Awareness About Cyber Security and Prevention Methods For Home User

Avinay Mehta , Sayan Chakraborty , Saurav Kapoor and John Singh . K
School of Information Technology & Engineering
Vellore Institute of Technology, Vellore
Email: avinay1165@gmail.com

Abstract

Today we are in the era of digital world. In digital world everything works on internet and computers. Internet makes our life so easy that with the help of internet we can do many things. Shopping, social networking, business everything is going on internet. With the increase in the technology there is also parallel increase in cyber-threats. Cyber-threats causes many problems to Home Users and they mainly attack on them because either they don't know about the security system or they are not much familiar with the technology But due to lacking of knowledge about cyber threats, people become addicted to this kinds of threats. This kind of threats can be in form of malware or virus and they can hack the entire data of the computer. It is necessary to take some security measures to secure our system from these kinds of threats. This paper discuss on some technique that help user to secure their system from cyber attacks, it is necessary because information is very valuable and if it goes on wrong hand then it might creates major risks to users. E-mail, or any application that user uses in his day to day life.

Keywords: Cyber-Threats, Home users, CMA, Malware, Security, Risks, Hacking, Technology.

I. Introduction

It is the era of computers where we spend most of the time with computers. In other words we can say that we are in digital world. The digital world makes our life easy and simple. We can easily communicate face to face with the person who is very far from us, purchasing products from online markets, to pay some money to others, everything becomes easy. With the increase in digitization, users of internet also become more. With the increase of use of Internet, threats also get increased. Threats like hacking of account, tracing of somebody transaction etc. These threats are commonly known as cyber threats. The person who does this kind of activities are known as criminals and these activities are known as cyber-crime. Cyber- crimes is the type of crime which is growing very rapidly in today's world where more and more criminals try to exploit the convenience provided by the Internet to do different types of criminal activities that may have no border. Now a day's cyber security is not bounded to only a personal workstations but also being used to suppress information of mobile phones as they have some less security issue. Every day, more and more home users connect to the Internet for business, social and networking purposes – or even simply to gather information. For this, they use all forms of computers and devices. Lately, though the trend has been increasingly towards mobile devices such as smart phones, tablets and the like. This leads to increase threads for home user security. To solve home user security issue all sectors, organizations comes together and they needs to understand the security threats faced by today's the computing world.

Security Measures For Home Users Home network mainly contains two or more interconnected system by which internet service provider provides many services to its users(ISPs).Node connects two or more devices via wireless or wired medium they also connects devices such as PAD, mobile, etc.

There are three categories to get security for home users are as follows:

1. Thick Security
2. Intermediate Security
3. Thin Security

Thick Security Oriented Home User:-

As we know that malware is a powerful irrelevant program that effect computer system and it also affect those systems that are directly or indirectly connected by the corrupted system. It rapidly increases and affect as much as system in the network. Now a day's many users depend on their own domain knowledge to prevent their devices from multiple threats.

This is the level of thick security home user where users are only responsible for all of their security issues in thick security there is no involvement of any party in respect to prevent users from unwanted threats users can find their solution by their own to protect their connected devices from security issues.

There are many problems faced by user:

- They forgot to download and updates.
- They do not keep up to date with the security related technologies and risks.
- They have inadequate and incorrect security protection.
- They lack information security awareness.
- Their password tends to be weak.
- They do not update their antivirus regularly.

