International Journal of Scientific Research and Engineering Development-– Volume 5 Issue 6, Nov- Dec 2022

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

# Social Media Network Attacks and Their Preventive Mechanisms

Naresh Sambhaji Ghorad

KeraleeyaSamajam's Model College, Khambalpada Road, Thakurli, Dombivli (East), Kanchangaon, Maharashtra
ghoradnaresh@gmail.com

## ABSTRACT

We live in a virtual world that mimics real life.The increasing reliance on the use of socialmedia networks around the world has raised major concerns aboutinformation security.One of the factors that make social mediaplatforms so popular is howthey bring people together around the world to connect, interact, share content, and cross geographic boundaries to explore common interests. Do you engage in exchanges? Behind all these incredible victories lies the equivalentof digital crime, which threatens physical socialization.Criminal Elements and Hackersabuses Social Media Platforms (SMP) to carryout many maliciousactivities to harm others. As detection tools are developed to control these crimes, hacker tactics and techniques are constantly evolving. Hackers areconstantly developing new attack tools and hacksstrategies to gain malicious access to systems and social network attacks, making it difficult for security administrators and organizations to develop and implement the proper policies and procedures necessary to prevent hacker attacks. The increase in cyber-attacks on social media platforms calls for urgent and smarter security measures to increase the effectiveness of social media platforms. This paper explores the manner and tactics of hackers' attacks on social media and ways to prevent their activities against users to ensure a safe social cyberspace and enhance virtualsocialization. Social media platforms are briefly categorized, different types of attacks are also highlighted with current state-of-the-art prevention mechanisms to overcome the attacks as proposed in research papers, finally a social media breach detection mechanism is proposed as a second line of defence to combat cybercrime on social networks.

## KEYWORDS

Hackers, Social Media Platforms,Intrusion Detection System,Machine Learning,Online Social NetworkIntrusion.

## INTRODUCTION

Social networking platforms provide mechanisms that increase the effectiveness of virtualsocialization in the globalvillage. It is a medium that enablesfamilies, friends and co-workerscommunicate and communicate seamlessly regardless of their location, distance and platform.Online social networking (OSN) is a platform for connection andcommunication that promotessocial interaction in virtual space. identified 7 categories of social networks. The Internet includes: e-mail services such as Gmail, Yahoo mail, Microsoft outlook, Hotmail,etc; Instant messenger like WhatsApp, Twitter, Yahoo messenger, Instagram, Telegram,Snapchat, etc.; Blogging platforms like Blogger, Tomblr, Wix, Linda, etc.; Social networking sites likeFacebook, TikTok, Quora, LinkedIn, etc.; Multimedia sharing systems such as YouTube, Skype,Flickr etc.; Auction platforms like Jumia, Alibaba, Konga, OLX, etc.; and social search engineslike Google, Yahoo, Safari, etc. All these platforms allow users to socialize and stay in touch with social reality in a virtual environment with various features. Omnipresent natureInformation and Communication

  

Technology (ICT) has greatly affected every aspect of human beingactivities; it also influenced social media users to see the platform as a virtual homethey store their sensitive information in the database of these platforms.

The growing dependence on the use of social networks around the world has resulted in greatconcern for information security. One of the factors popularizing social media platforms ishow they connect people around the world to communicate, share content and engage in discussionsacommon interest that knows nogeographical boundaries. Behind all these incredible gains is the majoritytraditional crimes now have a digital equivalent, enabling criminal elements and hackersusing social media platforms for many nefarious activities to harm others. Like securityadministrators and policy makers are developing detection tools to check these crimes and hacker tacticsand techniques are also constantly evolving. Hackers are cybercriminals who specialize in virtualterrorism that threatens legitimate users of the social media network platform (SMNP) in specific and the entire virtual community in general through various types of cyber-attacks.

