International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 07 | July - 2021 ISSN: 2582-3930

Application Security in Mobiles

Sejal Kaul[1], Pushkar Aneja[2]

[1]Department of computer science and engineering, Manav Rachna International institute of research and studies
[2] Department of computer science and engineering, Manav Rachna International institute of research and studies

---

Abstract - Mobile security is basically based on the process of securing and protecting portable devices such as smartphones, tablets or laptops. In this context, the focus will be on smartphones, which remain largely in relation to the other two. Regardless of the device's operating system, threats that affect the security of users and organizations increase. The most common threats can be malicious software installed unintentionally, illegal listening, unauthorized access, device theft and more. The increase in cyber-attacks makes such devices much more vulnerable and also, the increasing sales of mobile devices makes mobile security a very important factor in order to secure the sensitive data stored inside them. This review paper discusses the major threats to an application and techniques to protect the systems from them. Also, as a conclusion after all the studies done, it proposes an ideal mobile security model which can be deployed to secure the data from breach and help to maintain an effective application security in various devices, especially mobiles.

Key Words: *Data, application security, threat, malicious software, access control, encryption, spyware, authentication, authorization, Network Spoofing, Phishing*

1. INTRODUCTION

Web applications are one of the most common and known platforms for delivery of various services as well as for storing important data. But at the same time, as there is a gradual increase in the usage of applications, so is the increase in application security breaches thus, making application security as the need of the hour. Application security describes application-level security measures that are designed specifically to identify and prevent theft or piracy of application data or code. It includes security considerations that arise during application development and design, as well as systems and approaches to protect applications after their deployment.

Application security can include hardware, software, and procedures that majorly identify and minimize various security vulnerabilities. There are hundreds of threats that can exploit a vulnerability present in a system. So, it is important to carefully analyse various applications before they are installed in any device. There are many malicious software that can enter into the systems and cause loss of sensitive information such as various login credentials, card information and many other forms of data which can be misused by the attacker to gain privileges.
.

2. THREATS AND SECURITY IN MOBILE DEVICES

2.1 Data leakage - Nowadays, various freely available mobile applications are becoming a major cause of many unintentional data leaks. These free apps that can be found in official application stores can also send sensitive information about the user to untrusted sources, where it is retrieved by advertisers and, over time, by cyber criminals. Data breaches can also occur through threatening companies or organizations with branded multipurpose applications. These applications may contain versatile malware programs that use locally propagated code for popular mobile workplaces such as iOS and Android to obtain critical information of an authorized user.

2.2 Using unsecured Wi-Fi - Freely available open connections can be highly unsecured. Your social media credentials, phone data, text messages and even your transactions can be compromised using these open ports. In order to protect the data, it is advised to not to use the openly available free WIFIs specially to access confidential or personal services,

like banking or credit card information.

2.3 Network Spoofing -Network spoofing occurs when the attacker configures malicious access points that are real WiFi networks. Indeed, these open WiFi networks are traps set by them. Oftentimes, the victim is asked to create a free username and password to access open Wi-Fi networks, which excites the attacker as many users create the username and password they have already used on another platform. The attacker can even access and exploit them through identity theft.

2.4 Spyware - Spyware is the type of malicious program that tracks all authorized user activities at the same time. Also known as Stalker wave, a significant number of these apps are said to pile up on the lens device without your consent or information. A complete combination of antivirus and malware identification must use special filtering procedures for these types of programs, which, compared to other malware, require somewhat unexpected treatment derived from the way it invades your device and your motivation.

2.5 Phishing Attacks - One of the most common types of security attacks is a phishing attack. This usually happens when opening unknown or untrusted links which can make a user a victim. In such attacks, the attacker sends fraudulent messages mainly through emails and messages and tries to act as a legitimate sender on the reputation of a real source. The purpose of these phishing attacks is very clear, it is to remove the user's confidential information in order to misuse it. Your logical credentials, payment information, and identity proofs are some of the major sensitive information that hackers demand very much and implement phishing attacks on.

2.6 Outdated Operating System and Applications - Using outdated / non-updated operating systems and applications is another threat to your mobile devices. Attacks are evolving every day and along with it we should also keep our operating systems and applications with the upcoming patches. These patches by the developers contain new techniques to stop unwanted activities in your device up to an extent. With evolving attacking techniques developers also evolve with techniques to safeguard our devices and these are delivered to us in the form of updates / patches.

