International Journal of Computer Applications (0975 - 8887)
Volume 155 - No.1, December 2016

Current Computer Network Security Issues/Threats

Ammar Yassir
Arab Open University (AOU) - Oman Branch
Muscat, Sultanate of Oman

Alaa A. K. Ismaeel
Arab Open University (AOU) - Oman Branch
Muscat, Sultanate of Oman

ABSTRACT

Computer network security has been a subject of concern for a long period. Many efforts have been made to address the existing and emerging threats such as viruses and Trojan among others without any significant success. Worse, new issues and threats have been emerging given that technology changes and becomes obsolete in a short while. In this regard, this research delves into the current network security issues in order to give future directions of research in a bid to help security technologists know where to focus their resources.
This research examines the threats in terms of whether they are hardware or software issues. The need of this research is well articulated with the current security threats and countermeasures clearly outlined. The research found the following as the current major security threats: social engineering and phishing, malware infiltration through external hardware and removable media, malware infection through intranet and Internet, invasion through remote access, human sabotage or error, DDoS attacks, and cloud and extranet components being compromised.

Keywords

Computer Networks, Security, Threat, Attack

1. INTRODUCTION

Computer network security issues/threats are growing in sophistication by the day. The development of new and innovative ways to breach network systems is a continual process in an attempt to counter the security measures installed by security experts [1]. Unlike in the past where hacking involved a lone attacker;companies that specialize in attacking other organization and selling stolen data and malware have cropped up [2]. Computer networks are made up of software and hardware components each with its vulnerabilities. In contrast to software threats, the hardware risks are easy to detect [3]. This is because they cause harm on both the data and device while a software threat only harms the data. Knowing vulnerabilities that may arise in the network may help organizations in planning and building a successful network and countermeasures to apply in a case such threats arise [4].

2. HARDWARE AND SOFTWARE THREATS

Predictions by Gartner Research Company estimated that by the end of 2016, 6.8 billion connected devices would be in use representing an increase of 30% from 2015 [4]. The number is expected to rise to over 20 billion connected devices by 2020 meaning that for each human, there will be about two or three devices that are connected. Such high numbers of connected devices present an extraordinary opportunity for hackers thus increasing threats/security issues.
Hardware threats include physical, electrical, environmental and maintenance. Software threats are mostly external through an unsecured network or breaching a secure network. Software threats pose the most damage to any organization, as data may be corrupted or stolen. Security in software can be compromised when a developer provides certain features. Software security threats involve confidentiality, integrity, and availability [5]. Privacy aims at keeping data secure from unauthorized parties,where integrity aims at preserving data from being altered, and availability aims at availing data to legitimate users only. Companies, therefore, have to understand the nature of network security attacks and deal with them accordingly. Some of the current Security threats and countermeasures are discussed below.

2.1 Social Engineering and Phishing

Social engineering is the use of non-technical means to gain illegal access to certain information of systems. Phishing is the most common means of social engineering through which hackers execute their attacks today. Common phishing scams display the following features; attempts to acquire personal information such as social security numbers, names and addresses, use of embed links which redirects users to malicious URLs through which their information is captured and prompts the user through threats that manipulates one to act immediately by following the links [6].
Through phishing emails, social engineering exploits traits like respect for authority, belief helpfulness, fear, or curiosity [7]. Employees ate enticed or tempted to open malware containing attachments or follow links to malicious websites. Victim?s login credentials can be obtained through phishing attacks or malware distributed through these messages. Also, seemingly harmless attachments or links install Trojans or other malware when opened. Spear phishing refers to attacks where such emails are tailored to particular people with the intention of infiltrating the system [7].
Social engineering attacks are done in a cycle with different phases: gathering of information, relationship development, exploitation, and execution, as shown in Figure 1.
During information gathering, the attackers prepare for the attack by collecting necessary details that will enable them formulate texts that are likely to easily lure the users. Information gathered is also used to determine possible passwords, possible responses from the users and the attack vector to use. In developing relationships phase, the attackers build a rapport with the target so that a