These cyber-crimes have a significant negative impact on social media platforms and usersespecially. For ease of access, some social media users prefer to save themsensitive data on the network and when the account is hacked, this information can be useddefraud and defraud users; the user's social contacts on the platform are also highly compromisedthey were tricked by a hacker who could use their techniques by pretending to be authorizeduser. High-profile users like public and political leaders with private information they couldtarnish their image, if extracted, can be used to ransom the user.

Various approaches have been used to prevent hackers from infiltrating the social media networkplatform. Predominant is authentication using login data such as username and password, orPIN; biometric authentication such as using facialrecognition technology, fingerprint, patternmatching or voice recognition are different forms of authentication. Other methods are RolesBased Access Control (RBAC), Extended RBAC, Temporary (RBAC), Risk-Based Access Control. These security methods have many disadvantages, such as a weak password that can easily bethe hackers guessed using a dictionary attack. In an effort to enforce a stronger password forauthentication, users of social networks are forced to write their authentication data on paperwhich can also be stolen byhackers, these weaknesses have affectedmany researcherspropose several security mechanisms to limit the activities of these hackers. Some of theseproposals include: biometric authentication, a hybrid system for social network anomaly detectionnetworks, Network Intrusion Detection System, etc.

All these methods are not suitable for data warehouse security. A commonly used networksecurities software, such as firewall and antivirus, independently provide different servicesnetwork security, but can be bypassed by hackers. Hackers improvise new techniqueshacking into social media platformswithout being detected, two closepropositions regarding dataWarehouse Database Intrusion Detection System from and does not deter resistanthackers.Hence the need for intelligent intrusion detection(IIDM) model that is effective indisarming hackers from carrying out their cyber-crime activitiesagainst SMNP.

## THEORETICAL BASES

Social media platforms have become an integral part of the average user of virtual networkscommonwealth. Billions of devices connected to the internet operate on one social media platform or the other. According to a report in [1], over 500million IoT devices have beenimplemented globally2003, 12.5 billion in 2010 and 50 billion in 2020. There are about 3.5 billion people on social media with attacks estimated to generate over $3 billion annually for cybercriminals [2].An online social networking platform like Facebook includes several features such as

  

product andadvertising and sellingservices, making it relevant to almost all Internet userscollaborate or privately. This has also increased the activity ofcybercriminals on the platform. According to a recent survey by the Computer Emergency Response Team (CERT), the rate of cyber-attacks has increasedis doubling every year [3]. The online social network faces formidable securitychallenges[4]. Facebook is the most popular social network. It was launched in February 2004[5]With roughly 2.89 billion monthly active users in the second quarter of 2021, Facebook isthe largest social network in the world.

The Covid19 pandemic was fundamental to thegeometric shift towards virtual socialization. The technological shift to the cloud computing paradigm has also positively impacted ubiquitysocial media. This shift seems to have given hackers an advantage to carry out their crimes safelyacts because people are less involved. Cloud breach attacks are a set of actions that attempt to do thisviolate the integrity,confidentiality or availability of cloud resources on cloud SMNP. Uprisingthe decline in processing costs and the availability of the Internet also increases the vulnerability of users'various cyber threats and attacks.

Intrusion detection is designed to detect misuse or unauthorized use of computer systemsinternal and external elements [6]. IDS is an effective security technology that can detect,prevent and possibly respond to an attack [7], [8] believed that artificial intelligence plays andcritical role in security services such as intrusion detection.

## A SOCIAL MEDIA NETWORKS

A social media network is a platform that creates a virtual environment for social interactions between thema circle of like-minded friends and fans. "Social media platforms are internet applicationsaimed at broadcasting user-generated content" [9] It deals with the sharing ofinformation andmultimedia content between users on similar platforms through an electronic network, in particularinternet and cyberspace [10]. This platform has grown geometrically to become more than justan effective communication tool for personal and social use, but also an essential channel forbusinesses and official communicationchannels. There are thousands of social media platformswhich are used forvarious purposes today, a few of the most popular ones are highlighted below.

