International Journal of Recent Trends in Engineering & Research
ISSN (ONLINE) : 2455 – 1457
IMPACT FACTOR : 4.101

Wireless Network Security Fundamentals and Technologies

Rakesh V S[1], Ganesh D R[2], Rajesh Kumar S[3], Puspanathan G[4]
[1,2,3,4] *Department of Computer Science and Engineering, Cambridge Institute of Technology*

Abstract – In markets where devices are more widely used, there will be attacks on the devices themselves but quickly will be focused on transactions. As devices 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 equivalent to those existing today for wire-based networks. With the growing reliance on e-commerce, wireless network based services and the internet; enterprises are faced with an ever increasing responsibility to protect their systems from attack. In this paper we will discuss few of the security technologies developed to provide security for wireless networks.

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

I. INTRODUCTION

Wireless networks are too inexpensive to ignore. But, security has hindered many network managers looking to bring wireless into the corporate fold. The threat of data theft, perhaps, is more alarming to businesses. In order to prevent to prevent the interception of information as its being transmitted, all wireless transmission standards have security built in, but they're known to be fallible.

Because the wireless network is essentially everywhere, sniffing is an inherent problem in wireless. Sniffers must have access to physical parts of the network in order to break in the wired world. The problem is, with wireless, they don't even have to be in network. They can be in a van outside with a transmitter.

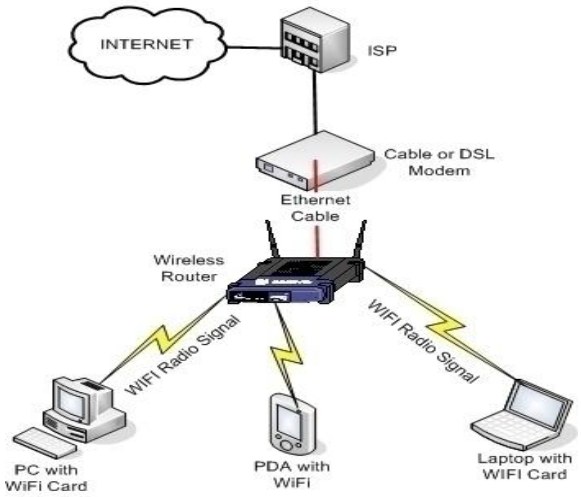

Figure 1. Wireless Network Set-up

There's been a lack of functionality and a lack of mature infrastructure globally. And, that's the only reason the wireless viruses of today have not been more damaging. For many IT managers, the wireless world, with its often incompatible alphabet soup of standards, may be new territory. Therefore, in order to fight the viruses and security breaches of the future, wireless network security vendors are busy developing products. In addition, within applications and on devices, they are also heading off problems on a wireless network level.

II. WIRELESS NETWORK SECURITY ATTACKS

It is understood that an individual with no understanding of networks can easily set up a flawed and vulnerable network. However, some executives need to be aware that even their system administrators could 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 internet and wireless networks.

2.1. Overview of DDoS Attack

A DoS attack is characterized by all explicit attempts by attackers to prevent legitimate user of a service from using that service. A DDOS attack deploys multiple machines to attain 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 later on, in conjunction with other wireless networking systems, will be called on to participate in an attack.

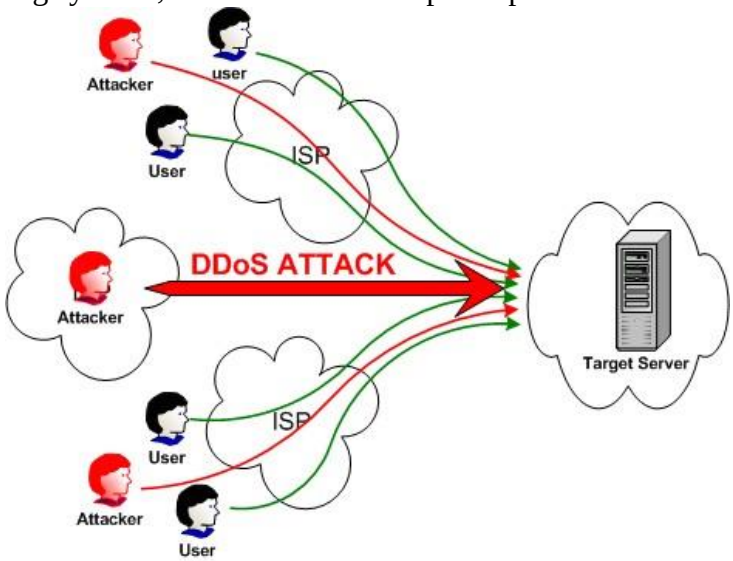

Figure 2. DDoS Attack

Because DDoS attacks deliver a much heavier volume of messages, they have the potential to be much more disruptive than relatively simple DoS attacks originating from a single computer. An attacker can build a veritable army of zombie systems to launch attacks at will [1].

