BKH1825010F

by Iftekhar Efat

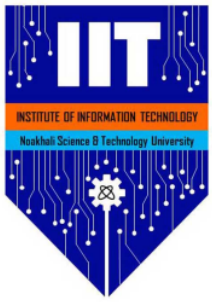
Submission date: 13-Mar-2022 03:02AM (UTC-0400)
Submission ID: 1782992215
File name: BKH1825010F.pdf (416.72K)
Word count: 2267
Character count: 12395

Major issues associated with the online mobile security which is given to the people

Sanzida Sultana
BKH1825010F

March 13, 2022

Report submitted for **CSE2205: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University



Project Area: **Information Security .....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

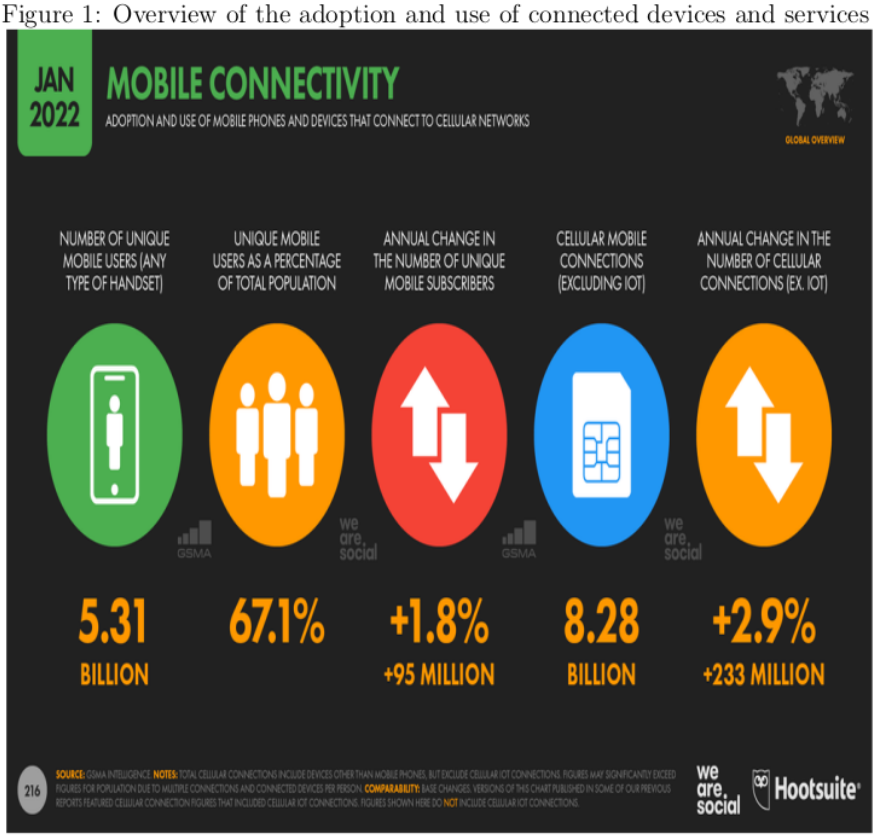
Abstract

Mobile devices have become an increasingly vital component of many organizations' IT infrastructure.The fast advancement of smartphone technology and Internet services in mobile devices allows for convenient access to online social networking (OSN) sites anytime, anywhere.Mobile security threats are assaults on mobile devices such as smartphones and tablets that aim to compromise or steal data. Malware or spyware are frequently used to provide bad actors illegal access to a device; in many cases, users aren't even aware that an attack has occurred.

1 Introduction

Current age is considered as the age of mobility. Modern mobile devices provide users with constant internet access to social sites, allowing them to locate the quickest way to a coffee shop, bank, hospital, or tourist attraction, as well as run their businesses.. Mobile devices are having applications for every activity of human life. Mobiles are used to perform bank transactions, and sensitive data transfer in the form of E-mails, messages, etc. Mobile devices are used to connect with family and friends through social networks. There are 5.31 billion unique mobile phone users in the world today, according to the latest data from GSMA Intelligence [6].