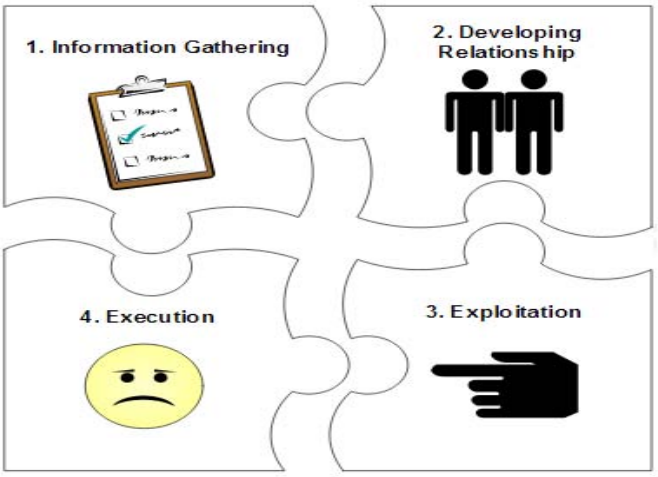

Fig. 1. Phishing of information and social engineering exploitation.

door can be opened for them to gain access into the users system. It is executed through close sharing of pictures or developing close friendship via social networking sites such as *Facebook* and with time the attacker gathers more information regarding to the user.
Exploitation is the third phase through which the attacker uses the information gathered and the links formed through relationship development to infiltrate the target. Exploitation begins and extends when the user begins to share passwords and usernames via the social network. The fourth phase, execution, is the stage at which the attacker accomplishes the ultimate goal by executing the attack and exiting the relationship in such a way that the target does not realize [8].
The fact that there is a cycle does not mean all the attacks are similar; each is unique and may involve one or multiple phases. An aggressor may employ many methods to collect data regarding a target such as birth dates and phone list among others. After collection, the aggressor can engage the target in a bid to gain his or her trust. Later, he may manipulate the target to give data such as passwords and then hack into the targeted item [9].
Countermeasures to be applied against social engineering and phishing attacks include training of employees to create awareness of such attacks and establishment of security policies as precautionary measures such as classification of information, back policies, policies on data destruction and handling of devices within the organization. The introduction of alarm channels in case of an attack or notice of suspicious activity. Finally, installation security mechanisms to the automatic detection of attacks or misconduct and maintaining backups for the restoration of data in the event of an incident [10].

2.2 Malware Infiltration through External Hardware and Removable Media

Employees regularly use removable devices such a USB drives or external hard drives for both work and personal purposes. Additionally, the use of notebook computers for either work, own purposes or maintenance purposes carries the risk of infection by viruses or malware [11]. The lack of awareness of the risk posed by such activities or the dire effects of malware on the company network leads to such practices. Potential threat/security issues/scenarios include infection of USB drives a private environment or office network and the malware infecting the Internet Computer System network (ICS), as shown in Figure 2.

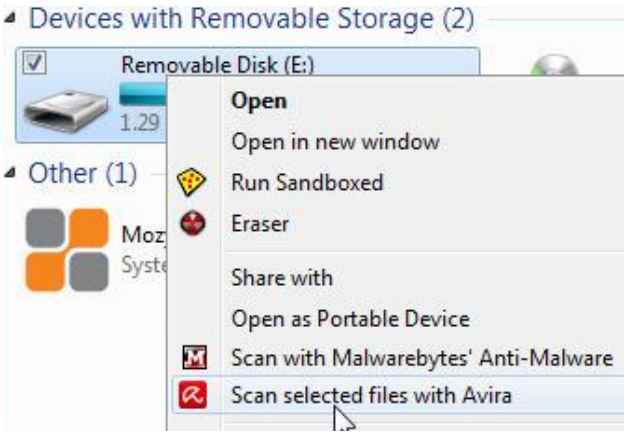

Fig. 2. Malware detection in USB storage drives.

