International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 12 Issue 8, August-2023, Impact Factor: 7.957

A study on attack and security in wireless Smartphone communication systems

Rakesh Kumar

ABSTRACT

Background: This Paper based on original research. Digital attack on mobile in Wireless mobile communication Technique has a bad effect on the livelihood and health of the family apart from the tragic loss of an economic situation and personal properties. Every year about 30% of smart phone users fall victim to this attack. This issue has been the subject of research for the past several years. To solve this problem and to test it has been studied very well. Suggestions for solutions are available. Suggested that there are three primary attack vectors for mobile phones. The first is when a mobile phone connects the internet; the second is when a mobile phone connects to a network; the third is when a mobile phone is stolen or forgotten. After connecting through this medium, the attacker attacks in the following way: Trajan, Spyware, Botnet, which is the app, the Smartphone user unknowingly downloads. Due to which the user's smart phone becomes a victim of the attacker.

Objective: To study the attack on Smartphone through wireless communication medium and to suggest security against this attack and to make people aware so that this dangerous attack can be avoided ***Method***. To study the wireless communication attack on smart phones, we have studied as follows: Based on the primary data, anonymous interviews were conducted. And read research articles based on secondary data.

Survey Report*:* In order to avoid Smartphone attack, it has been suggested in this paper that if any kind of greed is given to the smart phone user while sitting at home, then he should be cautious and also understand that no one gives anything to anyone easily. And whatever wireless mobile communication attacks happen, they are for money.

Conclusion: In this research paper, we have suggested the first aid to avoid the attack, how the attack can be avoided.

Keyword- Mobile Security, Smartphone, Malware, Botnet, Spyware, Phishing, Spam.

INTRODUCTION

Recent years have shown a significant increase in the popularity and ubiquity of mobile devices among users all around the globe [1]. In today's days, all humans keep smart phones. And all humans keep personal data in their smart phones. But the problem is this. When personal data is not safe in your smart phone, and no person can be sure that the data has not been seen by anyone else. This is a big problem. We want that the person to whom the data is sent should only go to that person. But for some reason the data is also collected by unauthorized persons. Operating systems may be out-of-date: Security patches or fixes for mobile devices' operating systems are not always installed on mobile devices in a timely manner.

It can take weeks to months before security updates are provided to consumers' devices. Example: From a person's smart phone, the secret user ID & password of the app is stolen and misused by another person. Smartphone users download malware by mistake while downloading an app, or download an app with malware. Due to which malware comes in his mobile. For this reason unauthorized persons start misusing the data. It is difficult for users to tell the difference between a legitimate application and one containing malware.

Mobile communications offer wireless connectivity that enables mobility and computing in many different communication environments. In an information society, availability, integrity and confidentiality are essential. Wireless transmissions are not always encrypted: Information such as e-mails sent by a mobile device is usually not encrypted while in transit. Mobile devices often do not limit Internet connections: Many mobile devices do not have firewalls to limit connections.

In addition, many applications do not encrypt the data they transmit and receive over the network, making it easy for the data to be intercepted. For example, an application could be repackaged with malware and a consumer could inadvertently download it onto a mobile device. Communication channels may be poorly secured: Having communication channels, such as Bluetooth communications, "open" or in "discovery" mode (which allows the device to be seen by other Bluetooth-enabled devices so that connections can be made) could allow an attacker to install malware through that connection, or surreptitiously activate a microphone or camera to eavesdrop on the user.

Therefore, we put forward the three following research questions:

RQ1. By using which technology does the attacker attacks someone's smart phone?
RQ2. What are the primary techniques to avoid attacks on smart phones?
RQ3. How many types of attacks do attackers make on smart phones?

To answer RQ1, we performed a literature review based on a combination of the keywords ― botnet,‖ ―threat,‖ and ―spyware‖ in an electronic search with Google web search engine and Google Scholar. These two platforms promptly rose to become dominant providers of information and scholarly literature.

To answer RQ2, we have secretly interviewed the Smartphone attackers.
To answer RQ3, we interviewed twelve random ATM machines using convenience sampling combined with non probability sampling. First told about myself that I am doing a survey to ask you some questions

The remaining part of this research paper is structured as follows. Section 2 presents the work done earlier in order. Section 3 Brief description of malware attack on Smartphone phones, Section 4 shows a comprehensive report of attacks and defenses made on smart phones. Section 5 presents the conclusion.

