Wireless Network Security Fundamentals and Technologies

MAYUR GANPAT SAKPAL, SREELAKSHMI NAIR

Abstract:
In markets where devices are more widely used, there'll be attacks on the devices themselves but quickly are going to be focused on transactions. As devices networks.develop more capabilities, the threats and attacks are expected to grow more serious and frequent. With increasing deployment of wireless networks, IT enterprises are working to implement security mechanisms that are appreciated by those existing today for wire-based networks. With the growing reliance on e-commerce, wireless network based services and therefore the internet; enterprises are faced with an ever increasing responsibility to shield their systems from attack. During this paper we will discuss few of the protection technologies developed to produce security for wireless networks.

Keywords - Wireless Network, Network Security, Security Mechanisms, Security Technology, Wire-based Networks.

INTRODUCTION:

Wireless networks are too inexpensive to ignore. But, security has hindered many network managers looking to bring wireless into the company fold. The threat of information theft, perhaps, is more alarming to businesses. so as to stop the interception of knowledge as its being transmitted, all wireless transmission standards have security inbuilt, but they're known to be fallible. Because the wireless network is actually everywhere, sniffing is an inherent problem in wireless. Sniffers must have access to physical parts of the network so as to interrupt within the wired world. The matter is, with wireless, they don't even need to be in network. they'll be in an exceedingly van outside with a transmitter

There's been a scarcity of functionality and a scarcity of mature infrastructure globally. And, that's the only reason the wireless viruses of today haven't been more damaging. for several IT managers, the wireless world, with its often incompatible alphabet soup of standards, could also be new territory. Therefore, so as to fight the viruses and security breaches of the long run,wireless network security vendors are busy developing products. additionally, within applications and on devices, they're also heading off problems on a wireless network level.

- *Mayur Sakpal is currently pursuing masters degree program in Information Technology in Mumbai University, India, PH-7506775960 Email: mgsakpal21@gmail.com*
- *Sreelakshmi Nair is currently a lecturer in Mumbai University, India, PH-8169119781. E-mail:sreelakshmi@mes.ac.in*

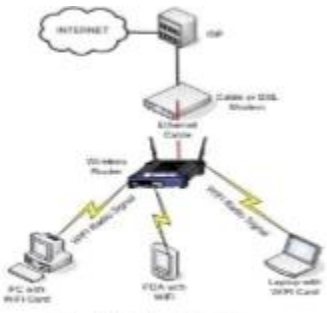

Figure 1. Wireless Network Set-up

II. WIRELESS NETWORK SECURITY ATTACKS METHODS:

It is understood that a person with no understanding of networks can easily founded a flawed and vulnerable network. However, some executives must remember that even their system administrators might be lacking in their understanding of wireless network implementations. Today, denial of service (DoS) and distributed denial of service (DDoS) attacks are still on the rise and getting worse. Denial of service attacks is becoming incessant. DoS and DDoS attacks are also growing in ferocity. DDOS attacks themselves pose an immense threat to the net and wireless networks

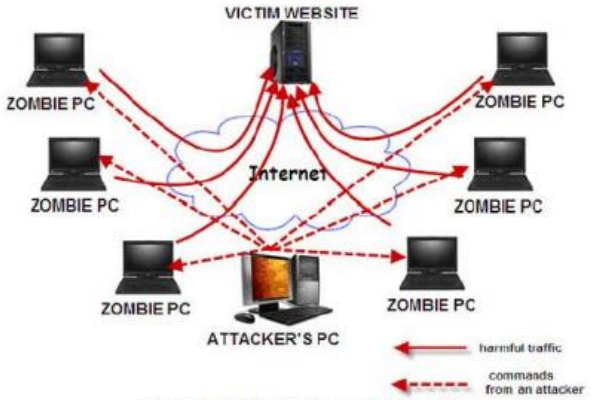

Figure 3. DDoS attack working model

Overview of DDoS Attack:

A DoS attack is characterized by all explicit attempts by attackers to stop legitimate users of a service from using that service. A DDOS attack deploys multiple machines to realize this goal. The service is denied by sending a stream of packets to a victim that either provides the attacker with unlimited access to the victim machine so he can inflict arbitrary damage or consumes some key resource, thus rendering it unavailable to legitimate clients. In DDoS attacks, a cracker installs a program on a machine that soon, in conjunction with other wireless networking systems, are going to be called on to participate in an attack

DDoS working and prevention:

The attacker has to recruit the multiple agent machines, so as to perform a distributed denial of service attack. By trying to find wireless network security holes that may enable subversion, this process is typically performed automatically through scanning of remote machines. For resource intensive computing tasks, including an enormous Dos attack, DDoS leverages one of the inherent benefits of distributed computing. By spoofing the source address or destination address fields of an IP packet, DDoS attacks exploit the inherent 'trust' that wireless networked computers have for every other. Wireless internet routers will route the packet to its marked destination. Thus, the receiver will reply to the cast source address. It's easy to launch a DDoS attack. The attacker has to select a web site to attack, once a zombie force is established. From a central 'command console' which may activate zombies located anywhere within the world, the attack itself may be initiated from one computer.

In defending against DDoS attacks, wireless network firewalls are indispensable for countering many types of malicious incursions. Firewalls are designed to manage an environment where everyone outside the enterprise is untrusted and everybody inside is trusted. However, the model of trusted and untrusted wireless networks isn't any longer viable in today's wireless internet, with service providers delivering the means for users to access the online. Advanced implementation of intrusion detection system (IDS) technology is required as an effective defense against DDoS attacks.

III. WIRELESS NETWORK SECURITY TECHNOLOGIES RESULTS:

Vendors do a decent job of improving security measures, and users are becoming an understanding of wireless security. Indeed, security is the biggest barrier to the adoption of wireless LANs. When it involves wireless networking, security continues to be the amount one concern for enterprises across all sizes. Gaining a higher understanding of wireless LAN security elements and employing some best practices can go a good distance toward enabling you to reap the advantages of wireless networking. Three actions can help to secure a wireless network.

· Discouraging unauthorized users through authentication

· Preventing unofficial connections through the elimination of rogue access points

Protecting data while it's being transmitted through encryption

1. Solutions for Wireless Security:
Three solutions are available for secure wireless LAN encryption and authentication:
1.Wi-Fi Protected Access (WPA)
2.Wi-Fi Protected Access 2 (WPA2)
3.Virtual private networking (VPN)

WPA & WPA2

WPA and WPA2 are standards based security certifications from the Wi-Fi alliance for enterprise, SMB and small/home office wireless LANs that provide mutual authentication to verify individual users and advanced encryption. WPA provides enterprise – class encryption and WPA2.

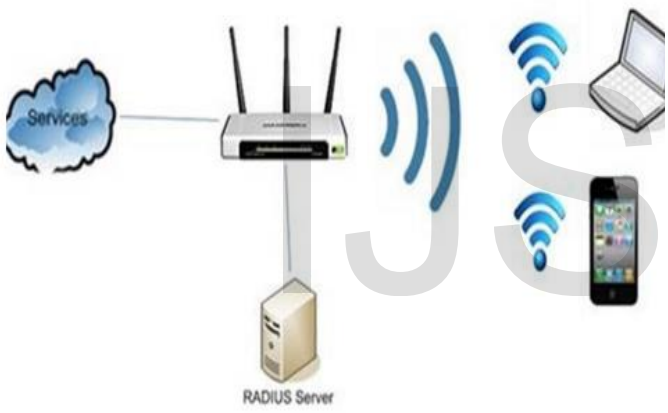

Figure 4. WPA / WPA2 setup

It is recommended that WPA or WPA2 be used for enterprise and SMB wireless LAN deployments. WPA and WPA2 provide secure access control, strong data encryption and they protect the network from passive and active attacks

VPN:
VPN provides effective security for users wirelessly accessing the network while on the road or far from the office. With VPN, user create a secure tunnel between two or more points on a network using encryption, whether or not the encrypted data is transmitted over unsecured networks like the public internet [4].

