JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

REVIEW ON MOBILE APPLICATION SECURITY

Ms. Rashmi Dagde
Assistant Professor
Computer Science & Engineering Department.
Priyadarshini Bhagwati College of Engineering, Nagpur, India.

Ms. Janhvi Pittulwar
Research Scholar
Computer Science & Engineering Department.
Priyadarshini Bhagwati College of Engineering, Nagpur, India.

Ms. Neha Sahare
Research Scholar
Computer Science & Engineering Department.
Priyadarshini Bhagwati College of Engineering, Nagpur, India.

Ms. Savari Kurrewar
Research Scholar
Computer Science & Engineering Department.
Priyadarshini Bhagwati College of Engineering, Nagpur,
India.

Ms. Akanksha Hatwar
Research Scholar
Computer Science & Engineering Department.
Priyadarshini Bhagwati College of Engineering, Nagpur,
India.

***Abstract* :** Mobile application security has tends to appear as a very important conception lately, the use of mobiles is done enormously than laptops and computers. One and the other institutions, companies, colleges etc. are connected with the internet which increases the risk of getting their personal data hacked. Mobile application security is used to secure the devices from the attacks and other malware activities. It can be accessed by tablets, mobiles, laptops, etc. In this paper, we will be studying about various threads and security measures and discuss about various protective tools which will keep our devices safe and secure.

Keywords : Mobile security, threads, risk, protective tools.

1. INTRODUCTION :

Mobile application security is the study of organization of mobile applications, it helps us to understand how the application works. Mobile application security reduces the threat and possibilities of the device getting hacked by recognizing how the hackers attacks the system. The purpose of Mobile application security is to secure personal and the company data stored within the application or the devices.

Nowadays, people mostly depends on the mobile application to escort them in every aspect of life, such as keeping a track of their schedule, health records, ordering food, booking train tickets, and many more. But as much as we rely upon those applications there are high chances of increasing in number of threats. Mobile apps have become an easy target for attackers which results into online frauds, account take over etc.

In a hurry to build new application with much more attractive features that improves user experience and engage new customers, some developers create apps with imperfect privacy and security policy which later results in issue of data leaking and puts each and every user at risk.

2. Application security risks :

One of the three types of mobile application security risks are as follows:-

2.1. **Lack of Input Validation**: Input validation is done to check weather the data entered is in the proper format as the software requires or not. This should be done as early as possible later it leads to lack of input validation. The data given by the user should be valid and syntatically correct, this is done to secure the data inserted by the user. Many times the client inserts improper credentials which allows the attackers to hack the backend data and gives them the easy access to the web application or website, this is called as lack of input validation. Input validation is done to prevent attacks and malware activities but cannot do all of it alone it can only reduce the chances of getting attacked or hacked.

When the invalid or corrupted data is inserted, an application shows some error, or fails to load the data, or sometimes returns incorrect data too and also crash the server. Hence, the data entered by the user should be in proper and valid format to reduce the risk of getting the data hacked.

2.2. **Insecure Communication**: Insecure communication generally belongs to the communication between the user and the server. While transfering the data from the sender to the receiver the data is insecured and has high chances of getting attacked, here the user and server communicate over unencrypted channel which has no guarantee of data security. It is important to encrypt the connection for the developer to keep his data safe and the developer should keep a check that server to database connection is encrypted or not.

Attackers try to steal the personal information such as passwords, financial data, documents, etc. there are various tools which shows the unencrypted data as encrypt data and the developer does not recognize it and transfers the important data insecurely. Some secured communication protocols are TLS/SSL, HTTPS, etc.

2.3. **Insufficient Authentication and Authorization Controls**: To maintain high security and to keep your data safe from the attackers you need to have high authentication control which does not allow the attackers to perform any malicious activities. Insufficient authorization control allows the attackers to access the application and perform various funtionalities, sometimes the developer allows offline authentication for the user which can result into the security risk. The developer should consider about these before the implementation of the application.

Many times the attackers execute high actions when their is insufficient authentication control which later turns into modification of the data, backend changes, data theft, etc. To implement proper authentication control the developer need to encrypt the data properly, the authentication request should be allowed to the server side only. The user should enter proper credentials.

3. LITERATURE SURVEY:

[1]: Investigation on mobile threats, mobile vulnerabilities, and many security-related issues for users of mobile devices. Physical-based threats, application-based threats, network-based threats, and web-based attacks are the many mobile dangers covered by their study. One threat to mobile vulnerabilities that involves earnest money is a botnet. They claim that one of the most significant security measures is Biometrics is the technique for mobile security and data privacy authentication. Every phase of developing a mobile application must include security mechanisms. The flaws discovered in health-related mobile applications were examined by Cifuentes. Based on the features of the apps, they divided mobile health apps into six groups. To conduct their analysis, they downloaded ten Android apps from the Google Play Store for each group vulnerabilities.

