Privacy and security issues in Facebook/Instagram (META)

Faton Haxhiu
Tandon School of Engineering
New York University
New York, United States
fh2300@nyu.edu

***Abstract* — social media plays an important role in our daily life, that it has the good things since helps to connects with other and share information, in this paper we have tried to show what issues their user can have in this case we have based our paper in Facebook and Instagram, the main issues focused are privacy and security of users.**

Keywords—*Meta, Privacy Security Tandon School of Engineering*

I. Introduction

Privacy is a crucial aspect of human life, where individuals expect to be free from unwanted observation by others. It is a concept that is influenced by culture and context. This study aims to explore how people perceive privacy and security issues by analyzing their views and opinions on Twitter posts. Different people have varying perspectives on social networks, the popular platforms with approximately 4.2 billion users worldwide [1]. The problem domain we are going to discussed in this paper is closely related with security and privacy have become one main problem because there are many types of things it can bring in society a lot of times people identify theft, and data breaches as well attackers use social media as starting point in launching malware and phishing attacks. What I will try to solve during this research paper is check for security methods and follow some sort of rules to protect the privacy of the user in social media. Even though social media has been here for more than a decade, still security and privacy of users seems an issue. This paper is going to consists of those sections, in the second section we have listed threat model, in third section we are going to talk about privacy protection and issues, on fourth section we are going to discussed about security issues and proposed solutions, and finally in fifth section we are going to give our conclusion and suggestions.

II. Threat Model

The methodology allows security experts to identify security risks, verify an application's security architecture, and develop countermeasures in the design, coding, and testing phases. Thread modeling for this paper are as follows: **Attacks**: Attack vectors such as phishing and malware can be used to compromise social media accounts. **Tracking/Surveillance:** Social media platforms are often used to collect user data, which can be used for tracking and surveillance purposes by governments and other organizations.

Model Threat	**Description**
Attacks	How attacks such phishing and malware work in social media.
Data Breaches	Unauthorized access to user data, such as personal information up to identity theft.
Tracking/Surveillance	Collecting user data and ways to trace online activity, which are used by government or other organizations.
Cyberbulling	Social media as well is used to bully or harass individuals.
Countermeasures	Tools and techniques to prevent security risks and privacy in social media.

Table I. Threat Modeling

Cyberbullying: social media can be used as a platform for cyberbullying and harassment, which can have a significant impact on individuals' mental health and well-being.

III Related Reseach

Facebook and Instagram platforms have become a central part of people's daily lives, providing users with various functionalities such as communication, sharing, and networking. However, the use of these platforms comes with inherent privacy and security concerns. One study examined the privacy and security implications of Facebook's Open Graph protocol, which allows developers to integrate Facebook into their websites. The study found that the protocol exposes users' personal information, including their name, gender, and location, to third-party websites without their explicit consent, thereby increasing the risk of privacy violations and identity theft. Another study analyzed the privacy and security implications of Facebook's advertising platform, which uses user data to deliver targeted ads. The study found that the platform's data collection and sharing practices raise concerns about user privacy and security, as it allows advertisers to access users' personal information, including their location, interests, and browsing history. In addition, research has also investigated the use of social media platforms by malicious actors, including cybercriminals and hackers. For example, one

study examined the use of social engineering techniques on Instagram, which involves tricking users into sharing their personal information or clicking on malicious links. The study found that attackers use Instagram to target users with phishing attacks, which can lead to identity theft and financial fraud. Moreover, research has explored the impact of privacy and security issues on users' trust and confidence in social media platforms. Previous studies, including those by Chakraborty et al., Adam et al., and Liang et al., have indicated that users express concerns about the privacy and security of social network sites.

IV. Evidence

Here are some examples of evidence that support the existence of privacy and security issues on Facebook and Instagram: Data Breaches: In 2018, it was revealed that the political consulting firm Cambridge Analytica had obtained the personal data of millions of Facebook users without their consent. This data was used to influence the 2016 US presidential election. Facebook has also experienced multiple other data breaches over the years, including a breach in 2019 that exposed the personal information of millions of users. Third-Party Apps: In 2018, Facebook banned the app myPersonality for sharing user data with third parties without users' consent. In 2019, it was revealed that many popular third-party apps on Facebook were sharing user data with advertisers without users' knowledge or consent. Privacy Settings: In 2018, a study by the Norwegian Consumer Council found that Facebook's privacy settings were "ambiguous" and "unclear." In 2020, Facebook settled a lawsuit for $550 million that accused the company of violating users' privacy by using their facial recognition data without their consent. Targeted Advertising: In 2018, it was revealed that Facebook had been collecting call and text message data from Android users for years. In 2020, Instagram agreed to pay $5.3 million to settle a lawsuit that accused the platform of using facial recognition technology to collect biometric data without users' consent. The aim of this research methodology is to develop a tool that can analyze social networking sites, detecting discussions related to malware issues, and filtering out these issues from the network. This will be achieved through conducting experiments and analyzing the results obtained from testing the tool on multiple networking sites. In the table below we have shown that data output when it comes to both social media of META. In this table we have listed results from the experiment related to downsides of both medias.

Social Networking Sites	Errors	Alerts	Features	Structural Elements	HTML 5 And ARPIA	Contrast Errors
Facebook	8	100	32	35	165	28
Instagram	300	63	35	99	124	201

Table 1. *Results for Facebook an Instagram

Among the various types of online accounts, social media accounts are the most searched in the context of cybersecurity. Specifically, Facebook tops the list with 67,940 searches, followed closely by Instagram with 36,220 queries. That is the reason why users of those two social media targets from hackers. Also, social media is also often used for harassment and cyberbullying. Some of the outcomes/facts when it comes to cyberbully are:

- The most common type of online bullying is mean comments 22.5%.
- 35% had shared a screenshot of someone's status or photo to laugh at them.
- 61% of teens who report being bullied say it was because of their appearance.
- 41% of US adults who use the internet have personally experienced online harassment.
- 77% of online harassment victims reported that they had been harassed on Facebook.
- 7 in 10 young people experience cyberbullying before they hit the age of 18.

When it comes to harassment, in the table below you may find the most common types of online harassment in the US.

Online rumors	Sexual content	Mean Comments	Other
20.1%	12.1%	22.5%	45.3%

Table 2. *Harassment Data

V. References

[1] M. Alshaikh, M. Zohdy, D. Debnath, Z. Gwarzo, R. Olawoyin, J. Alowibdi, "Social Network Analysis and Mining: Privacy and Security on Twitter", IEEE 2020. Link

[2] Sh. Alotaibi, K. Alharabi, H. Alwabli, H. Aljoaey, B. Aboolkhail, S. El Khediri, "Threats, crimes and issues of privacy of users information share on social networks", IEEE 2021. Link

[3] O. Haggag, S. Haggag, J. Grundy, M. Abdelrazek, “COVID-19 vs Social Media Apps: Dose Privacy Matter?”, IEEE 2021. Link
[4] M. Nakerekanti, Dr. V. B. Narasimha, “Analysis on Malware Issues in Online Social Networking Sites (SNS)”, IEEE 2019. Link
[5] B. Sanz, G. Alvarez, C. Laorden, P. G. Bringas, “A threat model approach to Attacks and Countermeasures in On-line Social Networks”, IEEE 2014. Link

*The data used has been used just as example case and it does not show real data