Software Security

Laboratory Assignment 4

Report

Name: Sree Lakshmi Hiranmayee Kadali.

T-Number: 20010920-T244.

Task 1:

I’ve selected the topic “Security threats of Smartphones” for this report.

Motivation:

Because the usage of smartphones for every activity these days has become quite popular, and security is the most needed for users.

Introduction:

The usage of smartphones now a days needs no introduction; the use of smartphones has outnumbered than the use of PC’S. Smartphones now offer abundance capabilities like PC’s along with a lot of connection options like 4G,5G, Wi-Fi, Bluetooth, Online Payments, Online Shopping, and other services etc. This superfluity of applications and properties of mobile phones has placed them in arm length away of every individual. The increase number of users also gives malicious attackers a chance to use smartphones as an ideal target in various ways. The lack of awareness of these attacks in users leads to digital fraud of almost 60 percent around the world. There are security threats with smartphones which can make user’s information sensitive to stealing.

Here are few important and biggest threats (malware, vulnerabilities & attacks) that are prone to smartphone security:

Malicious Software:

Malicious Software or Malware in simple terms can be referred to illegal software that is not installed by users but targeted by attackers by taking advantage of vulnerabilities present in the system and breakdown results like documents and information of the user.

The major malware attacks of mobile phones are:

Trojan: Trojan is a kind of malware which helps in transmitting and gaining access to unauthorized access of sensitive interactions like transactions under the cover of an real app.

Spyware: Spyware software is mainly used to collect information of the user regarding a specific subject and provide it to others without their consent. These can be in the form of adware for promotional purposes and user cookies.

Virus: Virus is a kind of malware which infect other apps and needs to be performed by the user to inject into the mobile. Once, virus is affected, it slows down the performance of mobile by effecting the hardware elements and making the elements unusable.

Worms: Worms are a kind of most harmful malware which necessarily have misleading information and doesn't require user interaction to be effective. The attackers mainly focus on Security vulnerability of the device to inject it. They are usually transmitted through SMS and emails.

Vulnerabilities:

Hardware: Security issues related to hardware vulnerabilities is primarily due to the agedness of the device where the device doesn't receive security updates after a certain time. And Inability of assuring safety while connecting to network or the internet which can give hackers and unsecure port to attack the device.

Software: Installing third party APK's, allowing permissions given during installations in google store or apple store leave vulnerabilities in software which can be prone to malware. Outdated software and devices which are stopped from receiving software updates are also prone to software vulnerabilities in mobiles.

Attacks:

An attack in an interference made from outside using different type of vulnerabilities present in the device. Attacks can be made in different ways like hardware based attacks, software based attacks, user based attacks and device independent attacks. Few attacks which are more popular among smartphone security challenges is:

Phishing Attacks: Phishing is a kind o OS-independent method which can be done on any type of device where the attackers usually try to steal passwords, credit card information, credentials etc by directing users to imitation websites.

QR Code Based attacks: QR code attacks have been rising in the recent popularity of QR code scan for ease of banking transactions. Attackers might include malicious URL's in the QR code which makes the device vulnerable.

Few other attacks like SSL proxy attacks, Forensic analysis, JTAG, Man in the Middle etc can be leave showing how security challenges of smartphones are.

Due to this complexity of Smartphone security, several security solutions can be implemented to bring safety and security among users from the attacks. Some countermeasures to mitigate them are:

- Keeping Smartphone OS up to date.
- Strong encryption for the device, so it is incredibly hard for someone to break or bypass when the device is lost.
- Encouraging people to install software for security so to prevent attacks like anti-malware, anti-theft, anti-phishing, anti-spam.
- Installing apps from trusted sources only.
- Preventing connecting to not protected and open wifis'.
- Few measures from anti-malware companies can be taken for malware analysis techniques. Machine learning based techniques for detecting patterns of unpredictable and known software, signature based techniques for producing a new unique signature for a known malware which can compare to a newly identified signature etc.

Task 2:

I've taken 3 articles for this study using the following keywords:

Keywords: Smartphone security, Mobile Security, Software security, malware, attacks, threats.

Related Work:

Research paper [[1]] "A survey on Smartphones Security: Vulnerabilities, Malware, and Attacks" written by Milad Taleby et al published in Academia provides an overview of security of smartphones for any researchers. The paper initially discusses the importance of smartphones ad their importance in our daily lives which has led in transparency and security issues of the user. The authors then present the classification of smartphone security threats based on different architecture layers of smartphones such as hardware, software, OS and application layer. The paper also talks about different type of vulnerabilities, attacks and threats of smartphones and different countermeasures to take for preventing them. It also provides insights into current state of smartphone security.

I have chosen this paper because it provides a comprehensive overview of security threats and mechanisms of smartphone's security.

Research Paper [2] "Secure Software Installation on Smartphones" written by David Barrera et al talks about the need and importance of antivirus applications for smartphones in the midst of increase in cyber security threats faced by smartphone users. The paper initially talks about security consideration of smartphones in different smartphone platforms like iOS, android, blackberry and Symbian. Then the researchers, discuss different security features in mobile phones and different installation models which can help in third party apps installation in the devices. The authors draw conclusions on pros and cons on different installation models and how security software installation is needed for every smartphone in the conclusion section.

I've considered this paper for this report because it shows the importance of security installation in smartphones.

Research Paper [3] "Cyber Security and Mobile threats: The need for Antivirus Applications for Smartphones" written by Jorja Wright et al discusses an overall review on mobile security with the increase in cyber security threats, and shows different attacks and vulnerabilities present in mobile security which can reveal personal and sensitive information. The paper mainly focuses on how the traditional software in mobile in vulnerable in nature and can become a target for cyber-attacks. The authors performed an analysis and provided quantitative results.

I've considered this paper because it shows the importance of security in smartphones with results after research. The findings prove that most of mobiles doesn't even have proper security.

Task 3:

Future Work:

In case of security in smartphones and terms of privacy for users, no one can figure out the number of attacks that can happen on devices but perform researches on how different types of attacks might occur and different ways to bring awareness among users to be precautious. Because it is important for the user to be aware of security issues with any device. Different ways, mobile security can work in the future is:

- Machine learning and deep learning can be used in mitigating malicious attacks. Machine learning techniques can help in providing real time behaviour analysis and identify imitating fake apps. Deep learning algorithms can be used for feature extraction during malware testing and in malware detection.

- All the popular OS mobile companies need to consider providing more security mechanisms so to prevent unpredictable attacks.

- Since, most of the users usually download apps from app market, it is difficult for them to differentiate between real and fake apps. So, researchers can investigate ways to monitor how fake apps behave using network monitoring and process monitoring etc.

References:

[1] M. Taleby, Q. Li, M. Rabbani, and A. Raza, “A Survey on Smartphones Security: Software Vulnerabilities, Malware, and Attacks,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 10, 2017, doi: 10.14569/IJACSA.2017.081005.

[2] D. Barrera and P. V. Oorschot, “Secure Software Installation on Smartphones,” *IEEE Secur. Amp Priv. Mag.*, vol. 9, no. 3, p. 42, 2011.

[3] J. Wright, M. Dawson, and M. Omar, “Cyber Security and Mobile Threats: The Need For Antivirus Applications For Smart Phones,” *J. Inf. Syst. Technol. Plan.*, vol. 5, pp. 40–60, Jan. 2012.