Social Media– A Mode for Cyber Attacks

Surbhi Jain[1], Ashwarya Arora[2], Shelja Sharma[3]
Department of Computer Science Engineering,
Faculty of Engineering & Technology, Manav Rachna International Institute of Research & Studies

ABSTRACT
Online networking is a platform, used to portray the collaboration of people in which they produce and share their views. The effect about social networks with respect to youngsters may be critical. Kids are experiencing childhood encompassed by versatile gadgets like tabs, mobile phones, laptops etcetera. Consequently, sites such as Twitter, MySpace and Facebook have become a regular part of their life. The social system is transforming those ways, over which youngsters connect to their parents & peers. The impacts of social media are twofold. The positive side is that, one can improve their skills, be more expressive and seek business opportunities. On the other hand, its negative side includes cyber crimes like cyber bullying, identity theft, loss and misuse of credentials. The purpose of this paper is to bridge the gap in the existing literature by exploring the predecessors of information disclosure of social media users. We present a systematic study of various Security Issues and Challenges in Social Networks. This paper also, throws light on the Procedure of Execution of various Attacks, Actions, Effects, Examples & Various Protective measures, pertaining to risks and crimes observed in social media platforms. Further, work can be done in the direction of developing an efficient mitigation technique to prevent various attacks.

Keywords
Social Networking, IOT Botnet, Spear Phishing, Ransomware, Mitigation Techniques

1. INTRODUCTION
A network is an anthology of numerous computer systems or any other devices, capable of transmitting & receiving signals, connected together to exchange information. Based upon geographical area span, There are four types of networks viz. LAN, MAN, WAN & PAN as shown in Fig.1.

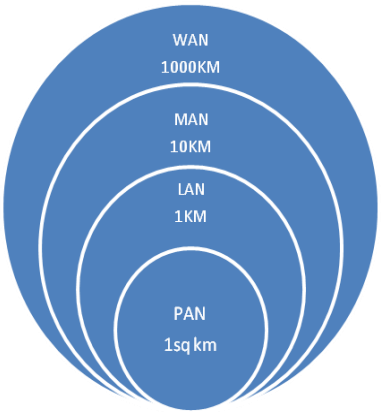

Fig 1: Types of Networks

Modern organizations ponderously rely on information systems, evolution of mainframe computers from timesharing computers in 1960's and 1970's, network systems in 1980s and Internet-based workstations in 1990s.Over the past years, the emergence of new example in communication systems has been seen [1]. As the technology advances, people are compelled to adopt different lifestyles. Internet usage developed quickly in the West from the mid-1990s and from the late 1990s in the growing world. In the two decades from that point forward, Internet utilization has grown 100-times, measured for one year, to more than 33% of the total population [2]. Six Degrees, the main noticeable social networking site, was made in 1997. It authorized users to transfer a profile and make acquaintances with different users. In 1999, the first blogging site ended up projecting, making an imprint social medium that is as yet mainstream even now [3]. Earlier people used to associate with club for gatherings and workshops. Nowadays, people communicate online through social networking. The most dominant example of a WAN (Wide Area Network) is the Internet, which provides us access to social networking as shown in Fig. 2.

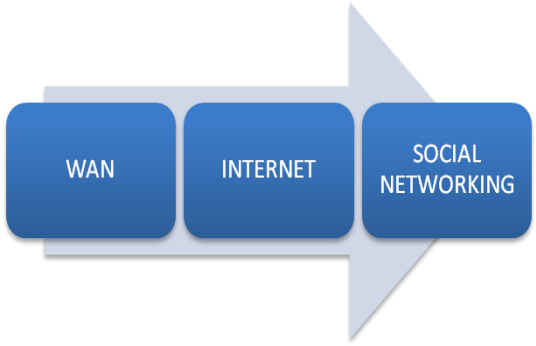

Fig 2: Access to Social Networking

A social networking site (also SNS or social media), is an Online Information highway, that people use to share their opinions, spirits, sentiments etc. without being biased. Examples of social media tools include blogs, social networking sites, micro-blogging sites, photo- and video-sharing sites, wikis, RSS feeds, and podcasting. Web sites like Facebook, LinkedIn and Twitter, allow users to make profiles, upload pictures, share information, send messages, interact and communicate with people all around the world. Everything has its pros and cons and of course social media is not an exception. It has many advantages such as, it helps to connect people all around the globe, one can share popular beliefs, seek a new job, find romance, access news, real time information sharing, Academic benefits, commonality of interest, Increased News Cycle Speed- like availability of every information from a terrorist attack to theft in a nearby bank alerting public and targeted advertisement. As per the saying, every coin has two sides, the cons of social media includes cyber-bullying, crime against children, and risk of fraud and time waster.

Social networking sites provide a single platform, for multiple users for information sharing and there's a lot of return on investment, for attackers in following them. Keeping social networking more secure, are the challenges that have been a major concern for every user as it has also become a novel attack ground for malware coders. They are scattering

damaging code and distributing spam messages by taking a benefit of the user's blind faith in their associated networks. Social networking sites act as a medium to spread these malware codes. Once the ignorant user falls in a trap and click on the malicious link, all his credentials are stolen. Thus, when the data is processed using technology, the originated risk warrants for the Information Security.