Figure 1: Overview of the adoption and use of connected devices and services



Most popular operating systems used in mobile devices are Android and iOS, Windows phone OS, and Symbian.There are different versions of Android operating systems like Nougat, Lollipop, Marshmallow, etc., similarly different versions of iOS are iOS 10, iOS 9, iOS 8, etc. Compared to iOS 86 percent only 11percent of An-

droid mobile users having the latest Android operating system.From the early nineteenth century to date, the development of mobile devices boosts massively.Today's smart phone Operating System (OS) allows other software to run on the phone to provide diverse functionalities to the users. Moreover, unfortunately, security and privacy are not one of the main targets of many small to big 3rd party app developers [2].Unsecure data storage and insecure communication risks are the most serious challenges in mobile security, according to the Open Web Application Security Project (OWASP)[4]

In 2014, Kaspersky discovered about 3.5 million malware pieces on over 1 million handsets. Kaspersky's in-lab detection systems processed 360,000 suspicious files per day by 2017. And 78 percent of the files were malicious software, resulting in daily detections of approximately 280,000 malware files, many of which target smart phones.[3].

In this report , we described some significant major issues associated with the online mobile security which is given to the people.

2 THE SPECTRUM OF MOBILE RISK

The Mobile Risk Matrix was developed by Lookout to help organizations comprehend the components and vectors that make up the mobile risk spectrum, as well as to give statistics that will allows enterprises better understand the presence and impact of mobile threats and vulnerabilities.

Figure 2: The moblie risk matrix

3 Top security issues of smartphones

According to OWSAP some of the top mobile risks are insecure data storage and insecure communications[5].

3.1 Data Leakage

Unintentional data leaking is frequently caused by mobile apps. According to Pargman, every mobile application gathers data from device. Name, date of birth, credit card and bank account information, location tracking, contact list, photographs, and more might all be included. If the systems are compromised or become exposed due to a technological issue, all of that information can be taken and utilized by crooks to commit fraud.

3.2 Unsecured Wi-Fi

When wireless hot spots are accessible, no one wants to waste their cellphone data—but free Wi-Fi connections are frequently insecure. Anyone nearby might simply snoop on all of your internet activities if anyone connect to open WiFi. Three British MPs who consented to take part in a free wireless security experiment, according to V3, were easily hacked by technical experts. Their social networking accounts, PayPal accounts, and even VoIP chats were all hacked. To be secure, only use free WiFi on smart phone when absolutely necessary. And never use it to get access to private or confidential details, such as banking or credit card numbers.

3.3 Malicious applications

An software may look to be beneficial provides free access to something that should be paid for but it really includes a malware. "People who fall for the hook and download these dangerous applications are frequently astonished to discover that instead of the promised free content, their whole device is locked, their value is collected, and they are threatened."

3.4 Network Spoofing

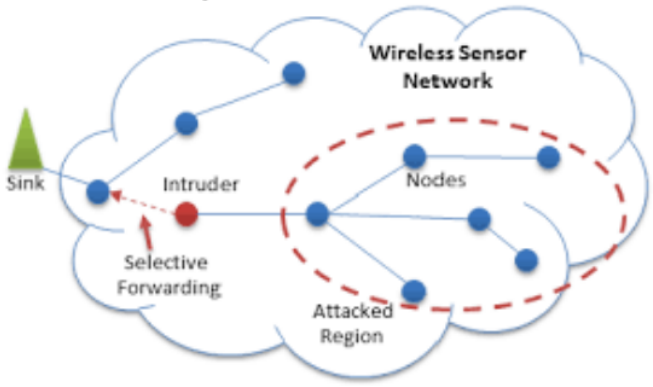
In high-traffic public places like cafés, universities, and airports, criminals put up false entry points that appear to be Wi-Fi networks but are actually hooks. To entice people to connect, fraudsters offer the connection points names like "Free Airport Wi-Fi" or "Coffeehouse." In certain circumstances, fraudsters ask people to create a "account" with a pin in order to use these free services. Attackers can compromise users' email, e-commerce, and other confidential material since many users use the same email and password combination for multiple accounts.

3.5 Blackhole Attacks

In a wireless sensor network, a black hole attack happens when an intermediate captures and re-programs a collection of nodes to block/drop packets and create false

messages instead of transmitting correct/true information to the base station. This attack can also be carried out selectively, with packets for a specific network target being dropped at a specific time of day. The action is referred to as a greyhound attack. If the infected router tries to delete all incoming packets, the attack may be detected rather fast using simple networking tools like traceroute. When other routers detect that the hacked router is losing all traffic, they will usually start removing it from their forwarding tables, and finally no traffic will be routed via it.