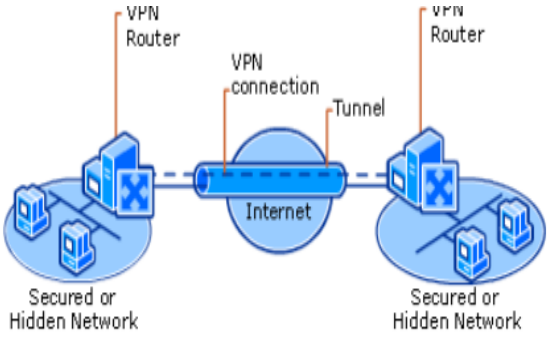

Figure 5. Virtual Private Network

IV.WIRELESS TECHNOLOGY
STANDARDS DISCUSSION:

True wireless network security means protecting every device with a wireless network card for every user everywhere they are going. For this we must know which security standards are implemented in our hardware and software.

Wireless technologies conform to a range of standards and offer varying levels of security features. during this paper, the discussion of wireless standards is prescribed to:
- WEP
- IEEE 802.11b
- IEEE 802.11i
- IEEE 802.1X

WEP

The IEEE 802.11 specification identifies several services to produce a secure operating environment. the protection services are provided largely by the Wired Equivalent Privacy (WEP)protocol to shield link – level data during wireless transmission between clients and access points. WEP doesn't provide end to finish security, apart from the wireless portion of the connection

IEEE 802.11b
WLANs are supported IEEE 802.11 standard, which IEEE first developed in 1997. In 1999 the IEEE completed and approved the quality referred to as 802.11b, and WLANs were born. Computer networks finally could achieve connectivity with a usable amount of bandwidth without being networked via a outlet. Suddenly connecting multiple

computers during a house to share an internet connection or play LAN games now not required expensive and ugly cabling

IEEE 802.11i

The body liable for the Wi-Fi standard is 802.11i. the quality provides the pliability to add new methodologies. This standards Robust Security Network (RSN) feature will deliver the level of security the wireless world is clamoring for.

IEEE 802.1X
The IEEE 802.1X, port based network authentication uses the Extensible Authentication Protocol (EAP) as its authentication framework.

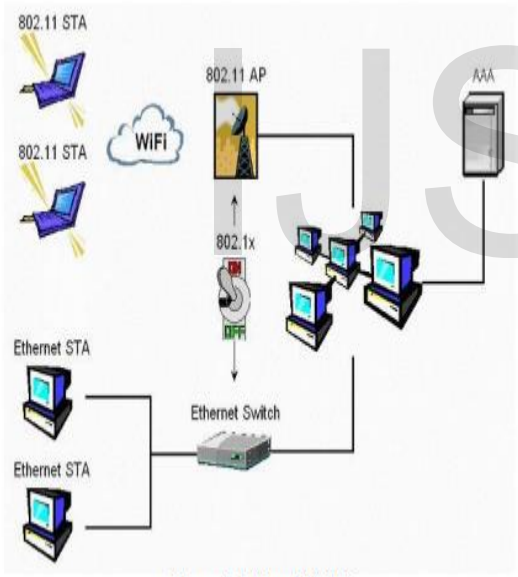

Figure 8. EAP and 802.1X

.EAP may be a transport mechanism, and any defined EAP method may be used within EAP, enabling support for a good type of Authentication credentials

V. CONCLUSION
In this paper we've discussed wireless network security fundamentals. Although wireless technologies have significantly improved their security capabilities, many of the features and abilities are available only in newer equipment for IT – managed infrastructure. Attacks have proven WEP security provided by the 802.11 standard to be insecure. The WLAN industry responded by creating WPA and 802.11i to accommodate these issues within the long term

REFERENCES:

[1] Jelena Mirkovic, Janice Martin, "A taxonomy of DDoS attacks and DDoS defense mechanisms", Technical report, 2002.

[2] Dell computer corporation, "802.11 wireless security in business", 2001.

[3] Dennis Fisher and Carmen Nobel, "New attack intercepts wireless net messages", 2001.

[4] Peter Rysavy, "Secure wireless networking using SSL VPNs", 2005.

[5] Fred Sandsmark, "Securing wireless networks", 2005.

[6] George Ou, "Understanding the updated WPA and WPA2 standards", 2005.