2.2. DDoS working and prevention

The attacker needs to recruit the multiple agent machines, in order to perform a distributed denial of service attack. By looking for wireless network security holes that would enable subversion, this process is usually performed automatically through scanning of remote machines.

For resource intensive computing tasks, including a massive 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 each other. Wireless internet routers will route the packet to its marked destination. Thus, the receiving system will reply to the forged source address.

It's easy to launch a DDoS attack. The attacker needs to select a website to attack, once a zombie force is established. From a central 'command console' which can activate zombies located anywhere in the world, the attack itself can be initiated from a single computer.

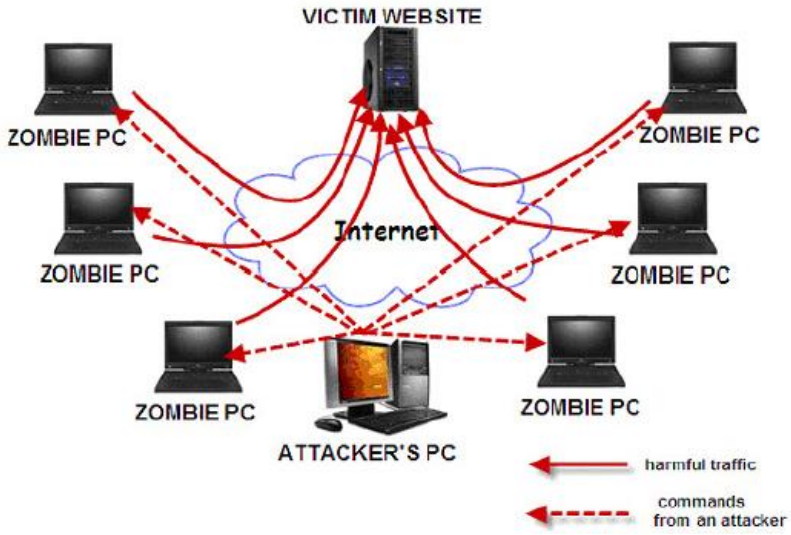

Figure 3. DDoS attack working model

In defending against DDoS attacks, wireless network firewalls are indispensable for countering many kinds of malicious incursions. Firewalls are designed to manage an environment where everyone outside the enterprise is un-trusted and everyone inside are trusted.

However, the model of trusted and un-trusted wireless networks is no longer viable in today's wireless internet, with service providers delivering the means for user to access the web. Advanced implementation of intrusion detection system (IDS) technology is required as an effective defense against DDoS attacks.

III. WIRELESS NETWORK SECURITY TECHNOLOGIES

Vendors are doing a good job of improving security features, and users are getting an understanding of wireless security. Indeed, security is the biggest barrier to the adoption of wireless LANs. When it comes to wireless networking, security is still the number one concern for enterprises across all sizes.

Gaining a better understanding of wireless LAN security elements and employing some best practices can go long way toward enabling you to reap the benefits of wireless networking. Three action 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 [5].

3.1. Solutions for Wireless Security

Three solutions are available for secure wireless LAN encryption and authentication:

- Wi-Fi Protected Access (WPA)
- Wi-Fi Protected Access 2 (WPA2)
- Virtual private networking (VPN) [3].

3.1.1. 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 [6].

3.1.2. VPN

VPN provides effective security for users wirelessly accessing the network while on the road or away from the office. With VPN, user creates a secure tunnel between two or more points on a network using encryption, even if the encrypted data is transmitted over unsecured networks such as the public internet [4].

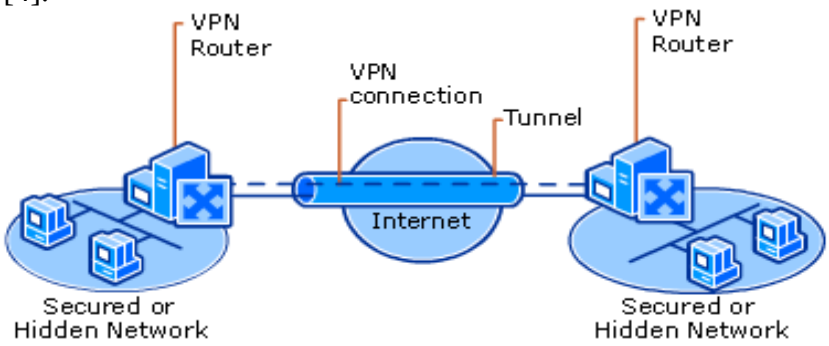

Figure 5. Virtual Private Network

IV. WIRELESS TECHNOLOGY STANDARDS

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

Wireless technologies conform to a variety of standards and offer varying levels of security features. In this paper, the discussion of wireless standards is limited to:

- WEP
- IEEE 802.11b
- IEEE 802.11i
- IEEE 802.1X

4.1. WEP

The IEEE 802.11 specification identifies several services to provide a secure operating environment. The security services are provided largely by the Wired Equivalent Privacy (WEP)

protocol to protect link – level data during wireless transmission between clients and access points. WEP does not provide end to end security, except for the wireless portion of the connection [2].

