MOBILE SECURITY THREATS: A SURVEY ON PROTECTION AND MITIGATION STRATEGIES

Teodor MITREA, Monica BORDA

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

Abstract: *The spectacular growth in the use of mobile devices is a natural consequence of the benefits they offer. However, most mobile users grant little importance to the security of information stored, processed and transmitted. Even more, the last two years can be considered years of reference for the mobile security industry - ranging from virulent mobile ransomware attacks to mobile IoT botnets and mobile security breaches through mobile malware, that have redefined security paradigms. It is clear that we are at a point of inflection and transition to another generation of cyber attacks and the tendency is that attacks on mobile devices will expand. The security of mobile devices is a topical issue and the main objective is to educate the user to know the risks to which he/she is exposed to and to offer him/her viable security solutions in order to protect himself/herself against mobile threats. In this article we are going to present some protection and mitigation strategies with recommendations for improvement.*

Keywords: mobile, threats, security, protection

1. Introduction

Modern mobile devices allow users permanent internet access to social networks to find the shortest route to a coffee shop, a bank, a hospital or a tourist destination or even to manage their business. Moreover, more than two-thirds of the global population, regardless of age or social category, from children to elderly, uses a smartphone depending on their preferences or hobbies in different ways[2]. Therefore, in the online environment, in return for some services, the users' personal data is extracted and associated with other data for commercial purposes.

Figure 1: Number of smartphones users worldwide from 2016 to 2021 (in billions).
(Source: Newzoo © Statista 2020)

Although mobile devices were designed for an interconnected world and with a built-in security model, it does not necessarily mean that all are completely secured by design. In fact, mobile technology is growing at an alert pace that sometimes it is too alert if we relate it to the ability of everyone involved in developing and implementing high

security standards in a context that cannot allow security to be a secondary goal. Besides the undisputed advantages of new mobile technologies, it is also worth mentioning and analyzing the increased security risks involved.

2. Mobile security challenges

Mobile devices have access to many valuable and sensitive personal data such as bank details, billing information and also hold the credentials used to access other resources, like cloud services that employees are using to access companies data in order to do their jobs [3]. In addition, mobile hardware and software developments have generated significant new threats to the mobile computing environment, highlighting the need for dedicated tools to help the developer community to deploy key security measures. In this respect, there is a multitude of evidence of the difficulty and failure to ensure the security of mobile landscape. Moreover, the fact that mobile device security has not been a constant concern can lead to a high level of vulnerability in relation to the growing number of mobile devices and applications. As shown above, there are heterogeneous security threats targeting mobile ecosystems either at application or operating system level, network, or device level, as shown in Fig 2.

Figure 2: Mobile ecosystems attack surface
(Source: NIST © Mobile Threat Catalogue)

Smartphones and tablets have inherent processing capabilities that, when exploited illegally, allow attackers to locate potential

targets, listen to their communications, access stored files, microphone, camera, and so on [4]. Often, it is said that the greatest danger is represented by the users themselves. However, vulnerabilities of mobile system users are represented by both the low degree of risk awareness of cyber threat, as well as the lack of knowledge or lack of interest in daily activities. Many users fall prey to social engineering, social platforms being the preferred environment for those who carry out such activities. Therefore, hackers use mobile devices as a starting point for attacks against other targets and security becomes both a major opportunity and a challenge [4].

3. Featured prevention and mitigation strategies

Mobile application security concepts derive from many of the fundamentals of web application security, but it also has to address complex risks that require the attention of both development and security teams. Moreover, mobile platforms and operating systems induce new risks for users and organizations and the attack area becomes considerably wider by the existence of multiple users, devices and distributed access points.

3.1. Poor encryption and insecure data storage

Encryption techniques have as their primary objective to make some intelligible data to ensure their security; 1.5% of the applications tested, according to the Open Web Application Security Project (OWASP) [8], reported deficiencies in encryption techniques that may facilitate unauthorized access to the sensitive data set. Encryption and authentication have been tough challenges not only for mobile environment, but also for all online activities.

Figure 3: Encrypting data for securing data stored/transmitted.

Generated risk prevention methods can be thus synthesized: encrypting and storing sensitive data using native device keys, avoiding storing encryption keys with data that encrypt them, disabling storing sensitive information that can be transferred and accessed from a computer.

Consequently, the privacy and security risks of mobile applications with online access can be diminished by using a high level of encryption and improved authentication protocols.

3.2. Data leakages

Data leakages can be determined by various vulnerabilities in mobile applications. For example, users appreciate that applications load very quickly after they have been dropped in the background without being closed. However, when an application went into the background, at a banking session, these data were saved to be available for resumption of the session, generating the risk of the data to be stolen if they were sent unprotected. Unintentional data leaks represent a common vulnerability for mobile applications because they can be easily overlooked - but the results can be serious and come mainly from innocent things, such as debugging messages, storing sensitive data in the device clipboard [7]. Although some prevention methods for generated risk could be the following: restricting data collection by the device, avoiding storing private data in public sites or on the device repository, closely monitoring how the application manages

copy-paste actions, passing into the background, managing cookies, URLs and the typing device cache.

