GAZI UNIVERSITY

FACULTY OF ENGINEERING – COMPUTER ENGINEERING

171180010 – Cansu AYTEN

CENG482 INTRODUCTION TO COMPUTER SECURITY

HOMEWORK 3

MARCH 2022

1. RISK

Risk is the sum of the probability of an event occurring and the probabilities of the effects of that event. It is the possibility of encountering negative consequences or being damaged due to any dangerous, harmful, bad, or undesirable event. Examples of these results are financial loss, loss of privacy, and sometimes loss of life. Uncertainties create risk.

Although the definition of risk differs for each area, the basis is always the same. According to the International Organization for Standardization (ISO) Guide 73, risk means "effect of uncertainty on objectives". The effect can be positive or negative. Objectives; health, finance, environment, goods, projects etc [1].

The definition of risk pertaining to information technologies is the possibility of a dangerous situation violating security or attempting to harm by taking advantage of the vulnerability. It is the possibility of harming important targets such as information, data, privacy and usability [1].

Three components are used when defining cyber security risk. These are threats, vulnerabilities, and consequences. Threats usually involve events that can harm systems made by criminal organizations, insiders, and some giants for financial gain and political purposes. Vulnerability is any state in which unauthorized users or attackers can gain access to a system. It is necessary to prevent these situations because if they do they can be exploited with bad effects. Finally, the consequence is the damage to the system as a result of an attack or event [2].

1.1 What are Mobile Application Security Threat Types?

Mobile application security threat types can be divided into four groups [3].

Mobile Application Security Threats: The permissions granted when downloading an app affect whether the app can access personal or business information inside the mobile device. There are applications that seem harmless to people, but that, when downloaded, access data on mobile devices that should not be accessed. Examples of these applications are malware or spyware.

Web-Based Mobile Security Threats: Although the entered site may seem innocent, it may contain malware behind it. In the case of entering the site, this software can be automatically installed on the phone as soon as you enter it, causing negative consequences on the phone.

Mobile Network Security Threats: It is necessary not to use free Wi-Fi networks in public places such as cafes and restaurants. This is because malicious people access unencrypted data over the same network.

Mobile Device Security Threats: It includes physical threats to the mobile device. For example, if a device is lost or stolen, it can be dangerous if it falls into the hands of malicious people.

1.2 Information Technology Risks

Examples of risks for Information Technologies [4,5]:

- Malware that disrupts the normal functioning of the system,
- Viruses that can disrupt processes and spread between systems,
- Stealing sensitive information,
- Hardware-software failure, data loss as a result of hardware or software failure,
- Damage to servers due to natural disasters,
- Vulnerable credentials,
- Human error such as incorrect data processing-carelessness, opening of virus-containing e-mails by people by mistake can be given.

2. RISK ASSESMENT

2.1 Threats

The table obtained as a result of the literature search for phone threats is given in Figure 1. This table contains a list of threats and CIA losses marked separately for each threat. C stands for confidentiality, I stands for integrity, A stands for availability. Most threats here also apply to my smartphone. Threats covered in the 2.4 title are T5, T10, T11, T13, T15, T17, T20.

Dimension	Threat	C	I	A
Network Connectivity	T1 Spoofing	✓	✓	✓
	T2 Scanning	✓		
	T3 Denial of Service, Network congestion			✓
	T4 Spam, Advertisements			✓
	T5 Eavesdropping	✓		
	T6 Jamming			✓
Device	T7 Loss, theft, disposal or damage	✓	✓	✓
	T8 Cloning SIM card	✓	✓	
	T9 Technical failure of device		✓	✓
Operating System	T10 Unauthorized device (physical) access	✓	✓	✓
	T11 Unauthorized Access	✓	✓	✓
	T12 Offline tampering	✓	✓	✓
	T13 Crashing			✓
Applications	T14 Misuse of Phone Identifiers	✓		
	T15 Electronic tracking/surveillance/exposure of physical location	✓		
	T16 Resource abuse			✓
	T17 Sensitive Information Disclosure (SID), Spyware	✓		
	T18 Corrupting or modifying private content		✓	✓
	T19 Disabling applications or the device			✓
	T20 Client Side Injection/ Malware	✓	✓	✓
	T21 Direct billing		✓	
	T22 Phishing	✓	✓	

Figure 1:Phone Threats [6]

2.2 Vulnerability

- **Poor Password Strength:** Malicious people can easily guess the password of users with weak passwords and gain access to the system of these users. If malicious people access the system in this way, they can access sensitive data. Therefore, bad password habits should be stopped. By not using weak passwords, avoiding predictable word types, and creating strong passwords of sufficient complexity, you can protect yourself from such threats. Two-factor authentication can help with this. Taking advantage of this technique when accessing applications will make it difficult for malicious people to access the system. With the authentication system that provides higher security, risks arising from passwords are minimized or even eliminated. Unauthorized access to a device using an authentication system can be prevented by face recognition and fingerprint recognition systems [3].

