Risk Assessment in Smartphones: Comprehensive Analysis

Mohammed Nasereddin
King Hussein School for Computing Sciences
Princess Sumaya University for Technology
Al-Jubaiha, Amman, Jordan
moh20188020@std.psut.edu.jo

Abdallah Qusef
King Hussein School for Computing Sciences
Princess Sumaya University for Technology
Al-Jubaiha, Amman, Jordan
a.qusef@psut.edu.jo

ABSTRACT

Smartphones are multi-purpose and widely used devices in various fields, in terms of personal use, and companies and governments. Increasing dependence on them opened the way for increased violations on its users, as it became a fat substance for criminals, for their illegal practices, so it encountered serious and targeted security threats. This paper presents a set of rules and controls that will reduce the risks that threaten smartphone users. Furthermore, this work provides the methods of risk assessment that are related to smartphones. It identifies the assets and lists several different threats that are relevant. Each risk has its impact on the assets, this is described by mapping it with the likelihood of each threat.

CCS CONCEPTS

• **Security and privacy → Security requirements**; • **Information systems → Mobile information processing systems**.

KEYWORDS

Risk assessment, Risk management, Information Security, Smartphones, Threats.

ACM Reference Format:
Mohammed Nasereddin and Abdallah Qusef. 2021. Risk Assessment in Smartphones: Comprehensive Analysis. In *International Conference on Data Science, E-learning and Information Systems 2021 (DATA'21), April 5–7, 2021, Ma'an, Jordan.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3460620.3460737

1 INTRODUCTION

Through the big revolution and development in interconnected networks such as the internet, the need of having the concept of mobility is also increased as well, so smartphones are now widely used all over the world as the studies show that almost every person has at least one mobile phone [7]. When technology is spread and developed, the vulnerabilities are increased at the same level, especially when the target is smartphones because they are used by many different types of people and ages, so the knowledge and awareness is different between them, this leads us to understand the estimated risks and threats on these devices. The dependence on smartphones has increased significantly these days, due to their small size and high capabilities in terms of data processing, communication, and hosting of third-party applications, while not neglecting its low price, which is a high advantage. Smartphone users use it throughout the day from different places and on different networks that aren't followed the terms of protection most of the time. Also, the diverse use of the phones is due to personal and business matters, and therefore contains a lot of sensitive data that is subject to violation. The use of smartphones has increased greatly in the world, as it has become an alternative to the desktop. Statistics have shown that a total of 3.2 billion people around the world owned smartphones in 2019, and the number is increasing tremendously, and it is expected that the number will reach 7.33 billion by 2023 [8], as most companies are now producing their applications and allowing their employees Dealing with all data by phone. Methods of risk assessment on smartphones are considered as the phone is one of the assets in an information system, it is classified as an entity, just like a personal computer and servers, where the process of assessing Vulnerabilities and threats on all system assets, which were developed mainly for companies [3]. Our Work: In this research, we will show the common risks and their threats on mobiles, specifically smartphones, with the impact for each of them and showing the likelihood, and the proposed solutions, as the work that is done covers almost all of the risks, vulnerabilities, and threats that are available in the smartphones' world. However, what isn't mentioned in the previous works [1, 2, 5, 6, 9] is doing a comprehensive analysis of all the countermeasures for each threat and how to reduce, mitigate the impact of the risk, which is very important for the users to understand how they can deal with the risk after identifying the assets that might be affected by the risk, or even understand the behaviors and actions that must be taken into consideration in order not to let the attacker exploit the vulnerability and compromise the data or the device itself. Studying risk types and the vulnerabilities in smartphones help the researchers classify the risk categories and put the solutions that help in managing and reducing the risks as much as possible, both on the technical side of the user behavior side.

The rest of this short paper is organized as follows; Section 2 reviews the background information of smartphones, assets, and data classification, then Section 3 explains the risk assessment process in terms of identifying threats and linking them to assets and their impact on them. Section 4 introduces the proposed controls for smartphone risks, and finally Section 5 concludes the papers.

2 LITERATURE REVIEW

In this section, we show the important terms that we will use during the research, in addition to the classification of the assets of smartphones, and data.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

DATA'21, April 5–7, 2021, Ma'an, Jordan
© 2021 Association for Computing Machinery.
ACM ISBN 978-1-4503-8838-2/21/04…$15.00
https://doi.org/10.1145/3460620.3460737

Table 1: Classification of Data

Type of Information	Personal	Financial	Business	Government	Authentication
Messaging	Fully	Fully	Fully	Fully	Fully
USIM Card	Some	Some	Some	Some	Fully
Device	Fully	Fully	Fully	Fully	Fully
Applications	Fully	Fully	Fully	Fully	Fully
History & Catching	Fully	Some	Some	Some	Fully
Sensors	Fully	-	Fully	Fully	-
Input method	Fully	Fully	Fully	Fully	Fully

2.1 Initial Definition

The term "Smart" means that the device provides information right when the user needs it and can present it in a more useful way, this is accomplished through Applications. This word "Smart" has two sides [1], a good one that lets the device behave smartly with the user to help the user achieve the work he wants or even achieve his entertainment, the other side which is the bad side that the device is vulnerable to several attacks whether on the operating system or on the hardware itself.