REVIEW OF LITERATURE

(1) N. Leavitt (2011) suggested that there are two primary attack vectors for mobile phones. N. Leavitt The first is when a mobile phone connects the internet; the second is when a mobile phone connects to a network. Because too much individual and financial data is being stored on a phone, this is making the mobile phone environment more and more appealing to hackers. 2010 saw a 46% boost in mobile phone security, according to McAfee Labs, and every day, more than fifty five thousands (55,000) new mobile malware variants are discovered there [4].

(2) K. Marko, (2011), while PCs are increasingly being used to establish mobile botnets, the main goal of mobile malware is to steal money and personal information. Similar to the emergence of android botnets, this issue has been a topic of discussion for the past year [5]. Due to the mobile nature of smart-phones, the aforementioned blogger, Marko, properly compares the concept of an Android botnet to a salesman who is on the road and infected with tuberculosis.

(3) Paweł Weichbroth, Łukasz Łysik (2019), It mainly discusses authentication in relation to mobile security. In this research paper, the survey method has been used to bring the report in percentage for the security of all types of authenticity [6]

(4) B. Guo, Y. Ouyang, T. Guo, L. Cao, and Z. Yu, (2011), These devices, based on a specific operating system, enable users to install a vast variety of Applications, commonly referred to as “apps,” from online sources called markets: Apple App Store, and Google Play [7].

(5) S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, (2011), The aforementioned apps are the essence of Smartphone, enriching their functionality and enhancing the everyday lives of their users. The app markets allow users to perform a quick search and installation of new apps, but at the same time, they are also a source of deferent kinds of malware disguised as normal apps. Nowadays, mobile devices are subject to a wide range of security challenges and malicious threats [8].

(6) A. Papageorgiou, The mobile revolution has empowered and impounded users to move almost all of their everyday operations into the mobile environment and so-called mobile applications. Hence, we can observe rapid growth in the domains of both mobile developers and users. Mobile devices are treated by their users as very personal tools, mainly used to facilitate everyday operations, but they also serve to store very sensitive personal information [9].

(7) G. Delac, M. Silic, and J. Krolo, In recent years, mobile applications have had to face a wide variety of external and internal security threats [10]. To address this growing issue, both research studies and business organizations have developed and promoted best practices to this extent. However, to the best of our knowledge, there are few (if any) comprehensive studies which diagnose the status of knowledge within this domain from these two antagonistic objectives. Therefore, the goal of this study is to identify and analyze security threats to mobile applications on the one hand and contemporary best practices on the other hand.

(8) D. He, S. Chan, and M. Guizani In recent years, mobile applications have had to face a wide variety of external and internal security threats [11]. To address this growing issue, both research studies and business organizations have developed and promoted best practices to this extent.

(9) P. Weichbroth, Secondly, security is a subject of study from two perspectives: technical and human factors the former focuses on the development of the systems, methods, and techniques which aim at mitigating risks associated with application code, user data, network trace, and others, as well as, on the contrary, testing and evaluating existing mechanisms and solutions. The latter examines the relationships between security and factors such as design and human disabilities [12].

(10) Raj Kumar Patel, Dr. Lalan Kumar Singh , Dr. Narendra Kumar, Risks usually connected with wireless communications include the loss of confidentiality and integrity and the threat of denial of service (DoS) attacks [13]. Unauthorized users have the potential to access agency systems and data, tamper with agency data, use up bandwidth on the network, negatively impact network performance, launch attacks that bar authorized users from using the network, and even use agency resources to launch attacks on other networks.

SMARTPHONE MALWARE ATTACK

To defend against malware, a two-level strategy can be deployed. The first level aims to prevent malware from getting into smart phones. The second level relies on tools to pro-actively detect the existence of malware. Once it is detected, it is removed and the smart phone systems are cleaned up. Below we first discuss this strategy for general scenarios. Then we will focus on some specific types of attacks.

Mobile malwares are characterized by their propagation behavior, remote control behavior, and malicious attack behavior. The propagation behavior refers to how malware may be transmitted to the victims. The remote control behavior indicates how the mobile malware makes use of a remote server to further exploit the infected device. The attack behavior refers to how the malware, after infecting a victim's devices, attacks the devices via different communication channels (e.g. Bluetooth). A more detailed description of the threats posed by malware is provided as follows.

