Security and Privacy Impact

Tulasi Pilli

Wilmington University

October 2014

Table of Contents

Introduction

In this world, technology has developed rapidly in the past few years. There is lot of improvement in our daily life with the evolution of modern technology. As the technology develops, threats also increase simultaneously with strong impact on networking and web applications. Many organizations, completely depend on networks and web applications for the daily business transactions. Many innovative security measures have been developed in order to face the network security issues. But still there is no end for the rise of threats. Research scholars Zeadally, Yu, Jeong & Liang explain some of the common security threats as “fraud, sabotage, theft of intellectual property and copyright violation” (2012, pp184). Moreover, computers connecting to networks and accessing online accounts are facing major security issues.

Network security

Network threats are quite different from computer threats, in which the operating devices are disabled at network level in order to malfunction many number of devices and systems instead of attacking a single computer and stealing the data. Network level threats are mainly two types namely, intrusion threats and denial of service attacks. Intrusion threats are mainly caused by the unauthorized personnel in order to gain complete access of a computer on a network and operate various operations against to the organization policies (Gercek and Saleem, 2005, p22). The process of intrusion can be easily completed by attacking the transmission control and user datagram ports of network. After attacking the ports, intruder may gain access to the local computer or network devices like router, switch. By gaining access to the network devices, or a computer, intruder can control the whole network and access the operating functions of devices officially. Employees of an organization are unable to know about the attacks, as intruders may not corrupt the data immediately, intruders will observe the entire operational functions and then attack the whole devices or network system in order to cause huge damage.

Denial of service attacks causes more damage by affecting the entire network instead of single computer system. Research scholars Gercek and Saleem explains that, “some of the well-known denial of service attacks include Ping of Death, SYN Flood, and LAND attacks” (2005, p22). The denial-of-service attacks have become more complicated by the evolution of distributed denial of services attacks, in which multiple sources or computers known as zombies are introduced to attack multiple points in a network instead of a single port, which leads to huge damage to the functions of network. Research scholars Yu, Fang, Lu and Li (2010) explain the concept distributed denial of service attacks as the attack which makes “server suffer in having low responses to clients or even refusing their accesses, may be exploited by one’s business

competitors expecting to gain an edge in the market or political enemies trying to stir chaos" (p1952).

Distributed denial of service (DDoS) attack is not made for fun, instead harmful traffic is created in the network by deploying destructive weapons in a distributed manner all over the network at various ports. There are many types of DDoS attacks like flooding of HTTP, SYN, ICMP, UDP and other TCP attacks. Research scholars Bhuyan, Kashyap, Bhattacharya and Kalita (2014) depicts the percentage of DDoS attacks caused by various types during a survey in the year 2011 as shown below in Fig.1

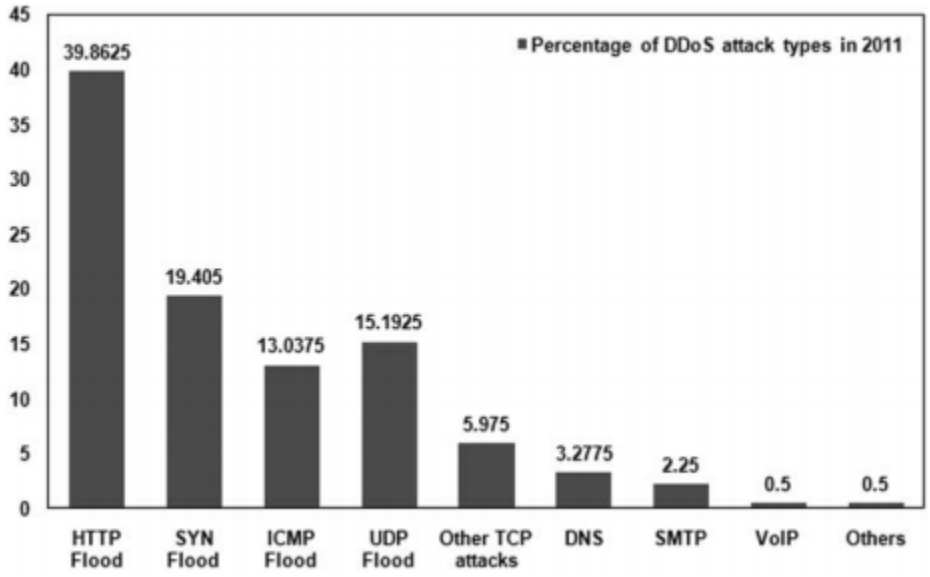

Fig. 1: DDoS attacks statistics by type in 2011

(Bhuyan, Kashyap, Bhattacharya and Kalita, 2014, p539)

As shown in above Fig.1, the majority of DDoS attacks are caused by HTTP flood with 40%, then SYN and UDP floods are heavily used by intruders with 35%. Voice over IP and other attacks are least used with 0.5%. Finally, the remaining types of DDoS attacks ICMP, TCP, DNS and SMTP with 25%.

