International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 5, Issue 12, pp 40-44, December-2021

https://doi.org/10.47001/IRJIET/2021.512008

Security in Social Media

[1]Aditi Gupta, [2]Shweta Mehetre, [3]Abhilasha More

[1,2]Student, Shri Bhagubhai Mafatlal Polytechnic, Mumbai, India
[3]Lecturer, Shri Bhagubhai Mafatlal Polytechnic, Mumbai, India
Email IDs: [1]aditigupta72003@gmail.com, [2]shwetamehetre110603@gmail.com, [3]abhilasha.maurya@sbmp.ac.in

***Abstract* - Social media provides both opportunities and risk for any organization. In recent years the Internet has made everything possible. It is booming as it is available at low cost with high speed. People are attracted towards the use of social networking due to the virtual method of socializing people using various social media apps such as Instagram, Whatsapp, Twitter, Facebook etc. even though it has advantages equally there are many threats arising day by day. Usage of social media is high but awareness is least which leads to serious cyber attacks. There are different types of threats which make the users in trouble of cyber security risk. This paper analyzes different threats done on social media and gives solutions to those threats and sees different detection techniques.**

Keywords: Security, Social Media, Whatsapp, Twitter, Facebook.

1. Introduction

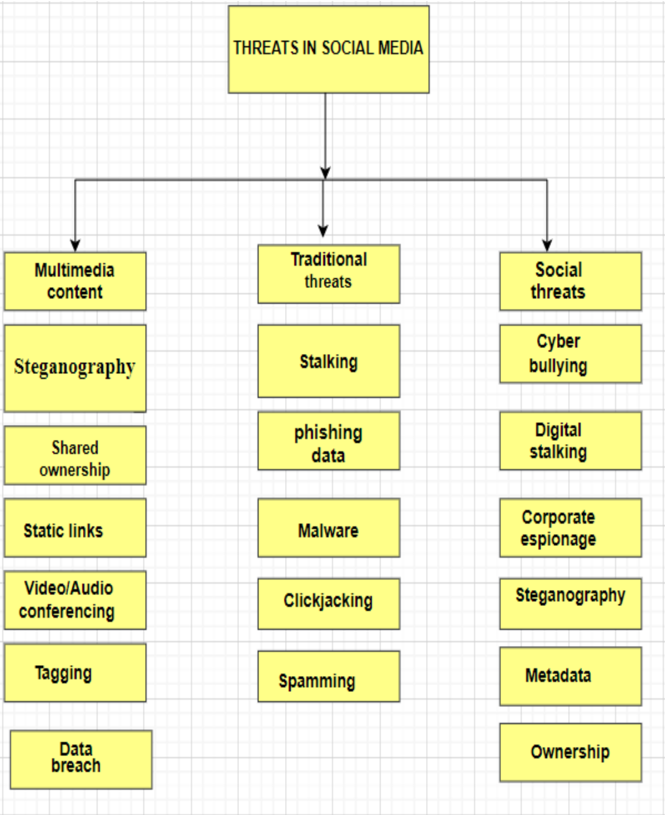
Social media is an interactive technology on which we share, exchange information's, ideas virtually using social networks. Social media are internet based applications. The development of social media began with simple platforms GeoCitieswas one of the earliest social networking services. Some of the most popular social media websites, with over 100 million registered users, include Facebook, Tweeter, Instagram, YouTube, Wechat, Snapchat,etc. People will use various social media applications for career opportunities, find people across the globe with like-minded interests, and share their thoughts, feelings, and emotions. In this process we share lots of our personal data, photos, and videos and fill many forms based on interest through which others come to know about you, your likes and dislikes.

Due to the large amount of data present in social media, social networks are found to be a desirable source for Hackers. Hackers can scan and misuse your personal information online at incredible speeds and a lot more information can be obtained by the attackers or hackers. In this paper we will study different threats done on social networking. The research will also suggest algorithms and what are the supporting researches done.

Threats in social networks which are also called cyber threats, where our own information shared to us may lead to cyber attack. Many social media publicly display users' profiles which include users personal data attackers can collect those data without user knowledge and go more depth into it. Even though there are number of prevention techniques threats are increasing day by day.