Once malware is installed on smart phones, it would try to gain access to the data stored in the devices, interfere with the normal functions of the devices, or open more security vulnerabilities such as enabling unauthorized remote access. In general, through malware, various types of attacks can be launched. Typically, threats include phishing, spyware, surveillance attacks, diallerware attacks, financial malware attacks, worm based attacks, and botnets, as listed in Table 1. Botnets are a Dangerous evolution in the malware world. They are being used to damage systems, steal information and Comprise Systems. [2]. [3]

Table- 01

Attack s/w	Description
Phishing	Smartphone attackers collect personal account details and credit card details and debit card details from Smartphone users through credentials, email or SMS, which are impersonated as genuine.
Spyware	Smartphone users' activities are being monitored, which means that personal information is being extracted or inferred from the Smartphone. Compared to a surveillance attack, spyware does not have specific target victims.
Botnets	A botnet is a set of zombie devices infected with malware so that a hacker can take control of them remotely and give them remote control.
Trojan:	When a user runs the trusted executable files that contain the harmful instructions (Trojan), the Trojan is triggered. Trojan can be used to steal data, disable some mobile device features, and allow an attacker to install other malware.

Worm	A worm is a malware and a type of attacker's weapon that replicates itself, usually without user intervention, to spread from one device to another using various means through existing networks.
Ghost Push:	After gaining root access to a mobile device, this malware downloads malicious apps, changes them to system apps, and then loses root access permissions.
Spam	Spam is any type of unsolicited, unsolicited digital communication that is sent in bulk. Spam is often sent via email, but can also be distributed via text messages, phone calls or social media.

Day by day the security attacks on mobile devices are increasing and most of them are insecure data storage and communication. Some of the critical and conspicuous mobile attacks are summarized below:

Table- 02

Honking Palace	**Description**
Security of Data Storage:	Many mobile applications use weak cryptographic techniques, and 87.7% of mobile apps save data in plain text format.
Security During Communication:	The majority of communications used a client-server approach on mobile devices.
Security from Cross Site Scripting Attacks:	One type of serious online application attack is cross-site scripting (XSS) assault
Security from Malware Attacks:	Without the user's awareness, malware or dangerous software is installed on their mobile device. Malware can propagate via insecure applications or the internet.

Below is a list of the various categories of the most prevalent mobile malware.

Table- 03

Replay Attacks:	Between a wireless device and access point, the intruder watches and records packets that are sent over the air.
DoS Attack:	A denial of service attack stops a network in its tracks by clogging the capacity with useless data.
Surveillance attacks	A particular Smartphone user is put under surveillance by using the built-in sensors of his/her malware-infected Smartphone.
Diallerware attacks	Smartphone attackers steal users' money by using malware that eavesdrops on premium numbers or SMS services.
Financial malware attacks	Smartphone attackers aim for such attacks to steal users' credentials from smart phones or to perform man-in-the-middle attacks on financial applications.

Below is a list of the various categories of the most prevalent Traffic.

Table- 04

Eavesdropping:	Data packets can be intercepted, copied, stored, or analyzed by attackers any time two (or more) computers interact over a network. Any wireless device can be modified to capture all data on a specific network channel or frequency
Analysis of Traffic:	The attacker gathers information by observing communication patterns in the transmissions. The messages that are sent back and forth between communicating parties hold a significant amount of information.
Rouge and Open Access Points:	Rogue access points are those that have linked to the network without the network administrator's consent. They might be applied to enable network entry for unauthorized users. They can also be set up to function as an authorized AP to wifi client.
High Gain Antennas:	Minimal power wireless networks like the 802.11b network seem to be impenetrable to outside intruders. It has been established that this is untrue. It has been shown that an intruder can connect to an 802.11b network using high-gain antennas from up to 15

	miles distant, despite the fact that the network is only intended to have a 300-foot maximum operational range.
Hardware Theft:	The physical theft of a gadget by an attacker is referred to as device theft. By using the WEP key and MAC address of the client, the owner of the device can join the wireless LAN.

Below is a list of the various categories of the most prevalent software Firewalls malware.

