AWARENESS OF CYBERCRIMES AND SECURING THE ORGANIZATION NETWORKS BY PACKETS DOUBLE FILTERING METHOD

Shreelakshmi K J[1], V.K. Annapurna[2]
M. Tech Student, Department of PG Studies[1], Associate Professor, Department of Computer Science Engineering[2]
National Institute of Engineering, Mysore, Karnataka, India.

Abstract—

Internet is accessible by everyone and has great significance towards communication and services. Internet users should have awareness about cybercrimes which they are being victims unknowingly. Cybercrime directly or indirectly makes use of communication channel and devices as medium for their vulnerabilities. Integrated defense system keeps one's or an organization data secured but can't escape by new attacks inventing day by day. This paper describes more security towards network of the organization by analyzing and cross checking each packet in the network which also increases efficiency of the network.

Keywords— E-mail spoofing, Netizens, High-end Routers, Phishing, UTM.

INTRODUCTION

Internet is the open source architecture worldwide due to the characteristics like scalability, anonymity, global reach and there is a proportional increase in cybercrimes. Growing Internet penetration and rising popularity of online banking have made India a favorite among the cybercriminals [1]. Cybercrime directly or indirectly makes use of communication channel and devices as medium [2]. Netizens (regular Internet users) must be know about Electronic mail(E-mail) spoofing and Phishing attacks which is a huge attack on individuals and organizations at present. This paper discusses these two attacks, its awareness and shows how to keep communication network secure. The next section gives an overview of cybercrime in India. In section III classification of cybercrime is introduced followed by the proposed work.

CYBERCRIME IN INDIA

In [1] the year 2013, India has been ranked one among the world's top five countries for highest number of cyber crimes, Indian organizations perceived that it is a top four economic crime and in 2015 crimes increased by 300,000. To control the cybercrimes every country has its own Cyber law or Internet law. Indian government also framed such law called the Information Technology Act, 2000. This act applies to whole India which is meant for legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication.

CLASSIFICATIONS OF CYBERCRIME

A. Electronic mail (E-mail) spoofing and other online frauds: A spoofed E-mail is one which originates from the attackers websites but seems to be trusted website. And ask to re-enter the password to confirm it. Here the target is to know the email password of the individual by re-entering it again at hacker's webpage. It is used in computer based social engineering attacks. The spam emails sent with a target of one organization which appears as genuine E-mails to all the employees. They think it is send by the administrator of the organization. If the employee get login using the link he will put the entire organization at risk.

Awareness:

- Never ever trust the website asking your information or some confidential logins.
- Don't reveal personal or financial details to emails.
- Be aware of fake emails.
- Don't open email attachments and pop-up windows, if any suspicious call the organization and confirm.
- Don't response to spam emails [3].

B. Phishing: A kind of identity theft, fraud-phisher tries to get the user's personal data such as credit card number, password, account data by sending spam emails. Phishers sends the emails by wearing the mask of genuine sites like HSBC bank, eBay, Amazon, Facebook. It includes URL manipulation, URL directs the netizens (regular Internet users) to spam website by making small change in URL by altering one or two letters, which is neglected by netizens. Example: www.google.com is registered as www.g00gle.com likewise www.microsoft.com as www.rnicrosoft.com . Android (mobile) phishing, android market sends frequent messages, mails to download the software that speed up the device. But it is a track of stealing the data and online banking credentials from the device.

Awareness:

- Be suspicious about all unknown callers. Do not trust caller ID**.**
- Call them back to check the number exist or not.
- Be aware and ask questions if they ask your details or financial information.
- Make sure before clicking on the links that redirects to other sites.
- Use phishing filter.
- Report to nearest cyber police cell.

Other types of cyber crimes:

- Spamming- spam is sending unsolicited bulk messages indiscriminatelythrough electronic messaging system.
- Cyber defamation- it spoil one's reputation through computer and Internet with victim identity sends defamatory information to all his friends.
- Computer Sabotage- the use of Internet to hinder the normal functioning of a computer system through the introduction of worms, viruses or logic bombs.
- Pornographic offenses- to reach and abuse children sexually worldwide Internet is being used highly by abusers.
- Password sniffing- programs that monitor and record the name and password of network users as they login at a site.
- Denial of service attacks- makes use of spamming technique and targeted sites are web servers of banks, credit card payment gateways, mobile phone networks and domain names**.**
- Virus attacks/disseminating viruses- A virus program that infects the programs/files of host system by getting control over host system.
- E-mail bombing/mail bombs- targets crash victim's email account or make victim's mail server crash by sending a large number of emails.
- Salami attack/Salami technique- it is a financial crime which is unnoticed and insignificant in a single case as "Small sharing for Big gains".
- Trojan horse- program which is malicious and harmful deployed with in harmless program or data to get control over the host.
- Industrial Spying/Industrial Espionage- type of Trojan or spyware attack to steal the corporate data. Intellectual property or yield of competitive advantages.
- Computer network intrusions-hackers from anywhere in the world performs the activity like stealing data, insert Trojan horses or change username and passwords.
- Software piracy-**c**oping the genuine software by illegally and distributing of product widely [5].

The next section describes the proposed work to avoid some of cybercrime attacks.

IMPLEMENTATION

A. Existing system

To control the cybercrime, individuals and organizations are using firewall, antivirus software. But attacker are inventing different form of cybercrimes every day, after infecting the system these antivirus will scan and block the viruses/worms by checking once [6]. In mean time attacker may get little bit of information of the system.