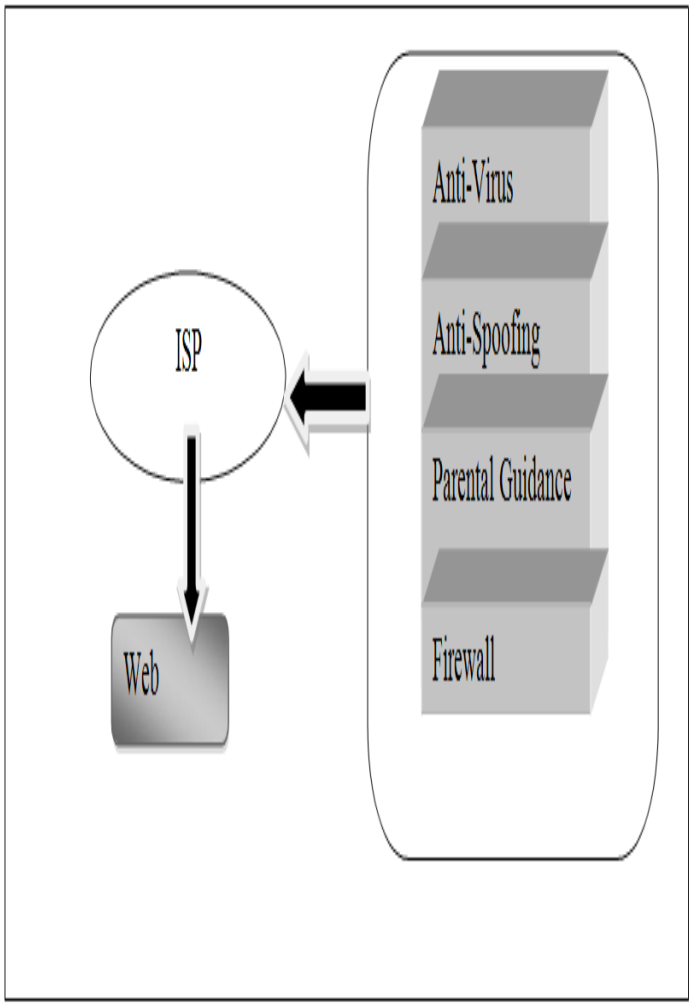

Fig.1: Thick Security-oriented home user

Intermediate Security Oriented Home user:-

At this level security issue is divided between user and a controlling entity (here controlling entity is regulating service-the ISP.) ISP provides users to connect to the internet. By the involvement of ISP. Some of the load of user were reduced because ISP will handled some aspects of security such as virus malware containment and alert users if any cyber threats have been detected.

This provides ISPs to make their users aware of cyber security problems and how they solve by their own. It is a very good start but intermediate approach is not fully solve the problems of users. Here we discussed other aspect of security prevention that make users free from all the responsibilities in concern with security.

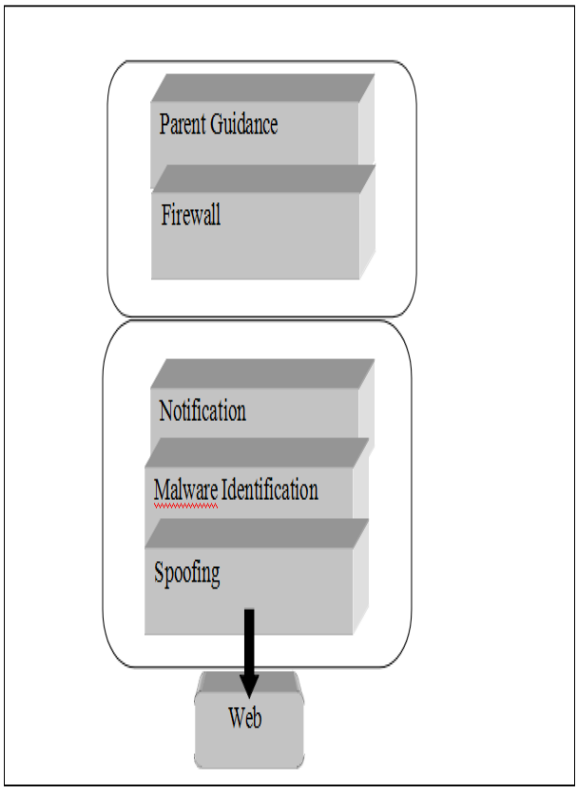

Fig.2 : Intermediate security-oriented Home User

Thin Security Oriented Home User:-

At this level, most of the responsibility for cyber safety is taken away from the home user and becomes the responsibility of the ISP. The home user will still have limited cyber safely issues (human related) to address but will be assisted by his or her ISP with the technical security aspects.

