INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND TECHNOLOGY (IJARET)

ISSN 0976 - 6480 (Print)
ISSN 0976 - 6499 (Online)
Volume 6, Issue 4, April (2015), pp. 51-59
© IAEME: www.iaeme.com/ IJARET.asp
Journal Impact Factor (2015): 8.5041 (Calculated by GISI)
www.jifactor.com

IJARET

©IAEME

CYBER SECURITY: A SURVEY ON ISSUES AND SOLUTIONS

Pranav Verma[1], Ankur Makwana[2], Salman Khan[3]

[1,2,3]Department of Computer Science and Engineering, Nirma University, India.

ABSTRACT

This is an era of technology and Internet is one of the them which has changed the world the most in last decades. It is open and so anyone can use it to get information about anything, people have been using it for educational, business, social connections and every day work purposes. But the matter of fact is door open in both directions, bad people with bad intensions stared using this technology for evil intensions. They are stealing personal data, financial information, government secrets and many others are target of those people. In this paper we will discuss about vulnerabilities present currently in the network, some case studies and later recommendations to avoid vulnerabilities and prevent them from exploitations are also discussed.

Keywords: Cyber Security, Vulnerabilities, Network Attacks, Malware, Privacy.

I. INTRODUCTION

In today's era we cannot imagine the world without Internet. It is present there in every commercial firms, government offices, research institutes, industries, academic institutions, defense field etc everything is directly or indirectly dependent on Internet. In government agencies they are providing facilities to every single person in the countries via Internet, as there are rural areas where it is not possible to deploy offices for everything government are planning. So people there are being connected by those programs using internet facilities. Online shopping has emerged as one of the largest growing area in this decade, people are purchasing products online, from daily usage grocery to heavy and costly electronics items are being sold and purchased over the Internet. With online shopping there is a huge growth in online fund transfer also, to pay for online shopping, fund transfers and other bill payments are now on finger's tip. Thus Internet is need of this generations everyday life and keeping it ruining smoothly and securely is one of the most important task for information based organizations.

But as Cesare Pavese said "Every luxury must be paid for." so there are several flaws in the use on Internet, especially if communication contains sensitive information like secrete data of defense organizations, company's financial details, individual's banking and personal details etc. There are people or organizations present outside who are interested to steal such sensitive information from one another, such actions in broad sense are called cyber attacks. A cyber attack is a deliberate exploitation of computer systems, technology-dependent networks and enterprises [1]. The attacker uses malicious software which are piece of code computer programs that can alter, manipulate or destruct the data, code, or logic that in turns can compromise the security of the data and network. There are various kinds of attacks for example DoS attack, MITM attack, Zero Day attacks, Information Attack[2] etc. Among all of them the Zero Day Attacks are known to be most dangerous and hard to be detected by the security mechanisms. According to the Open Web Application Security Project (OWASP: www.owasp.org) top three vulnerabilities are Injection, Broken Authentication and Session management and Cross-Site Scripting. Injection flaws, for example SQL-Injection attack, OS injection, and LDAP injection is possible when some un-trusted data is dispatched to an interpreter with command or the query. The attacker sends some improper data which is able to fool the interpreter and forces it to run unauthorized commands. In application some of the functions related to user identity authentication and session management are sometimes implemented incorrectly, which allows the attackers to compromise security of the application data. XSS flaws occur whenever an application takes un-trusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. These attacks are there since the evolution of the Internet and after so many years of development and security update the still exist, which tells that attacks are also being sophisticated with the pace of technology evolution.

II. THREATS

The major advantage for attacker community today are the open access of resources and large file and information sharing platforms availability [3] . And thus they are preparing more and more new kinds of attacks every other day. Software manufacturers who do not spend proper attention in their security modules causes vulnerabilities not only to their product but in turn the overall system and sometimes for the entire network becomes vulnerable because of one malicious product. For example, "exploit kits," and "infecting users" computers through a vulnerability without their knowledge are the most used techniques today. More than 90% of such attacks are through Java vulnerabilities in browsers which are example of insecure code development [4] [Fig-1].

