sciendo International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXV No 3 2019

MOBILE APPLICATIONS - (in) SECURITY OVERVIEW

Teodor MITREA, Vlad VASILE, Monica BORDA

Technical University, Cluj-Napoca, Romania
mitrea_theodor@yahoo.co.uk, vvasile@yahoo.com,
monica.borda@com.utcluj.ro

***Abstract*:** *Over the last years, there has been a real revolution of mobile devices, which has effectively translated into the exponential increase in internet access rates on a mobile device as opposed to accessing it on desktop systems. Given the growing importance of smartphones, it is important to assess the privacy and security risks of these devices in order to mitigate them. However, as we know, in modern mobile security architecture, applications represent the most critical elements. In this paper we review common mobile applications flaws involving network communications, data storage, user input handling and also exploring a number of vulnerabilities. While applications provide amazing features and benefits for users, they also represent the main attraction for cyber criminals. In order to have a true picture of the mobile security threat spectrum, this article presents the means of how mobile applications can impact systems security, stability and compromise personal data if they are not handled properly.*

Keywords: mobile, threat, applications, security

1. Introduction

Mobile devices have invaded our lives and every aspect of our society is affected by mobility: daily activities, business, banking, health [1]. Additionally, over the last years, there has been a real revolution of mobile devices, which has effectively translated into the exponential increase in internet access rates on a mobile device as opposed to accessing it on desktop systems, as shown in Figure 1. Besides internet browsing, accessing e-mail and social networks, mobile devices remain the primary communication tool for voice and messaging, both by standard GSM, SMS or by specialized mobile applications, usually free of charge.

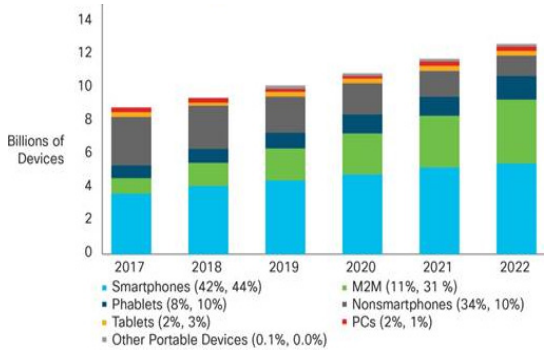

Figure 1: Global mobile devices and connections growth [6]

Undoubtedly mobile applications security has become, or ought to have become, essential for developers in order for users to "survive" in the increasingly hostile world of mobile malware, as shown in Figure 2, with cyber criminals who deploy

DOI: 10.2478/kbo-2019-0115

increasingly aggressive and versatile mobile exploiting tools.

Figure 2: Trends in mobile security threats[4]

Every month, thousands of mobile applications are launched on the dedicated market places and a recent study [7] reveals that only 29% are subjected to vulnerabilities resilience tests before being released. In addition, the lack of security measures over the applications development cycle determines that 31% of them are vulnerable to exposure to man-in-the-middle attacks, data leaks and much more.

2. Mobile applications security paradigm

On mobile devices, applications are, in fact, the most critical elements from security point of view. Moreover, users install them more or less voluntarily (more and more services are now available only through mobile applications) accepting the requested permissions and offering more or less access to the operating system and data. In addition to this, applications are also suspected of doing much more than the intentional and official actions they are designated to do. ***Can we trust such applications?***

Mobile devices are progressively becoming the unique point of interfacing our lives with the mobile information environment and with society as a whole as shown in Figure 3. In this respect two aspects are critical [1]:

- security of personal data - malware can infect personal devices and vulnerabilities can be exploited by an attacker to facilitate access to them;
- privacy of personal data - many data may "naturally" leak to suppliers or companies that sell/promote not only mobile devices but also various additional service; in most cases, these companies and us, as clients, do not share the same interests.

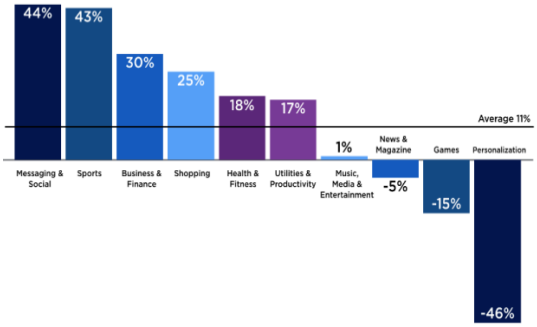

Figure 3: Mobile application usage rate - average annual growth of 11% [3]

At this time mobile applications offer a "fair" trade for users by being free of charge for installation, but instead annoying users with ads. In fact, with the consent of the person who installs such applications, a great deal of personal information is collected by them such as location, online search history, contact list, daily schedule, identity and all of this personal information is distributed to third parties advertising for creating the potential client profile and targeting with the most appropriate ads for the profile indicated. What really follows is, however, the continuous personal surveillance promoted through mobile applications and the unknowing acceptance of this intrusive marketing way. This constant "aggression" on data confidentiality will not disappear soon due to the fact that both application developers and advertising agencies are guided by economic interests and incentives.