II. Threats in Social Media

This session will discuss various threats done on social media and make the user aware about the threats done on social media.



III. Multimedia Content Threats

Static links: 48.6% of the users in social networking services use static links to share the interactive media information. Which results in Multimedia information exposure and loss of data?

Video/Audio Conferencing: People who upload their own video, audio content on social media to showcase their talent, thoughts with the world. There are some who misuse users' video by editing video and making it embarrassing and giving life threats.

Tagging: On social media you can tag someone in a photo or in text and the person will be notified of your tag and photo will be visible to their profile which can also be seen by their followers which leads to information exposure to the unknown person.

Steganography: Steganography is the art and science of embedding secret messages in such a way that no one can understand apart from the sender. Basically it is a technique of hiding secret data in image format, the receiver will not get to know the existence of a secret message.

For example a picture of a doll may have a malicious code which deletes or steals files of your system which result in information exposure without your permission.

Data Breach: Hackers gain unauthorized access to a computer system or network and steal private, sensitive, or confidential personal and financial information.

There are three different types of data breaches: physical, electronic, and skimming.

Traditional Threats

Phishing: Phishing is a technique of gathering sensitive information of a target such as password by disguising as a trustworthy entity. Phishing is a form of fraud where attackers commonly use phishing emails to distribute dangerous links.

Malware: Malware is malicious software; it comprises a number of harmful software that are a threat to all computer users. Malware is created for attack on privacy, spying, etc.

Clickjacking: Clickjacking is a malignant technique of tricking an end user into clicking on something different. This can cause users to unwittingly download malware, visit malicious web pages or purchase products online.

Spamming: Spam means unwanted messages or emails are known as spam. At times the internet is flooded with multiple copies of the same message, it is nothing but spam. Most spam is commercial advertising. In addition to wasting peoples time, spam also eats up a lot of network bandwidth.

Digital Stalking: Digital stalking refers to the use of the internet, email, or other electronic communication devices to stalk another person. Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly.

Metadata: Metadata can be defined as data about data. It describes the size, format and other characteristics of data are called metadata.

IV. Security Algorithms

A. Private Key/Symmetric Algorithms

Symmetric keys are called private key encryption; Symmetric key algorithms are sometimes referred to as secret key algorithms. Asymmetric key algorithms are generally considered more secure than symmetric key algorithms; the key is shared between the two systems in a symmetric key algorithm.

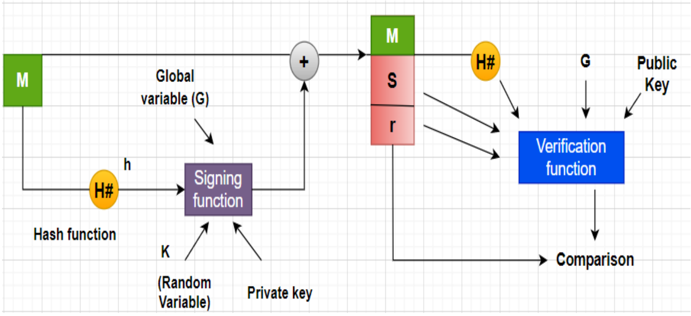
B. Public Key/Asymmetric Algorithms

Asymmetric cryptography called public key cryptography, is a procedure used for related keys i.e. public key and private key, to encrypt and decrypt a message and to save it from unofficial use. A public key is a cryptographic key that can be applied by any individual to encrypt a message and also be decrypted by the planned receiver with their private key.