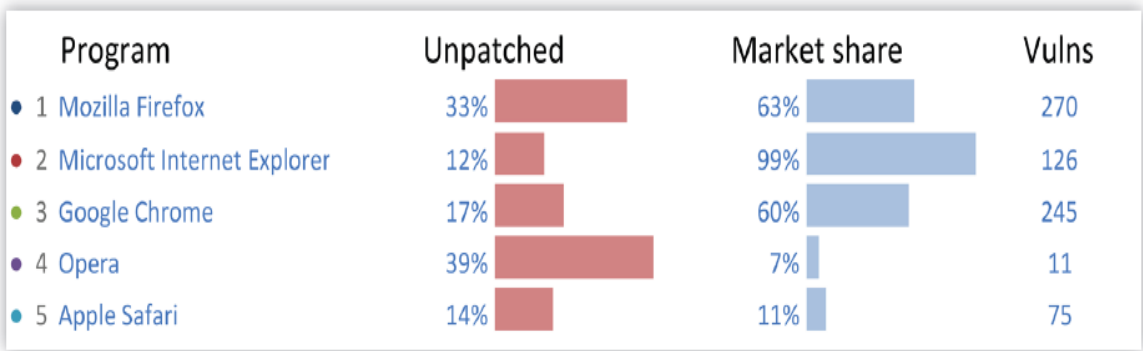

Fig-1: Browser Exposure by market share and un-patched users [4]

Next most vulnerable and most widely used software are pdf readers, as we know there is always one pdf reader tool available in every computer irrespective of the operating system. Fig-2 shows the vulnerabilities found in those software.

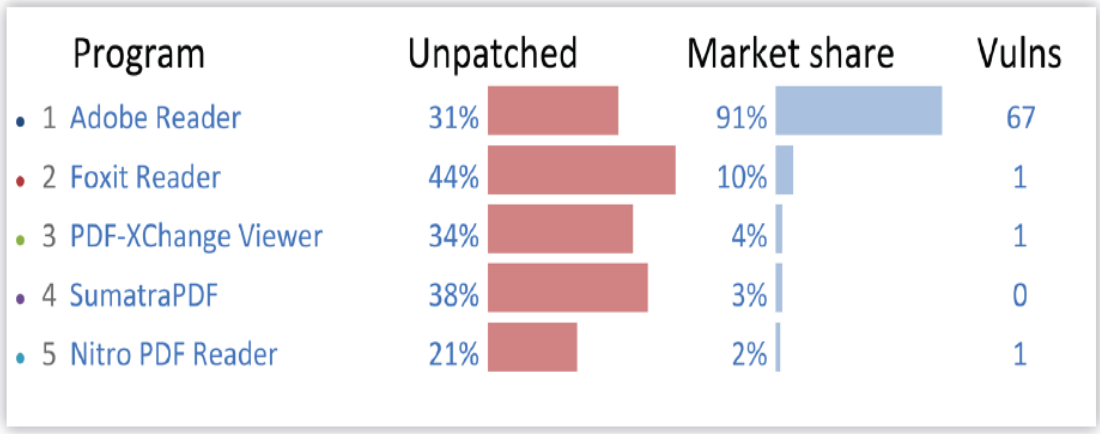

Fig-2: pdf Reader Exposure by market share and un-patched users [4]

2.1 Types of vulnerabilities

The OWASP has listed top 10 security vulnerabilities and attacks here [5]. Some of the top most attacks have been holding their position for a long time despite of so many security patches and updates are being installed by organizations. McAfee Labs a well known global computer security software company in their report previews 2015 Developments in Exploits and Evasion[6] in this document they have listed trends in 2015, here we are listing few from them:

2.1.1 Increased use of cyber warfare and espionage tactics

Cyber warfare is the next generation style wars, where without firing a single bullet or killing anybody one country can destroy the another. The countries have started preparing their cyber army for the same, if not to attack to anyone than to protect themselves from attackers. China recently has admitted that they have such Army all ready to tackle any un avoidable situation [7].