The criteria to establish information security includes, identifying the particular threats and vulnerabilities of a particular code. To assess the security, risk and susceptibility must be coupled to create a subsequent effect. That is, a precise risk must exploit susceptibility for an effective attack to occur. The criterion is divided into three main parts which are called as the CIA (Confidentiality, Integrity and Availability) triads of information security. Confidentiality makes sure that, only the lawful people have admittance to the data. Veracity, guarantees that the data is not tarnished in any way. Finally, accessibility ensures that the information is readily available to the authorized users. In spite of all the security measures, one should be self-aware and careful about uploading stuff online, being careless can lead to unexpected mishaps.

In this paper, systematic study of various cyber-attacks, that happened recently is being represented and also have discussed, the procedure of attack execution, effects, examples & Various mitigation measures, from risks and crimes prevailing on social media.

2. LITERATURE REVIEW

Presently, in the period of advanced Internet technology, Communal Networks turned out to be unimaginably well known platform on the Internet and is extensively used everywhere around the globe. It provides an easy means of sharing facts & figures with other clients, having a mutual interest such as likes, adores, dislikes, displeasures, job details, current town details, interests, relationship status, political views etc. It also helps in upgradation of academic, personal, professional and scientific knowledge of the user. Unfortunately, many users share personal information without being aware of the privacy risks associated. As per the Literature, there are several researchers who have highlighted the security risks through social media in their publications as mentioned below.

Abhishek Kumar et al. [4], presented the safety worries, the attacks and their respective anticipation practices in social media. They proposed the architecture for secure request, response exchange of information between clients. This architecture enhances the customization of profiles. They discussed that social networking sites give a virtual domain to individuals to share every last movement, their interests, and their circle of acquaintance with their family, companions, or even the unknown. This requires advancement in security conventions to protect against programmers. Their research recommends that exclusive and appropriate learning of the hacking methodologies will demonstrate the best guard in the war against cyber-attacks.

Wei Yang et al. [5], proposed a predictive framework to recognize potential collective actions considering the future development and additionally current circumstances. In the structure, a future sign to describe events is improved and the enhanced gray system theory is used to predict the evolution of the future sign. They also describe two phases: Identification and Prediction. In the Identification phase, the framework evaluates events based on the sentiment and a number of related tweets. The sentiment is analyzed using a sentiment analysis tool-semto strength. Thus, the number and sentiments are comprehensively transformed into the interpretation. On the off chance, if the whole sentiment is negative and the estimation of the interpretation is higher than a threshold, the related occasion is viewed as an aggregate activity. Otherwise, the signal related to the event is regarded as a weak signal in the Identification stage. The identification stage just considers the present circumstance, overlooking the future change of the number. For the production stage, gray system theory is utilized to judge whether the weak signal can advance into a strong signal, based on analyzing the sentiment and anticipating the change of the number, before the flashpoint of a collective action. At that point, the translation is utilized to judge whether the occasion has turned into an aggregate activity.

Jianqiang Hao et al. [6], proposed a structure for real time monitoring of public perception to security break occasions, utilizing web-based social networking metadata. Then, an experimental study might have been led by them with respect to a example about 1,13,340 related tweets assembled in august 2015 on twitter. By content mining an extensive number of unstructured, real time information, the author extracted topics, opinions and information about security breaches from the overall population. The time arrangement analysis recommends critical patterns for various points and the outcomes from sentiment analysis shows a significant difference among topics. This paper fill gaps by proposing a framework for studying the Online networking, observation on security breaches along with an experimental contemplate on shed light on public attitudes and concerns.

O' Donovan et al. [7], portrayed faith as the unwavering quality of a partner profile to distribute precise recommendations in the past. Authors have described the profile-level trust and item-level trust as two models of trust. The item-level trust for a client is characterized in view of his profile and rate of times that has made a precise rating estimation for the profile over some sets of clients.

Bo fu [8], proposed a trust model which is personable and special sable. Research into this area demonstrates that trust is a view that is incredibly different among individuals, circumstances and conditions. Trust management methods in OSNs have been constrained to get to control strategies that take an exceptionally rearranged perspective of trust and overlook different basic qualities of trust. Subsequently, they failed to give a customized way to manage the trust. In this manner, there is a need of architecture to figure out the credibility of the content and to figure reliability of the client with the state of having a distinctive user id based on the calculated credibility.

Hak J. Kim [1], has discussed various security risks through social media and also created a model through which these risks can be accessed. The criteria of evaluation include confidentiality, integrity and availability respectively. This model can figure out the risks and help to design good security systems for corporate.

Wu He [9], discussed numerous safety jeopardies and prevailing mitigation techniques in order to help organizations to address these risks in a better way. It aware users about 8 major threats, namely insufficient authentication controls, phishing, information leakage, cross site scripting, cross site request forgery, injection flaws, information integrity and insufficient anti-automation which was stated by The Secure Enterprise 2.0 Forum in 2009. It has also presented an in-depth discussion about these seven mitigation practices

(Developing a social media acceptable use and security policy, Software update, Archiving social media content, Develop a social media incident notification, Routine social media site monitoring, Monitoring employee's Internet activity, User education and training program and Response plan) to help organizations tackle with these risks.