2.2 Smartphones Assets

Now we have to identify the assets of the smartphones, as the asset can be identified by objectives of the attack [5] that are focused on threats and vulnerabilities. We can classify smartphone assets into the main four types:

(1) Data- information (i.e. Address book, photos gallery).
(2) Device (i.e. resources, like CPU, RAM).
(3) Applications and services.
(4) Connectivity channels: GSM services, Cellular networks, WLANs.

2.3 Classification of data

We can classify the data according to the two dimensions: Type of information, and the source. Table 1 shows the association of these dimensions that will be used later on to show the data impact valuation. After studying the table, we notice that personal data are directly related to the individual and this type of data is private and should only be known by the user, this includes the user's images, contacts…etc. As for financial data, it contains transactions, current financial status. Leakage, amendment, or loss of availability could result in economic loss or breach of contract. Disclosure of this data may lead to loss of confidence, legal action, and embarrassment. Business data reflect the data that is related to a specific work or contains information about the individual's job, which is usually found on the personal phone. Government data affects the relations, locally or internationally, and Government service organizations, this data is different than the business data because of its effects internationally. Due to the high importance of this data, any leakage with or without intention can, in addition to the loss of competitive advantage, have a severe impact locally and internationally. Authentication data refers to credentials or the rights that the user has to enter or use the resource, such as PINs, Passwords, etc… Leaking can lead to economic losses and legal consequences.

3 RISK ASSESSMENT PROCESS IN SMARTPHONES

To assess the risks on smartphones, the impact of its assets should first be assessed. These assets are then linked to threats that could threaten their security.

3.1 Asset Impact

First, the user must be involved in the initial impact assessment process. To measure the total risk, the risk analyst will then execute straightforward associations and aggregations. On the classified assets:

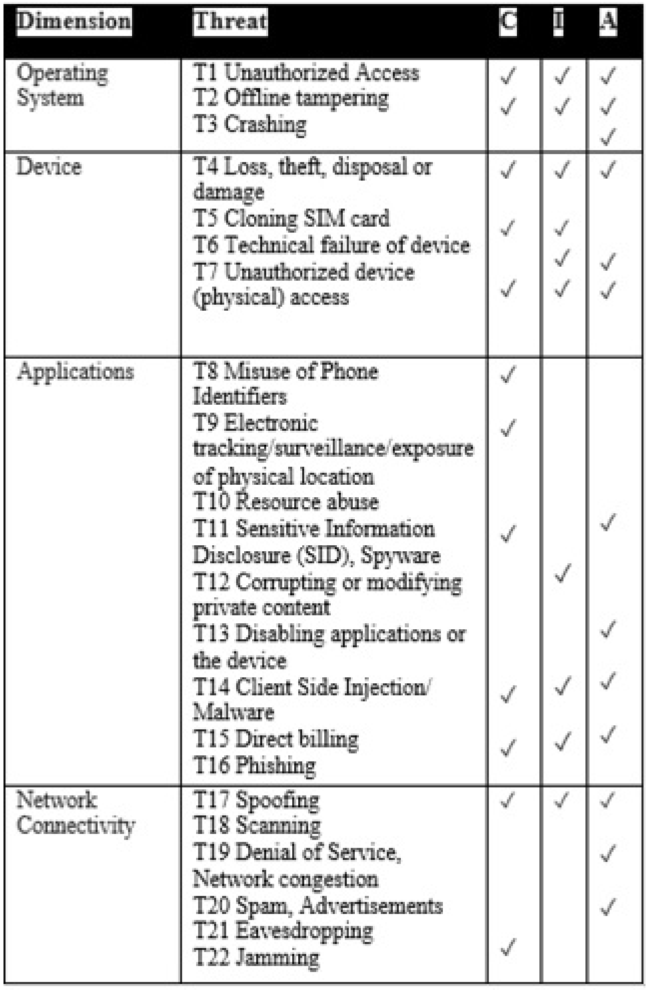
(1) Data: A Disclose, modification, or availability of the data can be evaluated by a variety of factors. ie. financial damage, international relations, public safety, processes, and business policy.
(2) Device: Physical assets, as regards replacement or reconstruction costs, are quantitatively evaluated in typical risk assessment methodologies. In case of loss, robbery, or damage, this refers to a smartphone's cost of replacement or repair. However, a smartphone also contains various kinds of information that needs to clarify about impact.
(3) Applications: This is intended for the importance of each application that is installed on the device of the user and its impact when it's compromised or modified, the assessment should take into consideration each application. Also, It often assumes that a user is informed regarding the value of an application, for example, use the program for a while. The evaluation of applications that the user deems most important may be a compromise. The assessment will adopt the same evaluation tables per procedure.
(4) Connectivity channels: The connectivity reflects the ability for the user to use the network, for example considering the consequences when the user is not able to make a phone call or even send an SMS, also what are the repercussions when an attacker catches the network (Wi-Fi) that the consumer uses and sends the information? The evaluation must confirm with the same valuation tables.
(5) Overall impact valuation: After the analyst assesses the four assets according to the impact of different scenarios (Disclosure, modification, and availability), these values should be compiled and used to assess the impact of all four asset classifications.

