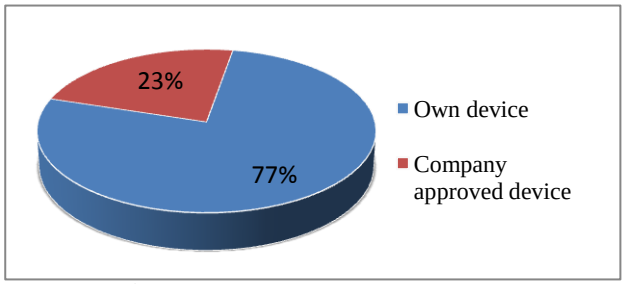

Fig. 3. Types of devices and their usage in the companies [19]

4. SECURITY ASPECTS AND SPECIFITIES OF OPERATING SYSTEMS

Today's operating systems of mobile terminal devices are different in large-scale in terms of security and management capabilities [6].

Atribute	BB 7.0	iOS 5	WP 7.5	Android 2.3
Built-in security	3.13	3.75	3.50	2.50
Application security	2.44	2.06	1.88	1.44
Authentication	3.90	2.00	3.20	2.00
Device wipe	4.00	1.25	2.25	0.63
Device firewall	4.50	0.00	0.00	0.00
Data protection	3.80	1.50	2.40	2.00
Device protection	3.50	0.63	2.38	2.00
Corporate managed e-mail	3.42	3.00	0.00	0.00
Mobile device management	3.50	2.50	1.25	2.00
Security certification	2.50	0.83	0.00	0.67
OS average score	2.89	1.70	1.61	1.37

Tab.1. Evaluation of security features of operating systems of mobile terminal devices [13]

According to the Tab.1. BlackBerry OS has the best security features of all most popular operating systems. As it can be seen, average score of BlackBerry OS is very high, but Android average score is very low. Every operating system needs to invest more in improving the security aspects of their operating system, and particularly this refers to Android OS and Windows Phone OS.

4.1 BlackBerry OS

BlackBerry devices, along with their back-end management through the BlackBerry Enterprise Server (BES) have been viewed by many as the bellwether for device security, with many endorsements and approvals of past versions of the OS. The strength in BlackBerry lies in the granular control - via IT policies - that are present on the BES itself.

BlackBerry Enterprise Server (BES) provides industry-leading security on both stored data and wireless transmitted data. BES uses encryption for wireless transmitted data. Every smartphone user has a secret key stored in a secure account of his company and in his device [12].

BlackBerry devices support the Federal Information Processing Standard (FIPS) 140-2 certification, making the software suitable for secure U.S. government use, as well as for use by additional organizations that demand proven, high-level data security [21].

4.2 iOS

iOS smart device security advantages are [20]:

a. Backup integrated
b. Memory encription
c. Remote wipe integrated
d. Applications are reviewed based on strict guidelines

Apple Inc. has very strict guidelines for the approval process of the applications that third parties develop. Security in iOS also extends to the physical attributes of the iPhone and iPad: there are no options for adding removable storage, which in effect provides another layer of protection for users. Security within the iOS construct takes on other levels, specifically where no application can be installed or updated without the express consent of the user. As for remote administration of mobile terminal devices, the IT department can configure certain things, but only once the user has provided certain permissions to the IT administrator [13].

Apple designed their operating system to provide security without the need 3rd party security products like antivirus or encryption software [18].

4.3 Android OS

Android not only leads in market share for the number of mobile devices; unfortunately, according to the data from the second quarter of 2011, it also leads in the amount of new malware [5].

Android OS represents an operating system where applications can't access the network without prior consent. Apps run in their individual sandboxed environment, and permissions are granted by the user on a per-app basis. Unfortunately, the end user often fails to closely inspect the permissions request dialogue in their

haste to use the app and, for the average end user, it is unclear when permissions are given and what the application is actually capable of. Once the application is installed, the OS doesn't recheck with the user and goes on to use the permissions without prompting the user again. This model has the net effect of putting each user in charge of their own security, rather than the operating system. Android is currently the preferred platform by cybercriminals. Attackers are using Android app stores as distribution mechanisms [13].

4.4 Windows Phone OS

Windows Phone OS uses a security model similar to the Android platform, in that minimum privileges and isolation techniques are used to sandbox processes or, in Windows Phone terminology, to provide chambers that act as individual process spaces.

Each chamber is defined and implemented using a policy system. The security policy of a specific chamber defines what operating system (OS) capabilities the processes in that chamber can access [22].

