Literature Review

"Enhancing Cyber Security by Increasing Client Side Privacy for Network Information "

[1] *ATUL KUMAR VISHWAKARMA - CSE , SCHOOL OF RESEARCH AND TECHNOLOGY , PEOPLE'S UNIVERSITY*

[2] *PANKAJ SAVITA (Second Author) ASSO.PROF HEAD CSE, SCHOOL OF RESEARCH AND TECHNOLOGY , PEOPLE'S UNIVERSITY*

Abstract - We have use a social media network may be a social association ended beginning persons & associations called node, we have associated by 1 or more unambiguous sort of inter-dependency approximating companionship, common concentration & substitute of finance associations of beliefs, understanding or reputation. A cyber thr-eat are often both not deliberate & premeditated target or non-targeted, And it can come from a spread of sources, including foreign nations engaged in intelligence & information warfare, criminals, hackers, virus writers disgruntled workforce and contractors working within a conglomerate . Social networked sites are not only to speak or interact with peoples globally, but also one ineffectual way for big business encouragement. A this paper, we examine & study the cyber threats in community networked web-sites. We submit yourself to the gathering times gone by of online social web-sites, pigeonhole their types & also talk about the computer-generated threats suggest the anti-threats strategies & see in your mind's eye the longerest terms trend of such hoppy well-liked Web-sites.

CSPs are implemented as standard directives involving HTTP headers or page tags that specify which domains, subdomains, & resources a browser can load from a website. CSP use is according to the browsers any user would likely use including Chrome, Firefox, Safari, & Edge. The goal is that if malicious code is resident on a site, then visitors to that site would be prevented by the CSP from being directed to the hacker's domain.

***Key Words*:** Privacy, Security, Cyber threats, Social Net-working Web-sites.

1.INTRODUCTION

All Social Media Website security settings for a lot of social media Website account like that Face-book & therefore are many the aptitude 2 procession an a accounts 2 "Privates" on other like that Twitter & Instagram, peoples like that would like to gain right to use to this uncreative in progression can over & over again find away.

That in a today are of smart-phones & computers the internet hasn't change a idea of announcement . Due the be deficient in of security an assortment of cyber-crimes have emerged in the past decade. Cyber security plays a significant role in the current development of information technology & services. Cybersecurity is thus an attempt by users to keep their personal and professional information intact from the attacks on the internet. The main function of cyber security is to protect networks, computers, programs from unauthorized access, & loss. The maxi-mum number of users are not aware of the high risks & share their in sequence unintentionally & their lack of knowledge make them defenseless to cyber-attacks. So cyber security is the main apprehension in today's world of compute.

Definition: Cybersecurity or in sequence knowledge of security are the modus operands of defensive computers net-works programs & data from unauthorized access & attacks that are aimed for development .

Description : Major & most areas cover in cyber security are:

i. Network Security
ii. Disaster recovery
iii. Information Security
iv. Application Security

Best Social Media Web-Site & Website security encom-passes procedures && countermea-sures like that are taken for the duration of the happening life-cycle to guard applicat-ion from intimidation which ware come from beginning to end flaws with-in the application designed develop-ment, deployment upgrade & destruction Some indispensable techniques used for application security are

- Auditing & logging.
- Session management parameter exception management and manipulation
- User/Role Authentication & Authorization
- Input parameter validation

Companies like Google have rolled out CSP successfully & are using it to stop attacks against their web applications daily. However CSP is deployed only lightly in most web application environments . The challenge with CSP implementation has been its complex administration . Tala Security researchers have found, for example that roughly 2 percent of website operators in the top Alexa 1000 websites deploy the standard to prevent client-side attacks. Assisting with this administrative challenge may be a primary motivation for client-side platforms.

2. RELATED WORK

Cyber safety events for Social Networking Sites : Issues, challenge & explanation Rituparna Das, Mayank Patel, *April 2017*

As growing popularity there for community Networking website these became a most important objective in computer-generated - crimes & attacks. Cyber-crime is becoming a widespread & posing a serious threat to the national & economic security. Both public and personal institutions in sectors of public healt information & tele-communication defense, banking & finance are in danger . So the organizations should take proper security measures to be cyber - misdemeanor safe & therefore the users should protect their personal information to avoid & fraud or misuse. The cyberspace is becoming a big area for cyber-crimes & thacker try 2 attack on crucial information. So-there's a requirement of worldwide partnership of countries to figure together to weighing machine sponsor the constantly growing replicated intimidation

As the internet usage has increased in India cyber-crimes have also increased respectively. More than 32000 cyber-crimes were

