COMP- 597: Master Thesis
Spring-2021

Cybersecurity and Privacy of Social Media

Department of Computer Science
California State University, Channel Island

Student Name: Sadaf Tarannum

Instructor: Dr. Evren Eryilmez

Project Summary

State of the objective: Social media cyber-attacks and prevention. As new threats are developed every single hour, this project aims to come up with a strategy that can be used by the industrial organization to stay ahead of malicious parties that are out to destroy their work.

The detailed procedure of the lab: As the world becomes highly interconnected due to digital networks' development, there has been a significant migration to digital platforms. The adoption and use of these technologies have had significant life improvement and enhanced all life areas. They eliminate human errors and maximize the capacity and productivity of resources available. For example, through the use of automation and industrial controls, industries have enhanced their productivity (Calvo, et al., 2016). The innovative process of new technologies has taken the industrial revolution and catapulted them into the information age. Automation and networking processes have improved efficiency and productivity (Plant Automation Technology, 2021). However, the wide adoption has also created a new platform for evil characters to exploit for their personal goal. Therefore, cybersecurity has emerged as a significant concern as people seek to defend their servers, computers, mobile devices, data, and electronic systems from malicious individuals and attacks. The global threat experienced in cybersecurity continues to grow, as indicated by data breaches annually. In 2019 approximately 7.9 billion records were threatened and exposed through data breaches. Statistics show an upward trend as the threats represented a 112% increase in the violations experienced in 2018 (Kaspersky, 2020).

1. Introduction

Vulnerability refers to any kind of weakness existing in a computer itself, in a set of procedures, or in something that allows records security to be uncovered to a threat. It is viable for network personnel and anyone who use computers to guard computers against vulnerabilities utilizing usually updating software program protection patches. These patches are successful in

solving flaws or protection holes determined in the initial release. Network personnel has to additionally continue to be knowledgeable about modern-day vulnerabilities in the software they use and appear out for approaches to defend in opposition to them. There are some common vulnerabilities such as weak passwords, missing data encryption, software that is already infected with the virus, bugs, SQL injection, missing authorization, OS command injection, butter overflow, path traversal, use of broken algorithms, missing authentication for critical functions, URL redirection to untrusted sources, cross-site scripting and forgery, unrestricted upload of dangerous file types, download of codes without integrity check and dependence on untrusted inputs in a security decision.

In every system, vulnerabilities exist and there are two kinds: acknowledged and unknown. Known vulnerabilities regularly exist as the result of needed capabilities. For instance, if someone requires different human beings to use a system to accomplish some enterprise process, he has a known vulnerability: users. Another example of an acknowledged vulnerability is the capability to communicate over the Internet; enabling this capability, someone opens an access pathway to unknown and untrusted entities. Unknown vulnerabilities, which the proprietor or operator of a system is now not conscious of, can also be the result of terrible engineering, or might also arise from unintended consequences of some of the wanted capabilities.

Computer vulnerabilities exist because programmers fail to thoroughly understand the internal programs. While designing and programming, programmers don’t virtually take into account all elements of laptop structures and this, in turn, causes computer system vulnerability. Some programmers code in a dangerous and flawed way, which makes worse the laptop system vulnerability. The harm of laptop system vulnerability can be presented in several aspects, for example, the disclosure of confidential data, and extensive Internet virus and hacker intrusion, which can cause splendid damage to agencies and man or woman customers using bringing about foremost financial loss. With the steady improvement of the degree of information, very extreme computer system vulnerabilities can grow to be a risk to countrywide

protection in the elements of economy, politics, and military. Computer safety vulnerability can harm five sorts of machine securities that include: two Reliability, confidentiality, entirety, usability, and undeniable

It’s often on the actual user to be aware of online threats and stay safe. Social media users need to watch for most of the common challenges they may encounter while using social media.

1. **Phishing attempts**

Hackers have become incredibly skilled at spoofing real websites, including social media sites. If you receive a login alert or warning that your account has been hacked, make sure the message is legitimate – don’t click through on links received by email or in messenger. Go back to the source itself (the actual social media site, for example) and check your account there rather than blindly clicking a link.

2. **Oversharing**

There are two kinds of oversharing to be aware of on social media. First is the real-world kind – giving away vacation plans or sharing personal details that could be used to invade your private information puts you at risk. But also, think about the information we may give away that could give hints to frequently used passwords. Yes, it’s best practice to avoid things like your child’s first name and birthday as your password, but many people still do so and hackers know it. Think twice before taking that quiz that asks you your mother’s maiden name or what high school you went to.

3. **Social engineering**

The bad guys know how to prey on fear, and they’re very good at doing so. Direct messages on social media asking for immediate action – whether it’s a spoofed account from someone in your network asking for help, an urgent call for a donation, or an irresistible link to an article all could lead to giving away valuable information or even downloading malware from an unsafe website.

It’s not always the user who is the weak link in security, though. LinkedIn, for example, had data breaches in 2012 and 2016 exposing the passwords of millions of users.

