Cybersecurity and digital forensics year 3

Module: individual project

Supervisor: Mrinal Sharma

Student ID: M00729531

Chapter 1 project proposal

Table of Contents

1.Title

IOT (internet of things) security flaws and mitigations.

1.1 Topic focus:

Security vulnerabilities In Samsung smartphones.

2. Keywords

Vulnerabilities, security

3. Introduction and context description

IOT or the internet of things is an important part of user's daily lives due to the interconnection of everyday objects such as devices using the internet to share data and process data [1]. this research study project will evaluate the security of IOT devices, in particular smartphones devices. The key interest is to evaluate the security structure of smartphones and what security issues they have that could jeopardize the integrity of user's data.

Smartphone devices have become facilitators in user's daily lives by performing several tasks at the same time and being effective at delivering results. However, users are often required to insert and store sensitive information in those devices and the risk of a data breach have kept users always worries that their information can be leaked due to the vulnerabilities in smartphones that are often exploited by attackers. One of the most popular smartphone brands is Samsung which has a market share of 38% [2]. Samsung, being popular sets itself as a target to threat actors that evaluate the different mobile phone models of the brand in search of security flaws that could be exploited. The Samsung brand, especially its smartphone, has shown to have vulnerabilities that can be easily exploited by malware or can be manipulated by attackers which in many cases exposes user's information that could be used for ransomware or blackmailing.

This research study project aims at attempting to uncover vulnerabilities in Samsung devices and provide and apply the best mitigation measures to counter such issues for data protection. The research will use vulnerability assessment tools that will evaluate different mobile applications software that is used in smartphones such as the Samsung brand, in particular system apps that are pre-installed unlike third-party apps. This project will use a Samsung device to facilitate the process of examination of different mobile

applications which will be the core of this project since system apps and third-party apps mainly handle and process user's information and ensures the information is well safe guarded. This research project shall produce an extensive report on all aspects of Samsung device's security structure and history of known security flaws of Samsung. Furthermore, the research project shall also conduct experiments on a Samsung device to test the security of Samsung devices, security issues, potential impacts of those security issues and recommend the best standard practices to combat issues of data security.

4. Background of study

Samsung devices are among the widely used devices in the world closely next the iPhone devices from apple [2]. The functionalities of those smart devices increase each time a new operating system in introduced such as the android OS (operating system) that is used by Samsung devices. However, the vulnerabilities of Samsung devices have increased significantly. It is a critical issue for Samsung devices since some Samsung devices vulnerabilities are not addressed appropriately through updates or do not receive consistent security updates and patches among different models [3]. Ensuring user's data protection is a crucial issue in this age of modern advanced technology that can handle a large some a data and process data.

5. Problem statement

Samsung implements vast and robust security measures in their devices. However, security vulnerabilities are still present in different Samsung smartphones. Security experts on smartphones still discover security vulnerabilities in smartphones and including Samsung devices and document the findings to a common vulnerability and exposure or known as CVE which details the vulnerability discovered and the potential impact of it to user information and privacy [4]. This research study aims to evaluate the characteristics of vulnerabilities of a Samsung device and the potential impacts to user's information.

6. Aims & objectives

6.1 Aims

This research study aims to investigate Samsung security vulnerabilities by examining a Samsung device. The evaluation shall be documented and reported in detail on the security vulnerabilities and their potential impact on the device and user data.

6.2 Objectives

- Identification of security vulnerabilities in a Samsung device (Samsung A12)
- Analysis of the impact of the security vulnerabilities in the Samsung device.
- Evaluation of security measures in place for mobile smartphone devices and recommend enhanced security measures that can be undertaken to mitigate the identified vulnerabilities.

7. Research questions

- What type of user input vulnerabilities are most common in apps on the Samsung A12 device?
- How do these vulnerabilities vary between third-party apps, system apps and high-risk apps that handle sensitive data such as financial apps?
- What are the potential negative impacts of the vulnerabilities uncovered on user data security?

The research questions are based on the Samsung device that will be used to search and uncover mobile security vulnerabilities. As mentioned in the questions, this research will use a Samsung A12 device and fulfill the research questions extensively.

8. Key Deliverables

1. This research study ensures to deliver a comprehensive report on security vulnerabilities of Samsung devices. The report shall provide all aspects of Samsungs devices, in particular the security aspect of Samsung devices which will be the focus of the study since it deals with user data and the impacts of security flaws to user data.
2. This research study shall provide a detailed comprehensive analysis on the impacts of security vulnerabilities on user data and how security vulnerabilities can affect different mobile applications that share user permissions.

3. This research study shall conclude the report with a set of recommendations that security measures that can be implemented to improve the security of Samsung devices.

9. Project plan

ACTIVITY	PLAN START(week)	PLAN DURATION(week)	ACTUAL START(week)	ACTUAL DURATION (week)	PERCENT COMPLETE
Project proposal	1	5	1	6	100%
Data collection	9	4	9	4	1%
Data analysis	13	2	13	2	1%
Report writing	15	9	15	9	1%
Final report (chapter 1,2,3)	23	3	23	3	1%
Project presentation (recorded)	26	1	26	1	0%

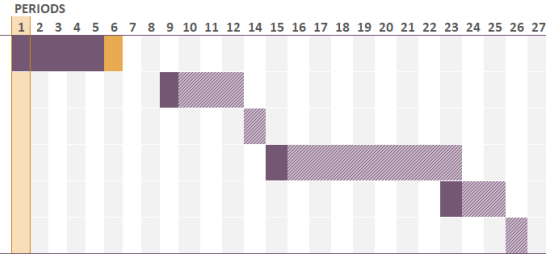

Figure 1:project plan.

The above figure 1, elaborates the project plan with the duration of each task in the project. In the right-hand upper side to the project plan in figure 1, shows numbers that represent weeks, and the purple color and faded color represents the progression of each task in the project. The project plan is for the full course of 26 weeks and each task has its assigned starting week and duration up until the last week for the project report presentation that shall mark the completion of the project.

10. Key contributions

1. Delivering a vast understanding of security vulnerabilities in Samsung deices and the severity of such vulnerabilities.
2. Delivering practical recommendations to users and developers of applications of Samsung devices to improve the overall security of those devices.

11. bibliography

[1]
"What is IoT? - Internet of Things Explained - AWS," Amazon Web Services, Inc. Accessed: Jun. 28, 2024. [Online]. Available: https://aws.amazon.com/what-is/iot/

[2]

F. Okeke and Y. Khlebnikova, “Samsung Surpasses Apple in US Smartphone Sales,” 2024. [Online]. Available: https://www.techopedia.com/news/samsung-surpasses-apple-in-us-smartphone-sales

[3] “Samsung Mobile Security.” Accessed: Jun. 29, 2024. [Online]. Available: https://security.samsungmobile.com/workScope.smsb

[4] “Samsung : Security vulnerabilities, CVEs.” Accessed: Jun. 29, 2024. [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-822/Samsung.html?page=1&order=1&trc=921&sha=34b1760ca48a5c0068004ec43136ad5c6d912cc8