- **Facebook** is an online social media platform that provides several services such as socialnetworking of friends and fans, online advertising, voice calls, instant messaging, video calls,video sharing and viewing, online marketplace, virtual gifts for young and old,private and legal entities. It was launched on February 4, 2004 by Mark Zuckerberg. Ithad over 1.18 billion monthly active users as of August 2015and 2.85 billion activesusers in 20201 according to statisticsinvolving more than 4 billion viewsvideos every day on the net. Approximately 2.14 billion people can be reached through web advertisingFacebook [11].
- **WhatsApp** is a cross-platform internet instant messaging application that enables smartphone users can exchange text, picture, video and audio messages for free, provided the device containshas access to the internet.It was developed in 2009 by Brian Acton and Jan Koum. WhatsAppbecame the most popular messaging app in September, 2015 with around 900 million active users.
- **MySpace** is a social networking website offering a user-provided interactive networkfriends,personal profiles, blogs, groups, photos, music and videos. It was the largest social media platform until 2008 when Facebook overtook it. It was co-founded by ChrisDeWolfe and Tom Anderson
- **Twitter** is a social networking platform that allows users to write

  

and read short charactersmessages called tweets. It revolves around the principle of followers who are equal users,who choose to follow another Twitter user and can thus view tweets have sent by that user.While unregistered users can read tweets, you must register to send tweets. It wasfounded in March 2006 by Jack Dorsey [10].

- **Instagram** allows users to uploadmedia that can be edited withfilters and organizedusing hashtags and geotagging. Posts can be shared publicly or with pre-approved postsfollowers. Users can browse other users' content by tag and location and view trendscontent. Users can like photos and follow other users to add their content to a personal channel.Instagram has 1.38 billion active users with 500 million daily active Instagram user'sstories, 1.16 billion people can be reached through Instagram ads [11]
- **YouTube** is a video sharing servicethat allows users to watch videos posted by other usersand record your own videos. Thanks to the ubiquitous use of smartphones, this platform hasto become the first choice in personal broadcasting and video sharing. It was co-foundedChad Hurley, Steve Chen and Jawed Karim in February 2005. In November 2006 it wasbought by Google and now run by Google
- **LinkedIn** is a social media platform for professional networking. It's a social networktool available for job seekers and professionals where users can invite other users and evennon-users to connect. Invitees who receive multiple rejections from invitees' risk being rejectedaccounts restricted or closed. On this platform, users can familiarize themselves with the network's contacts, new job and business opportunities, exposure of products and services in your companyprofile pages, list of vacancies and search for potential candidates
- **Skype** is an IP telephony service provider that can be used for free voice and video callsover the Internet to any Skype subscriber or any other non-user at low call rates. It isfairly easy to download and install software that works on most computers andtelephones. A dedicated Skype phone or desktop computers, laptops, tablets,mobile phones and other mobile devices equipped with a headset, speakers, microphones or USBphone. Skype also enables file transfer, text messaging, video chat and video conferencing.
- **Viber** is a mobile application that allows phone calls and text messages to all other users,whether mobile or landline, free of charge. It is available via Wi-Fi or 3G with high sound qualitybetter than a regular call with mobile operator charges when used over 3GSew. Once the app is installed, calls can be made to numbers that don't have themViber at lowprices with ViberOut. Viber works on most android, iPhone, blackberry,windows, mac, Nokia and bada devices.
- **Tumblr** is a microblogging and social networking platform whose service enables userspost multimedia and other content on a short blog. Users can follow other users' blogs.Bloggers can also set their blogs to private. There are many website features for bloggersaccessible from the "dashboard" interface. It was founded by David Karp in 2007.
- **WeChat** is a Chinese multipurpose instant messaging, social media and mobile payment applicationdeveloped by Tencent. It was first launched in 2011 and became the largest stand-alone

  

mobile phone in the worldapp in 2018 with over 1 billion monthly active users. It has been described as a Chinese “appfor everything" and "super app" due to its wide range of functions. Provides textmessaging, call-hold voicemessages, one-to-manymessaging, videoconferencing, video games, photo and video sharing, and location sharing.