Candid Wuest [10], discussed the major threats aiming on different social media platforms. The malware authors are spreading various worms and spam throughout the social networking websites. The major security risks include phishing, resetting passwords, befriending someone to extract information, Scripted threats, etc. Sometimes due to curiosity, ignorant users click on wrong links and become victim of these attacks. Thus, the users should be cognizant of the vulnerabilities and risks of social media.

Rakesh Singh Kunwar et al. [11], provided a detailed study of threats, security risks and different types of attacks using social media. Anyone can attack through social media by applying these steps: gathering information through social media, Building a huge online network, Sniffing, Disclosure about network and infrastructure, other threats. They also discussed, detailed study about threats like spamming, manual script attacks, malware attacks, click jacking etc.

3. RECENT ATTACKS AND MITIGATION TECHNIQUES

This section discusses the various risks, which can take place while accessing social media. In today's world social media has become a part of people's daily routine and people love to post things online. Unfortunately, large numbers of people are unaware of the various kinds of risks and undesirable circumstances associated with it. This section represents the introduction, types, and steps of execution, recent examples and mitigation techniques of various major recent attacks, including major attacks of the year 2017 yet.

3.1 Ransomware

Ransomware is a sort of pernicious programming, meant to block access to a PC system until an amount of money is paid. Although it's hard to think, but the very first Ransomware attack emerged in the past 27 years ago in the year 1989, termed as "AIDS Trojan". The two malwares trending these days are Encrypting- Ransomware and Locker- Ransomware. Encrypting- Ransomware is based on encrypting algorithms. The attacker blocks the target files & the system and denies the access until the victim pays a sum of money. Based on this condition, the victim is provided with the decryption key. Locker- Ransomware is the attack in which the attacker only unlocks the victim's operating system and allows the access to destopand applications when the victim pays him the desired amount [13]. 'Locky', has become a very common ransomware these days. It arrives as a word document and asks for macro's to be enabled. Once done, this word file runs the 'Locky Code' and scrambles all the systems, data and then demands for bitcoin [12]. Hospitals, police stations and educational institutes become the most common places to suffer such attacks.

3.1.1 Steps of Ransomware Attack Execution [31]:-

a. Exploitation and Infection: An attack to be effective, the malicious ransomware document needs to execute on a computer. This is regularly done through a phishing email or an exploit kit- a sort of malicious toolbox used for adventure security openings in programming applications for the purpose of spreading malware.

b. Delivery and Execution: The ransomware executable is conveyed to the victim's framework, which normally takes only a few moments, depending upon system latencies. We frequently, observe the executable documents placed in folders underneath the user's profile. To enhance detection, your association can screen for those occasions and set up a line of defense.

c. Backup Spoliation: After the malware is executed, the ransomware targets and expels backup records. Generally, it needs to evacuate any methods the victim needs to recover from the attack without paying the ransom. This function is unique to ransomware, as different sorts of crime ware and even APTs don't try to erase backup records.

d. File Encryption: Once the backup is totally evacuated, the malware will perform a safe key exchange with the command and control (C2) server, setting up those encryption keys that will be utilized in the local system. Unfortunately, the majority of the variations today use strong encryption, for example, AES 256, so the victim won't be ready to break the encryption on their own.

e. User Notification and Cleanup: With the backup documents evacuated and the encryption dirty work done, the demand instruction for blackmail and installment are introduced. Regularly, the victim is given a couple days to pay, and after that time the ransom increments. Once paid, the malware wipes itself off the victimized system so as not to abandon behind scientific confirmation that would enable form to better defenses against the malware.

3.1.2 Examples of Ransomware Attack

- The Wannacry Ransomware attack began on 12 May, 2017 and within a day infected more than 230,000 computers in over 150 countries, Parts of Britain's National Health Service (NHS), Spain's Telefónica, FedEx and Deutsche Bahn were hit, along with many other countries and companies worldwide [27].
- In February 2016, Hospital, Hollywood Presbyterian Medical Center in Los Angeles became the victim of ransomware attack. The systems were blocked and to regain the access, hospital was asked to pay $3.4m, which was later reduced to $17,000 [14].

3.1.3 Following measures should be considered, in order to prevent a system from such attacks [13]:-

- One should turn off the macros, in MS office.
- One should keep; back up of data, one on external hard disk and the other on cloud.
- Never open emails from unknown sender.
- Keep the operating system and software up-to-date.

3.2 Business Process Compromise Attack

Business Process Compromise (BPC) is a kind of attack that has come into concentration recently. It especially focuses on one of a unique process or machines encouraging these procedures to discreetly control them for the attacker advantage. Attackers infiltrate the enterprise and search for vulnerable practices, susceptible systems, or operational loopholes. Once a weakness has been distinguished, the procedure is modified to profit the attacker, without the enterprise or its client identifying the change. The victim trust on the procedure is continuing as expected, however, in reality the attacker are as of now picking up either finances or

products from the venture. These attacks are conceivable because numerous employees basically make a cursory effort of business procedures, trusting policy that have always worked and are required to keep working with no issues [15].