4. **Identity Theft:** As millions share their personal information for getting registered in one or more social media platforms, these data become vulnerable as hackers and identity thieves use this information’s to reset passwords, apply for loans, or other malicious objectives.
5. **Romance Scams:** A romance scam is a fraudulent scheme in which a swindler pretends romantic interest in a target, establishes a relationship, and then attempts to get money or sensitive information from the target under pretenses.
6. **Whistle-blower**: People are often impulsive on social media; they show their vexation with their colleagues or bosses without thinking. They may deliberately reveal sensitive data in their posts, which can cause significant damage to the reputation of the organization.
7. **Cyber Stalking**: It refers to harassment over the internet. Cyberstalks harass victims on social media by sending unpleasant and lewd messages. They morph photos of victims and circulate them on social media, alleging rumors making the victim’s life unbearable.
8. **Cyber Bullying:** It refers to bullying through the digital medium. It can take place on social media, gaming platforms, messaging platforms, etc. It is aimed at scaring, shaming, or annoying the targeted victim.
9. **Cyber Terrorism:** Nowadays, social media is also used to facilitate terrorism-related activities. It can support, promote, engage, and spread terrorism propaganda like incitement to terrorism, recruitment, radicalizing training, and planning of terrorist attacks.

Most Facebook users want to keep some level of controlled exposure so they can interact better with others. Seeing that tagging is a popular and convenient feature, users have tended not to disable it. It seems reasonable to assume that users are not willing to expose their friends to obviously embarrassing situations, and those who are doing it with their own responsibility. However, it is not always clear which

kind of impression a user is trying to convey by his Facebook profile. So, for example, if Alice has added some co-workers as her friends, and wants to convey a professional identity, she might feel embarrassed when her friend Bob tags her in a picture of her long-forgotten freshman years. Of course, regular users can promptly delete their tags, but this might lead to socially unpleasant situations.

4. Research Objectives

Through research and development of cyber-security methods in the Social-media industry, I can plan and develop a robust security infrastructure to provide social-media user's safety so that their data don't get stolen. The objective is to develop and research cyber-security methods so that the social-media industry can mitigate the cyber-attacks by implementing solid encryption software and multifaceted confirmation to passenger data. Another significant aspect is to prepare the employees and IT staff to keep away from such incidents.

3.1 Using Wireshark to analyze the network, capturing packets, troubleshooting issues and to scan the security issues so that we can stop the DDOS or any attack that breach privacy in social media

It's important to mitigate against denial of service (DoS) attacks that could bring the system down. I will try to formulate a plan to implement cyber-security methods inspired by nature in the social-media. I plan to implement security aspects of availability such as physical issues to stop unauthorized from coming into contact with computing resources, technical issues to confine unapproved people from disrupting services, and administrative issues to implement access control policies, operating procedures, user training. Developers and security professionals can help keep away from many computing stages that prompt the deficiency of availability. I plan to use Wireshark because it catches traffic and changes over that parallel movement into a human- readable format. This makes it simple to distinguish what traffic is crossing the system, its amount, how now and again, how much latency there is between certain hops.

While Wireshark bolsters more than two thousand network protocols, a significant number of them exclusive, unprecedented, or old, the modern security expert will observe breaking down IP packets to be of quickest helpfulness. Most of the packets on our system are probably going to be TCP, UDP, and ICMP.

3.2 Scanning the system for open ports, live hosts and potential vulnerabilities and try to implement the firewalls so that the hackers cannot break into the system

I will learn from nature and use the traditional cryptographical methods to develop new cyber-security methods for Social-media Industry, Nature will serve as a source of inspiration towards developing these techniques. I plan to build up a fundamental methodology for the security group, survey the current technical state and focus on control execution. The Framework can be executed in stages and henceforth can be customized to address any association's issues. The Framework is planned to enhance, not supplant, an affiliation's network safety program and hazard organization structures. Social media can utilize Kali for running data security tests to distinguish and fix potential vulnerabilities in their programs. I will be using Kali Linux Tool Nmap because Nmap utilizes various strategies to perform filtering, including scanning of TCP connect TCP invert ident checking, FTP bob examining. I can utilize Nmap to detect the live hosts, open ports, vulnerability and Nmap provides a lot of features such as host disclosure and to detect the operating system. These highlights are extensible by scripts that offer further developed assistance detection, vulnerability location and different highlights. also plan to implement firewalls whenever I see an open port or potential vulnerabilities.

3.3 Security and protecting the entire company’s IT infrastructure by setting up a layered approach to our defense and it is very important to train employees so that they can keep the social media safe from malicious attacks

I plan to develop an IT infrastructure that will become the foundation of the security infrastructure for the Social-media industry. I will implement cybersecurity framework core to identify, protect, detect, respond and recover any cyber threats and implementation tiers to consider adaptability in execution and acquire ideas of development models, and to reflect how an association carries out the framework core works and deals with its danger. By implementing a layered security approach, the system can have mechanisms such as access limitations, two-factor verification, encryption, and threat detection. Most of the hackers use artificial intelligence these days to break into the system. Situations are controlled with the end goal that

most penetrates include some sort of human mistake. So, associations ought to in this way train their employees to stay away from assault from social engineering to ensure their major assets for directing business and immaculately connect with clients. Employees perform an imperative part in guarding the social media from malicious sources. Thusly, training in cybersecurity is presently an essential piece of business manageability and requires dynamic strides to manage appropriately.

5. Research Goal:

This project aims to investigate and come with robust strategies for addressing cyber-security, specifically in Social-media. It will seek to identify how these technologies can be configured to avoid access by malicious persons. Further, it will seek to ensure that as the information age continues to grow and impact every arena of life, the gain acquired is not undone by security threats pose.