2.7 Weak transport layer protection - Sensitive data must be protected when it is transmitted through the network. Such data can include user credentials and credit cards. As a rule of thumb, if data must be protected when it is stored, it must be protected also during transmission.

2.8 Client-side injection - Client-side injection results in the execution of malicious code on the client side which is the mobile device, via the mobile app. Typically, this malicious code is provided in the form of data that the threat agent inputs to the mobile app through a number of different means.

3. APPLICATION SECURITY PROCESS

For knowing the security structure of devices, the basic parameters on which the process of application security is based, must be understood. The five basic steps for application security are as follows:

3.1. Identify the threats: The first and foremost step towards securing a system is to identify the types of threats that can breach your device and the data stored in it.

3.2. Identify the vulnerabilities: there can be multiple vulnerabilities in an application that could be exploited to cause an attack by the attacker. So, whenever a vulnerability is found, it should be kept as a record in the logs so that it can be mitigated and prevented from being exploited.

3.3. Access risk explore: in order to look deeper into various threats, users must explore various risks associated with the vulnerabilities identified so that those risks can be accessed and mitigated before they lead to loss of data.

3.4. Respond to cyber security accidents: in case when the risk cannot be mitigated or avoided, it leads to cyber-attack. In that case, users must respond to them efficiently by looking for an effective incident response method.

3.5. Establish a contingency plan: when an attack has happened and responding technique towards that particular attack has been identified, the next step is to build a framework or plan for the same and this is followed by the maintaining logs for the same so that we already have the technique to deal with that attack if it occurs in the future again.

4. APPLICATION SECURITY FEATURES

Different types of application security features include Authentication, Authorization, Encryption, Access Control, Logging, and Application Security Testing.

4.1. Authentication: When software developers create procedures in an application to ensure that only authorized users can access them. Authentication procedures ensure that a user is who he claims to be. This can be accomplished by prompting the user for a username and password when logging into an application. Multi-factor authentication requires more than one form of authentication: the factors can be something you know (a password), something you own (a mobile device), and something you are (a fingerprint), or facial recognition.

4.2. Authorization: After a user is authenticated, the user can be authorized to access and use the application. The system can verify that a user is authorized to access the application by comparing the user's identity with a list of authorized users. Authentication must precede authorization so that the application only matches the user's credentials that have been validated against the list of authorized users.

4.3. Encryption: Once a user is authenticated and uses the application, other security measures can prevent a cybercriminal from viewing or even using sensitive data. In cloud-based applications, where data traffic containing sensitive data is transported between the end user and the cloud, this data traffic can be encrypted to ensure data security.

4.4 Access Control: It is a security technique that regulates the access depth / access level of resources to a user in an application. It plays an important role in protecting an application, both from a developer and a consumer perspective.

4.5. Logging: If an application finds a security breach, the log can help determine who accessed the data and how. The application log files contain a timestamp indicating which aspects of the application have been viewed by whom.

4.6. Application security testing: it is an important process to ensure that all of these security controls that are deployed work properly.

5. METHODS TO SECURE THE APPLICATIONS INSTALLED ON THE DEVICES

5.1. Frameworks and policies:

In order to attain an effective application security, various frameworks and policies are defined, granting various permissions described by an application. In particular, an application that declares authorization defines the conditions under which various permissions are granted to other applications during installation. The existing security model of the mobiles allows / does not allow the granting of permissions based on rules independent of the application or user input. Some factors that must be taken care of, are:

- 5.1.1 Always protect the application with encryption
- 5.1.2 Analyze the source code for vulnerabilities.
- 5.1.3 The application code should be easy to update and rebuild, and portable between devices and operating systems.
- 5.1.4 When saving the application, consider its size, performance, memory, data and battery. Having

better security but losing the power of applications or users is not what you want.

5.1.5 Do not trust the approval of the App Store. It may or may not be accurate.

5.2. Have security measures to protect data and deny unauthorized access:

Take a look at the Application Programming Interface (API) to prevent sensitive information from falling into the wrong hands. Create encrypted containers to store data securely. Encrypted data and encrypted connections via a virtual private network are particularly secure and must be followed.