The ISP will provide the home user with a number of technical requirements needed to provide protection against cyber threats. In addition, each home user will be advised of all the technical services provided and enforced by the ISP.

Examples of such services are:

1. Continuously updating virus-protection.
2. Immediate patching of vulnerabilities when patches become available.
3. Time to time scanning of the user computer to detect malware.
4. Protection against spam.

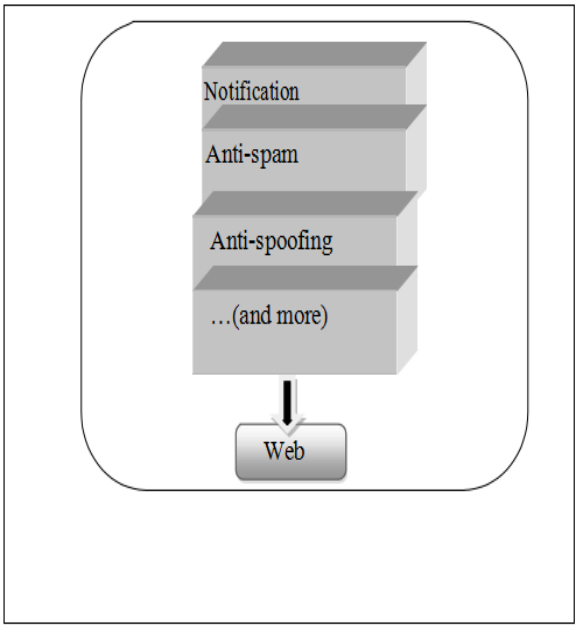

Fig.3: The Thin security-oriented home user

II. Related Work

In [1] author proposes three-step model to assist the cyber security threats amongst home-users. In first step, it involves home users to take whole responsibility for their own securities related to cyber. Currently, in most cases, these kinds of situations are not initially planned and that's why most of the cyber security incidents, breaches and fraud cases happen. The reason for happening these kinds of situations are generally that most of the home users are not able to understand the kinds of threats or they do not properly implemented the required safety measurements related to cyber threats. The first step is referred to the "thick security-oriented home user". The paper also proposes the next step of cyber security that will help to assist home users, so that they can manage their cyber-actions. This step is referred as "intermediate security-oriented home user". The last step proposes that when a wide and complete range of technical responsibilities related to cyber securities are moved towards some relevant Internet Service Providers (ISP). This step is referred as the "thin- oriented home users".

In [2] is focused on providing the cyber security to home users as in India the many people excess internet from their home but many of them doesn't belongs to technical fields and do not have any idea about cyber threats to their data or information and they don't know how to protect their important data and information from these threats while connected to internet. It is therefore vital that home users be assisted to ensure that they are "cyber secure". So in this paper the author has proposed three ways to address cyber security among home user. The first step involves home users taking full responsibility for their own cyber security. Currently this is the adhoc situation in most cases and it is the cause of most of the cyber security incidents, breaches and cases of fraud that occur. The reason for this is that most home users do not understand and/or do not implement proper cyber awareness principles."Thick security-oriented home user" is refer as a first step . In the second step of cyber security that will assist home user to manage their cyber actions. The main focus of this step is to move some of the responsibility to regulating bodies for e.g.: ISP(Internet Service Provider). At last in the third step the all the responsibility of cyber security will be given to their Internet Service Providers.

As in today's world the internet has become vital part of ever field and emerging at an increasing rate. [3] examines the problem of cyber crime and the difficulties that it face by the way that it is being placed in England and Wales. In this the author focused on the area of hacking. Keywords— computer misuse act; cyber crime; hacking; regulation of IT law, internet technology. CMA that is mainly computer misuse act established in 1990 to deal with the cases of cyber crimes but in now a days it seems to be failed because of new technology arrived in this emerging era. Today is the generation of smart phones which made one's life easier but it creates problems also, like hacking some personal data of an individual or hack the account and many more. There is some provision in the legislation like CMA 1990, RIPA 2000, DATA PROTECTION ACT 1998. One of the provisions in RIPA is that under section 1 of RIPA act if someone commits any illegal activity in relation to computer or network either public or private intentionally then he or she gets a life

imprisonment of 2years.