C. Signature Algorithms

Federal information processing standard for digital signature.In digital signature implementation two primary algorithms are used first is RSA and second is DSA, it covers the process from key generation to signature verification. DSA does not encrypt messages digest using private key or decrypt message digest using public key. Instant it uses mathematical function to create a digital signature consisting of 2161 bites number which are originated from message digest the private key, DSA also provide 3 benefits:

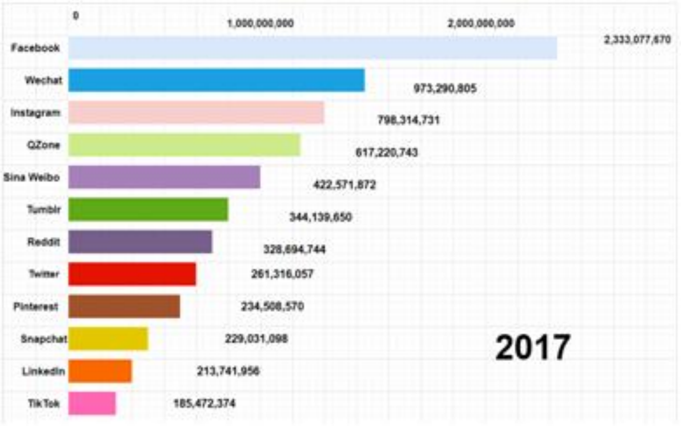
1. Message authentication
2. Integrity verification
3. Non repudiation

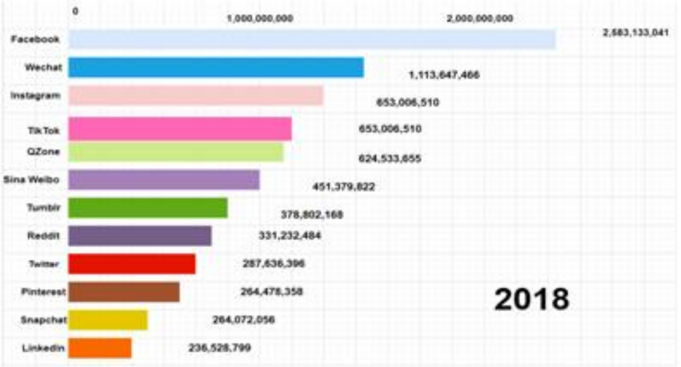


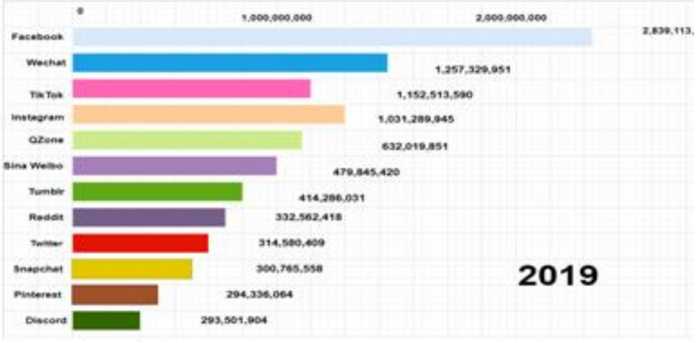
D. Hash Algorithms

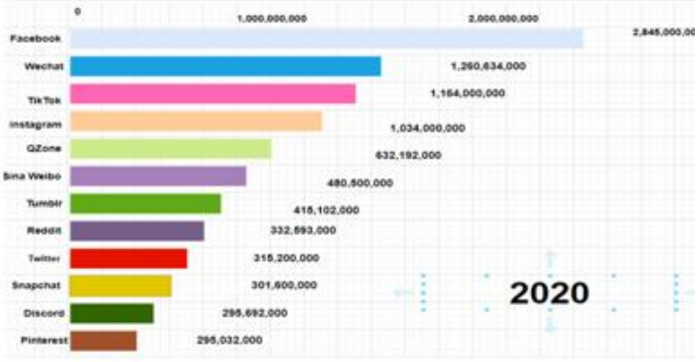
A hash function is a function which takes input of any length and then returns a special character string. This special identifier can recognize the data in the special form. Through this key one can identify the data. Hash counts are the things returned by the hash work which are also known as hash codes, digests or just hashes.