3.2 Threats

Threat likelihood can be assessed using the following:

(1) Experience, knowledge, and applied statistics.
(2) Vulnerabilities.
(3) Current controls, as well as how effectively they can reduce vulnerabilities [3].

This section introduces a smartphone threat list and discusses how to assess the threat likelihood. In Figure 1, a threat list is diplayed to expand the lists that are available in the previous works [3–5, 9, 10]. Threats are divided into suitable attack dimensions. The security aspect (C: Confidentiality, I: Integrity, A: Availability) which affected or weakens is associated with its threat. The permission acceptance in smartphones depends on the decisions of authorization [10], where it differs from computers, as accredited by the security model.



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

Figure 1: List of Threats

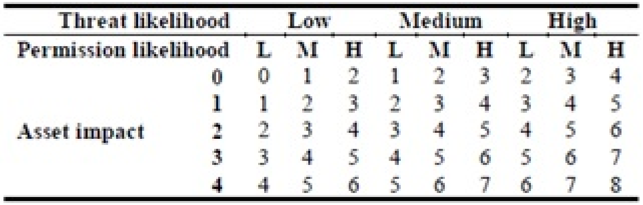
3.3 Risk Determination

Risk in the smartphone world is considered a risk if it uses one or more of the vulnerabilities that are defined to compromise or affect the smartphone asset. The threat is determined by:

(1) The threat incident likelihood, in addition to permission combination for dangerous functions required [9].
(2) It's the impact on the asset through exploits the vulnerability.

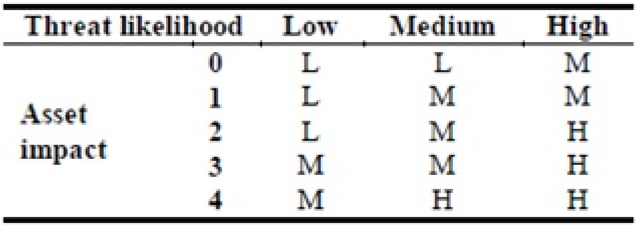
The well-known risk matrix is used to determine the risk quantitatively, which is represented by (0-2), Medium (3-5), or High (6-8). Where the risk is calculated, for example, for the 'Sensitive Information Disclosure' threat, on the asset "Messaging" by affecting Confidentiality. Figure 2 illustrates the process.

As for the risks that cannot be quantitatively linked with specific permissions, such as Spoofing, Spam, Jamming, the risks are calculated qualitatively through the use of expertise or statistics. Figure 3 illustrates the process.



Threat likelihood		Low			Medium			High		
Permission likelihood		L	M	H	L	M	H	L	M	H
	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
Asset impact	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Figure 2: Quantitatively Risk Matrix



Threat likelihood		Low	Medium	High
	0	L	L	M
	1	L	M	M
Asset impact	2	L	M	H
	3	M	M	H
	4	M	H	H

Figure 3: Qualitatively Risk Matrix

4 PROPOSED CONTROLS AND AWARENESS FOR SMARTPHONES RISKS

After studying the various types of risks that might affect any smartphone negatively regardless of its operating system, here we present some proposed controls that must be taken into account to avoid several of the risk dimensions and their impact on the assets as much as possible.

4.1 Device Dimension

Theft/Loss of smartphone: In this case, the mobile phone must be locked using a pin code, and the best practice is to put a lock code on every application or the important applications that contain sensitive information only, also the phone must have the ability to be wiped remotely after being stolen(by using a mobile application that can do so) so the stealer cannot access the data, these countermeasures can be taken into consideration after the device has been stolen but the data and the important information must be saved somewhere or enable auto synchronization with the cloud or the main account of the device. Device Infection: The device might be infected by viruses or spyware applications that are installed unintentionally, to avoid that the user has to do the following:

(1) Keeping the smartphone up to date.
(2) For some operating systems that allow installing the applications from unknown sources, the user should disable the "Allow installation from unknown sources".
(3) When the application asks the user to give it permissions, the user has to make sure that the application is not requesting extra or unneeded permissions.
(4) Spreading smartphone security awareness among ordinary users.