2.1.2 Greater Internet of Things attack frequency, profitability, and severity

Internet of things is said to be the next generation thing and we have already started using some of them like smart TV, smart air conditioners, Refrigerators, vehicular networks etc. But with the increase in connecting devices there is also increase in security threats, unless these small devices are manufactured with security controls built in their architecture they cannot be secured by external mechanisms. according to the McAfee Labs report entitled Cybercrime Exposed: Cybercrime-as-a-Service, the cybercrime community currently values stolen health credentials at around $10 each, which is about 10 to 20 times the value of a stolen U.S. credit card number.

2.1.3 Ransomware evolves into the cloud

Ransomware are demanded in exchange of user's data. The information stored on the clouds can be compromised if clouds are attacked and then the information is encrypted with some secrete known only to the attacker. Then the attacker asks for ransom in exchange of the key or the data. In another attack the attacker can first led space in some popular cloud, upload his malicious code there and then can infect a large number of other users on the cloud and gain access of their workstations.

2.1.4 New mobile attack surfaces and capabilities

Android has changes the world completely, it made technology handy and Internet users grown like anything since the evolution of android devices. It is a vital part of Internet of Things, and thus keeping it secure is as important as securing a workstation. New mobile technologies are

expanding the attack surface on such devices [8]. Un trusted application stores are the major threat to mobile malwares. There are numerous places which claims to provide the authentic application from the publishers at the lower price, and people are being tricked by them.

III. CASE STUDY OF RECENT ATTACKS

Various Attacks in recent years which caused most damage worldwide are:

3.1 Red October

In October 2012 this cyber espionage malware was discovered. The instructing fact about this malware was that it was there in the systems worldwide for five years since it was discovered by the Kaspersky Lab. Red October was termed an advanced cyber espionage campaign intended to target diplomatic, governmental and scientific research organizations worldwide. This malware installs from the attachments in the emails which exploited the vulnerabilities of Microsoft Word and Excel

3.2 GhostNet

A large scale cyber spying operation discovered in 2009. This group has its command infrastructure based in China, but there was no evidence found that can claim the involvement of Chinese Government. It has compromised security of New York City and London and mostly targets the embassies and foreign ministries and Dalai Lama's Tibetan exiles in India.

3.3 Titan Rain

Again the Chinese attacker attacked on White Hall and left no clues about their identities. A series of coordinated attacks made in 2003 and said to be continued for further three years. The attackers used proxy, zombies, bots, infected systems and remain un detected till date.

3.4 IceFog

In 2013 Kaspersky Lab published a paper[9] in which they discussed about IceFoga a small APT group which was focused to target South Korea and Japan. It was hit-and-run type of attack where attacker do not keep persistence access of system to eliminate the possibilities of being caught.

3.5 Attack on eBay

This was the case in 2014 when e-commerce website ebay faced embarrassment. In may 2014 ebay accepted that the hackers successfully steal 200+ millions of user records. Later a group from Syria called "Electronic Army" took the responsibility of this attack.

3.6 Evernote and Feedly

These two companies were attack on continuous days, it was not clear that whether both of those attacks were linked or not. Evernote which was attacked first with a DDoS (Distributed Denial of Service) went down for few couple of hours. On the other hand Feedly, attacked on next day went down for a long duration and it was asked from some ransom to stop the attacks. Attacker group remain unknown.

3.7 Heartbleed

In April 2014 a sever bug was found in OpenSSL, an open source security protocol which is used by most of the major websites including facebook, Google, yahoo, Microsoft etc. This was discovered by a team from Google and Finnish security firm Codenomicon.

3.8 South Korean banks and broadcasters

In March 2013 attackers targeted three South Korean broadcasters and two banks in a coordinated attack. The attackers remained un identified but South Korean Internet Security doubted on North Korea, they also have claimed that North Korea has been preparing such team of hackers.

3.9 Home Depot

This firm was attacked by hackers and nearly 56 million accounts were compromised. The firm overall spent $90 million to replace its debit and credit cards from customers. Even after such

huge attack and urges of security consultants the company did not encrypted its data until September 2014.