Windows Phone does not support the use of removable data storage media, and the SD slot in the device is only for use by the original equipment manufacturer. Developers need to register before any application can be distributed on the web in-store (Marketplace Hub). Prior to registration of any developer performs is the verification of his identity.

5. CONCLUSION

It is possible to classify several categories of sources of potential security threats of modern terminal devices. They differ primarily on the type of threat, the size of the risk of such threats and possible damage to such emerging security threats. However, it is almost impossible to generalize about the amount of damages as a result of some security threat, given that each user/company has its own priorities and values contained in its modern terminal device.

Sources of security threats are also not permanent and they complementary depend on the imagination of the attacker and using of some new technology or method. Specificity of the operating system, security standards and quality of investment in the security aspects of a particular operating system of modern mobile terminal devices is an important issue when it comes to security of those devices.

Diversity and opportunities that are needed to improve a particular operating system are the description of the advantages and disadvantages of those operating systems with the scalability and the possibility of changing them. The fact is that some operating systems meet higher safety standards than others, but given the almost daily updates of operating systems and awareness of the security risks, large investments are made in the security of each OS.

6. REFERENCES

[1] European Network and Information Security Agency: *Smartphones: Information security risks, opportunities, and recommendations for users*, Greece, 2010

[2] Juniper Networks, Inc.: *2011 Mobile Threats Report*, United States, 2011

[3] Centar Informacijske Sigurnosti: *Programi za zaštitu pametnih telefona*, Zagreb, Croatia, 2011

[4] Sophos Ltd.: *Security Threat Report 2012*, United States, 2012

[5] McAfee Inc.: *Securing Mobile Devices: Present and Future*, Report, United States, 2011

[6] Becher M.: *Security of smartphones at the Dawn of their Ubiquitousness*, Doctoral dissertation, Universitët Mannheim, Mannheim, Germany, 2009

[7] http://www.gartner.com/it/page.jsp?id=1924314, (2012) Gartner, Inc., Press Releases, *Accessed on: 2012-07-02*

[8] http://www.computer-network-security-training.com/what-is-a-spoofing-attack/, (2012) 365 Computer Security Training, *Accessed on: 2012-06-11*

[9] http://www.themobileindian.com/news/1611_Phishing-gets-smarter-for-smartphones, (2012) The mobile indian, *Accessed on: 2012-06-21*

[10] http://cellphones.about.com/od/smartphonebasics/a/what_is_smart.htm, (2012) About.com, *Accessed on: 2012-06-15*

[11] http://www.gartner.com/it/page.jsp?id=1622614, (2012) Gartner, Inc., Press Releases, *Accessed on: 2012-08-02*

[12] http://www.cse.wustl.edu/~jain/cse571-11/ftp/mobiles/index.html, (2012) Fei Yu, Survey paper, *Accessed on: 2012-07-05*

[13] Trend Micro Incorporated: *Enterprise Readiness of Consumer Mobile Platforms*, United States, 2012

[14] http://www.abiresearch.com/press/1015-recycled+Handset+Shipments+to+Exceed+100+Million+Units+in+2012, (2012) ABI research, Press Release, *Accessed on: 2012-07-14*

[15] Husnjak, S.: *Razvoj aplikacije za mobilne uređaje u funkciji podsjetnika temeljenog na lokaciji korisnika*, University of Zagreb, Faculty of transport and traffic sciences, Zagreb, Croatia, 2010

[16] Lookout Inc.: *Lookout Mobile Threat Report*, California, United States, 2011

[17] http://www.webopedia.com/TERM/B/BYOD.html, (2012) Webopedia, *Accessed on: 2012-07-22*

[18] Karow, O.: *Apple iOS Security in the Enterprise*, White Paper, Symantec GmbH, Germany, 2012

[19] Veracode, Inc.: *10 Simple Things You Can Do to Protect Yourself and Your Organization from Today's Mobile Computing Threats*, Burlington, United Kingdom, 2012-07-09

[20] Computer Incident Respnse Center Luxembourg, *Security of iOS based devices*, Luxembourg, 2012

[21] http://advice.cio.com/al_sacco/14621/rims_blackberry_6_os_gets_fips_140_2_u_s_govt_security_certification, (2012) CIO article, *Accessed on: 2012-06-26*

[22] Microsoft Corporation: *Windows Phone 7 security model*, Window Phone 7 for IT professionals, 2010