On the other hand a mobile application is trustworthy according to a minimum set of security requirements if and only if the following mandatory conditions are met [1]:

- does not contain hidden functions;

- collecting user information must be motivated by explicit functionality;
- web communications involving personal user information must be encrypted;
- the application contains no known vulnerabilities.

3. Common mobile applications vulnerabilities – costs of negligence

In addition to network vulnerabilities, aspects of operating systems and mobile malware are the main threats to mobile privacy as presented in Figure 3. It should be noted that, according to Pradeo [3], that 61% of Android mobile applications and 36% of iOS mobile applications send data to remote servers, and in most cases data is streamed through built-in tracking and marketing libraries.

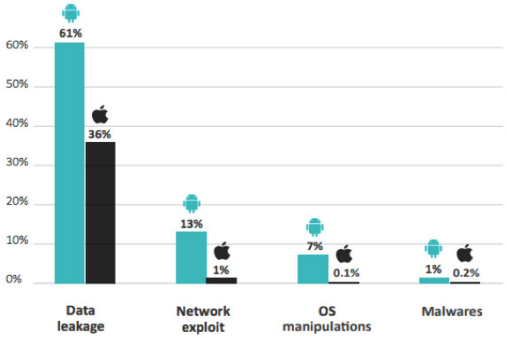

Figure 4: Data privacy violations, malware and vulnerabilities related to mobile apps [3]

Above all, the most targeted data are banking credentials and "disguised" malware is developed to "hunt" this data to access banking services. This type of malware collects sensitive data through compromised web pages then sends them remotely to a command and control server. 83% of all mobile malware is targeting mobile applications, a domain where data theft is expected to grow. For example, ransomware type of malware and, in general, most types of malware developed for Android typically have the definition of trojan-like virus: it spreads through concealing in a legitimate application. Without a doubt mobile applications were the main attraction for cyber criminals last year being used as attack vectors for major mobile threats in about 86% of reported incidents.

In order to have a true picture of the mobile threats spectrum, it is important to observe how mobile applications can compromise data confidentiality. A mobile application may endanger user data security in two ways [5]:

- by performing malicious actions, compromising their functionalities - purpose: stealing sensitive data through a game, compromised tool or other means;
- by exploiting vulnerabilities amplified by application security bugs.

Furthermore, many applications, such as popular games or pornography applications, are often used to increase the likelihood of the victims downloading malware. In some cases, malicious application packages only bear the name and icon of some legitimate applications, while in other cases malware developers take over existing applications and add malicious code while retaining their original functionalities. To spread corrupted applications, malware developers use increasingly sophisticated methods such as encrypting and hiding malicious code as in-depth as possible in the application, and sometimes even by moving packages to media folders. Aplications so compromised do not show elements that indicate other hidden functions but actually run with decryption functions, being able to decrypt and run the ransomware code. After successful installation, most of the malware "constantly" reports information about devices (model, IMEI, network settings, etc.) to command and control servers, and in some cases by establishing a permanent connection with command and control servers, attackers can execute commands on compromised devices by creating botnet networks at the attacker's disposal. Some examples of the malware implementations are: device deletion/blocking, PIN reset, opening of random URLs in the phone's browser, sending SMS to the entire contact list, redirecting incoming SMS, theft of contact list information, displaying

redemption messages, erroneous Android update to other versions, enabling/disabling mobile/Wi-Fi data connection, GPS tracking, etc.

Conclusions

As technology evolves and more devices are connected to the network, whether we are talking about desktop systems, mobile devices, or IoT devices, it also diversifies and complicates the global threat spectrum. The methods by which users can secure mobile devices can be, first of all, the awareness of ransomware threats and the application of active and preventive protection mechanisms. Among the most important active methods to apply are avoiding unofficial applications stores and the requirement to install and constantly update a security application on every mobile device. Additionally, it would be useful to perform a functional back-up of the important data stored on the device.

References

[1] Eric Filiol, Paul Irolla - *(In)Security of Mobile Banking and of Other Mobile Apps*, White Paper, Black Hat Asia 2015.

[2] Robert Lipovsky, Lukas Stefanko, Gabriel Branisa, *Trends in Android Ransomware,* Whitepaper*,* ESET, 2017 https://www.welivesecurity.com/wp-content/uploads/2017/02/ESET_Trends_2017_in_Android_Ransomware.pdf.

[3] *Mobile Threat Landscape Report,* Pradeo, 2018 - https://www.pradeo.com/media/mobile_threat_landscape_S12018.pdf.

[4] *Avast Threat Landscape Report: 2018 Predictions*, Avast, 2018 - https://press.avast.com/hubfs/media-materials/kits/Avast-Threat-Landscape-Report-2018-Predictions/Avast-Threat-Landscape%20Report-2018%20Predictions.pdf?t=1517564995066.

[5] Sachin Sharma, *The Mobile Threats Lurking In Our Applications,* VMware EUC Blog, March, 2018.

[6] Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017–2022 White Paper - https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html.

[7] Ponemon Institute – The State of Mobile Application Insecurity, 2017.