In [4] author discuss about home network model and star topology. In star topology the home server is considered as the center. The device can be supplied through the various communication method (LAN, ZigBee, Bluetooth etc) can communicate through home server as well as home manager e.g. to your family members like father or mother or both can be controlled by home network service. Also the method suggest by the author is user authentication technique by biometric information. It should be the better option for home user network model. And it can be useful to provide user authentication process for matching Identity, Password and Certificate etc. In this home network model author conclude that the home server plays the vital part and it must be prevented by the any kind of cyber threat.

In [5] the author worked on very efficient Home security system where the security to the home users is provided in very low cost Wi-Fi. The user will get notification on his/her mobile if any threat occurs to the system. It also tracks the intruder whoever try to create threat to users security. In this the author is basically trying to provide high level of security so that anyone can afford his or her security at very low cost.

In [6] focus on the security issues seen by home user and their lack of knowledge in understanding it. Sudden increase of internet in a country causes millions of home user to utilize the internet and in the same time it creates many security related issues to home users due to lack of security awareness. This study shows that the mind of people about data security is improved only by awareness and by implementing interface that would be user friendly. The sample that would be stored during working phase shows a significant proportion in context of user that they are in doubt and they were prevented from finishing the task that they are assigned. We say that if we develop a small application we must have knowledge to implement the security in the applications but end users are fail to achieve the desired security. This causes a separation among user in which one can tackle their security issues but other cannot recognized that the security threats has been occurred. There are many options in the internet like cookie, block popup are very hard to understand by a simple end user. By saving free software from internet and at the same time by allowing yes to all these option they are trap in a threat and they also don't know about this that they are trap into the threat. For effective and secured protection for users advanced software were developing to point the end user behavior and also track the software that is installed in system and by tracking the system they protect user without having any problems to users. It has many functionality to enable or disable the cookie data and user are not want to reply to such controls.

In [7] the author proposes the user authentication mechanism for user perspective or convenience in home network. It means that user can be verified or authenticated in technical terms, by user's favorite verification or authentication methods so that he/she can easily access to the content servers. The author proposes that when user authentication mechanism is applied, the user not need to remember all user verification information which is enrolled by user to various content servers and more importantly user's all important information like biometric information that can be protected from home network enterprises as well as Internet Service Provider(ISP). Further more user need not carry any kind of certificates to log on to the content servers that required any kinds of certificates.

Home user network [8] gives services without any intervention by knowing user compatibility with home device that is very much familiar with end users. So that without knowing the security of home user it causes many problems. In this paper writer aimed at access mechanisms which is based on home users. They not just provide security to home user network but also they protect them from insider and outsider and block those irrelevant data access to services.

In [9] author proposes the introduction of security concerns from a cross-layer perspective on modern cyber-physical system's securities. The author also introduced the vulnerabilities, consequences and counter measures on the system-device and hardware levels. The author also mentions that the existing solutions are sometimes not enough to secure the future CPS that are currently being used widely in national critical infrastructure. The paper also discuss about the research directions in this particular area as a guideline for future perspective and all kinds of researches.

In [10] writer survey the theory on data privacy and cyber security in CPS (Cyber Physical System). The CPS (Cyber Physical Systems) cyber security and data privacy mainly divided into four cyber physical system applications: 1) smart grids 2) ICS 3) smart cars 4) medical devices. In this writer also describe the types of threats, malware, current attack, current controls. Framework that handles CPS falls in the categories of security aspects. Mainly framework shows or capture how CPS domain were attack and that result in some unexpected consequences in domain with its solution and vice versa is also possible. The writer also focuses the challenging and some hidden pieces in the CPS research, cyber security

III. Modified Home Security Technique

ISP is not in the position to handle all the problems of user because ISP has limited functionality due to:-

- Client is not in a position to pay money for their Security.
- Due to some legal problem.