- **Reddit** This social media platform allows you to submit content and vote on its latercontent. Voting determines whether content moves up or down, which it eventually doesorganized by areas of interest (known as subreddits). Number of active users permonth: approximately 100 million.

All social media platforms including those highlighted above can be categorizedbased on their support for the types of data they exchange or based on their aspect of supportsocial interaction.

Social networking platforms can, based on their support for the types of data they exchangecan be divided into four main types:

i) Text-based platform: used for text-based social communication forsending/receivingnews. Messenger platforms are a good example.

ii) Visual platforms: used for image-related social interactions such as posting andreceiving images. A good example is the Flickr platform

iii) Audio-visual platforms: used for social interactions related to video, e.g.,sending/receiving video data). A typical example is YouTube,

iv) Hybrid platforms: this platform combines the functions of more than one of the texts,visual and audio-visual platforms. A typical example is Facebook

## SOCIAL MEDIA NETWORK PLATFORMS ATTACKS

There are several attacks against social networking platforms. It is importantknow them because a more thoroughunderstanding of these types of attacks equips social mediathe user armours defensive measures and knowledge to reduce the likelihood of beingmisused [12].Aug 6, 2009 Twitter, Facebook,LiveJournal, Google's Blogger andYouTube was hit by a Distributed Denial of Service (DDoS) attack in October 2021,a similar service interruption occurred. [10] identified the seven deadliest attacks onsocial networksnetwork platforms. These attacks are highlighted as follows

**1. Attacks on social network infrastructure:** here the attacker launches an attack ona platform that provides social service insight into disconnecting users from access toservices provided by the platform. The main attack used against social networking infrastructurethat directly affects users is DDoS.

**2. Malware attacks:** in this type of attack, the hacker develops malicious softwareintent to gain control and use the user's device to execute some malicious codeactivities such as launching a DoS attack, logging keystrokes, stealing credentials, credit card numbers orbank connection, etc. The method of infecting the user's device on social networks is usually through links orimages sent to a user's inbox knowing that the user is likely toopen it because it comes from aconnected social contact. Once the user is infected, the hacker uses the compromised social networkmedia account to spread the worm by delivering the message to other users with whom they are friendsan infected user containing an enticing link to a third-party website where they are thenpromptedperform an action such as "register to view the full image", "update Adobe Flash Player so thatbetter view” etc. Once the action is done, the worm automatically infects the deviceall connected friends who followed a link to a third-party site. Common malwarecategories are Crimeware, Spyware, Adware, Browser Hijackers, Downloader, Toolbars andNumerals. Hackers take advantage of the openness of social networks where users generatetheir content; large number of users; and the trust that is implied where users

  

assume everythingfriends must be trusted tolaunch attacks on billions of users connected. The most effectivemethod is by using Cross-Site Scripting XSS to implement malicious codes on social networking site.

**3. Phishing attacks:** as the name suggests, this is a hacking technique where the hacker lures the userusing the "bate" that is most attractive to the user, with the intention of ensnaring the user. In majorityIn such cases, the user is rude and reveals sensitive information that will then be used to attack theuser.

**4. Evil twin attacks:** in this type of attack, the hacker uses the target to create a profilean account impersonating an authentic user. This attack can also be called cyber impersonation. Newthe account is then used to send a friend request to contacts on the social media platformallow an attacker to use friend privileges and gain access to users on the platform.

**5. Identity theft:** in this type of attack, the user's credentials are stolen and used to secureaccess the user's social media platform. Once an attacker successfully gains access, theylaunch their pre-packaged attacks while impersonating an authentic user.

**6. Cyberbullying:** a way to threaten or intimidate social media users either throughmessages or posting objectionable content on a social media network for the purpose of harassment or intimidationtarget user.

**7. Physical threats:** in this attack, the hacker launches a physical attack against the selected user.This could be in the form of bypassing the physical security of the platform by threatening the userremove device security.

All of these threats can use any of the following attack methods to execute their threats.