Viruses infiltrates through the external hardwares and removable storages quite easily because more often these devices are not included in the drive selections for virus scanning by the antivirus. Any device ought to be included in the virus scanner by default so that it is always scanned. Management of viruses infiltrated through removable disks is further complicated by the fact that they are highly portable hence managing their movements is difficult. High portability exposes it to more viruses which may contract and transmit to the system [12].
Also, computers used for maintenance purpose, have been infected through office networks or the internet and may affect the ICS network with malicious code [10]. Project files may also contain malware/malicious code resulting in a data leakage or an infection.
Countermeasures against infection through external hardware or removable media include instituting strict technical controls and policies regarding removable media and notebook computers used for external maintenance. Removable media can be monitored through; creation of security boundary for removable media, encrypting individual data, exclusivity in use of ICS network and barriers preventing connection of removable media to the network [13]. For notebook computers used for external maintenance, data should only be exchange through removable media, quarantine networks introduced to enable external access computers, scanning for vulnerabilities before connecting to the network and encryption of such equipment [10].

2.3 Malware infection through Intranet and Internet

Networks within most enterprises make use of core components such as databases, webservers and operating systems some of which have a connection to the internet or intranet. New vulnerabilities arise in such a system where malware may be deployed into the intranet sometimes through removable media. Unlike in previous days where there were no linkages to the ICS network, the thing has changed because of Ethernet-based networks. Once malware finds away into the intranet, it becomes only a matter of time before it infiltrates the ICS network. Potential threats in such a system include manipulation of web pages to infect victims who access them, attacking web pages belonging to the enterprise and

attack by undetectable viruses/malware [10]. Figure 3 shows a recent increase of malware attacks in the Middle East with the United Arab Emirates having the highest percentage of security attacks [5].

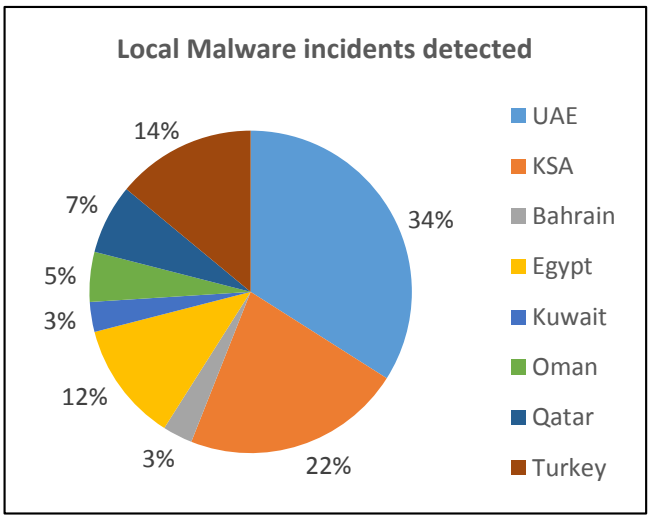

Fig. 3. Kaspersky lab observes an increase in malware attacks.

This analysis and findings have helped to reveal the number of malware attacks that has occurred recently in the Middle East region countries in the 2013 third quarter. The unwelcome table had the UAE topping on the list which had 34% of the total attacks that occurred with Saudi Arabia following with a 22% of the malware attacks. Turkey appeared third in the list with a 14% of the attacks. Egypt took the fourth place with 12% and Qatar being fifth in the list with 7% followed by Oman 5% then Kuwait and Bahrain who had the least attacks of 3%.

A total of 978,628,817 threats were detected by the Kaspersky Lab products. 500, 284, 715 out of the total threats were launched from online resources all over the world. Kasperskys Lab protection was able to block 476, 856, 965 threats that were directed to the users who had installed the Kaspersky security. It was noted that most of the threats originated from the United States which were generated through malicious web resources and accounted for 45% of the total threats. However, when it comes to internet based malwares, local threats take the lead. Win32.Sality was the kind of malware that was widely spread in the Middle-East countries which was spread through network shares and removable media. Turkey hosted 90% of the total malicious threats.