Table- 05

Configuration	Access Points must be configured by network managers in accordance with established security requirements and policies. A vendor's software default setup contains a number of vulnerabilities that can be mitigated by properly configuring shared keys, SSID, Ethernet MAC Address Filtering, encryption settings, and default settings.
Software Upgrades:	When recognized software security flaws are discovered, vendors typically work to fix them. Security updates and upgrades are how these fixes are made.
Authentication:	A method for network access authentication limits access to authorized parties. Network access authentication is used to join a LAN. The system should approve the specific session after authenticating the entity. The system should ideally verify each packet after the entity has been verified and the session has been approved to prevent the session from being "hijacked" in the middle of it.
Firewalls:	Resources on public wireless networks are typically less protected than those on private networks, making them more vulnerable to assault. Personal filters provide some defense against specific attacks. Software-based personal firewalls can either be remotely or client-managed and are installed on the client's computer.
End to end encrypted:	If data is sent in wireless LANs without encryption, the substance of the data can also be seen. Data that has been encrypted is changed into an unreadable state that must be recovered through effort. Data should be shielded from eavesdropping assaults if encryption is used correctly.

Below is a list of the various categories of the most prevalent mobile authentication.

Table- 06

Intrusion Detection Systems (IDS):	In order to determine whether unauthorized users are trying to access the network, have already accessed it, or have compromised it, IDS watch real-time network traffic.
VPN:	The ability to send data safely between two network devices over an insecure data transport medium is made possible by VPN technology.
Smart Card:	Smart cards might provide an additional layer of security. Smart cards offer the additional feature of authentication in wireless networks. In environments requiring authentication that goes beyond a username and password, smart cards are useful.
Biometric:	Optical scanners, such as retina and iris scanners, facial recognition scanners, and speech recognition scanners are examples of biometric devices. They also include fingerprint and palm print scanners. When used either by themselves or in conjunction with another security measure, biometrics offer an extra layer of security.
PKI:	Public key certificates can be created, produced, distributed, controlled, and recorded using PKI's infrastructure and services. It gives applications with secure encryption and authentication of \network interactions as well as data integrity and non repudiation, using \public key certificates to do so.

SURVEY REPORT

RQ1. By using which technology does the attacker attacks someone's smart phone?

I studied through Google for the solution of this question. This is known as secondary data. It took 15 days to complete the study

There are two primary attack vectors for mobile phones: The first is when a mobile phone connects the internet; the second is when a mobile phone connects to a network.

Worms, Trojans, Spyware, Botnet etc., using this technology, the attacker does the same thing through both internet and network. Infecting people's smart phones. After that the remote control takes over that smart phone. Due to which it steals private data, Financial ID & Password and identity from its storage.

