Impacts of Vulnerabilities on Security and Confidentiality in Online Social Networks along with Preventive Measures.

[1st]Mr. Tabassum Tamboli
School of Computer Science
Pune, India

[2nd]Mr. Aditya Shende
School of Computer Science
Pune, India

[3rd]Mr. Archana Varade
School of Computer Science
Pune, India

***Abstract*—In today's era people are associated with multiple social networks like Facebook, Instagram, Twitter, WhatsApp etc. Social networks provide users with many functionalities, few are desirable and few may cause issues by exposing users to hackers and attackers. Online social network users provide their personal information like full name, contact number, address, photos, date of birth, e-mail address, relationship status, etc. This information may get sold on dark-web or deep-web on a large scale and it may create potential threat to the nation's security resulting in weakening of people's faith on national security. This paper explores how security and privacy is threatened when data gets breached or leaked and how it affects the community in general. It is observed that instances of Mass data disclosure of administration authority, private services keys, private employee information, and publicly accessible databases are happening. This paper explores not only the potential threats but also preventive measures and potential cures. An extensive case study analysis has been carried out to reveal potential threats and vulnerabilities in online social networks.**

Keywords*— *Phishing, cyber security, social networks, cyber attacks

I. INTRODUCTION

In today's world it is almost becoming impossible to live without getting associated with multiple social networks like Facebook, Instagram, Twitter, WhatsApp etc. Social networks provide users tremendous functionalities and possibilities. Though most of these are desirable, few may cause potential harm by exposing users' data to hackers and attackers. In the field of social networks people think that they are secure but the thing is cyber security is just an illusion. Every day new technical things are getting invented making the security inadequate and vulnerable. This paper explores the issues of cyber security in social networks, to handle security threats and vulnerabilities. The key aspects of security like data breach, unauthorized access, insecure protocol and the attack mechanism are investigated further.

The organization of the paper is as follows:

Section I presents Introduction. In Section II attacks and vulnerabilities are described. Section III presents the preventive measures for above mentioned attacks and vulnerabilities. We conclude this paper in section IV.

.

II. ATTACKS AND VULNERABILITIES

A. *Data breach:* A data breach comes as a result of a cyber-attacks that allows cyber criminals to obtain unauthorized access to a computer system or network. With such access they can steal the private, sensitive and confidential personal data of the users [2].

SQL injection: SQL injection is a very old method to break into the system and breach the data, but it is still relevant methods because Structured Query Language (SQL) which is an extremely popular way to interact with databases. Attacks of SQL injection are going on in the last 2 decades and fact is most of the data breaches happened under SQL injection. In these most-attacked databases are Oracle, PostgreSQL, MySQL and MongoDB and most-attacked platforms are WordPress, Drupal, and Quest. It is very important to secure any product against SQL injection to prevent data leaks.

In January, 2020 A customer support database holding over 280 million Microsoft customer records were left unprotected on the web. Microsoft's Exposed Database disclosed email addresses, IP addresses, and support case details. Microsoft says the database did not include any other personal information. [4]

Downgraded server versions: Most of the companies have not updated server versions in an industry which is very dangerous because downgraded versions can be hacked easily by zero-day attacks and can be harmful for organization. It can lead to massive data breach.

In the 2018 Cosmos bank's server was hacked by hackers by just putting malware in a server system which was downgraded and led to fraud of 90 corers and massive data breach of credit/Debit card information like Username, Card expiry, CVV.

B. *Phishing:* It is a method in which hacker tries to gather information using illusionary websites Emails. In which recipients are tricked by malicious links which look like important mail from a particular website. Clicking the supplied link users will be directed to a malicious login page designed to capture user's username and password. If a user doesn't have multi-factor Authentication (MFA) enabled, the cybercriminals will have everything they need to hack into your account. While emails are the most common form of

phishing attack, Short Message Service (SMS) text-messages and social media SMS systems are also popular with scammers. [5]

Clickjacking: Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to accidentally download malware, visit malicious web pages, and provide credentials or sensitive information. Clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it. Most of the people influenced by some illusionary stuff and then later realize that their personal information is no more private.[6]

Around 360 million user's data were breached by hackers using clickjacking from Myspace.