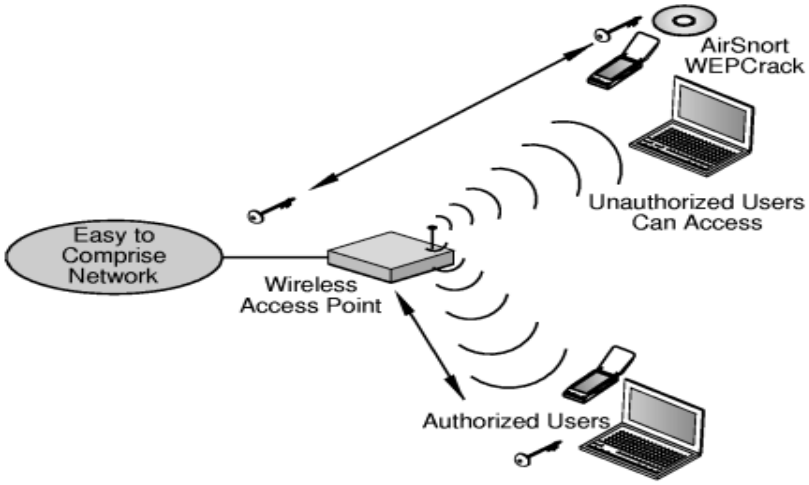

Figure 6. WEP

4.2. IEEE 802.11b

WLANs are based on IEEE 802.11 standard, which the IEEE first developed in 1997. In 1999 the IEEE completed and approved the standard known as 802.11b, and WLANs were born. Computer networks finally could achieve connectivity with a usable amount of bandwidth without being networked via a wall socket. Suddenly connecting multiple computers in a house to share an internet connection or play LAN games no longer required expensive and ugly cabling.

4.3. IEEE 802.11i

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

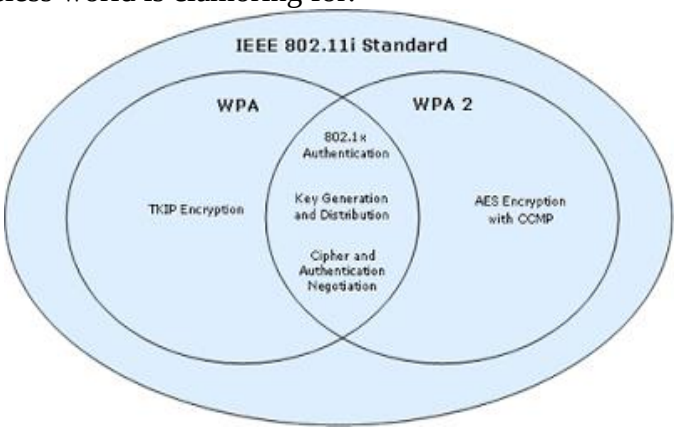

Figure 7. 802.11i Architecture

4.4. IEEE 802.1X

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

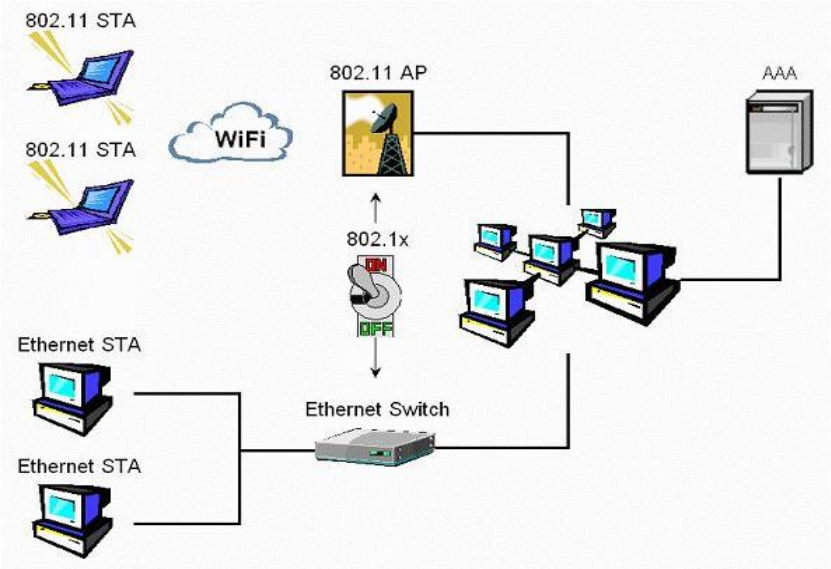

Figure 8. EAP and 802.1X

EAP is a transport mechanism, and any defined EAP method can be used within EAP, enabling support for a wide variety of Authentication credentials.

V. CONCLUSION

In this paper we have discussed about 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 address these issues in 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.