[2]: In 60 mHealth apps, a total of 157 vulnerabilities were found. Their findings indicate that remote monitoring applications have the greatest amount of vulnerabilities and that these apps also have high-risk levels of vulnerabilities. Their findings indicate that 64% of mHealth app vulnerabilities were caused by unreliable input. Cryptographic vulnerabilities in mobile applications were categorized by Chatzikonstantinou into weak cryptographic algorithms, poor cryptographic keys, weak implementation of cryptographic methods, and weak parameters. They manually conducted static and dynamic analyses on 49 arbitrary Android apps that they downloaded from the Google Play Store. According to their findings, 12.2% of Android apps have no cryptographic methods at all, while nearly 87.8% of Android apps utilize weak cryptographic algorithms.

A new key agreement and authentication methodology for electronic health record systems was put into place. Since the EHR system has a variety of users, including doctors, lab workers, patients, and insurance agencies, authentication and appropriate key agreements are crucial. The suggested protocol is based on a commitment mechanism and will halt communication if authentication is unsuccessful. They claimed that man-in-the-middle assaults on wireless communications are extremely effectively avoided due of the binding or hiding nature of protocol.

4. Methodology:

4.1.**TOP ISSUES FACED BY MOBILE DEVICES:** If you don't use a strong password, PIN, or biometric authentication, or if you utilize unencrypted apps and services, your lost, stolen, and unattended devices could be compromised. Without screen locks, passwords, or other security measures, phones are open to unauthorized access, which may compromise critical data stored on the mobile device. Human error, like allowing unauthorized users to access the network, corporate espionage or deliberate acts of sabotage, physical destruction of servers or equipment due to terrorism or natural disasters.

Avoid using your gadget in public and think about bringing your laptop in a non-traditional bag. Observe your surroundings carefully. If you must use a laptop or mobile device in a public setting, be aware of your surroundings. All of these comes under physical security.

4.2**. MALWARE ATTACKS:** Malicious software is placed on a user's mobile device without their knowledge. Malware can propagate over the internet or through unprotected programs. Malware has the ability to broadcast messages to the whole contact list, unwanted numbers, and steal vital information to give to attackers. Attackers have full access to the mobile device with that malware. The many categories of the most common mobile malware are broken down below. Similar to a regular computer worm, Mobile Worm multiplies itself and spreads to more mobile devices. Mobile worms can spread through SMS or other communication channels without user interaction. Trojan: The Trojan is activated when a user runs a trustworthy executable file that contains malicious instructions

4.3**. Developer Security Measures:** When creating mobile applications, developers must take security seriously and take appropriate precautions at each level. Use of robust cryptographic methods with lengthy keys and correct TLS/SSL implementation for secure communication between the mobile app and server are a few examples of security practices. Correct Updates: Whenever a security flaw is discovered in a mobile application, developers must publish an update. If libraries used by your apps have received a security update, update them.

4.4. V**ersion apps and operating systems as part of user security measures:** Users of mobile apps must do this whenever the developer publishes a new version. Updates are occasionally made available by developers to fix security problems with their apps. Compared to software updates. The most crucial updates are to the operating system .

Don't Root Devices: Gaining complete access to various subsystems on Android mobile devices is known as rooting. The installation of harmful apps is possible after rooting a mobile device, which compromises its security architecture. These harmful apps are able to obtain information from other apps. Putting in Unknown Programs: Before making programs public, reputable app hosting companies like Google Play Store or Apple App Store rigorously scan them for dangerous content. There will therefore be relatively few security risks when downloading programs.