Network threats have become a severe challenge to many organizations, which may result not only in financial loss but also reputational loss. Some solutions have been developed in order to improve the security levels of network. Research scholars Gercek and Saleem (2005) explain the solution to intrusion threats is the usage of personal firewall that consists of logs to provide the history of networking during the forensic data analysis in order to restrict the unwanted port transactions (p23). On the other hand, distributed denial of service attacks can be restricted by trust management in which client entering the network is verified and then allows into the network. Some of the properties in designing the trust management is explained by the research scholars Yu, Fang, Lu and Li (2010) as follows:

- Performance of the network can be enhanced by deploying at the server
- Processing delays can be reduced by applying light weight processor mechanisms
- Accessing the trust mechanism independent of server details
- Concurrent requests have to be differentiated by the trust mechanism (p1955).

Firewall

The existing network security policies like firewall protection, and authentication are easily cracked by hackers. Many organizations are implementing security measures with huge amounts of money investment. Despite of huge investments, networks are intruded and loss of data takes place in many companies. Research scholars Sher, Wu, & Magedanz, (2006) explain the attack of TCP/SYN flood as shown in below figure 2.

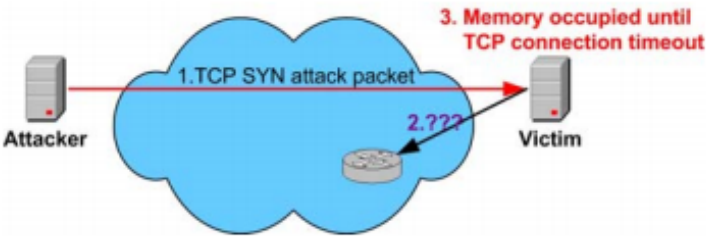

Fig. 2: TCP/SYN Flood attack

(Sher, Wu, & Magedanz, 2006, p40)

As shown in above figure 2, during the step 1, attacker sends packets to various IP addresses randomly and identifies the source address of victim. The source address is reverted in step 2 through which an intruder can gain access and forges the data. An intruder can access the data of victim until the timeout of TCP connection, which is clearly shown in step 3 (p40). So, securing the firm's data with firewalls becoming extinct. It was supported by research scholars Gercek and Saleem that networks are easily attacked by:

- Lack of efficiency in firewalls implemented by the firm
- Viruses intruded by downloading various web applications
- Poor composition of web, file, and mail servers
- Email attachments sent by unknown personnel
- Lack of proper designing and configuring wireless LANs (2005, p18)

Network Security in Future

Many organizations follow certain set of standards for improving the network security. Along with authentication, some specific policies like minimum 8 characters which consists of upper case, lower case, and also one special character credentials are practiced. Unfortunately, technology is helpful to crack the complicated credentials, which proves the weakness of existing network security. In order to secure the data, virtual private network has been implemented along with credentials. Moreover, network engineers have to verify the network frequently in order to detect the issues before losing the data (Kocan and Sundresh, 2006, p2). Hackers try to intrude the IP protocols in order to obtain the crucial communication of an organization. So, every

organization has to follow a set of security policies in order to identify and restrict the network access to unauthorized personnel.

It is very important to maintain a set of security standards. Research scholars McClure, Scambray, and Kurtz (2009) say that "It is important to test and audit each program" (p315). Because programs are written manually which may consists of human errors in order to reach the project deadlines. So, it is crucial to self-check each and every program. One of the major testing processes implemented by a firm is to hack own network by regular intrusions into the company wireless network (Fox, 2002). In this process, if the network engineer is able to intrude, then the firewall and the intrusion detection and prevention systems are weak enough to lose the data of organization. It is the responsibility of an organization to secure the data by implementing virtual private network (VPN), which displays a unique code changing for every thirty seconds. The unique code is considered as one of the credentials used to access the online accounts. Moreover, the virtual private network gateway has to be placed inside the firewall or else, VPN can be easily cracked. So, the network engineers can expect the failure of unique code displayed by virtual private network in upcoming days. Research scholars Kocan and Sundresh supported that, hackers are going to crack the virtual private network and rise new security issues (2006, p2).

Network security for Mobile devices

In this electronic era, many smart phones were developed which can perform similar functions of a computer and many firms deal crucial transactions on telephone communications. Many people think that, security issues may not affect the data on mobile devices which is just an assumption. Coming to reality, security threats have extended to telecom sector by eavesdropping and intruding voice over internet protocol (VoIP). Research scholars Biswas and

Ali (2007) explain that “Eavesdropping is the reading of messages and conversations by unintended receivers” (p14). As the wireless communication uses the RF spectrum, communication calls can be easily intercepted by tuning to appropriate frequency and also inject fake messages.