3.2.1 Steps of Business Process Compromise Attack Execution [32]:-

a. **Reconnaissance:** The meaning of reconnaissance is to look at a circumstance before making a move. Before propelling an attack, attacker initially recognizes a vulnerable target and investigates the most ideal approaches to endeavor it. What is the authoritative structure? Who are the weakest connection workers? The initial target can be anybody in or associated with an association, whether an official or an administrator or an outsider provider. The attackers essentially require a single point of access to get started.

b. **Scanning:** Once the target is recognized, the next stage is to distinguish a weak point that enables the attackers to get entrance. This is normally expert by examining an association's system with tools effortlessly found on the web to find entry points. Then the attackers search for vulnerabilities.

c. **Access and escalation:** Since those weaknesses in the target system are recognized, the next stage in the cyber-attack is to get entrance and after that escalate to moving through the system undetected. In all such cases, privileged access is required because it enables the attackers to move unreservedly within the environment. Rainbow tables and comparative tools enable intruders steal credentials, escalate benefits to administrators, and after that get into any system on the network that is open through the administrator account. Once the attacker increase elevated benefits, the system has viably assumed control and "claimed" by the intruders.

d. **Exfiltration:** With the opportunity to move around the system, the attackers can now access systems with an association's most sensitive information – and extract it voluntarily. In any case, taking private information is not only action intruders can take this time. They can likewise change or erase records on compromised systems.

e. **Sustainment:** The attackers have now gained unrestricted access all through the targeted system. Next is sustainment or remaining set up discreetly. To accomplish this, the hackers may secretly introduce malicious programs like root packs that enable them to return as frequently as they need. Also, with the elevated benefits that were gained before, dependence on a single access point is no longer fundamental. The attacker can go back and forth, however they please.

f. **Assault:** Fortunately, this progression is not taken in every cyber-attack; it is the phase of an assault when things turn out to be especially awful. This is the point at which the programmers may adjust the functionality of the victim's equipment, or debilitate the equipment totally. During the assault stage, the assault stops to be stealth. However, the attackers have successfully taken control of the environment, so it's too late for the ruptured association to protect itself.

g. **Obfuscation:** Generally the attackers need to conceal their tracks, yet this is not all around the situation – particularly if the programmers need to leave a "calling card" behind to boast about their endeavors. The motivation behind trail obscurity is to confuse, disorientate and divert the forensic examination process. Trail obfuscation covers an assortment of systems and tools including log cleaners, spoofing, misinformation, Trojan commands and more.

3.2.2 Example of Business Process Compromise Attack

- In year 2016, the Bangladesh Bank Occurrence is another notable BPC assault, where the attacker figured out how to introduce various layers of malware into the bank's system and exploit the communication process between the bank and SWIFT. The programmers sent solicitations from Bangladesh to the Federal Reserve Bank of New York, requesting millions to be transferred to accounts across Asia. They timed it to coincide with the end of the work week and also altered the printing system utilized by the bank to avoid discovery. An aggregate of US $81 million was lost and it happened simply because of a spelling blunder, the attacker found and further loss was prevented [15].

- After the Bangladesh Bank heist, two more banks announced that they were compromised through SWIFT-related procedures also. Vietnam's Tien Phong Bank distinguished false SWIFT messages that asked for an exchange of US $1.3 million- fortunately it was blocked. Banco del Austro in Ecuador was not so lucky, they apparently lost $12 million in 2015 from compromised transfer [15].

3.2.3 Following measures should be considered, in order to prevent a system from such attacks [15]:-

- Organizations should have a comprehensive view of their network, in order to prevent from such attacks and have the capacity to recognize typical operations from unusual and conceivably malicious activities.

- They should also perform risk assessment and incorporate third party in their assessment. As observed in past cases, the transaction processes amongst vendors and suppliers are normally targeted.

- The Crucial system requires File Integrity Monitoring and Application Control/System Lock Down.

- Employees should be made aware, trained & educated on identifying anomalous behavior.

- Organizations should also pay consideration for implementing cyber security measures.

3.3 IOT(Internet of Things) Botnet

It's a collection of compromised computers infected with malware that permit an assailant to control them. Botnet herders are able to regulate the machine in their botnet by using IRC (Internet relay chat) issuing commands to carry out malicious events such as DDos attacks, sending spam email and information threats. Botnets are zombie computers which form a zombie army and target the computers by sending spam emails, deliver ransomware and other spyware [16].

3.3.1 Steps of Botnet Attack Execution:-

a. Scan the Victim's system for vulnerabilities and installs the exploit pack.
b. A script is executed on the infected code, called the shell code.

c. An image of actual bot is fetched by the shell code.

d. The Victim's computer, then runs the malicious code on its own, every time the computer is rebooted.

e. A command and control channel is established in order to communicate with a control server.

f. The bot now receives and executes commands which are via command and control channel (IRC) by the attacker.

g. The bot's connection with the bot master is maintained continuously and they keep the bot-master updated about their binary code.

h. The bot master uses DNS (domain name system).