Figure 3: Blackhole attacks



4 The top ten security threats for mobile devices according to OWASP:

OWASP stands for Open Web Application Security Project. The OWASP Foundation is a non-profit organization dedicated to enhancing the security of online applications and associated technologies throughout the world. Every year, OWASP provides a list of the top 10 web application vulnerabilities. The list was first published in 2007 and has subsequently been upgraded. It covers everything from basic programming to cyber-attacks. Although these are not the only risks that software developers should be aware of before deploying an app into production for usage by customers, clients, and workers, they are the most prevalent [1].

4.1 Broken Access Control

A system that regulates access to information or functionality is alluded to as access control. Access protections that are weak allow attackers to evade authorisation and conduct actions as privileged users like administrators. Failures frequently result in unauthorized information disclosure, alteration, or loss of all data, as well as the execution of a business function outside of the user's capabilities.

4.2 Insufficient cryptography

Many online services and APIs do not use robust encryption to secure sensitive data. In order to commit credit card fraud, identity theft, or other offences, hackers may steal or manipulate such poorly secured data. At rest and in transit, confidential data must be encrypted using a current (and suitably configured) cryptographic techniques.

4.3 Injection

When untrusted information is supplied to a software interpreter via a form input or other data submission to a web application, an injection attack occurs. An adversary may put SQL database code into a form that requires a plaintext username. If the form content is not sufficiently protected, the SQL code will be run. An SQL injection attack is what this is called.

Figure 4: Broken access control

4.4 Insecure Design

Insecure Design is a new category for 2021, focusing on dangers associated with design defects. We need more threat modeling, safe design patterns and concepts, and reference architectures if we actually want to "move left" as an enterprise. Because appropriate security safeguards were never built to fight against specific threats, an insecure design cannot be solved by a perfect application.

4.5 Security Misconfiguration

The most prevalent risk on the list is security misconfiguration, which is frequently the result of utilizing default setups or giving too verbose errors. For example, a software may provide overly-descriptive failures to a user, which may indicate program faults. Dynamic testing can aid in the discovery of security flaws in your app.

4.6 Vulnerable and Outdated Components

In web applications, many professional web developers include components like libraries and frameworks. Front-end frameworks like React and smaller modules used to add share icons or a/b testing are examples of these components; they allow developers reduce duplicate code and provide key features.

4.7 Identification and Authentication Failures

An attacker can execute functionality within the mobile app or the backend server utilized by the mobile app anonymously if security protocols are poor or lacking.Poor authentication for smartphone apps is quite common due to the input form factor of a smartphone.Simple passwords, generally based only on 4-digit PINs, are heavily encouraged by the form factor.

4.8 Software and Data Integrity Failures

Programs and infrastructure that do not guard against integrity violations are referred to as software and data integrity failures. A program that uses plugins, libraries, or modules from untrusted sources, repositories, or content delivery networks is an example of this (CDNs). Unauthorized access, malicious code, or system compromise can all be risks of an unsecured release pipeline. Finally, many programs now have auto-update features, which allows upgrades to be obtained without necessary integrity checks and deployed to previously trustworthy software.

4.9 Security Logging and Monitoring Failures

Inadequate logging and monitoring, along with lacking or inadequate incident response functionality, enables hackers to continue attacking networks, retain persistence, pivot to new devices, and modify, remove, or delete data. Most breach studies suggest that it takes over 200 days to notice a breach, which is usually found by third parties rather than internal processes or monitoring.

4.10 Server-Side Request Forgery

When a web application accesses a remote service without verifying the user-supplied URL, it is vulnerable to Server-Side Request Forgery (SSRF) issues. Even when secured by a firewall, VPN, or another sort of network access control list, it permits an intruder to force the program to submit a forged request to an unintended location (ACL).

5 Conclusion

The amount of smartphone device security risks is growing, and their reach is expanding. Users must grasp typical attack vectors and prepare for the next generation of malicious activities in order to secure their systems and sensors. Only 20% of Android smartphones have the most recent version, and only 2.3 percent have the most recent release. Everything from the operating system to social media applications may be used by intruders to get access to smartphones devices. Updating software provides the best defense against the majority of mobile security risks. Malicious malware installed on the client system, as well as assaults launched remotely across the network, might compromise user authentication. We could eliminate attacks leveraging the weakness of the client computer if trustworthy platforms for mobile devices could supply the trust environment.