5.3. Activate a good mobile encryption policy:

Use various file-level encryption techniques to manage the access to your sensitive information. Align the codes of application as the passwords and data are not directly saved in the device. In case they have to be stored, make sure that they are encrypted.

5.4. Authorization technology of API add an extra layer of security:

Make sure that the APIs used in the application only allow access to the most important parts of your applications.

5.5 Review and test the techniques: Session Management and Test Data Security Issues Penetration testing helps correct weaknesses in the system. Emulators explain the performance of an application on any device or operating system in a simulated environment.

5.6 Alert user**:** Developers and testers can't always be a user's protectors. In that case, include sufficient pointers if any kind of vulnerability is detected. Warn the users to download only from authorized sites.

5.7. Using some extra precautions: Protect your devices with an antivirus, firewall and antispam Allow only authorized devices Block transactions of rooted devices and jail systems.

5.8. Coordinated vulnerability platforms: There are many automated tools available that test an application for security vulnerabilities, often at a higher false positive rate than that of a human. These are application security solutions that are offered by many websites for hackers and software developers. They enable users to identify and compensate for reporting errors.

THE PROPOSED ANDROID SECURITY MODEL

Android is a multiprocessing system in which each application runs its own process. In this proposed security model for mobile security, many features must be taken care of in order to attain a device with secured information. The proposed model must work on the basic framework of scanning the application that is being installed in a particular device.

Various applications, after being installed, must only be run on the basis of authorization mechanisms which must deal with access control in order to verify the identity of the end user using that particular application. Authorization names are part of a security policy that restricts access to each component of an application. This authorization mechanism must be followed by a detailed check of the information that is being provided to the application server, for e.g.; card credentials, personal ID number etc. All controls and operations must be verified before they are implemented. Every device uses security policies to determine whether permissions should be granted or denied for applications installed on the operating systems of mobiles and hence, must be checked. These security guidelines do not allow you to specify the rights or permissions of the application granted to you because they are based on the user and the operating system. They run the risk of allowing malicious applications to access confidential information on the phone. Applications such as browsers, email clients, software markets, music players, etc. are to be used in a secure way by carefully keeping a check on the cookies. Apart from this, a regular update has to be performed of each application so that it can get introduced to the new security patches and identify the vulnerabilities to prevent the data breach.

CONCLUSION

Mobile devices also transmit and receive information over the Internet, unlike a private network, which makes them vulnerable to attack. Organizations can use virtual private networks (VPNs) to add a layer of mobile application security to employees connecting to applications remotely. IT departments may also decide to review mobile applications and ensure they comply with company security policies before allowing employees to use them on mobile devices connected to the company network. Application security is important because today's era involves much usage of mobiles and mobile applications. These applications are often available on different networks and connected to the cloud, leading to increased vulnerabilities, threats, and security gaps. There is increasing pressure and

incentives to provide security not only at the network level, but also within the applications themselves. One reason for this is that hackers now have more access to applications than before. Application security testing can reveal application-level vulnerabilities and help prevent these attacks.

Moreover, application security can be achieved by continuous update of the security patches, implementing encryption techniques on the sensitive data, analysing access control and building advanced frameworks that can act as defensive tools against the attack

ACKNOWLEDGEMENT

In the present world of competition there is a race of existence in which those are having will to come forward, succeed. With this thought we began this particular research. We would like to acknowledge our parents for the constant support and encouragement to complete the research in and out.

REFERENCES

1. https://www.vmware.com/topics/glossary/content/application-security
2. https://www.zdnet.com/article/mobile-malware-attacks-are-booming-in-2019-these-are-the-most-common-threats/
3. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.31.3950&rep=rep1&type=pdf
4. https://ieeexplore.ieee.org/abstract/document/9347435
5. https://link.springer.com/chapter/10.1007%2F978-3-319-51064-4_7
6. https://www.csoonline.com/article/2157785/five-new-threats-to-your-mobile-security.html
7. http://eprints.utm.my/id/eprint/86306/1/LimKahSeng2018_TheApproachestoQuantifyWebApplicationSecurity.pdf
8. https://web.archive.org/web/20180603013024id_/http://ijarcsse.com/docs/papers/Volume_7/4_April2017/V7I4-0195.pdf
9. https://www.researchgate.net/publication/336845625_MOBILE_APPLICATIONS_SECURITY_AN_OVERVIEW_AND_CURRENT_TREND