1. Denial of Service (DoS), where an attacker tries to prevent legitimate users from using aservice
2. Probe attack where the attacker tries to find information about the target host through methodssuch as scanning victims to obtain information about available services and operating system
3. User to Root (U2R), where there is unauthorized access to local superuser rightsgranted
4. Remote to Local (R2L), where unauthorized access from a remote computer viaapproaches such as password guessing to obtain a local account on the victim's host
5. Advanced Persistent Threat (APT) is a targeted attack against a high value asset or physicalsystem where attackers often use stolen user credentials or zero-day exploits to avoidtriggering alerts

## SECURITY MEASURES FOR SOCIAL MEDIA NETWORK

The "juicy prospect" of social media networking platforms has prompted hackers to constantly use the devicetechniques to disrupt and usurp users. They have two compound goals which are social mediausers and SMNPs that they break into and control for their own selfish gain. On usersat the end, hacking activities are prone to threats that include identity theft, eviltwin, password reset, sim clone, brute force, fake links, phishing, information leak,celebrity spoofing, fake account, impersonation, etc. They also use code embeddingvia a malicious SQL script to disrupt the network. Existing security mechanism for DWinclude Role Based Access Controls (RBAC), Extended RBAC, Temporal RBAC (TRBAC),Risk-based access control [4] which is all about username authentication andPassword. [9] were the first to propose database intrusiondetection systems (DIDS) for DW. [4]improved it by incorporating second level authentication, instant messenger like WhatsApp alsouses two-step verificationwhere the user is asked to enter a PIN codeat certain intervals to prevent hackersfrom the network whenever an anomaly isdetected, but hackers still use social engineering to do sotrick users into compromising an account that doesn't detect role-based accessmanaged systems.

  

In order to hack into a social media network, attackers must perform basic stepsoperation. These steps are:

i. Target selection: the attacker selects a target social network user target

ii. Attack Selection: The attacker determines the type of attack to launch against the target,e.g., infrastructure, malware, phishing, evil twin, identity theft, cyberbullying, physicalthreat, celebrity spoofing, etc.

iii. Strategizing: the strategy depends on the type of attack used. If selectedattack is to launch a DDoS attack, then the attacker will have to recruit accomplices(botnet) to use when launching an attack eitherthrough a call, e-mail, posting to usergroups,or creating a website to which users are redirected due to infection.

iv. Army Training: Provide accomplices with a packet containing the attack, time, date,and instructions on how to execute the attack.

v. Initiate the attack: here the attacker initiates the attack, waits and watches the executionattack.

To overcome the various attacks highlighted on the social media network platform, the usershould:

i. Ensure your device has up-to-date antivirus software as a primary line of defence

ii. Don't open emails from people you don't know.

iii. Do not click on unknown links

iv. Do not visit unknown sites

v. Disable JavaScript.

vi. Maintain and ensure regular software patch updates.

vii. Implement browser security policies such as blocking pop-ups and limiting the number connection.

viii. Implement platform privacy security policies such as “who can see my personal information”,"Who can post on my wall", status, etc

ix. Implement IDS/IPS as a second line of defence against attackers.

## INTRUSION DETECTION MECHANISMS

An intrusion detection system (IDS) is a device or software application that monitors a system,network or applicationfor malicious activity or policy violations in order to detect them.The two main IDS highlighted in the literature are Host-based and Network-based. These IDS are notsuitable for intrusion detection inapplications related to intrusion attacks. It gave rise todevelopment of an application-specific IDS that is application-based.

Researchers have proposed various methods to detect abnormal operations in a system.In general, IDS consists of four main components: Traffic Collector, Analysis Engine,Signature database, management and reporting interface. Network, host, orApplication-based intrusion detection systems use one of the signature mechanisms to detect intrusionsor anomalous approach. The signature approach uses rules to make classification decisionsknown intrusion-based breach profile. Anomaly, on the other hand, classifies the operation asa disturbance based on a deviation from the known normal operation of a given system.

