International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 2, No. 2, June-August, 2017 | Pages 24-29

Network Security In Computer Network

R. Ganeshan[1], Dr. Paul Rodrigues[2]

[1]Assistant Professor, Dept of CSE, St. Joseph College of Engineering Sriperumbudur. India
[2]Professor, Dept of CSE, Indra Gandhi College of Engineering and Technology Chengalpattu. India

Abstract:

The security of computer networks plays a strategic role in modern computer systems. In order to enforce high protection levels against malicious attack, a number of software tools have been currently developed. Intrusion Detection System has recently become a heated research topic due to its capability of detecting and preventing the attacks from malicious network users. A pattern matching IDS for network security has been proposed in this paper. Many network security applications rely on pattern matching to extract the threat from network traffic. The increase in network speed and traffic may make existing algorithms to become a performance bottleneck. Therefore it is very necessary to develop faster and more efficient pattern matching algorithm in order to overcome the troubles on performance.

Keywords: Enemies, Effect of enemies, Security.

1. INTRODUCTION

Health of every organization. Over the past few years, Internet-enabled business, or e-business, has drastically improved efficiency and revenue growth. E-business applications such as e-commerce, supply-chain management, and remote access allow companies to streamline processes, lower operating costs, and increase customer satisfaction. Such applications require mission- critical networks that accommodate voice, video, and data traffic, and these networks must be scalable to support increasing numbers of users and the need for greater capacity and performance. However, as networks enable more and more applications and are available to more and more users, they become ever more vulnerable to a wider range of security threats.

Fig.1.Security

To combat those threats and ensure that e-business transactions are not compromised, security technology must play a major role in today's networks. Security incidents are rising at an alarming rate every year. As the complexity of the threats increases, so do the security measures required to protect networks. Data center operators, network administrators, and other data center professionals need to comprehend the basics of security in order to safely deploy and manage networks today. As time goes on, more and more new technology will be developed to further improve the efficiency of business and communications. At the same time, breakthroughs in technology will provide even greater network security, therefore, greater piece of mind to operate in cutting edge business environments. Provided that enterprises stay on top of this emerging technology, as well as the latest security threats and dangers, the benefits of networks will most certainly outweigh the risks. Trojan horse programs, or trojans, are delivery vehicles for destructive code. Trojans appear to be harmless or useful software programs, such as computer games, but they are actually enemies in disguise. Trojans can delete data, mail copies of themselves to e-mail address lists, and open up computers to additional attacks. Trojans can be contracted only by copying the trojan horse program to a system, via a disk, downloading from the Internet, or opening an e-mail attachment. Neither trojans nor viruses can be spread through an e-mail message itself—they are spread only through e-mail attachments.

2. RELATED WORK

Virus protection software is packaged with most computers and can counter most virus threats if the software is regularly updated and correctly maintained. The anti-virus industry relies on a vast network of users to provide early warnings of new viruses, so that antidotes can be developed and distributed quickly. With thousands of new viruses being generated every month, it is essential that the virus database is kept up to date. The virus database is the record held by the anti-virus package that helps it to identify known viruses when they attempt to strike.

Fig.2.Ad HOC Architecture

Reputable anti-virus software vendors will publish the latest antidotes on their Web sites, and the software can prompt users to periodically collect new data. Network security policy should stipulate that all computers on the network are kept up to date and, ideally, are all protected by

the same anti-virus package if only to keep maintenance and update costs to a minimum. It is also essential to update the software itself on a regular basis. Virus authors often make getting past the anti-virus packages their first priority. A firewall is a hardware or software solution implemented within the network infrastructure to enforce an organization's security policies by restricting access to specific network resources. In the physical security analogy, a firewall is the equivalent to a door lock on a perimeter door or on a door to a room inside of the building—it permits only authorized users, such as those with a key or access card, to enter. Firewall technology is even available in versions suitable for home use. The firewall creates a protective layer between the network and the outside world. In effect, the firewall replicates the network at the point of entry so that it can receive and transmit authorized data without significant delay. However, it has built-in filters that can disallow unauthorized or potentially dangerous material from entering the real system. It also logs an attempted intrusion and reports it to the network administrators.

3. PROPOSED SYSTEM

Wireless networking is inherently insecure. From jamming to eavesdropping, from man-in the middle to spoofing, there are a variety of attack methods that can be used against the users of wireless networks. Modern wireless data networks use a variety of cryptographic techniques such as encryption and authentication to provide barriers to such infiltrations. However, much of the commonly used security precautions are woefully inadequate. They seem to detract the casual sniffer, but are unable to stop the powerful adversary. In this article, we look into the technology and the security schemes in IEEE 802.11, cellular and Bluetooth wireless transport protocols. We conclude that the only reliable security measure for such networks is one hat is based on application level security such as using a VPN.The wireless communication technology also acquires various types of security threats. This paper discusses a wide variety of attacks in WSN and their classification mechanisms and different securities available to handle them including the challenges faced. Wireless technologies, in the simplest sense, enable one or more devices to communicate without physical connections without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data, whereas wired technologies use cables. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) and cell phones to simple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link. WLANs allow greater flexibility and portability than do traditional wired local area networks (LAN).Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point device. An access point communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ- 45 port. Access point devices typically have coverage areas

of up to 300 feet(approximately 100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network device. Access point cells can be linked together to allow users to even "roam" within a building or between buildings.