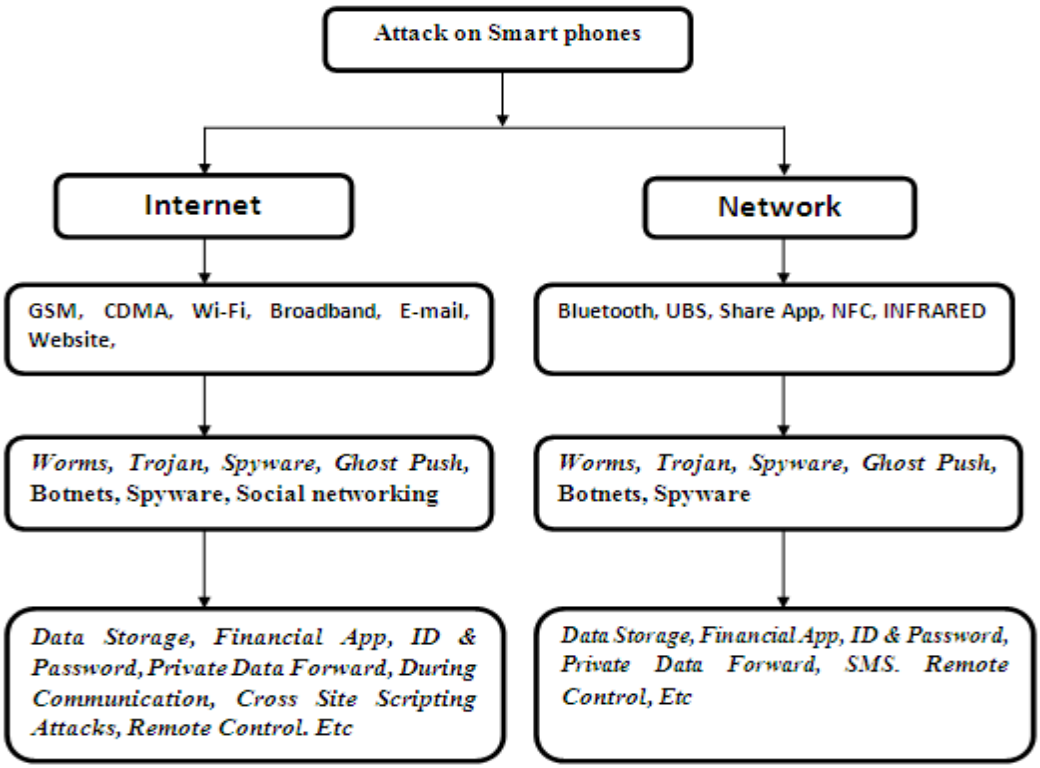

Figure 1: Technology does the attacker attacks someone's

Users may need to perform a factory reset on their mobile devices to get rid of these infections. This kind of malware can rob users of their private data.

RQ2. What are the primary techniques to avoid attacks on smart phones?

An interview with a Smartphone attacker revealed that an attack cannot happen if you keep the phone only for making calls. If your caller's mobile number is registered with the bank and you agree to the temptation then you may be financially attacked

An anonymous interview has shown that people are attacked on both smart phones and non-smart phones. Non-smart phones are attacked because their mobile number is registered with the bank account, attackers attack by luring them. If the mobile number is not registered then there is no danger. Second, there are three types of attacks on smart phones. First when the smart phone is stolen, second when the Smartphone connects to the internet, third when the Smartphone connects to the network.

The attackers who attack smartphones live in almost all areas. For research study on this topic, we joined that group and focused our study. When my studies were completed, I left that group to write my research paper. The research study is as follows:

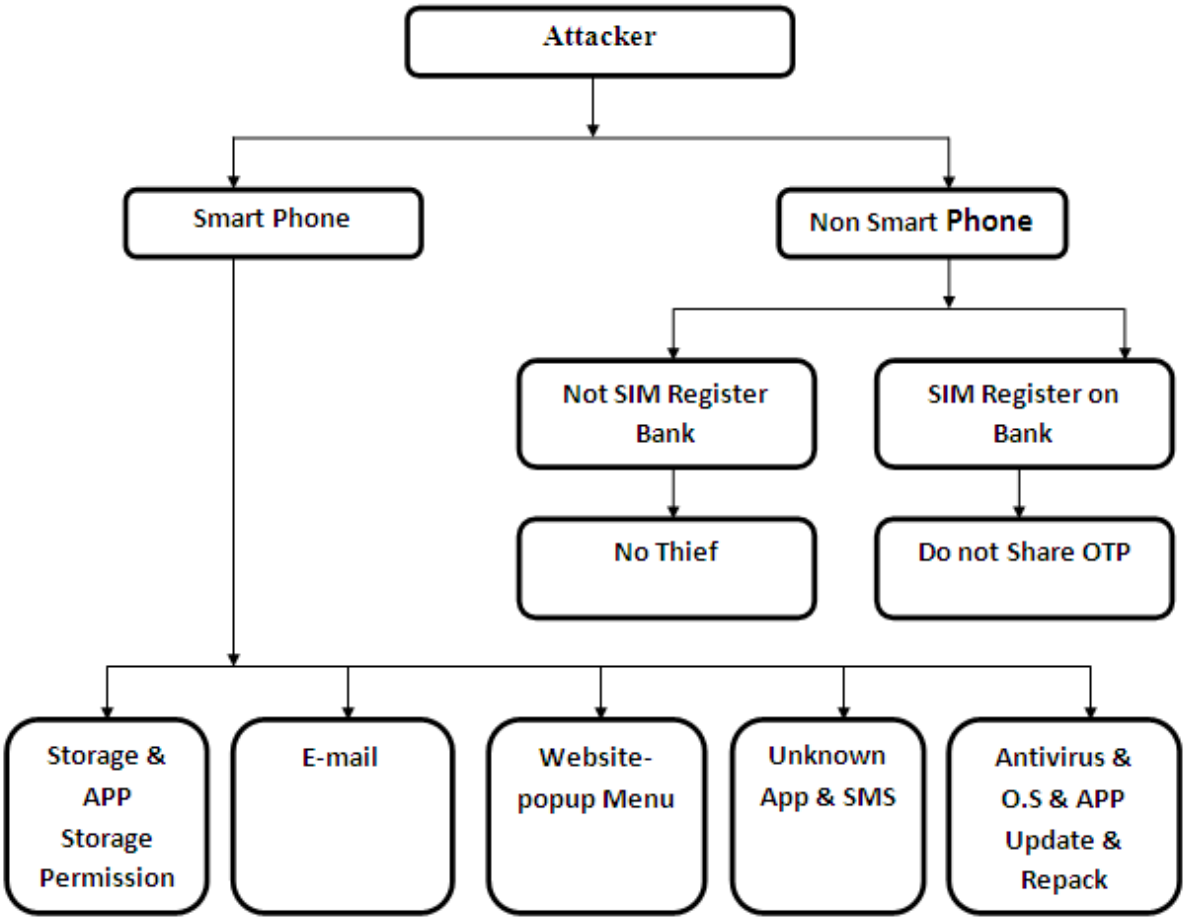

Figure 2: Primary techniques to avoid attacks on smart phones

Researchers use all this technology to suggest smart phone security. On the other hand people find techniques or techniques to attack it. This cycle will continue forever.

By addressing security considerations in areas such as 5G, IoT, blockchain, and machine learning, the future of secure mobile communication systems can ensure the integrity, confidentiality, and availability of communication and data. Embracing emerging technologies and implementing innovative security solutions are crucial in shaping a secure future for mobile communication.

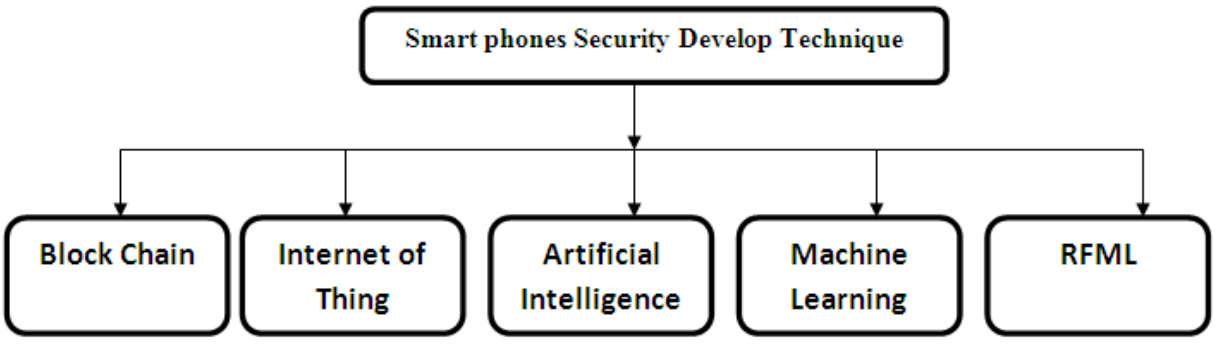

Figure 3: Smartphone security develop technique

A review of literature survey concluded that there are three primary means of attack for smart phones. The first is when a mobile phone connects the internet; the second is when a mobile phone connects to a network; the third is when a mobile phone is stolen or forgotten.

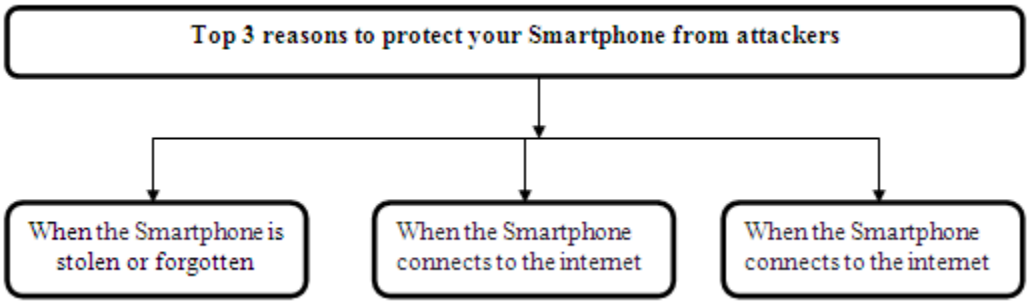

Figure 4: Three way to attack on Smartphone

RQ3. How many types of attacks do attackers make on smart phones?