Reported between 2011 & 2015, across India & quite 24000 of those cases are registered under the IT Act & therefore the remaining cases under the various sections of IPC & other State Level Legislations (SLL).Cyber-crimes are registered under

three broad heads in India the Indian Penal regulations (I P C), the IT Act & other State Level Legislations (S L L). The cases registered under information technology Act include

1 :-Tampering with computer source documents

2 :-Loss /damage to computer resources

3 :- Attempt

4:- Accessing Digital Signature Certificate by misrepresentation of facts

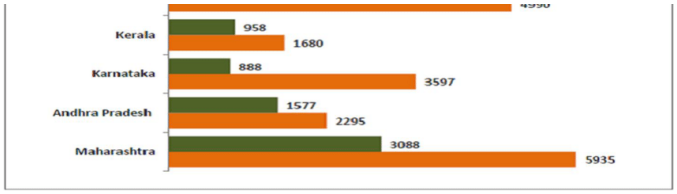
5:- Publishing false Digital Signature Certificates

6:- Fraud Digital Signature Certificate

7:- Breaking of confidentiality or privacy

8:- Failure to assist in decrypting the knowledge intercepted by agency

9 :- Cyber-crimes have increased more than 3 times in 5 years



Year	IT Act		IPC	
	Cases Registered	Persons Arrested	Cases Registered	Persons Arrested
2011	1791	1184	422	446
2012	2876	1522	601	549
2013	4356	2098	1337	1203
2014	7201	4246	2272	1224
2015	8045	5102	3422	2867
Total	24269	14152	8054	6289

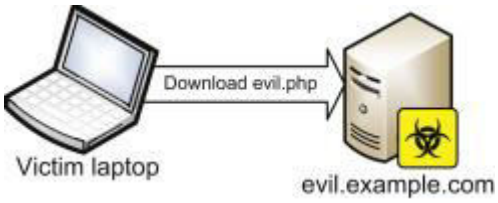
3.2:- Eric Conrad Joshua Feldman, in Eleventh Hour CISSP® (Third Edition), 2017

Client-Side Attacks

Client-side attack come about when a consumer downloads malevolent comfortable. The flow of understanding is wrong side up compare are to member of staff serving at table side attack: client-side attacks set off from the victim There are many download content from the mugger. consumer side attack are easier said than done to mitigate for association that consent to Internet right to use. customers include data processing software, spreadsheet media dramatis personae, network browsers etc. a good number firewall in this time a large quantity more encouraging inbound measure up to to outbound they were designed to “keep the bad guys out,” & take the edge off server-side attacks originating from unfrosted set of connections. They over and over again be unsuccessful to put off customer -side attack.

3.3:- Security Engineering (Engineering & Management of Security) Eric Conrad Joshua Feldman in CISSP Study Guide (Third Edition), 2016

This time very important is client side attacked when a all type of user malware attack all type of social media platform so kindly you have download any content like that image and video and files attested come in your system automatic malware virus so you have protect yourself so may hacker are used to malware virus so we have i means victim is attacked



We have provide many company and organization allow to internet provider and access with client including small organization and many type of software arable to acess like that media player such as avable many internet browser like that chrome, Internet Explore and firfox are ally browser collect plug-in software in 3 party include in this system this is a very challenge to protect your self this type generate a client side attacked system .important topic is a client side attacks proform to attacked in user side that is called

We have all user used a social media platform Most common firewallare other important restr-ictive inbound with a social media compared by outbound social media platform: thair were designing to “keep to move of the bad guys out,of control and doing attect on social media platform and you hacking to you have pri-mitive action account try ” & mitigate server-side attacks on mid attected originating from unfrosted networking information. They often fail to prevent CIA.

3. Material & Methods Study Design

As the internet usage has increased in India cyber-crimes have also increased respectively. More than 32000 cyber-crimes were reported between 2011 & 2015, across India & more than 24000 of these cases have been registered under the IT Act & the remaining cases under the different sections of IPC and other State Level Legislations (SLL). Cyber-crimes are registered under three broad heads in India, the Indian Penal set of laws(IPC) in IT Act & other State LevelLegislations (SLL), The cases registered under on IT Act include

1:- Tampering with computer source documents

2:- Loss /damage computer resources

3:- Attempt Hacking

4:- Accessing Digital Signature Certificate by misrepresentation of facts

5:- Publishing false Digital Signature Certificates

6:- Fraud Digital Signature Certificate

7:- Breaking of confidentiality privacy

8:- Failure to aid in decrypting the information intercepted by Government Agency than 3 times in 5 years

Source of data :- I am generate a self data for a demo purpose this data used for example in my thesis

4. CONCLUSIONS

Social media cyber security This method will help to prevent the privacy of anyone who crimes on social media or violates the privacy of others

I have created my profile at socialmedia together with Facebook-Twitter LinkedIn-Instagram & other social-media(SM) sites. My aim is that anyone can download photos from their profile or download videos, so that they can be captured easily. & by editing and uploading videos, it can be captured easily and I can also know who downloaded my photos and videos. Has done this information to help cybercrime too, this will benefit in cybercrime and social media privacy.