4.2 Applications Dimension

Infecting the device by applications: This could happen if some applications are installed from an untrusted source or the application itself contains a virus or malware, to avoid that the user can do the following:

(1) Keeping the applications up to date, given that the developers of these applications updated them continuously and strengthen the protection aspect.
(2) Install applications from a reliable site.
(3) Awareness of not installing the applications from unknown sources, by disabling the "Allow installation from unknown sources".
(4) When the application asks the user to give it permissions, the user has to make sure that the application is not requesting extra or unneeded permissions.
(5) Use security applications (i.e. antivirus).

4.3 Operating System (OS) Dimension

Most of the devices today provide operating-system-level encryption either enabled by default or as an option, but this is not enough and does not prevent the users from sharing information, so one of the effects that could affect the operating system is: Compromise the OS: Some attackers can reach the operating system in different ways, so the user should:

(1) Use safe and secure file sharing.
(2) The user shouldn't allow the information synchronization to be enabled unless the user trusts the cloud and makes sure that no one can access it.
(3) The user must ensure the ability to restore data when the OS is corrupted or compromised.
(4) The user must ensure the ability to wipe the device and erase every piece of information.
(5) Frequently check the installed applications, because some applications work in the background thread of the OS, and may not be seen in the running tasks.

4.4 Network Connectivity Dimension

The Sniffing happens when there is an attacker in the middle of the connection between the device and the network who can receive the data transmitted over the network and take a look at it or modify the content of the data then retransmit the data to the recipient, this could be avoided by:

(1) The user must be aware of using a secure network and avoid connecting to anonymous networks such as public Wi-Fi because he/she would be vulnerable to penetration by anyone on the same network.
(2) To increase the security of data sent over the network, data can be encrypted before it is transmitted.

5 CONCLUSIONS AND FUTURE WORK

In this short research, the risks and threats of smartphones are presented with the guidelines of the assessment of these mentioned risks. Moreover, the assets of the smartphones are defined and put with the likelihood of impact for each asset, in addition to the countermeasures proposed for the threats and how to try to reduce them and get over the vulnerabilities.

Future work can be developed to include a broader analysis of the risks affecting smartphones, linking threats and vulnerabilities to assets, to access information systems containing controls that minimize the impact of risks more and more. Taking into account the continuous tremendous technological development.

REFERENCES

[1] Michael Becher, Felix C Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, and Christopher Wolf. 2011. Mobile security catching up? revealing the nuts and bolts of the security of mobile devices. In *2011 IEEE Symposium on Security and Privacy*. IEEE, 96–111.

[2] William Enck, Damien Octeau, Patrick D McDaniel, and Swarat Chaudhuri. 2011. A study of android application security.. In *USENIX security symposium*, Vol. 2.

[3] International Organization for Standardization. 2008. ISO/IEC 27005:2008 Information technology — Security techniques — Information security risk management. https://www.iso.org/standard/42107.html

[4] Wayne Jansen and Karen Scarfone. 2008. Guidelines on cell phone and PDA security. *NIST Special publication* 800 (2008), 124.

[5] Woongryul Jeon, Jeeyeon Kim, Youngsook Lee, and Dongho Won. 2011. A practical analysis of smartphone security. In *Symposium on Human Interface*. Springer, 311–320.

[6] Thomas Lederm and Nathan L Clarke. 2011. Risk assessment for mobile devices. In *International Conference on Trust, Privacy and Security in Digital Business*. Springer, 210–221.

[7] D Metev. 2020. 39+ smartphone statistics you should know in 2020. *Review* 42 (2020), 39.

[8] M Milijic. 2020. 29+ Smartphone Usage Statistics: Around the World in 2020. https://leftronic.com/smartphone-usage-statistics/

[9] Asaf Shabtai, Yuval Fledel, Uri Kanonov, Yuval Elovici, Shlomi Dolev, and Chanan Glezer. 2010. Google android: A comprehensive security assessment. *IEEE Security & Privacy* 8, 2 (2010), 35–44.

[10] Shigeaki Tanimoto, Susumu Yamada, Motoi Iwashita, Toru Kobayashi, Hiroyuki Sato, and Atsushi Kanai. 2016. Risk assessment of BYOD: Bring your own device. In *2016 IEEE 5th Global Conference on Consumer Electronics*. IEEE, 1–4.