3.3.2 Examples of Botnet Attack

- Mirai botnet source code has been updated with major changes, after it leaked. On February 2017, the US College suffered a 54 hour attack by the Updated Mirai Botnet Malware. It was a "Layer 7" attack, which focused on exhausting server resources, rather than obstructing the college's bandwidth with junk traffic. This attack maintained a flow of 30,000 HTTP requests per second during the whole 54 hours of flooding the network [17].
- In October 2016, a Botnet comprised of 100,000 compromised IoT devices, thumped an Internet framework supplier halfway disconnected. Bringing down that supplier, Dyn brought about a course of impacts that, at last created a long list of prominent sites, including Twitter and Netflix, to temporarily vanish from the Internet [18].

3.3.3 Mitigation measures to prevent from such attacks [19]:-

- Block the inbound traffic at one firewall. The attacker can't activate the system, if the contact is not possible.
- One can knock down known botnets by running up-to-date antivirus.
- An intrusion detection system can be installed to analyze malicious activities and alert the user.
- Block outbound traffic on port 25.

3.4 Spear and Whaling Phishing

Spear phishing targets a group of people of specific companies, customers of a specific company or even a specific person. In one version of a successful spear-phishing assault, the attacker finds a website page for their target association that provisions contact data for the organization. Using accessible details to make the message appear to be valid, the attacker drafts an email to an employee on the contact page that seems to originate from a person who may sensibly ask for confidential data, for example, a network administrator. The email requests the employee to sign into a bogus page that demands the worker's username and password, or tap on a link that will download spyware or other malicious programming. If a single employee falls for the spear phisher's ploy, the attacker can take on the appearance of that individual and utilize social-building strategies to increase additionally access to sensitive information [21].

3.4.1 Steps of Phishing Attack Execution:-

a. **Fake login page:** First of all, a fake login page of any web account, one wants to hack is required.

b. Creating phishing.php file: A PHP script is required which will collect all the form data. After collecting the form data, the following code is copied into a text editor and it should be saved as phishing.php.

c. **Creating an index.html page:** Go to xxxxx.com, right click anywhere in the browser and choose the view page source. Open the source code in a text editor.

d. **Word action:** Now a new window pops-up where all the HTML code can be seen. Here there is a need to look for word action. By pressing CTRL+F and searching for action, a link like this action https://www.xxxxx.com/login.php/login_attempt=1 will be found.

e. **Replace the link:** After the above steps, the link is replaced with phishing.php like action "phishing.php" and the page is saved as index.html.

f. **Create account:** An account on a free hosting website like YYY.com is created.

g. **Upload files:** Now "phishing.php" & "index.html" are uploaded to the folder that was created inside the fake website. So when uploading part can be done, the link to the phisher can be www.yourname.YYY.com/xxxxx/index.htm with any message like "change your Facebook password" etc. if anybody logs in on the fake page, then their usernames and passwords are stored on the free hosting websites account in log.txt file.

h. **Send the link to the victim:** Now the link of this fake site in sent to the victim, as soon as they login, a file named login.txt will store in the account of free hosting website with passwords of the victim. And the fake login page will redirect to a real login page which will ask the victim to verify the password.

3.4.2 Example of Spear and Whaling Phishing attack

- In May 2017, airline travelers, particularly focused on a campaign aiming to infect a system with malware and the British Foreign Office targeted in a maintained attacker intended to trap staff into giving over email accreditations. Even more recently, the French presidential elections have been damaged by the cyber espionage Fancy Bear focuses on Emmanuel Macron trying to introduce malware on his campaign site [20].
- In June 2015, the organization lost $46.7 Million as a result of a spear phishing email. A report by the U.S. Securities and Exchange Commission demonstrates that the attack was carried through "employee impersonation and false demands from an outside entity targeting the Company's finance department. This fraud brought about exchanges of assets accumulating $46.7 million held by an organization backup joined in Hong Kong to different abroad records held by third parties." The exchanges were performed specifically by Ubiquiti workers that were tricked into thinking that they were getting legitimate request from officials on account to spoofed email addresses and clone spaces. Fortunately the genuine organizational frameworks were not compromised, but the incident shows the relative simplicity with which a spear phisher can trap victim into performing activities directly using impersonation and data broadly accessible on the web to produce realistic spoofed e-

mails [30].

3.4.3 Mitigation Measures to Avoid such Attacks [21]:-

- The best measure to safeguard your business against being the victim of a successful Spear Phishing assault is staff security awareness.
- Rules or ideally an approach embraced by the CEO, should be issued to all staff instructing them, NOT to tap on website links or connections in spontaneous messages or messages from untrusted sources. If all else fails, they ought to check with the IT security chief. Issue normal suggestions to this impact and highlight this necessity in any security mindfulness preparing.
- Use anti-malware solutions and stay up with the latest and consider other specialized countermeasures that may be suitable for your framework.