B. Proposed system

Packet analysis and verification is done through two times filtering of coming packets before it is routed in to organization server. It is used to control the attacks like E-mail spoofing, phishing, spamming, cyber defamation, computer sabotage, password sniffing, denial of service attacks, virus attacks, mail bombs, salami attack, Trojanhorse, Industrial spying/Industrial espionage, computer network.To secure the organization resource access from attackers, there is a double filtering (cross checking) of packets from public Internet and organization Intranet as shown in the figure 1.

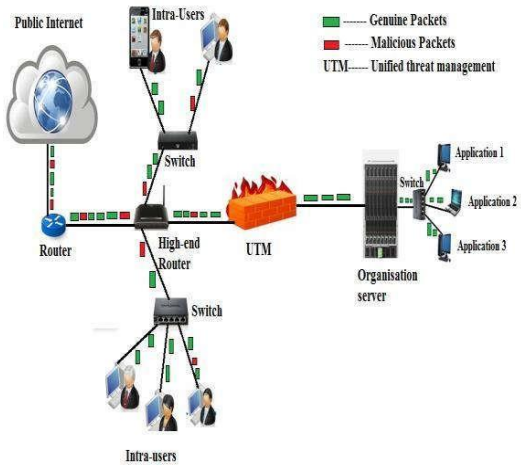

Fig. 1.High security-Double filtering packets

Step 1: Public users send the request to server, while this network path contains numerous security devices before accessing the server.

Step 2: The user's packets routes through the organization router initially, which contains both genuine and malicious packets as shown in figure 1.

Step 3: High-End Router has built-in features like firewall, Network access control (NAC), trace route, stateful packet filters and blocking spam websites. Firewall detects malicious and vulnerable packets based on IP address and port number which provides source address, destination address in the header of each packets, NAC examines the network path from where the packets are routing and observes the working of first router i.e, will not leave the first router to be maliciously compromised. Trace route detects the path a packet takes to get to a remote device through the Internet. Stateful packet filtering inspects packets and their content by providing high level security and good performance.

Step 4: Now the network traffic from first router and organization traffic from Intra-users through switches routes to High-End Router which is the first level security.

Step 5: After this level, filtered packets are routed to unified threat management (UTM) is a security software and second level filtering has built-in high capacity firewall as compared to high-end router's firewall. In addition UTM has three high stage security features like Accesslist (ACL), Intrusion prevention system (IPS) and filtering packets based on applications.

Step 6: ACL is a form of stateless packet filtering implemented at network security which filters unwanted packets from the network filter based on the conditions defined in the list of ACL. It is also used in decision made on per packet basis, inspecting packet header and filters network traffic.

Step 7: IPS monitors potentially malicious traffic by inspecting the entire packets and blocks it as a precautionary measure in security it also sends the message to network administrator. Attackers perform network mapping through port scans and TCP stack scans, IPS detects and block the activity. It also detects DOS attack, different forms of worms, viruses and application vulnerability.

Step 8: Third feature explains, instead of port number filtering, application filters the packets based on socket filters. It also examines the process ID of data packets defined by set of rules at local process during data transmission. UTM has multi-function security appliance, so that some form of worm or other malwares can be unleashed from the network.

Step 9: After double filtering is done, UTM routes only the genuine packets to organization server. Here the server is highly protected by two level packet filtering. And organization server will not be affected maliciously by attackers. The genuine packets are switched to its application related hosts as shown in figure 1. The advantage from this system is it reduces traffic load initially at high-end routers by blocking/dropping unwanted packets and selecting genuine packets. Doubly verifying malicious packets and blocking them gives more trustable services to clients.

CONCLUSION

There is an increase improvement of global communications in Internet. This makes more efficient use of e-commerce as beneficial to society. Unfortunately, cybercrime poses a substantial threat to all these positive outcomes by harming the communication network to steal or modify data as required by attackers. This paper highlights different forms of cybercrimes. And precautionary measures taken at network level packet transmission as well as application based high security to the organizations.

ACKNOWLEDGMENT

First and foremost we express our sincere gratitude to the almighty for the successful initiation, execution and completion of this paper. We would like to thank our colleagues in college sincere support, help and guidance. Also the cyber lawyers, cyber Police, and scientist's involved and spreading consciousness on the cybercrime topics. Our sincere thanks to one and all that may not find a mention but have always wished only success.

REFERENCES

[1] Dr. P. N. Vijaya Kumar, "Growing Cyber Crimes in India: A Survey", IEEE, 2016.

[2] Vinit KumarGunjan, Amit Kumar and Sharda Avdhanam3,"A Survey of Cyber Crime in India", IEEE, 2013.

[3]D.Mooloo and T.P.Fowdur, "An SSL-based client-oriented anti-spoofing email application", IEEE, 2013.

[4]Jordan Crain, Lukasz Opyrchal and Atul prakash, "Fighting Phishing with Trusted Email", IEEE, 2010.

[5]M.Uma and G.Padmavathi, "A Survey on Various CyberAttacks and Their Classification", International Journal of Network Security, Vol.15, No.5, PP.390-396, 2013.

[6] Mohammed Ibrahim Al-saleh, Antonio M. Espinoza, and jedediah R. Crandall, "Antivirus performance characterization: system-wide view",IET, vol. 7, pp.126-133, 2013.