Voice over IP converge the wireless and wireline in order to improve the quality of communication. Intruders target the ports of network utilizing the VoIP and trap the phone calls by using many devices and software programs available in the market (New technologies, 2005). So, the networks have to be more protected in the upcoming days with implementation of trust management and improving the security levels in telecom sector.

Conclusion

Technology is useful to make man’s life easier, at the same time many issues have been identified. Though, many innovative techniques are developed to face the challenges of network security, new issues are rising every day. The extinct of firewall protection is the best example to prove the evolution of network issues over security measures. So, it is the responsibility of network engineers to plan for the upcoming threats. Moreover, organizations of telecom sector and mobile industry have to implement high standards of network security. Thus the extinct of firewalls, network security threats and solutions, and the importance of network security in utilizing mobile devices were discussed in this paper.

References

Bhuyan, M. H., Kashyap, H. J., Bhattacharyya, D. K., & Kalita, J. K. (2014). Detecting Distributed Denial of Service Attacks: Methods, Tools and Future Directions. Computer Journal, 57(4), 537-556. Retrieved on May 3, 2015 from http://search.ebscohost.com.mylibrary.wilmu.edu/login.aspx?direct=true&db=aph&AN=95330755&site=ehost-live

Biswas, K., & Ali, M. L. (2007). Security threats in mobile ad hoc network. Paper submitted to the Department of Interaction and System Design, School of Engineering at Blekinge Institute of Technology. Retrieved on May 3, 2015 from http://www.bth.se/fou/cuppsats.nsf/all/3878ec739b12f80ac12572c2003f7d58/$file/Final_Thesis.pdf

Fox, P. (2002). No Wires, No Security, No Solution. Computerworld, 36(15), 24. Retrieved on May 2, 2015 from http://search.ebscohost.com.mylibrary.wilmu.edu/login.aspx?direct=true&db=aph&AN=6502575&site=ehost-live

Gercek, G., & Saleem, N. (2005). Securing Small Business Computer Networks: An Examination of Primary Security Threats and Their Solutions. Information Systems Security, 14(3), 18-28. Retrieved on May 2, 2015 from http://search.ebscohost.com.mylibrary.wilmu.edu/login.aspx?direct=true&db=aph&AN=17391995&site=ehost-live

Kocan, K. F., & Sundresh, T. S. (2006). Networks of the future become reality. Bell Labs Technical Journal, 11(1), 1-4. doi:10.1002/bltj.20140. Retrieved on May 3, 2015 from

http://search.ebscohost.com.mylibrary.wilmu.edu/login.aspx?direct=true&db=aph&AN=20877381&site=ehost-live

McClure, S., Scambray, J., Kurtz, G., & Kurtz. (2009). Hacking exposed: network security secrets and solutions. McGraw-Hill. Retrieved on May 3, 2015 from http://stepheneshort.com/other/library/_non%20fiction/_computing%20and%20internet/Hacking%20Exposed%20-%20Network%20Security,%20Secrets%20and%20Solutions,%203rd%20Ed%20[2001].pdf

New technologies, new threats. (2005). Communications News, 42(6), 10. Retrieved on May 3, 2015 from http://search.ebscohost.com.mylibrary.wilmu.edu/login.aspx?direct=true&db=aph&AN=17287068&site=ehost-live

Sher, M., Wu, S., & Magedanz, T. (2006, September). Security threats and solutions for application server of IP Multimedia Subsystem (IMS-AS). In IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation (pp. 38-44). Retrieved on May 3, 2015 from http://www.diadem-firewall.org/workshop06/papers/monam06-paper-28.pdf

Yu, J., Fang, C., Lu, L., & Li, Z. (2010). Mitigating application layer distributed denial of service attacks via effective trust management. IET Communications, 4(16), 1952-1962. doi:10.1049/iet-com.2009.0809. Retrieved on May 2, 2015 from http://search.ebscohost.com.mylibrary.wilmu.edu/login.aspx?direct=true&db=aph&AN=55032891&site=ehost-live

Zeadally, S., Yu, B., Jeong, D. H., & Liang, L. (2012). Detecting Insider Threats: Solutions and Trends. Information Security Journal: A Global Perspective, 21(4), 183-192.

doi:10.1080/19393555.2011.654318. Retrieved on May 3, 2015 from http://search.ebscohost.com.mylibrary.wilmu.edu/login.aspx?direct=true&db=aph&AN=76349820&site=ehost-live