4. ANALYTICAL ANALYSIS OF VARIOUS RECENT ATTACKS WITH THEIR MITIGATION TECHNIQUES

This section presents the procedures of attack, actions, effects, examples and mitigation techniques of various recent attacks in Table 1 and Table 2, presents the experimental work carried by the various researchers on various attacks discussed in table 1.

Table 1: Analysis of Attacks & Their Mitigation Techniques

ATTACK	PROCEDURE OF ATTACK	ACTIONS	EFFECTS	MITIGATION TECHNIQUE	EXAMPLES
Ransom-ware	(a) As a first step, attacker infects the computer, then malware find the files with JPG, XLS and PNG extension. (b) Hackers will encrypt the files having important images and documentation. (c) After encryption, malware tells that the data is being held for ransom and gives a site to access. (d) Now, the user needs to access the browser named TOR. (d) Then, the user also needs to buy the bitcoins to pay the hacker. So that hackers will decrypt their important documents [22].	'Locky', has become a very common ransomware these days. It arrives as a word document and asks for macros to be enabled. Once affected, the infected word file runs the 'locky code' and scrambles all the system's data and then demands for bitcoin [12].	a) Permanent or temporary loss of sensitive information [23]. b) Disruption of regular operation, harm to the organizations reputation [23].	(a) Turn of the macros, in MS office. (b) Back up of data, either on external hard disk or on the cloud. (c) Never open emails from unknown senders [13].	(a) In Feb 2016, hospital Hollywood Presbyterian medical center in Los Angeles became the victim of Ransomware attack [14]. (b) Wannacry ransomware attack [27].
Business process compromise attack	(a) Attackers infiltrate the enterprise and search for vulnerable practices, susceptible systems, or operational loopholes. (b) Once a weakness has been distinguished, the procedure is modified to profit the attacker, without	The Executive has impersonated by the cyber criminal and sensitive information is transferred by the employee to the phisher.	a) Fraudulent transfer of money [15].	(a) Organizations should have a comprehensive view of their network, and have the capacity to recognize typical operations from unusual and conceivably malicious activities. (b) Perform risk assessment and incorporate third party in their assessment. As	The 2016 Bangladesh bank is the example of business process compromise attack, assault [15].

	the enterprise or its client identifying the change. (c) The victim then trusts the procedure is continuing as expected, however, in reality the attacker are as of now picking up either finances or products from the venture [15].			observed in past cases, the transaction processes amongst vendors and suppliers are normally targeted, crucial system should be considered for file integrity monitoring and application control/system lock down [15].	
IOT botnet	(a) Scan for the Internet accessible IOT devices. (b) Exploit the device with factory default or hard-coded username or password. (c) Affected device turned into bots which is used in DDoS attack. (d) Now it waits for the instruction to attack the target.	(a) Scan the system of victim for vulnerabilities and install the exploit pack. (b) A script is executed on the infected code. This script is called shell code. (c) The image of actual bot is fetched by shell code. (d) The victim's computer, then runs the malicious code on its own, every time the computer is rebooted. (e) A command and control direct is built up keeping in mind the end goal to speak with a control server. (f) The bot now receives and executes commands which are via command and control channel (IRC) by the attacker. (g) The bots connection with the bot master is maintained continuously and they keep the bot-master updated about their binary code. (h) The bot master uses [DNS (Domain name system).	a) Network performance issues. b) DDos attacks in scanned networks [24].	(a) Block the inbound traffic at one' firewall. The attacker can't activate the system, if the contact is not possible. (b) One can knock down known botnets by running up-to-date antivirus. (c) Install an intrusion detection system to analyze malicious activities and alert the user. (d) Block outbound traffic on port 25 [19].	(a) Mirai botnet source code released [17]. (b) In October 2016, a Botnet comprised of 100,000 compromised IoT devices, thumped an Internet framework supplier halfway disconnected. Bringing down that supplier, Dyn brought about a course of impacts that, at last created a long list of prominent sites, including Twitter and Netflix, to temporarily vanish from the Internet [18].

Spear phishing	(a) The attacker drafts an email to an employee on the contact page that seems to originate from a person who may sensibly ask for confidential data, for example, a network administrator. (b) The email requests that, the employee has to sign into a bogus page that demands the worker's username and password, or tap on a link that will download spyware or other malicious programming	Potential victims are targeted by fraudsters via email [25].	a) Loss of employee productivity. b) Financial loss. c) Loss of customers. d) Loss of brand reputation [26].	a) Staff security awareness. b) Staff MUST NOT click on website links or attachments in unsolicited emails. c) Use anti-malware solutions and keep the systems up-to-date [21].	(a) In May 2017, airline travelers, particularly focused on a campaign aiming to infect the system with malware, and the British Foreign Office targeted in a maintained attacker intended to trap staff into giving over email accreditations. [20]. (b) In the case of Ubiquiti Networks Inc., an American network technology company for service providers and enterprises [30].