Identity Clone Attacks: Using this technique, attackers duplicate a user's online presence either in the same network, or across different networks, to deceive the cloned user's friends into forming a trusting relationship with the cloned profile. The attacker can use this trust to collect personal information about the user's friends or to perform various types of online fraud. An example of an identity clone attack occurred recently with NATO's most senior commander, Admiral James Stavrides. His profile details were cloned and then used to collect data on defense ministry officials and other government officials by tricking them into becoming friends with the newly cloned Facebook profile.[1]

Open Source Intelligence Tool (OSINT): OSINT has inherent vulnerabilities which can lead to mass data breaches and cyber-attacks from unknown sources. In this type of data breach there is information like personal Email address, Date of Birth, Geographical location, Credit card data, Bank related information. Data breached from this tool found on the deep web or dark web in large amounts.

28 May 2014, cyber threat actors are using more than a dozen fake personas on social networking sites (Facebook, Twitter, LinkedIn, Google+, YouTube, and Blogger) in a coordinated, long-term cyber espionage campaign. At least 2,000 people/targets are, or have been, caught in the snare and are connected to the false person.[7]

C. Insecure Networks: Insecure networks can lead to data breach because Wi-Fi is one of the main sources or is an excellent medium which enables network for users with their personal devices. Failure to properly secure that the network can breach your defenses. And when your defenses are breached, your data is compromised, potentially resulting in what is known as a "data breach". Because of lack of role-based access control, unencrypted network data in transit over Wi-Fi can be viewed by prying eyes. The data being sent over the network that isn't encrypted can be seen by unauthorized users. This is how data gets breached by using insecure networks.

According to a survey 72% of business data breaches came via unsecured wireless devices.

Publicly Available Wi-Fi: There are many free Wi-Fi available while we are roaming in hotels, café, bus-stand, stations, etc. Free Wi-Fi seems like lifesaver for us but be aware while using those free networks could make you an easy target for hackers and putting your personal information. One of the dangers of using a public Wi-Fi network is that data over this type of open connection is often unencrypted and unsecured, leaving you vulnerable to a Man-In-The-Middle (MITM) attack. This gives a hacker access to sniff out any information that passes between you and the websites you visit details of browsing activities, account logins.

Hackers hit the routers of 277 different hotels, convention centers and data centers in 29 different countries, including the U.S., the U.K., Australia and Cuba.

Hypertext Transfer Protocol (HTTP): It is a ubiquitous protocol and is one of the cornerstones of the web in this case requests and responses are sent in plain text so it is a quite risky method for sending and receiving responses while browsing.

On March 21st, 2019 during a security review, Facebook found that the passwords of around 600 million users were stored as plain texts since 2012 and on storage systems which were accessible to thousands of its employees and developers. The company issued a statement accepting the fault and also said that they will notify the affected users to change their passwords as a precaution.

Open File Transfer Protocol (FTP) Access: FTP proves to be a great way to move files between systems, users and networks and it is fast, simple to deploy, simple to use, controlled by IT and most importantly it is inexpensive. Open FTP servers are risky because they could be used to store malicious tools or as proxies to launch other attacks. There are also worse scenarios, such as the uploading of objectionable material on purpose.

Arkansas-based Med Evolve misconfigured its open FTP server and exposed the data of 205,000 patients from two separate providers.

III. PREVENTIVE MEASURES

A. Data breach: From past few years, all types of industries are facing above attacks and data breach. Prevention of data breaches has become one of the big assignments for so many industries. It can be prevented by many ways if proper training and awareness spread. In this section we suggest some solutions for data breaches and attacks.[3]

SQL injection: Before assuming that code for any application is secure just check for its vulnerabilities like Structured Query Language (SQL) injection. It can be prevented by examining security policies, password strength, encryption of private data, genuine use of admin passwords, use of filtered SQL queries and update code to use prepared statements or stored procedures.