There is a huge list of such cyber attacks on global level organizations where they have their dedicated security team to prevent malicious activities. In the next section we will see some of the security measurements which are affective to defend the system from attackers. Various types of attacks and their examples have been tabulated in Table-1 below.

Sr. No.	Name of the Attack	Description	Example
1	**Access Attacks**	Attack go get unauthorized access of a device.	a) Port trust utilization b) Port redirection c) Dictionary attacks d) Man-in-the-middle attacks e) Social engineering attacks and Phising
2	**Cyber espionage**	Spying on others on the Internet	a) Tracking cookies b) RAT controllable
3	**Cyber terrorism**	Causing the Destruction using Internet.	a) Crashing the power grids by al-Qaeda via a network b) Poisoning of the water supply
4	**Reconnaissance Attacks**	Type of attack which involves unauthorized detection system mapping and services to steal data	a) Packet sniffers, b) Port scanning, c) Ping sweeps and d) DNS(Distributed Network Services) Queries
5	**Denial of Service**	Attacking on system by making Internet resources unavailable for authorized persons.	a) Smurf b) SYN Flood c) DNS attacks d) DDos(Distributed Denial of Services)
6	**Non Malicious Attacks**	Unintentional attacks, happens because of some sort of mistake.	a) Registry corruption b) Accidental erasing of hard disk
7	**Active Attacks**	An attack with data transmission to all parties thereby acting as a liaison enabling severe compromise	a) Masquerade b) Reply c) Modification of message
8	**Attacks on WSN**	Targeted on Sensor Network, it make sensor unable to work properly and send the data to other nodes.	a) Application Layer Attacks b) Transport Layer Attacks c) Network Layer Attacks d) Multi Layer Attacks
9	**Cyberwar**	One nation attacks on the other on to destruct target nation's network. Reason for target can be to gain secrete information, making network unstable, injecting backdoors etc.	a) Russia's war on Estonia (2007) b) Russia's war on Georgia (2008)
10	**Passive Attacks**	Listening to communications and stealing data without actually doing anything suspicious on the network.	a) Traffic analysis b) Release of message contents
11	**Malicious Attacks**	Intentional attack to harm the systems over the network.	a) Sasser Attack
12	**Attacks in MANET**	Exploitation of issues of MANET properties. Attacking the node's communication.	a) Byzantine Attacks b) Black Hole Attack c) Flood Rushing Attack d) Byzantine Wormhole Attack

IV. RECOMMENDATION

To make the system and network secure from attacks several security measurements are to be taken care of in the organization, starting from the network deployment, hardware configurations, software installation and making users aware of those tools. Let us discuss in detail about these

4.1 Network Deployment

In an organizations security should be considered in mind when the network is designed and deployed for the very first time. The DMZ (Demilitarized Zone) approach is very common in organization where they have data servers accessible to clients from outside the network. The LAN of organization remains inaccessible to user from outside at the same time they can access the data server, this adds an additional layer of security. Placing a firewall at the single entry points of the internal network is another wise step to take. More number of entry point in the network make it weak and also it becomes required to watch over at multiple points simultaneously, so it's a better idea to make a single point from where all the internal network will connect to the network outside the organization which is generally the Internet. Deploying a firewall at such points is very important to make the network unbreachable.

The design must be scalable, meaning that the network size is not static and it is not going to be same as today. There will be change in number of workstations, their physical locations and change in user's access rights. It must be forward compatible; always adaptive for an upgrade to latest technologies, hardware up-gradation, software updates etc. When designing the network the accepted traffic must be taken into consideration, what kind of traffic and amount of the traffic must be accurately predicted by the designer so that appropriate hardware can be deployed according to the requirement.

Proper documentations of the network design is another important aspect, when someone is designing the network then it must be easy to troubleshoot; as it is impossible to make a network 100% error proof. The documentation helps network administrators to troubleshoot network issues more efficiently, especially if the network designer and administrator are two different persons. Also the design should be in such a way that administrator can monitor his network from a single place, and if possible he should be able to run basic troubleshot steps from monitor room itself.