V. The Rise of Social Media





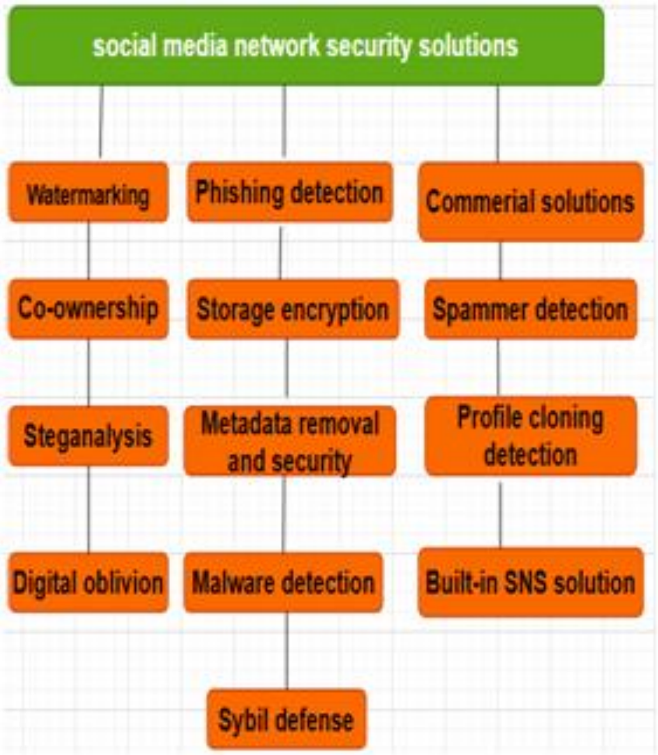




The internet has brought about many changes into our day to day life. The internet has opened up communications across the boundaries of the world. Due to easy availability of the internet people have become more active. Social networking helps people to interact with your friends, enhancing their careers and providing more opportunities virtually. Users on social media have taken a huge rise. In 2020, over 3.6 billion people were using social media worldwide. As you can see various social media platforms are taking a high rise. Facebook is the most used platform due to the increase of people on social media there is an increase of threats.

The most used social media platforms are Facebook, Instagram, and wechat. People on these platforms are increasing day by day and opening their personal data publicly which leads to threats. People share their personal data as stories, posts and by mentioning each other people on such platforms share their personal data to hackers unknowingly which leads to serious attack users also share their video as an entertainment but attackers edit those videos in wrong way and start blackmailing as users are increasing on social media users should avoid sharing intimate data such as birthdays, phone number, address, hometown specially your location which can lead a massive attack. Avoid sharing post on social network unless you have a tight grasp over your privacy settings and are comfortable with the group of people you are connected with.

Graph shown makes clear on which social network users should be aware and take care of personal data.



ISSN (online): 2581-3048
Volume 5, Issue 12, pp 40-44, December-2021
https://doi.org/10.47001/IRJIET/2021.512008

VI. Solutions

In this section, we will briefly discuss social media network security strategies to prevent threats.

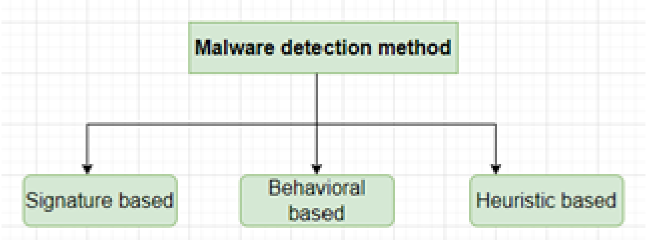
Storage encryption: In storage encryption the use of encryption for data both in transit and on storage media .Data is encrypted when it is passed to storage devices, for eg: individual hard disks, storage encryption is a good way to make sure the data is safe.

Malware detection: Malware detection is the method of scanning the devices and files to detect malware. Malware is a malicious code which is developed to harm a computer or network. The malware detection and prevention equipment are widely available for servers and mobile devices. We can find malware, spyware or virus using netstat and tcpview.

There are two types of malware:

1) Known
2) Zero day threat (unknown)

Types of detection:



1) Signature

Signature based malware detection is the most common method used by commercial antiviruses, but it can be used in the cases which are completely known and documented.

2) Behavior

The main advantage of the behavior based malware detection techniques is the ability to detect the kind of malwares that signature base techniques are unable to detect like unknown and polymorphic malware variants.

