WIRELESS NETWORKING IS INHERENTLY INSECURE

Sailaja .p, PUJITHA MANDAPATI, MEDE CHITTI BABU
4.G.AMIRTHAYOGAM, 5.KALYAN KUMAR
Assistant Professor, Department of Computer Engineering,
Ellenki college of Engineering and Technonlogy, patelguda (vi)' near BHEL ameenpur (m),
Sangareddy Dist. Telangana 502319.

***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**

***Index Terms*—About four key words or phrases in alphabetical order, separated by commas.**

I. 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

Submit your manuscript electronically for review.

1. 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

2. 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 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.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. 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).

I. 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.

II 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)",NIST Publication-800-48.Augest 2007.
3. Tom karygiannis, Les Owens, "Wireless Network Security for IEEE 802.11a/b/g,Bluetooth(DRAFT)",NIST Publication-800-48.November 2002
4. Ahmed M. Al Naamany , Ali Al Shidhani, Hadj Bourdoucen, "IEEE 802.11 Wireless LAN Security
5. "Applied Cryptographhy" By Bruse Schneier.
6. "Advanced Computing Applications, Data bases and Networks" By Shahin

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-3, ISSUE-10, 2016
DOI:10.21276/ijcesr.2016.3.10.3