- **Unsecured Public WiFi:** Public and free Wi-Fi networks can be unsafe. One of the reasons is the encryption protocol used by networks. WEP, an old encryption protocol, is a weak protocol. Networks with this protocol can be easily hacked. This situation creates a problem in terms of data security. WPA, a more secure protocol, was designed due to the weaknesses of WEP. Another reason is connecting to a fake Wi-Fi network. People connecting to this fake Wi-Fi hotspot created by malicious people are at risk. The online traffic of connected victims can be monitored. This attack is called Man-in-the Middle (MITM) attack. In order to protect from such risks, it is necessary not to connect to public, free Wi-Fi. VPN can be used to avoid these risks [3, 8].
- **Out of Date Operating Systems:** A situation that allows attackers to access systems is out-of-date software and operating systems. Keeping it up-to-date will protect the system, as risks such as security vulnerabilities, if any, in operating systems will be fixed with the next patch [3].
- **End-to-End Encryption Gaps:** End-to-end encryption used by most platforms ensures secure communication in messaging applications. If this technology is available in the system, only the sender and receiver can access the messages. Data on the server is encrypted. Thus, it protects the privacy and ensures that data is safe. Not being encrypted means that attackers can easily access this data. Public, free Wi-Fi networks and some services that are not encrypted therefore pose a risk to users [3, 9].
- **Spyware, Malware Download:** Malware is software that causes seemingly innocent users to click on it and download it to the device. If such software is downloaded, it can access users' data. Some programs can be used to protect the device from such software. Thanks to these programs, malicious software is detected and eliminated [3].

2.3 Asset Impact

A phone contains many assets. These are;

- Applications and services,
- Private information such as location information, call history
- Financial assets,
- Device-resources,
- Connection etc.

From this point of view, it can be said that there are many types of information in mobile device. Some of the information in my phone is personal data. For example, my address, pictures, and

videos are in my personal information and are private. Another part is financial information, for example, my financial assets and transactions, my credit card numbers. Another part is authentication data. These could be my passwords, biometric data. The other is my data related to network connections. It contains information such as network history, MACs. Since I am a student, there is also information about my school. Examples of this could be programs, notes.

A vulnerability in authentication data could pose a risk to my financial or personal data. Any data being at risk from here may cause my other data to be at risk as well. Therefore, some of my data's effects have a High sensitivity level, some Moderate, and some Low sensitivity.

A High level indicates that corrective action should be taken as soon as possible. A Moderate level indicates that necessary action should be taken within a reasonable time. In Low, the system owner determines whether to take corrective action or not [7].

Data in Personal, Financial, Authentication, Connection types have High sensitivity level and important, while School type data has Low sensitivity level.

2.4 Risk Assessment Results

Threat	**Vulnerability**	**Likelihood**	**Impact**	**Risk**
T5	Unsecured Public WiFi	Low	High	High
T10	Poor Password Strength	Moderate	High	High
T11	Poor Password Strength, Out of Date Operating Systems	Moderate	High	High
T13	Out of Date Operating Systems	Moderate	High	Moderate
T15	Unsecured Public WiFi	Low	High	Moderate

T17	Spyware, Malware Download	High	High	High
T20	Spyware, Malware Download	Moderate	Moderate	Moderate

REFERENCES

1. Risk. (2022). *Wikipedia* https://en.wikipedia.org/wiki/Risk
2. Security Scorecard. (2021). What is Cybersecurity Risk? Definition & Factors to Consider. https://securityscorecard.com/blog/what-is-cybersecurity-risk-factors-to-consider
3. Gontovnikas, M. (2021). The 9 Most Common Security Threats to Mobile Devices in 2021. https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021
4. What is an information technology risk. (2020). https://www.business.qld.gov.au/running-business/protecting-business/risk-management/it-risk-management/defined
5. Sotnikov, I. (2022). How to Perform IT Risk Assessment. https://blog.netwrix.com/2018/01/16/how-to-perform-it-risk-assessment/
6. Theoharidou, M., Mylonas, A., & Gritzalis, D. (2012). A Risk Assessment Method for Smartphones. Information Security and Privacy Research, 443–456. doi:10.1007/978-3-642-30436-1_36
7. Brooks, R. (2022). Risk Analysis Example: How to Evaluate Risks. https://blog.netwrix.com/2020/04/07/risk-analysis-example
8. Johansen, A. (n.d). Public Wi-Fi security: Why public Wi-Fi is vulnerable to attack https://us.norton.com/internetsecurity-wifi-public-wi-fi-security-101-what-makes-public-wi-fi-vulnerable-to-attack-and-how-to-stay-safe.html
9. Berlove, O. (2021). What is end-to-end encryption & how does it work? https://securityboulevard.com/2021/03/what-is-end-to-end-encryption-how-does-it-work/