One example of a behavior based detection approach is the histogram based malicious code detection technology patented by Symantec.

A behavior-based detector basically consists of the subsequent components

- Data Collector: This component collects dynamic / static information about the executable.
- Interpreter: This component converts raw information collected by data collection module into intermediate representations.
- Matcher: it's wont to compare this representation with the behavior signatures.

Built-in SNS solutions: A Social Network Service (SNS) is a web service for beginners for all practical connections between people with similar interests, backgrounds. A SNS allows its users to find new friends and enlarge their circle of friends. In SNS data sharing is a key feature where users can be able to share their interests, activities, photos, etc.

Co-ownership: A co-owner is an individual or group that shares ownership in a valuable thing with another individual or group. Whether started by law or by agreement of the co-owners, the property is impressed with a Fiduciary nature so that each co-owner becomes a trustee for the benefit of his co-owners.

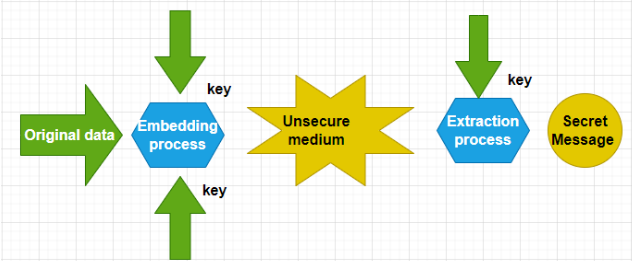
Watermarking: Watermarking is the practice of hiding a message about an image, audio clip, or other work of media within the work itself. The watermark becomes visible as a result of a special viewing process.

Example:

- Sending a message to a spy by marking certain letters in a newspaper using invisible ink.
- Adding sub-perceptible echo at a certain place in an audio recording.

Digital watermarking: Digital watermark technology is a digital signal or pattern inserted into a digital image now drawing attention as one of the useful methods of protecting copyright and security of digital contents.

Steganography: Steganography the tactic of disguising a message, video, record or picture inside another message, video, document or picture is named Steganography. The word steganography comprises a Greek word steganos, which implies "anchored, guaranteed, or disguised,". All the favored Social Media Networks provide the user with the functionality to upload high resolution images; this might lead to users using this data for spreading malicious code with Steganography. There exist many steganalysis methods which might detect malicious pictures and media. Steganalysis is finished primarily using ML techniques within which an oversized data-set is employed to coach the machine so as to urge it to find out about regular images and this then filters out the malicious images and doesn't let it spread.



VII. Conclusion

After evaluation, it has been discovered that 78.nine% of the threats that actuate the social media networks do not appear to be truly security faults rather they feed on the users lack of knowledge[3] on dealing with computer systems and traversing the net. By means of deceiving such users and making they click on malicious links and making them download malicious code they breach the privacy of these customers. Although businesses like Google and fb use complicated gadget getting to know algorithms for spam detection, they even have a 5% risk of no longer having the potential to detect spam.[9] by means of educating users of unsolicited mail emails and phishing, we are able to clearly negate 70% of threats being faced.

REFERENCES

[1] G. Jacob, H. Debar, and E. Filiol, “Behavioral detection of malware: from a survey towards an established taxonomy,” Journal in Computer Virology, pp. 251–266, 2017.

[2] Shailendra Rathorea, Pradip Kumar, Sharmaa Vincenzo, Loiab Young Sik Jeongc Jong, Hyuk Parka Social network security: Issues, challenges, threats, and solutions.

[3] Barinka, Bad Day for Newsweek, Delta Amid Social-Media Hackings, Online; accessed 04 April 2017.

[4] Sangho Lee et al WARNINGBIRD: Detecting Suspicious URLs in Twitter Stream.

[5] El Asam et al “Cyberbullying and the law: a review of psychological and legal challenges” Comput. Hum. Behav. 65 (2018).

Citation of this Article:

Aditi Gupta, Shweta Mehetre, Abhilasha More, “Security in Social Media” Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 5, Issue 12, pp 40-44, December 2021. Article DOI https://doi.org/10.47001/IRJIET/2021.512008

****