The work done in can be consulted for further reading as it compared different approachesusing the features, advantages and disadvantages of each approach.

## RESEARCH/KNOWLEDGE GAP

Currently, there is no developed intrusion detection system for social media platform to limitthe activities of hackers who have turned their attention to the platform. Most literaturereviewed do not have the intelligence to detect social media account usage anomalies.

Role Based Access Control (RBAC), Extended RBAC, Temporary RBAC (TRBAC), Risk Basedaccess control etc. has no ability to detect an attacker gaining access to the systemusing some compromised credentials. Intrusion Detection System (IDS) and some otherscustomized security solutions for DW including the second level were also designedauthentication. But the same mechanism used to avoid first-level authentication can still beuses second level authentication to bypass security access. Therefore, deceivean attacker with a bogus response will provide a better DW

  

penetration boostdetection/prevention mechanism.

Most previous designs used the KDD-CUP-99 and DARPA 98/99 datasets for training, butthese datasets have become outdated with limitations on updating new attacks. Theseearlier models may not work well due to the fact that attackers change their signaturesregularly to avoid detection.

## CONCLUSION

The social media network has become the nerve centreof a virtual community that connectsbillions of heterogeneous users to interact with each other. Due to its dynamic nature where userscan freely share content among friends and followers, hackers are seriously exploiting this richa platform for evil intent. There are different strategies for attacking social media usershighlighted in this paper by various preventive approaches proposed by researchers. Despite everything these preventive approaches, hacking activities on the platform are on the rise, and therefore social media an intrusion detection system will be highly recommended as a second line of defence against hacker attacks on social networking platforms.

### ACKNOWLEDGEMENT

I would like to express my sinceregratitude and respect to all those who have given me tremendous support andguidance. Also, I would like to express my sincere gratitude to my parents and friends for their unwavering support and encouragement throughout my college years and during the process of researching and writing this thesis. Without them, this achievement would not have been possible. Thank you very much.

## REFERENCES

[1] O. Logvinov, “Standard for an Architectural Framework for the Internet of Things ( IoT ),” 2021.

[2] “Social Media Attacks,” 2020.

[3] A. Singhal and S. Jajodia, “Data warehousing and data mining techniques for intrusion detection systems,” Distrib Parallel Databases, vol. 20, pp. 149–166, 2006.

[4] K. Musial and P. Kazienko, “Social networks on the Internet,” World Wide Web, pp. 31–72, 2012.

[5] P. Jucevi and G. Valinevičienė, “A Conceptual Model of Social Networking in Higher Education,” Electron. Electr. Eng., vol. 6, no. (102, 2010.

[6] G. N. Prabhu, K. Jain, N. Lawande, Y. Zutshi, R. Singh, and J. Chinchole, “Network Intrusion Detection System,” Int. J. Eng. Res. Appl., vol. 4, no. 4, pp. 69–72, 2014.

[7] H. Vora, J. Kataria, D. Shah, and V. Pinjarkar, “Intrusion Detection System for College ERP System,” J. Res., vol. 03, no. 02, pp. 69–72, 2017.

[8] B. Shanmugam and N. B. Idris, “Artificial Intelligence Techniques Applied To Intrusion Detection,” in Proceedings of the Postgraduate Annual Research Seminar, 2005, pp. 285–287.

[9] C. F. Noonan and A. .Piatt, Global Social Media Directory. USA: U.S Department of Energy, 2014.

[10] E. S. Dandaura, U. M. Mbanaso, G. N. Ezeh, and U. C. Iwuchukwu, “The Use of Social Networking Service among Nigerian Youths between Ages 16 and 25 Years,” 2015.

[11] J. Bagadiya, “367 Social Media Statistics You Must Know In 2021,” Social Pilot, 2021. [Online]. Available: https://www.socialpilot.co/blog/social-media-statistics. [Accessed: 12-Oct-2001].

[12] C. Timm, Seven Deadliest Social Networks Attacks. USA: Elsevier Inc., 2010.

  