ISP provides many awareness to protect their data they cannot ensure that users really understand and sufficient for implementing safeguard for them.

As we discuss above the three categories as THICK, THIN, INTERMEDIATE here the functionality of ISPs and users are different that in one case we see that all the security measures of user are only dependent on user itself he only need to select the appropriate choice to reduce its cyber threats, in other case we see that the function is divided between ISPs and user here both can access the security and provide better solution to a problem, similarly in other case the all security responsibility went to ISPs hand from the user here in this case there is no intervention of user only ISPs is responsible for every single threats.

The following diagram is given below:-

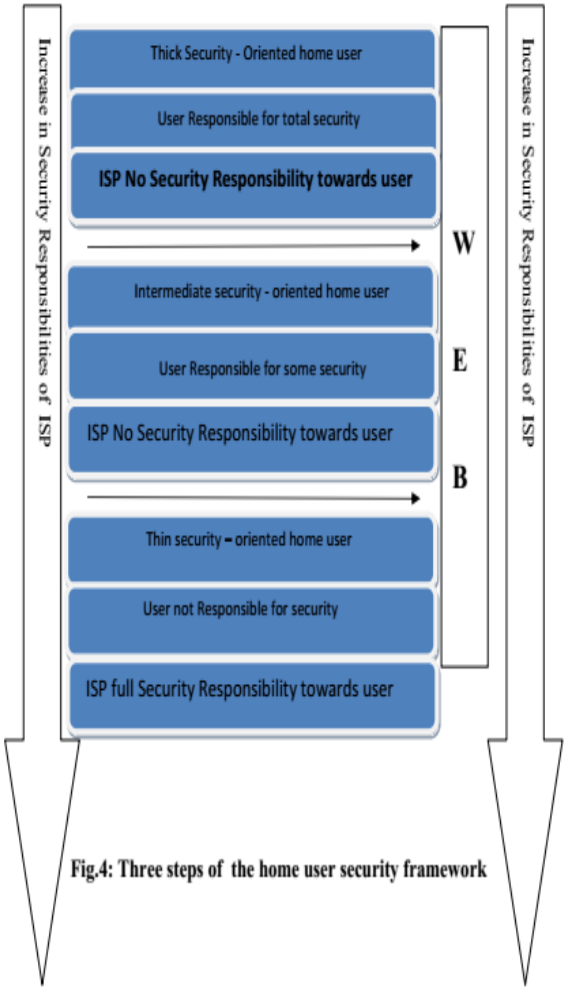

Fig.4: Three steps of the home user security framework

In above three technique we see that there is some security issue still exist because there is no equal access to both ISPs and user. In the above cases either ISPs or user will handle security or they access some limited security at intermediate level. So in worst case if one of them is not able to provide security then it causes many troubles for user like some outsiders can get access to your confidential data and files. For example if someone is using THIN ORIENTED SECURITY he handover all the security responsibilities to ISPs (Internet Service Provider). But in some point if ISPs is unable to provide security to the user then user is not able to secure himself because he do not have any security access to protect him by himself.

So we come up with is another new technique to overcome this problem is shown below:-