Table 2: Experimentations on Various Attacks and Results

SNO	AUTHORs NAME	TITLE OF THE PAPER	EXPERIMENTAL WORK	RESULTS OF THE EXPERIMENT
1.	Jan-Willem Nijhuis	Effect of IoT botnets on Cryptocurrency [33]	An author analyzed cryptocurrency mining, in order to determine at what extend botmasters will use the processing power of IOT botnets. Thus, raspberry pie 2 is used to determine, whether the value obtained from other sources are accurate or not. In the same context, Author find the hashrates with the help of the program, called a cpuminer. This program requires a pool address to work for and store the mined currency which is used to mine bitcoin.	There is a minor variation in results obtained by the experiment with respect to the data from the sources. The hashrates results are also generated after running cpuminer on the raspberry pi.
2.	Monika, Pavol Zavarsky, Dale Lindskog	Experimental analysis of ransomware on windows and android platforms: Evolution and Characterization [34]	In this paper the authors detected the evolution and characterization of ransomware families by using various tools and detecting techniques such as APKtool, PEiD tool, PE View and RegShot. They also discussed the lifecycle of ransomware on windows and android environment.	Their results revealed that very similar characteristics are exhibited by the significant number of ransomware families.
3.	Tzipora Halevi, Nasir Memon, Oded Nov	Spear-Phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks [35]	The authors tried the experiment of phishing, which was based on the deception without revealing the details of the employees. In this they included two stages: The first stage in which the participants filled out the survey and then a phishing email were sent to them. All these experiments were started with the permission of IRB.	The results revealed that, out of the 40 participants who filled the questionnaire, 25 participants clicked on the link and 12 clicked on the 'download plug-in' button. Overall, 30% of the participants were phished, with 40% of the women and 26% of the women responded to the phishing attack. All the results in this paper were calculated using the Bivariate Pear-son two-tailed correlation. The

				results were ranked from 1 to 5.
4.	Joseph Barjis	The importance of business process modeling in software systems design [36]	In this paper, the author proposed a method of business modeling process and their method is based on the innovative language-action perspective. The following criteria are used for defining the aspects of the proposed method such as syntactic quality, pragmatic quality, expressivity capability, theoretical foundation and adequacy features, which can help in adhering the business process modeling tool. They have also tried to overcome a remedy of lack of direct model checking feature.	Their results with respect to criteria-syntactic quality, pragmatic quality, expressivity capability, theoretical foundation and adequacy features, highlights the importance of business processing model in system software design and also used to overcome the remedy of direct model checking features.

5. CONCLUSION

Social networking has become a major part of people lives these days. They tend to post every little detail of their lives on social media to share it with their friends and families. This could lead to unexpected and unavoidable risks. Social media basically acts as a medium, to spread malware and capture all the private data. Some of the major risks are discussed in this paper along with the measures to avoid them. One should use social media in a way such that, all the benefits of social media can be accessed, without being a part of any risk.

We have aggregated a few major recent cyber-attacks, that affected multiple organizations recently. Some of the prevention and mitigation techniques have also been discussed along with each attack to safeguard the user from it and experimental work carried by the various researchers on some of the mentioned attacks has been discussed. In future work, we aim to analyze the behavior of various mitigation algorithms and their efficacy in prevention from the various attacks. Moreover, work can be done in the direction of developing an effective mitigation technique to safeguard from various attacks and to avoid victism.

6. ACKNOWLEDGEMENTS

We would like to express our thanks of gratitude to Accendere Pvt. Ltd. for Motivating us to complete this paper.

7. REFERENCES

[1] Kim, H. J. (2012). Online social media networking and assessing its security risks.International Journal of Security and Its Applications.6 (3).11-18.

[2] Internet. (2017, May 15). Retrieved May 17, 2017, from https://en.wikipedia.org/wiki/Internet.

[3] Hendricks, D. (2013, May 06). Complete History of Social Media: Then And Now. Retrieved May 17, 017, from https://smallbiztrends.com/2013/05/the-complete-history-of-social-media-infographic.html.

[4] Kumar, A., Gupta, S. K., Rai, A. K., & Sinha, S. (2013). Social networking sites and their security issues.International Journal of Scientific and Research Publications.3(4).1-5.

[5] Yang, W., Cui, X., Liu, J., & Liu, Y. (2016). Identification of Potential Collective Actions Using Enhanced Gray System Theory of Social Media. IEEE Access.4. 9184-9192.

[6] Hao, J., Hao, J., Dai, H., & Dai, H. (2016). Social media content and sentiment analysis on consumer security breaches. Journal of Financial Crime.23(4).855-869.

[7] J. O' Donovan and Barry Smyth, "Trust in Recommenders Systems, "IUI'05, pp. 167-174, ACM, 2005, New York, USA.

[8] Bo Fu, "Trust Management in Online Social Networks, "M.Sc. Dissertation, Department of Computer Science, University of Dublin, Trinity College, pp. 5-12, 2007.

[9] He, W. (2012). A review of social media security risks and mitigation techniques.Journal of Systems and Information Technology, 14(2), 171-180.

[10] Wüest, C. (2010). The risks of social networking. Symantec Corporation.