Through random sampling, I conducted interviews sitting outside ATM machines and this work went on for 14 days. After that I went inside the bank and interviewed the customers as well, which took 9 days.

The interview survey revealed that there are two types of attackers attacking people's smart phones. The first is by installing directly related to the person and the second is through malware through various mediums like email, website, mobile app, repack app, from the infected computer via Bluetooth.

149 people have participated in this sampling. Based on this the result has been drawn. Two types of questions were asked to them - the first which was directly related to the subject and the second related to age, qualification, experience, and department.

Person	Age
85	18 <= 30
64	31 <= 55

Person	Qualification
94	05 <= 05
55	06 <= 12

Person	Experience
94	01 <= 05
55	06 <= 12

Person	Department
85	Technical
64	Non Technical

Figure 5: Data Presentation

Type of Smart Phone hack (1) Direct Hack- 70%
(2) Indirect hack- 30%

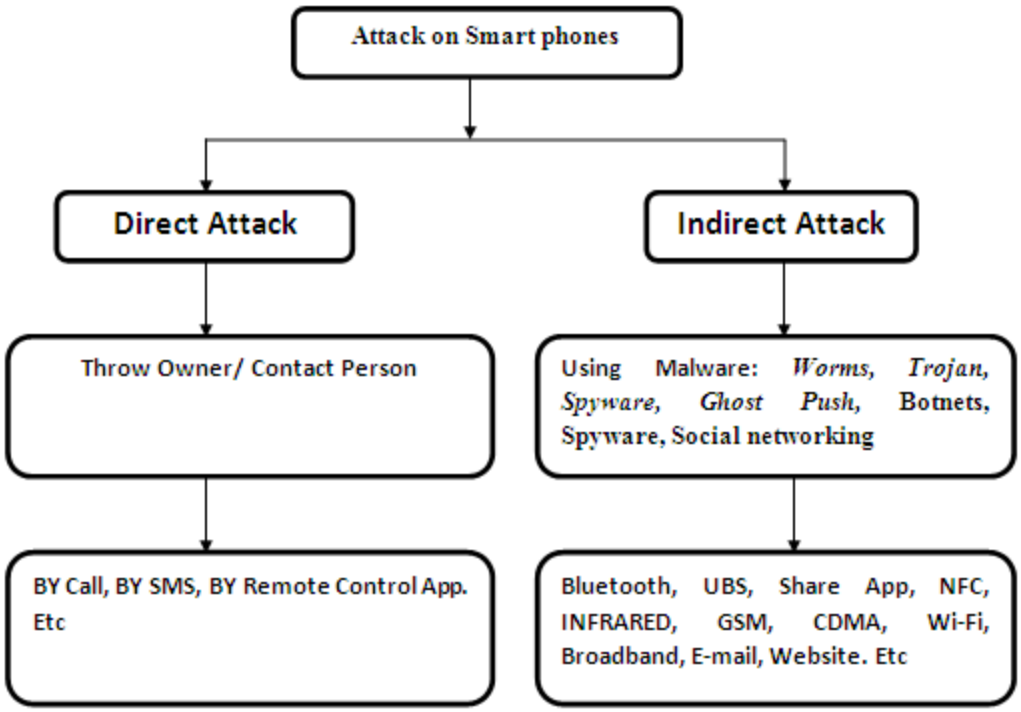

Figure 6: Direct / Indirect attack on smart phone

More recently, another new way to attack direct Smartphone phones has been discovered. The thing is that first he records the voice of a particular person, then with the help of AI, he talks to his family members in the same voice and by making some kind of excuse, asks for money on another mobile phone. As my mobile got broken due to car fall and the injury is too much, we are in the hospital, send money to this number. This is how the director Smartphone attack is happening.