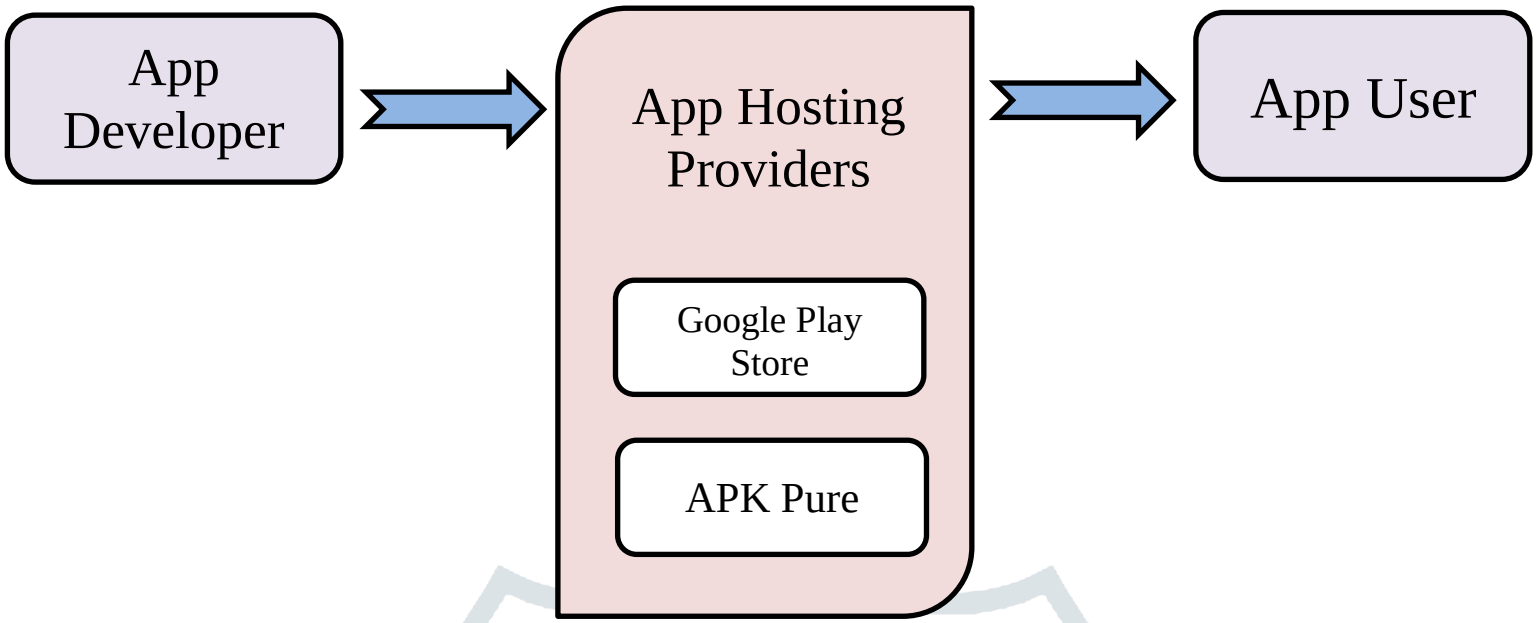

Fig 2.1. APK file flow from Developer to User

5. **Conclusion:** This review paper states that it is to secure mobile apps and devices while safeguarding users. We have access to a special collection of mobile security data thanks to our strengths in mobile app testing, device tracking, forensics, and security intelligence.

In order to share some of those data and the conclusions that followed with the public, we published this research paper. We also want to assist businesses in managing and protecting the mobile apps and devices that connect to their corporate assets every day.
An alternative strategy is needed for mobile security, one not centered on malware, leaky applications that transfer or keep personal information are safe.

References:

[1]Chatzoglou, E., et al.: "How is your wi-fi connection today? dos attacks on WPA3-SAE". J. Inf. Secur. Appl. **64**, 103058 (2022).

[2] Kampourakis, V., et al.: "Revisiting man-in-the-middle attacks against https. Netw. Secur." (2022).

[3] Pirayesh, H., Zeng, H.: "Jamming attacks and anti-jamming strategies in wireless networks: a comprehensive survey". IEEE Commun. Surv. Tutor. **24**(2), 767–809 (2022).

[4] Kampourakis, V., et al.: "Wpaxfuzz: sniffing out vulnerabilities in wi-fi implementations". Cryptography **6**(4), 53 (2022)

[5] Jabiyev, B., et al.: "Preventing Server-Side Request Forgery Attacks", pp. 1626–1635. "Association for Computing Machinery", New York, NY, USA (2021).

[6] Sadqi, Y., Maleh, Y.: "A systematic review and taxonomy of web applications threats". Inf. Secur. J. Global Persp. 1–27 (2021).

[7] Almaiah, M.A., et al.: "Classification of Cyber Security Threats on Mobile Devices and Applications", pp. 107–123. Springer, Cham (2021).

[8] Karaçay, L., Bilgin, Z., Gündüz, A.B., Çomak, P., Tomur, E., Soykan, E.U., Gülen, U., Karakoç, F.: "A network-based positioning method to locate false base stations. IEEE Access **9**, 111368–111382 (2021).

[9] Mohammadnia, H., Slimane, S.B.: IoT-NETZ: "Practical spoofing attack mitigation approach in SDWN network". In: 2020 Seventh International Conference on Software Defined Systems (SDS), pp. 5–13. IEEE, April 2020.

[10] Mylavarapu, R.M., Nigam, A., Hegde, V.B.: U.S. Patent No. 10,686,819. U.S. "Patent and Trademark Office", Washington, DC (2020).

[11] Huang, X., Tian, Y., He, Y., Tong, E., Niu, W., Li, C., Chang, L.: "Exposing spoofing attack on flocking-based unmanned aerial vehicle cluster: a threat to swarm intelligence". Secur. Commun. Netw. **2020** (2020).