Spyware: Nowadays hackers are widely using spywares for data breach. It is important to train people about spyware such as don't click on unknown links in emails from unknown senders, don't download any file from unauthorized sources, use proper firewall and antivirus and don' t click on pop-up advertisement from unknown sources.

Downgraded server versions: Many downgraded server versions are vulnerable for zero-day attacks and can be easily hacked by hackers. So, it is very important to update server

versions from time to time or use upgraded versions only. It secures data from such attacks.

B. *Phishing:* Solution to prevent phishing attacks is to make people are aware about phishing attack types and to identify proper web applications for social networking sites on which they provide their personal information. To safeguard from this type of attack users should know about their security and privacy settings available on social networking.

Clickjacking: In clickjacking most of the time hackers create fake dummy sites which look just like the original site in this case it is important for users to verify the website information like source, Internet Protocol (IP). Before providing credentials or any personal information to any social networking site just check whether it is genuine or not.

Identity clone attacks: To prevent identity clone attacks users should make their profiles visible for known sources and friends only. Users should not accept friend requests from unknown people. Don't give any information through social networks even if you know that person because that person may be cloned.

C. *Insecure networks*: Nowadays hackers are using insecure network to breach data. In insecure networks mainly people use Free Wi-Fi which is very risky because we connect our personal devices to unprotected networks which is an open invitation for hackers to steal the data. So, make sure when You are using any network is secured or not. Do not connect your device to any free or publicly available network.

Hypertext Transfer Protocol (HTTP): Hypertext Transfer Protocol send and receives request and response in plain text so make sure when you are browsing any social networking site is using Hypertext Transfer Protocol Secure (HTTPS) which sends all data in encrypted form to server. So, even if hackers try to perform man in the middle attack won't be able to decrypt data provided by users.

Thus, above are some solutions to prevent data breach on social network.

CONCLUSIONS

Online social networks have become the most important part of our day-to-day life. Social networks provide users tremendous functionalities and possibilities like sharing their pictures, experiences, doing online chatting, and entertainment. Though most of these are desirable but few may cause potential harm by exposing users' data to hackers and attackers. Day by day the number of attacks on social media platforms are increasing widely. It can be any attack like fraud, data breach, and cyberbullying. To prevent these attacks, it is very necessary to train or guide people about their safety and security. It is also important to make them aware about different attacks which are mainly used by hackers and their consequences. In this paper we explored how security and privacy is threatened when data gets breached or leaked and how it affects the community in general. The preventive measures regarding privacy and safety of data which inturn helps to enhance security are suggested. An extensive case study analysis has been carried out to reveal potential threats and vulnerabilities in online social networks. Users must stay attentive while posting information on social networks and make sure about the privacy of data.

REFERENCES

[1] M. Fire, R. Goldschmidt and Y. Elovici, "Online Social Networks: Threats and Solutions," in *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2019-2036, Fourthquarter 2014. doi: 10.1109/COMST.2014.2321628
[2] Cyber security basics, Data breach and preventions. [Online] Available: https://www.malwarebytes.com/data-breach/
[3] Why data breach occurs? [Online] Available: https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html
[4] Structured Query Language (SQL) injection. [Online] Available: https://portswigger.net/daily-swig/sql-injection
[5] Phishing Attacks. [Online] Available: https://www.imperva.com/learn/application-security/phishing-attack-scam
[6] Clickjack attack – the hidden threat right in front of you! [Online] Available: https://www.troyhunt.com/clickjack-attack-hidden-threat-right-in
[7] What is Open Source Intelligence Tool (OSINT). [Online] Available: https://www.sentinelone.com/blog/what-is-osint-how-is-it-used