4. ANALYSIS

Access Points can be programmed to allow access to the WLAN by MAC address. This security mechanism is designed to deny access to all clients except those explicitly authorized to use the WLAN. The effort required to implement and maintain access lists is large. This mechanism does not scale well and is only useful for small WLANs. Access Lists can easily be defeated by an attacker with minimal tools. It provides no protection from the insider, who is an authorized user of the network. An outsider who obtains a wireless network access card (WNIC) that is authorized entry into the WLAN is effectively an insider. An outsider can also sniff the traffic between the AP and the client collecting a valid MAC address. She can then craft packets with a forged MAC address for easy access to the WLAN. Although not a scalable security measure, this mechanism will stop an attacker without any specialized attack tools. It effectively raises the bar, albeit only a small amount, and therefore meets the Blazing Saddles Principle described earlier. The ad hoc mode does not use APs. Ad hoc mode is sometimes referred to as infrastructure less because only peer-to-peer STAs are involved in the communications. This mode of operation is possible when two or more STAs are able to communicate directly to one another. Examples are laptops, mobile phones, PDAs, printers and scanners being able to communicate with each other without an AP. One of the key advantages of ad hoc WLANs is that theoretically they can be formed any time and anywhere, allowing multiple users to create wireless connections cheaply, quickly, and easily with minimal hardware and user maintenance. However, an ad hoc WLAN cannot communicate with external networks. A further complication is that an ad hoc network can interfere with the operation of an AP-based infrastructure mode network that exists within the same wireless space.

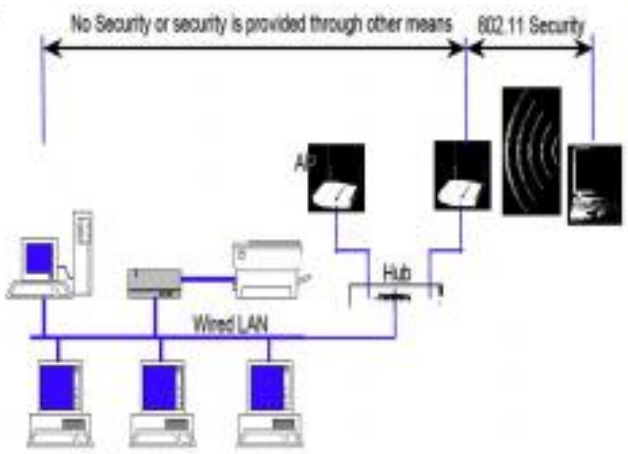

Fig.3.Wireless Structure

The IEEE 802.11 standard permits devices to establish either peer-to-peer (P2P) networks or networks based on fixed access points (AP) with which mobile nodes can communicate. Hence, the standard defines two basic network topologies: the infrastructure network and the ad hoc network. The infrastructure network is meant to extend the range of the wired LAN to wireless cells. A laptop or other mobile device may move from cell to cell (from AP to AP) while maintaining access to the resources of the LAN. A cell is the area covered by an AP and is called a "basic service set" (BSS). The collection of all cells of an infrastructure network is called an extended service set (ESS). This first topology is useful for providing wireless coverage of building or campus areas. By deploying multiple APs with overlapping coverage areas, organizations can achieve broad network coverage. WLAN technology can be used to replace wired LANs totally and to extend LAN infrastructure. A WLAN environment has wireless client stations that use radio modems to communicate to an AP. The client stations are generally equipped with a wireless network interface card (NIC) that consists of the radio transceiver and the logic to interact with the client machine and software.

CONCLUSION

Wireless networking provides numerous opportunities to increase productivity and cut costs. It also alters an organization's overall computer security risk profile. Although it is impossible to totally eliminate all risks associated with wireless networking, it is possible to achieve a reasonable level of overall security by adopting a systematic approach to assessing and managing risk. This paper discussed the threats and vulnerabilities associated with each of the three basic technology components of wireless networks (clients, access points, and the transmission medium) and described various commonly available countermeasures that could be used to mitigate those risks. A combined effort of users, employers and system administrators is required in order to fight against such malicious activities. Appropriate countermeasures in every form can help the organization minimize the risk of illegal penetration. Up to date tools, constant monitoring, proper management and appropriate countermeasures are the ultimate weapons to fight against wireless security attacks.

REFERENCES

1. Mitchell Ashley , "A Guide to Wireless Network Security" Information systems Control Journal ,Volume 3,2004.
2. Karen Scarfone, Derric Dicoi, " Wireless Network Security for IEEE 802.11a/b/g,Bluetooth(DRAFT)",NISTPublication-800-48.Augest 2007.
3. Tom karygiannis, Les Owens, "Wireless Network Security for IEEE 802.11a/b/g,Bluetooth(DRAFT)",NISTPublication-800-48.November 2002
4. Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen, "IEEE 802.11 Wireless LAN Security Overview", IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, May 2006.

5. Omar Cheikhrouhou & Maryline Laurent & Amin Ben Abdallah & Maher Ben Jemaa, "An EAP-EHash authentication method adapted to resource constrained terminals", Institute TELECOM and Springer- Verlag.Hal-00506549,Version 1-28 July 2010
6. "Applied Cryptographhy" By Bruse Schneier.
7. "Advanced Computing Applications, Data bases and Networks" By Shahin Ara Begum, Prodipto Das.