Additionally, Kaspersky indicated that spread of malwares has been accelerated y social networks such as Twitter and Facebook. This has been occasioned by a rise in number of social network users by 88% in the region. It was also indicated that the developers of malwares took advantage of the high interest in political news about Middle East and most of the threats were spread through political news links [10]. Further, Kaspersky observed that use of drive-by downloads is increasingly becoming the major means of spreading the malwares apart from removable media and local networks. It was also noted that Android mobile malware is rapidly spreading in the Middle East and has prompted the companies to adopt a strategy called Bring Your Own Device.

Countermeasures against infiltration through the internet or intranet include the creation of an air gap/isolating different networks using firewalls to remove attacks directed to the ICS network. Another countermeasure includes creating of a perimeter or safeguards on the system, monitoring of login data to check for unfamiliar connections while limiting access to sensitive enterprise information. Additionally, it may involve patching of office applications, operating systems, and back-end networks regularly and promptly [10].

2.4 Invasion through Remote Access

In ICS installations, it is common to allow external access for the purpose of maintenance. During this process, poorly secured networks may be at risk of foreign attack. Also, there is sometimes lack of authentication for systems or lack of limits during external access using VPN (Virtual Private Networks). External service providers and product suppliers are also often contracted programming and maintenance purposes thus posing security challenges, as there are several external parties involved [14]. Potential threats include attacks originating directly from the support point of access or an indirect attack on the service provider's IT systems with external access. A direct attack may occur in the form of attack on access points protected by passwords, use of a previously recorded password or specific attacks through the web [15]. Conversely, indirect attacks may occur in the form of Trojans taking advantage/exploiting the external system of the service provider, theft of login details or theft of notebook computers that are used for gaining external access [15].

Countermeasures against remote access auditing of systems to find vulnerable points of access, deleting/blocking passwords given by product supplier or encryption of systems and having secure authentication/authorization procedures. Also, networks should be segmented to prevent remote access, having a demilitarized zone for access by the external maintenance instead of directly to the ICS network and having firewalls for monitoring and permitting access to the system. Finally, remote access for maintenance purposes for a specified duration then logging off after maintenance is complete and personalizing means of access such that only a single user login is permitted at a time [10].

2.5 Human Sabotage or Error

Employees in an ICS environment both internal and external are usually in a position that determines the security of the organization. Although regulations are required to ensure proper security protocols, security cannot be assured through these controls alone. Security threats arising from members of staff are because of human error or sabotage and espionage. Potential threats posed by human sabotage or error include improper configuration of safety components, ICS components, and network components. Also, weak patches/updates installation, placing of wiretaps, damaging of installations and devices, and use of unauthorized hardware or software to compromise the system are instances of either sabotage/espionage or human error [10].

Several countermeasures need to be applied to prevent such errors or sabotage from happening. Firstly, the organization should introduce a principle of need to know to ensure information is only shared with the required individuals. Secondly, hiring competent, qualified and motivated staff and training them to understand the system to avoid errors. Also, the process of staff recruitment as well as external contractors should be standardized. Thirdly is the implantation procedures and policies for usage technical systems. Finally, monitoring of configurations and health of the system automatically and filling configurations and projects securely [10].