References

[1] Radhwan M Abdullah, Abedallah Zaid Abualkishik, Najla Matti Isaacc, Ali A Alwan, and Yonis Gulzar. An investigation study for risk calculation of security vulnerabilities on android applications. *Indonesian Journal of Electrical Engineering and Computer Science*, 25(3):1736–1748, 2022.

[2] Rebecca Balebako and Lorrie Cranor. Improving app privacy: Nudging app developers to protect user privacy. *IEEE Security & Privacy*, 12(4):55–58, 2014.

[3] Alexander Gostev, Roman Unuchek, Maria Garnaeva, Denis Makrushin, and Anton Ivanov. It threat evolution in q1 2016. *Kapersky 2015 Report, Kapersky L*, 2016.

[4] Shubham Kumar Lala, Akshat Kumar, and T Subbulakshmi. Secure web development using owasp guidelines. In *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pages 323–332. IEEE, 2021.

[5] PMD Nagarjun and Shaik Shakeel Ahamad. Review of mobile security problems and defensive methods. *International Journal of Applied Engineering Research*, 13(12):10256–10259, 2018.

[6] Niall Winters. Mobile learning in the majority world: A critique of the gsma position. *The SAGE handbook of digital technology research*, 10(9781446282229):n27, 2013.

BKH1825010F

ORIGINALITY REPORT

51%	31%	4%	44%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.ripublication.com Internet Source	6%
2	v1.overleaf.com Internet Source	4%
3	snyk.io Internet Source	4%
4	Submitted to Modern College of Business and Science Student Paper	3%
5	Submitted to The Hong Kong Polytechnic University Student Paper	2%
6	Submitted to Liverpool John Moores University Student Paper	2%
7	Submitted to Taylor's Education Group Student Paper	2%
8	core.ac.uk Internet Source	2%

9	Submitted to Edith Cowan University Student Paper	2%
10	Submitted to Middle East College of Information Technology Student Paper	2%
11	Submitted to Computer College Student Paper	2%
12	global.oup.com Internet Source	2%
13	preprod.rd.com Internet Source	2%
14	Submitted to Australian Institute of Higher Education Student Paper	2%
15	Submitted to University of Hertfordshire Student Paper	2%
16	Submitted to Kaplan University Student Paper	2%
17	Submitted to Sri Lanka Institute of Information Technology Student Paper	1%
18	www.coursehero.com Internet Source	1%
19	Submitted to University of Waikato Student Paper	1%

20	www.cloudflare.com Internet Source	1 %
21	datareportal.com Internet Source	1 %
22	journal.uad.ac.id Internet Source	1 %
23	Munmun Bhattacharya, Sandip Roy, Ashok Kumar Das, Samiran Chattopadhyay, Soumya Banerjee, Ankush Mitra. "DDoS attack resisting authentication protocol for mobile based online social network applications", Journal of Information Security and Applications, 2022 Publication	1 %
24	Submitted to Nottingham Trent University Student Paper	1 %
25	Submitted to University of North Texas Student Paper	1 %
26	Submitted to American Public University System Student Paper	1 %
27	www.publicnow.com Internet Source	1 %
28	Submitted to Kingston University Student Paper	<1 %

29	itseg.org Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

BKH1825010F

PAGE 1

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

PAGE 3

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Confused You have used **An** in this sentence. You may need to use **a** instead.

PAGE 4

Article Error You may need to remove this article.

Wrong Form You may have used the wrong form of this word.

PAGE 5

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Missing "," You may need to place a comma after this word.

PAGE 6

Missing "," You have a spelling or typing mistake that makes the sentence appear to have a comma error.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Missing "," You may need to place a comma after this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Article Error You may need to use an article before this word.

Confused You have used **An** in this sentence. You may need to use **a** instead.

Confused You have used **a** in this sentence. You may need to use **an** instead.

PAGE 7

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

PAGE 8

Confused You have a spelling mistake near the word **An** that makes **An** appear to be a confused-word error.

PAGE 9

Article Error You may need to use an article before this word. Consider using the article **the**.

Wrong Form You may have used the wrong form of this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 10

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Confused You have used **An** in this sentence. You may need to use **a** instead.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

PAGE 11