CONCLUSION

In this research paper we have suggested two types of attacks: First Direct Attack- That is the attacker collects bank account data from somewhere and directly connects to Smartphone user through call/message/advertisement/remote control app and lure By giving, empties the bank account. Second Indirect attack- In this, the attacker creates a network on the Smartphone through a malware app and the malware app gives remote control to the attacker. If the Smartphone user with malware does anything new in his Smartphone, then the message is forwarded to the attackers. For example malware app is as follows: botnet, spyware etc.

Wireless mobile communication attacks have three Primary causes: the first occurs when the attacker connects via Internet the second is when one joins via network link; the third is when smart phone is lost or stolen.

Wireless mobile communication attacks have four secondary causes: the first occurs when the attacker connects via a call; the second is when one joins via an SMS link; the third is when connecting through the Remote Control app; and the fourth happens when the mobile goes into someone's hands or is forgotten.

In this research paper, we have suggested the first aid to avoid the attack, how the attack can be avoided.

Smartphone attackers attack wireless communication! It is a big problem for human life. It has been suggested to avoid it in many research papers. Many researchers have given security related proposals to the companies making mobiles. The government also gives suggestions from time to time through SMS to avoid this attack. Bank Origination also suggests cyber attacks to its customers from time to time. Ultimately the solution to the problem is that people need to be aware.

To enhance mobile communication security, future research should focus on 5G and beyond, investigating the unique security challenges and developing advanced security mechanisms. IoT security solutions should be explored, addressing the specific requirements and constraints of IoT devices. Emerging technologies such as blockchain, machine learning, and

AI hold potential for enhancing security measures. User-centric security approaches, including intuitive authentication methods and user-friendly controls, should be developed. Enhanced threat intelligence and collaboration among researchers, stakeholders, and regulatory bodies are also crucial in developing standardized security frameworks and protocols.

REFERENCES

[1]. Statista, Smartphones—Statistics & Facts, Statista, Hamburg, Germany, 2020, https://www.statista.com/topics/840/smartphones/.
[2]. Pranay Jadhav1, "Mobile Botnet Detection" International Journal for Research in Applied Science & Engineering Technology (IJRASET), Volume 11 Issue III Mar 2023.
[3]. B. Guo, Y. Ouyang, T. Guo, L. Cao, and Z. Yu, "Enhancing mobile app user understanding and marketing with heterogeneous crowdsourced data: a review," IEEE Access, vol. 7, pp. 68557–68571, 2019.
[4]. N. Leavitt, "Mobile security: Finally a serious problem," Computer, vol. 6, no. 44, pp. 10-15, 2011.
[5]. K. Marko, "Rise of android botnets.," Informationweek - Online, 2011.
[6]. Paweł Weichbroth, Łukasz Łysik, "Mobile Security: Threats and Best Practices"Hindawi Mobile Information Systems Volume 2020, Article ID 8828078, 15 pages
[7]. B. Guo, Y. Ouyang, T. Guo, L. Cao, and Z. Yu, "Enhancing mobile app user understanding and marketing with heterogeneous crowdsourced data: a review," IEEE Access, vol. 7, pp. 68557–68571, 2019.
[8]. S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," IEEE Access, vol. 4, pp. 4543–4572, 2016.
[9]. A. Papageorgiou, M. Strigkos, E. Politou, E. Alepis, A. Solanas, and C. Patsakis, "Security and privacy analysis of mobile health applications: the alarming state of practice," IEEE Access, vol. 6, pp. 9390–9403, 2018.
[10]. G. Delac, M. Silic, and J. Krolo, "Emerging security threats for mobile platforms," in Proceedings of the 34th International Convention MIPRO, pp. 1468–1473, IEEE, Opatija, Croatia, May 2011.
[11]. D. He, S. Chan, and M. Guizani, "Mobile application security: malware threats and defenses," IEEE Wireless Communications, vol. 22, no. 1, pp. 138–144, 2015.
[12]. P. Weichbroth, "Usability of mobile applications: a systematic literature study," IEEE Access, vol. 8, p. 55563, 2020.
[13]. Raj Kumar Patel, Dr. Lalan Kumar Singh , Dr. Narendra Kumar."Literature Review of Distributed: Denial of Service Attack Protection ", Volume 11, Issue I, International Journal for Research in Applied Science and Engineering Technology (IJRASET) Page No: 1032-1036, ISSN : 2321-9653, www.ijraset.com