2.6 Cloud and Extranet Components Being Compromised

Outsourcing IT components is a practice growing in popularity in the ICS sector. The concern, however, lies in the area of big data and cloud-based solutions. Big data refers to data capture and processing for interpretation externally by use of complex models meant to optimize processes like manufacturing or configure machines [16]. Security components also offered through cloud-based solutions such as maintenance through remote access through the cloud. Such solutions although advantageous, especially for small enterprises, leave the owner with little control on security issues while the components are still directly linked local production. Threats arising from such operations include interruption of communication between outsourced components and local production. Access to externally stored data due to insufficient security and collateral damage because of attacks on other cloud services [10].
Use of certified and trusted service provider is an effective countermeasure against such threat. Additionally, a contractual obligation by service providers of external components is vital to provide and maintain sufficient security. It could be achieved through cryptographic mechanisms strong enough for protection of stored data. Finally is to ensure secure connectivity of external components and local production. VPN have to be in use [10].

2.7 DDoS Attacks

Distributed denial-of-service DDoS attacks occur in two ways. Firstly, ICS components use both wireless and wire communications, and when interruption of such connections occurs, transmission of data ceases. Secondly is overloading components with many inquiries thus slowing the system making it unable to provide appropriate and timely answers. Such attacks are meant to cause a breakdown in the system deliberately. DDoS attacks on remote components? internet connection are one of the potential threats of these attacks (See Figure 4). A study by Roozbahani and Azad found that in DOS, other clients can utilize the resources, data, and communication. [17].

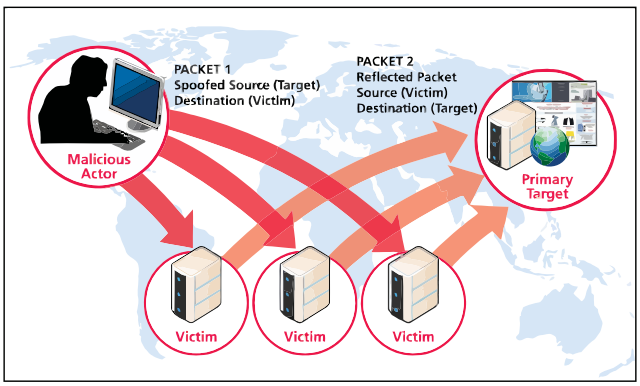

Fig. 4. A DDoS attack reflection with netflow.

Hacktivism groups have become notorious for such attacks. DoS attacks can also be launched on individual component where it causes such a component to crash affecting central components such as databases. Also, DoS attacks can happen on wireless connections like mobile communications networks or WLAN by jamming transmitters, sending tailored data packages or using the fake base station to force systems into relation to the wrong networks [2].

Hardening of communication channels and access points through stick configuration of systems is one countermeasure to deal with DDoS attacks. Additionally the use of systems that detect intrusions during DDoS attacks and raise alarms. Ensuring that the application can handle high traffic volumes, confirming that updates and patches are of current security standards, ensuring that lockout policies for the application cannot be exploited, as well as, configuring operating systems and application with DDoS attacks in mind are also efficient countermeasures [2].

3. DIRECTIONS FOR FUTURE RESEARCH

The computer and Internet are a growing concern because technology advances by the day and hence, the old techniques become obsolete in a short period [18]. This makes computer network security a current and timely topic, which needs progressive research so that the new threats can be identified and improved solutions given. This can only be possible if computer technologists are up-to-date with the dynamic technology world. Thus, it is important to devote resources in research and development programs. The society ought to receive continued resilience and security. Here, the private segment should join hands so that cyber security scholars can be empowered to formulate advanced security ware, which can be used effectively even online [19].

4. CONCLUSION

In summation, cyber security has become a major issue to contend with in the recent past as attack has increased. Understanding the vulnerabilities that may occur in a system or network will help organizations build better security mechanisms to protect their systems. Weaknesses/network security issues facing companies include DDoS attacks, attacks on the cloud and extranet, invasion through remote access, human errors/sabotage, malware infiltration through external hardware, removable media, internet and extranet and social engineering and phishing. Putting a PC in a bank vault with security officers with shot firearms and Rin-tin-tin won't secure the PC's information. To secure personal information and data one should consolidate the utilization of unique Data Security programming alongside Physical Security strategies. The discussed cyber threats on computer networks are just some of the few currently trending issues facing organizations. Computer systems security threats are too many to be counted while other risks are being created on a daily basis. Companies have to stay informed and alert to defend themselves against the ever-increasing attacks.