3.3. Network connections and insufficient TLS protection

Mobile applications require sometimes wireless connectivity for authentication processes but, on the other hand, they can require many other components to provide offline access. This, among other things, shows that common authentication protocols can fetch greater risks, for example, the ability of attackers to access device's administrator accounts. Moreover, due to their features, these attacks are very hard to track, enabling, in the worst situation scenario, full anonymous control over the administrative rights of the application. If mobile applications do not use SSL/TLS, especially when they are used in the Wi-Fi mode, except during authentication sessions or based on expired or incorrectly configured user certificates, data may be compromised or intercepted, allowing attackers to obtain administrator privileges and easy access through MiTM simple attacks [6]. The client-server connection within mobile applications must be closely audited in order to prevent such attacks.

Figure 4: MiTM attacks (Source: NowSecure - The Analyst's Guide to MiTM Issues in Mobile Apps).

However, some prevention methods for generated risk could be the following: disabling online access of the application if it does not require this, implementing two-factor authorization if the application has a higher degree of sensitivity, using the

access control service that provides developers with an easy way to authenticate and authorize independent users, the use of an encrypted database for the storage of sensitive information, constant monitoring of network traffic to trigger potential attacks, configuring applications to enable and use SSL/TLS sessions, updating SSL certificates and ensuring compatibility with all mobile application domains

3.4. Weak server side controls and client side injection

Due to the fact that the application communicates with an unsafe backend allows unauthorized users to access the data stored and represents the most exploited threat to the mobile application security. For this reason, when a mobile application is developed and deployed, one of the focus areas regarding security must be on the server side's protection mechanisms.

In fact, mostly downloaded Android applications that run on the client side are vulnerable to SQL injection and XSS (Cross Site Scripting), which could lead to unauthorized access to sensitive data and also device management accounts. In this case, some prevention methods could be summarized: developing, with great care, the control elements for mobile devices in the server area, validating and encoding all data stored on the device, monitoring and parameterizing the log files to detect non-compliant actions if SQLite is used.

3.5. Mobile malware

A malware program is specifically designed to disrupt, destroy, or gain unauthorized access to a legitimate device or data while the victim is unaware of this activity. This type of software can have different functionality in line with the attacker's objective and can combine various products to determine a unique attack type. Even if mobile applications containing malware are sometimes available through official application stores, most come from third-party, unofficial platforms, and the more

people download and install these applications, the greater the number of infected devices will continue to grow.

Figure 5: Mobile malware lifecycle (Source: Lookup - Mobile Security Report).

Currently, the mobile environment lacks well-grounded security standards that regulate how network entities must interact to ensure end-points security and, according to the OWASP [8], 1 out of 3 mobile applications available on the market places is vulnerable.

Conclusions

The ever-expanding spectrum of mobile devices and applications with precarious security has become attractive for cyber criminals who can maximize their profits by pooling multiple infected devices and by combining complex attacks across different infrastructures. As it can be seen, latest research on mobile security has highlighted that both customers and manufacturers believe that mobile security is important, but it is a feature that does not deserve larger budgets. As a result, this may discourage actors involved in developing new end-to-end mobile security solutions tailored to market needs and requirements. There is, therefore, a fundamental gap between the desire for security and the willingness to pay for it. Evolving trends and precarious preoccupation to ensure mobile security will multiply the vulnerabilities of the new technologies, triggering the need to step up research into appropriate solutions. Developing such

solutions will be one of the most important challenges for computer science and scientific research communities.

Given these points, organizations must adopt prevention strategies prevention and not merely rely on detection or remediation of mobile vulnerabilities.

References

- [1] Mobile security threats and prevention - <https://www.soti.net/media/1590/ebook-mobile-security-threats-and-prevention.pdf>
- [2] 2018 Mobile Threat Landscape - <https://www.trendmicro.com/vinfo/in/security/research-and-analysis/threat-reports/roundup/2018-mobile-threat-landscape>
- [3] The Spectrum of Mobile Risk - <https://www.lookout.com/info/spectrum-of-mobile-risk-report-lp>
- [4] The growing threat of mobile device security breaches - https://blog.checkpoint.com/wp-content/uploads/2017/04/Dimensional_Enterprise-Mobile-Security-Survey.pdf
- [5] Follow the Data: Dissecting Data Breaches and Debunking the Myths - <https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/follow-the-data>
- [6] Billions of Bluetooth devices vulnerable to MITM attacks; no user action - <https://www.scmagazineuk.com/billions-bluetooth-devices-vulnerable-mitm-attacks-no-user-action/article/1474116>
- [7] New Approach Secure Mobile Banking Apps - <https://www.arxan.com/resources/downloads/new-approach-secure-mobile-banking>
- [8] N. Jeyanthi and R. Thandeeswaran, Eds., "Security Breaches and Threat Prevention in the Internet of Things," *Advances in Information Security, Privacy, and Ethics*, 2017.
- [9] „Fortinet Threat Landscape Report,” *Computer Fraud & Security*, vol. 2018, no. 6, p. 4, Jun. 2018.