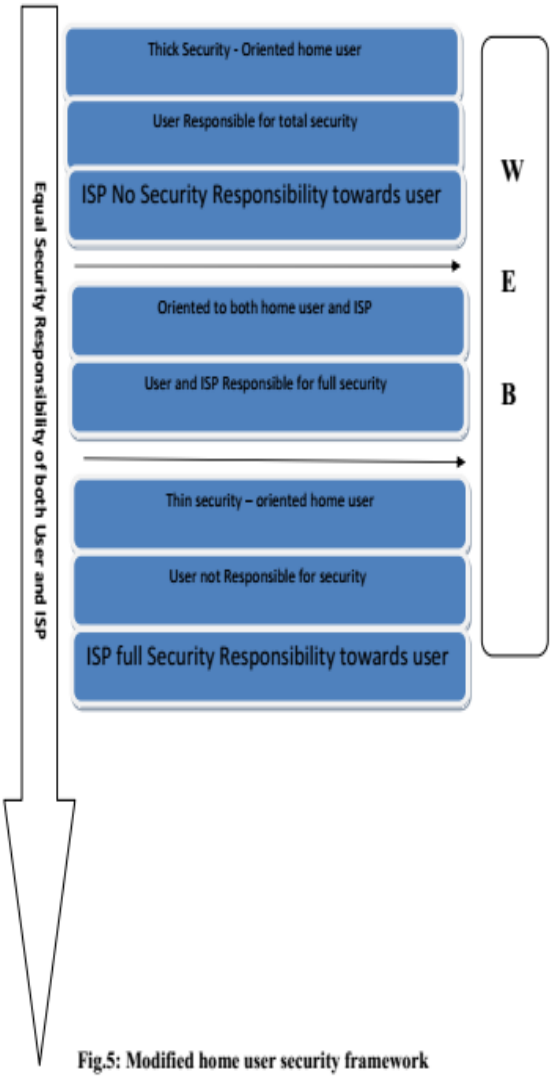

Fig.5: Modified home user security framework

IV.CONCLUSION

Here this paper proposed a new technique that both the user and ISPs has equal amount of access to the data so that in worst case if any of them are unable to resolve the threat then other can resolve it. In this technique we do not want to worry about security threats that we face in thick and intermediate there either we are only responsible or both we and ISPs are responsible there we have not full access to security that's why in worst case if (ISPs) loose to handle the security then user can't do anything to help himself that's why equal access to both user and ISPs are necessary to protect the device from unwanted threats and provide better security to user.

REFRENCES

[1] E Kritzinger "Providing the cyber security to home user as in India", In proceeding of IEEE International Conference on Science and Information, pp 340-345,2013.

[2] SH von Solms :"Home User Security-from Thick Security-oriented Home Users" In proceedings of IEEE International Conference on Science and Information 2013 London UK, pp 340-345,2013.

[3] Reza Montasari Pekka Peltola, Victoria Carpenter "Gauging the Effectiveness of Computer Misuse Act in Dealing with Cybercrimes" In proceeding of IEEE International Conference on Science and Information ,pp 250-260,2015.

[4] Yun-kyungLee , Hong-il Ju , Dowoo Kim and Jong-wook Han "Home Network Modeling and Home Network User Authentication Mechanism Using Biometric Information" ,In proceedings of IEEE International Symposium Conference on Consumer Electronics, pp 1- 5,2006.

[5] S.M. Brundha, P. Lakshmi and S. Santhalakshmi; "Home Automation in Client- Server Approach with User Notification along with Efficient Security Alerting system" ,In proceeding of IEEE International Conference on Smart Technologies For SmartNation,pp-596-600.

[6] Umesh Hodeghatta Rao Xavier and Bishwa Praksh Pati,"Study of Internet Security Threats Among Home Users", In proceeding of IEEE Conference on Computational Aspects of Social Networks, pp217-221,2014.

[7] Yun-kyung, Jee-hye Par,"User Authentication Mechanism Using Authentication Server in Home Network", In Proceedings of IEEE Conference on Advanced Communication Technology, pp500-506,206.

[8] Geon-Woo Kim, Do-Woo Kim, Jun-Ho Lee, Jin-Beon Hwang, Jong-Wook Han."Consideration on Security Model of Home Network", In proceedings of IEEE Conference on Advanced Communication Technology,Volume-1 Issue4,pp 112-120,2006.

[9] Jacob Wurm, Yier Jin, Yang Liu, Shiyan Hu, Kenneth Heffner,Fahim Rehman and Mark Tehranipoor"Consideration to Cyber-Physical System Security:A Cross-Layer

Prespective", IEEE transactions on Multi-Scale Computing System, Volume-3, Issue-3, pp 215-227,2017.

[10] Abdulmalik Humayed, Jingqiang Li, Fengjun Li, and Bo Luo "Cyber-Physical Systems Security-A Survey", IEEE Internet Of Things Volume:4, Issue6 , pp 1802-1831,2017.