4.2 Hardware

When deploying the network using the appropriate hardware is as important as the network design. Without compatible hardware the network may not function as intended to, for example if the organization is deploying a server which is expected to handle more than thousands of request at a time, and if the server machine is not capable enough to handle such huge traffic then there is no use of such service.

Compatibilities among hardware devices is vital when deploying a large network. Since the network has to be there for very long duration, the hardware must be compatible to most recent technologies and at the same time with older machines also. It is not always easy to completely upgrade all the workstations and networking devices matching to the latest technologies, so the hardware must be compatible with each other. Special care must be taken care while purchasing proprietary hardware as they might not be compatible to work with devices from other manufacturers. Such proprietary devices also demands for specific software to perform in better way, those software may or may not be able to fulfill your requirement specific to a particular organization. Some of the manufacturers have their own protocols implemented, so working with different protocols and different proprietary hardware can be challenging task for the network administrator.

The hardware may cause the security vulnerabilities also, if the manufacturer has not given attention to security concerns then it is hard to make such devices secure using external software tools. In case of Internet of Things and sensor networks, where memory is too small and we cannot have enough security software installed on them, the hardware becomes more vital. Wireless router are too common in organizations, it helps people to always be connected even if they are not on their desks. But keeping those wireless access point at the right place is also very much important. There are attacks like war drivers, evil twins etc. which are targeted to wireless networks specially. If the signals of wireless access point are going out of the organization premises, then it cannot be considered as good design, that is the place where the network becomes weak, as wireless access points are more vulnerable than wired routers.

4.3 Software

Use of hardware firewall is not sufficient to make a network completely secure. Writing correct policies on the firewall is also very important. The policies are designed keeping in mind the need of organization and potential attacks. Individual workstations are also required to have software firewall installed and properly configured on them. Keeping all the installed software updated and applying important security patches provided by developers is one of the mandatory steps. Administrator access on every system is not generally required by every user, so it is a good strategy to disable the admin rights it help users not to install malware un-intentionally. The software tools required in the organization must be purchased from authentic and official dealers, and maintenance of such tools must be done by experts only.

Anti malware programs are must to prevent the system from infections via emails, as one cannot write policies on the firewall for malicious emails. As we discussed in previous section emails are most common entry point for attackers to install malwares on target workstations. Keeping them updated is most important, as every other day there are new Trojans created by hackers to evade the systems. Security labs keep eye on such malwares and work hard to countermeasure them. Security updates are released as soon as any new virus or malware is detected by such labs, so keeping it update makes the system more secure to new kind of attacks.

Choosing an operating system is crucial for organizations, as there are too many operating systems available in the market each with their own advantages and drawbacks. It is completely depend on the organization's need that which operating system is to choose. Choosing operating system also depends on the hardware, certain hardware manufacturers recommends to particular operating systems. Major operating system providers at present are Apple, Microsoft, Red Hat, Ubuntu, etc.

4.4 People

All the security tools and mechanisms will be failed if not used properly. Using the appropriate tools properly is as important as having them. Every organization must keep their employees aware of cyber attacks and train them to be secure from such attacks. Training of using the latest technology available in the market to keep individual's system secure should be provided. It has seen that even after belonging from computer background and being a tech person, employees often use very weak passwords for their systems and login accounts. Keeping people in confidence and making them loyal to the organization is one of the most important task for the companies. It is observed that insiders were responsible for 48% of data breaches in 2009, and of that percentage, 90% were the result of deliberate and malicious activity [4].

Use of external storage devices should be avoided inside the organizations. This should be in policy of the organization and management should train employees to not use their personal storage drives on organization's machines. This is one of the major way to infect the machines from inside, also it prevents the data leakage from organization. The employees must keep their password safe,

and should choose passwords carefully. There have been several tools to keep track of one's passwords at one place, but it is again not trustworthy.