5. REFERENCES

[1] Libicki, M.C. and Ablon, L. and Webb, T., *The Defenders Dilemma: Charting a Course Toward Cybersecurity*, ser. Research report (Rand Corporation). RAND Corporation, 2015. [Online]. Available: https://books.google.com.om/books?id=f-n7CQAAQBAJ

[2] Meier, JD and Mackman, Alex and Dunner, Michael and Vasireddy, Srinath and Escamilla, Ray and Murukan, Anandha, "Improving web application security: threats and countermeasures," *Microsoft Corporation*, vol. 3, 2003.

[3] Geetha, S. and Phamila, Asnath Victy, *Combating Security Breaches and Criminal Activity in the Digital Sphere*, ser. Advances in Digital Crime, Forensics, and Cyber Terrorism. IGI Global, 2016. [Online]. Available: https://www.amazon.com/Combating-Security-Breaches-Forensics-Terrorism/dp/1522501932

[4] Taylor, Harriet, "Biggest cybersecurity threats in 2016," October 2016, http://www.cnbc.com/2015/12/28/biggest-cybersecurity-threats-in-2016.html.

[5] Himma, Kenneth E., *Internet Security: Hacking, Counterhacking, and Society*. Jones & Bartlett Learning, 2007. [Online]. Available: https://books.google.com.om/books?id=M5d-yuCME0AC

[6] R. Valecha, R. Chen, T. Herath, A. Vishwanath, J. Wang, and R. Rao, "An exploration of phishing information sharing: A heuristic-systematic approach," 2015.

[7] Parsons, June Jamrich, *New Perspectives Computer Concepts 2016 Enhanced, Comprehensive*. Cengage Learning, 2016. [Online]. Available: https://books.google.com.om/books?id=epZ4CgAAQBAJ

[8] E. E. Lastdrager, "Achieving a consensual definition of phishing based on a systematic review of the literature," *Crime Science*, vol. 3, no. 1, p. 1, 2014.

[9] Allen, Malcolm, "Social engineering a means to violate a computer system," 2016, https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529.

[10] Federal Office for Information and Security, "ndustrial control system security: Top 10 threats and countermeasures 2016," 12 October 2016, https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529.

[11] Franklin, D.N., "Detecting malicious software," Feb. 10 2015, uS Patent 8,955,118. [Online]. Available: https://www.google.ch/patents/US8955118

[12] J. Andress and S. Winterfeld, *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier, 2013.

[13] Suleiman, Husam and Alqassem, Israa and Diabat, Ali and Arnautovic, Edin and Svetinovic, Davor, "Integrated smart grid systems security threat model," *Information Systems*, vol. 53, pp. 147 – 160, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0306437914001896

[14] Vacca, John R., *Network and System Security, Second Edition*, 2nd ed. Syngress Publishing, 2013.

[15] Jacobson, Doglas, *Introduction to Network Security*, ser. Chapman & Hall/CRC Computer and Information Science Series. CRC Press, 2008. [Online]. Available: https://books.google.com.om/books?id=50DMBQAAQBAJ

[16] Ma, Zongmin, *Managing Big Data in Cloud Computing Environments*. Hershey, PA,, 2016.

[17] Roozbahani, Fatemeh Soleimani and Azad, Reihaneh, "Security solutions against computer networks threats," *International Journal of Advanced Networking & Applications*, vol. 7, no. 1, pp. 25–76, July 2015.

[18] Bohli, J. M. and Gruschka, N. and Jensen, M. and Iacono, L. L. and Marnau, N., "Security and privacy-enhancing multicloud architectures," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 4, pp. 212–224, July 2013.

[19] Pathan, Al-Sakib Khan, *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET*, 1st ed. Boston, MA, USA: Auerbach Publications, 2016.