In my social media, posts in my room, which can contain photos and videos, if someone downloads the photos and videos, then a notification will come to me that your photos and videos have been downloaded through this account for the exam. I will know the account name and information.

And if the person who downloaded it uses the proxy, then the details of the proxy will come to me as soon as the proxy will use it, the proxy details will be received and its real IP address can be obtained in network details and other types of details. So that its location can be easily detected.

ACKNOWLEDGEMENT

Suppose if anyone uploads my videos and photos. On social media, I can tell that the person with this account has downloaded from my social media. And if I go to a cyber cell and give my report or information that it has been done to me, then the cyber cell owner can easily catch the problem. With this, through which videos of cyber cells are uploaded very easily and which proxy is used, along with the proxy, you will get real network information so that the criminal can be captured very easily.

I will create a social media platform in it, in which I will put all this data for demo and present it in complete process so that in the coming time, the privacy of the people can be better protected and the criminal activities can be easily stopped.

REFERENCES

[1] Cyber Security for Social Networking Sites: Issues, Challenges and Solutions Ritupama Das, Mayank Patel, April 2017
[2] Eric Conrad, Joshua Feldman, in Eleventh Hour CISSP® (Third Edition), 2017
[3] Security Engineering (Engineering and Management of Security) Eric Conrad, ... Joshua Feldman, in CISSP Study Guide (Third Edition), 2016
[4] Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling Stefan Marksteiner Nov 2019

[5] http://www.ic3.gov/ "Internet Crime Report 2015"
[6] Most number of cyber crime reports. Available: https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/
[7] National Cyber Security Policy 2013. Available: https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013
[8] Security, Privacy and Trust in Social Networking Sites. Richa Garg, Ravi Shankar Veerubhotla, Ashutosh Saxena. CSI Communications ISSN 0970-647X| Volume No. 39| Issue No. 2| May 2015.
[9] Exploiting Vulnerability to secure user Privacy on a social networking site. Pritam Gunecha, Geoffrey Barbier, Huan Lui. ACM, SIGKDD International conference on knowledge Discovery and Data Mining, August 2011.

[10] Latest inphishing 2016. Available: https://info.wombatsecurity.com/blog/the-latest-in-phishing-first-of-2016
[11] Malware statistics. Available:https://www.av-test.org/en/statistics/malware/
[12] Dolvara Gunatilaka"ASurvey of Privacy and Security Issues in SocialNetworks"www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.
[13] "Facebook Privacy Basics", [Online]. Available : https://www.facebook.com/about/basics.
[14] BrowserSecuritySettings. Available: http://its.ucsc.edu/software/release/browser-secure.html
[15]http://www.onlineschools.org/blog/history-of-social-networking/
[16}Social networking sites search engine, /http://findasocialnetwork. com/search.phpS.
[17] B. Stone, Is Facebookgrowing up too fast, TheNew YorkTimes, March 29, 2009
[18] "Using Facebook to SocialEngineer YourWay Around Security",http://www.eweek.com/c/a/Security/Social-Engineering-Your-Way-Around-Security-With-Facebook-277803/ 05.20.2010
[19] www.securelist.com,«"Instant"threats», Denis Maslennikov, Boris Yampolskiy, 27.05.2008.
[20] Won Kim , Ok-Ran Jeong, Sang-Won Lee , "On Social Websites" , InformationSystems 35 (2010), 215-236.
[21] Kaven William,AndrewBoyd, ScottDensten, Ron Chin, DianaDiamond,Chris Morgenthaler, " Social Networking PrivacyBehaviors and Risks",Seidenberg School of CSIS, PaceUniversity,White Plains, NY 10606, USA.
[22] Abdullah Al Hasib, "intimidationof Online Social Networks", IJCSNS, Vol. , No 11, November 2009.
[23] Anchises M. G. de Paula, "Security Aspects and prospect tendency of Social Networks", IJoFCS (2010) , 1, 60-79.
[24] D.Boyd,N.Ellison,Social set ofconnections sites:definition, olden times, and fellowship,Journal of Computer-MediatedCommunication 13 (1) (2007) article 11