Social websites must be blocked inside the organization network. Though some of the big name in IT industry has allowed it's employees to use some of the social networking sites like facebook, twitter, LinkedIn etc. but again it is not free from risk [10]. There are people spreading malwares through social sites. Online games and flash videos can be sources of malicious codes. Cookies kept by such websites are way more dangerous they can be used to gain session access of a system and help to bypass the firewall.

In very crucial organization like research institutes and defense organizations employees should not be allowed to carry their cellular phones or any communication devices for that matter. Using organizations hardware for personal usage should also be avoided by the employees, as the devices are somewhat safe inside the organization's network but when they use systems in internet outside, it becomes very much vulnerable to malwares.

Physical access to important devices like servers or monitor rooms must be blocked. Such places should only be accessible to the network administrators and other designated personals of the organizations. If the security of those places is compromised and someone not legitimate person has got physical access of those devices, then there is very little chances that the network can remain safe. Similarly communication channels must grounded and should not be accessible to unauthorized people, wiretapping is an old and still very strong way to steal sensitive data.

V. CONCLUSION

Cyber world is vast and has no boundaries, it is open for everyone. In recent years cyber security is gaining implicit importance. Cyber crime is getting more and more sophisticated, aimed, collaborative and serious. It is mostly targeting economical and national organizations as we seen in most of the case studies. Cyber warfare is the next generation attacks countries are preparing for, national securities are on the stake. Security of personal data and privacy of individuals are the next thing on the line of target. With growing cyber crime there is need of security experts who can design robust network designs, and countermeasure latest malwares. Future belongs to technology and making it secure is a huge challenge.

VI. ACKNOWLEDGMENT

Pranav Verma would like to take this opportunity to thanks to Tejaskumar Chauhan for his support to prepare this paper.

REFERENCES

1. Youngsoo Kim, Ikkyun Kim, Namje Park, “Analysis of Cyber Attacks and Security Intelligence,” in Analysis of Cyber Attacks and Security Intelligence. Springer Berlin Heidelberg, Germany.
2. Patcha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. Computer Networks, 51(12), 3448–3470. doi:10.1016/j.comnet.2007.02.001
3. Ramamohanarao, K., Gupta, K., Peng, T., & Leckie, C. (2007, December 16–20). The curse of ease of access to the internet. In P. McDaniel & S. K. Gupta (Eds.), Information Systems Security, Third International Conference, ICISS 2007 Proceedings, Delhi (pp. 234–249). Berlin Heidelberg: Springer.

4. PandaLabs (2013). Pandalabs quarterly report January – March 2013. Retrieved form http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Quaterly-Report.pdf.
5. OWASP top 10 2013 - Top 10 www.owasp.org/index.php/Top_10_2013-Top_10.
6. McAfee Labs Threat Reports. Third quarter November 2014. www.mcafee.com/us/ resources/reports/rp-quarterly-threat-q3-2014.pdf.
7. china has army
8. Potts, M. (2012). The state of information security. Network Security, 2012(7), 9–11.
9. Kaspersky Labs, IT Security Risk Survey 2014: A Business Approach to Managing Data Security Treats.
10. The 2012 data breach investigations report. Retrieved from
11. www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf.
12. Goverdhan Reddy Jidiga and Dr. P Sammulal, "Machine Learning Approach To Anomaly Detection In Cyber Security with A Case Study of Spamming Attack" International journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 3, 2013, pp. 113 - 122, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.
13. Pratik Karnik, "Malwares, Vulnerabilities and Its Analysis And Mitigation" International journal of Computer Engineering & Technology (IJCET), Volume 4, Issue 6, 2013, pp. 110 - 120, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.
14. Anju S, Sheema M, Prof. P.Jayakumar and Dr. S.Sasidhar Babu, "Exposing Transient Secrets and Detecting Malware Variants Using Control and Data Flow Analysis" International journal of Computer Engineering & Technology (IJCET), Volume 5, Issue 12, 2014, pp. 31 - 36, ISSN Print: 0976 – 6367, ISSN Online: 0976 – 6375.