[11] Kunwar, R. S., & Sharma, P. (2016, April). Social media: A new vector for cyber attack. In Advances in Computing, Communication, & Automation (ICACCA) (Spring), International Conference on (pp. 1-5). IEEE.

[12] Magee, T. (2017, February 15). Most dangerous new cyber security threats 2017. Retrieved May 17, 2017, from http://www.computerworlduk.com/galleries/security/most-dangerous-new-cyber-security-threats-2017-3654719/.

[13] What is Ransomware and 15 Easy Steps To Keep Your System Protected [Updated]. (2017, May 15). Retrieved May 17, 2017, from https://heimdalsecurity.com/blog/what-is-ransomware-protection/.

[14] Staff, S. X. (2017, May 10). Hospitals must be prepared for ransomware attacks. Retrieved May 17, 2017, from https://medicalxpress.com/news/2017-05-hospitals-ransomware.html.

[15] Security 101: Business Process Compromise. (n. d.). Retrieved May 17, 2017, from https://www.trendmicro.com/vinfo/us/security/news/cybe

rcrime-and-digital-threats/security-101-business-process-compromise.

[16] What is a Botnet & How to Your PC From Being Enslaved. (2016, November 04). Retrieved May 17, 2017, from https://heimdalsecurity.com/blog/all-about-botnets/.

[17] Dima Bekerman (2017, March 30). New Mirai Variant. Retrieved March 30, 2017, from https://www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html.

[18] Schneier, B. (2017, April 06). Why website takedowns and other Internet mischief are still increasing. Retrieved May 17, 2017, from https://www.technologyreview.com/s/603500/10-breakthrough-technologies-2017-botnets-of-things/.

[19] Mitigate botnets in five steps. (n.d.). Retrieved May 17, 2017, from http://searchsecurity.techtarget.com/tip/Mitigate-botnets-in-five-steps.

[20] CEO. (n.d.). Retrieved May 17, 2017, from http://www.thecsuite.co.uk/ceo/information-technology-ceo/protecting-your-employees-from-spear-phishing-attacks/.

[21] Spear Phishing Attacks and Countermeasures. (2016, October 04). Retrieved May 18, 2017, from http://resources.infosecinstitute.com/spear-phishing-attacks-and-countermeasures-to-mitigate-against-them/.

[22] How Ransomware Spreads and Works. (n.d.). Retrieved May 17, 2017, from http://combofix.org/how-ransomware-spreads-and-works.php.

[23] What is the possible impact of Ransomware? (n.d.). Retrieved May 18, 2017, from https://security.berkeley.edu/faq/ransomware/what-possible-impact-ransomware.

[24] Catalin Cimpanu (2016, October 27). Botnet of 100,000 IoT Devices Behind Dyn DDoS Attack. Retrieved October 27, 2016, from news.softpedia.com › News › Security › Incidents.

[25] A. (2017, February 28). Phishing, vishing and smishing. Retrieved May 18, 2017, from http://www.actionfraud.police.uk/fraud-az-vishing.

[26] C. (2016, April 14). Survey Reveals Spear Phishing as a Top Security Concern to Enterprises. Retrieved May 18, 2017, from https://blog.cloudmark.com/2016/01/13/survey-spear-phishing-a-top-security-concern-to-enterprises/.

[27] WannaCry Ransomware Attack. Retrieved May 12, 2017, from https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

[28] Gambhir, M., & Doja, M. N. (2015, February). Novel Trust Computation Architecture for Users Accountability in Online Social Networks. In Computational Intelligence & Communication Technology (CICT), 2015 IEEE International Conference on (pp. 725-731). IEEE.

[29] Al Hasib, A. (2009). Threats of online social networks.IJCSNS International Journal of Computer Science and Network Security.9(11).288-93.

[30] Spear Phishing: Real Life Examples. (2017, March 02). Retrieved June 14, 2017, from http://resources.infosecinstitute.com/spear-phishing-real-life-examples/#gref.

[31] The Five Step Ransomware Defence Playbook. (n.d.). Retrieved June 15, 2017, from http://itspmagazine.com/from-the-newsroom/the-five-step-ransomware-defence-playbook. 7 steps hackers take to execute a successful cyber attack. (2016, February 03). Retrieved June 15, 2017, from http://www.information-age.com/7-steps-hackers-take-execute-successful-cyber-attack-123460872.

[32] 7 Steps hackers take to execute a successful cyber attack.(2016, February 2003). Retrieved June 15, 2017, from http://www.information-age.com/7-steps-hackers-take-execute-successfule-cyber-attack-123460872.

[33] Nijhuis, J. W. (2017). Effect of IoT botnets on Cryptocurrency from semanticsScholar.org.

[34] M., Zavarsky, P. & Lindskog, D. (2016). Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization. Procedia Computer Science. 94. 465-472.

[35] Halevi, T., Memon, N. & Nov, O. Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-efficacy and Vulnerability to Spear-Phishing Attacks.

[36] Barjis, J.(2008). The importance of business process modelling in software system design. Science of Computer Programming. 71. 73-87.