Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 05, pp.30389-30392, May, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

WIRELESS SECURITY SYSTEMS

*Arnaja Sen, Lipika Mahajan, Priyanka Kuwor and Asha Khatri

K. J. Somaiya College of Engineering, Mumbai, Maharashtra, India

ARTICLE INFO

Article History:
Received 15th February, 2016
Received in revised form
27th March, 2016
Accepted 26th April, 2016
Published online 10th May, 2016

Key words:

Elvin twin, Sniffing, Rogue access points, Protocol, Sniffing, Bluesnarfing, Bluejacking, Authentication, Encryption.

ABSTRACT

Wireless technology has been gaining rapid popularity over the years. Nowadays, security is considered as one of the most critical parameter for the acceptance of any wireless networking technology. Although implementation of technological solutions is the most common way to respond to threats of wireless security systems and susceptibility, wireless security is basically a management issue. Effective management planned after analyzing current threats will help to sort out issues in a better way. In this paper, we analyze the security related protocol (WEP, WPA, WPA2) and current scenario of the wireless network security systems. We also figure out various issues that allow hackers to monitor and even change the integrity of transmitted data and discuss a number of available solutions to counter those threats.

Citation: Arnaja Sen, Lipika Mahajan, Priyanka Kuwor and Asha Khatri, P. 2016. "Wireless security systems", *International Journal of Current Research*, 8, (05), 30389-30392.

INTRODUCTION

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. Now a days, companies and individuals are using wireless technology progressively for important communications they want to keep private and secure, such as e-commerce transactions, email, and other corporate data transmissions. At the same time, as wireless platforms mature, become more popular, and store valuable information, hackers are increasing their attacks on these new targets. Security mechanisms in wireless networks are essential to protect data integrity and provide security, access control, authentication, quality of service, user privacy, and continuity of service. They also play a critical role to protect functionality of wireless network (Yang Xiao *et al.*, 2007).

Wireless security protocols in place

Various wireless security protocols were developed to protect wireless networks. These wireless security protocols include WEP, WPA, and WPA2, each with their own features.

WEP (Wired Equivalent Privacy)

As its name implies, WEP was designed to provide the same level of security as wired networks. WEP has three settings: Off (no security), 64-bit (weak security), 128-bit (a bit better security). The wired equivalent privacy protocol provides security to a wireless network by encrypting the data (Arash habibi lashkari *et al.*, 2009). If the data is accessed, it will be unrecognizable to system that hacked the data, since it is encrypted. However, systems on the network which are authorized will be able to recognize the data because they all use the same encryption algorithm. Systems on a WEP-secured network can be typically authorized by entering a network password. However, WEP has many well-known security bugs, is difficult to configure, and is easily broken. It is not difficult to crack, and using it reduces performance slightly.

WPA (Wi-Fi Protected Access)

WPA is a security protocol designed to create secure wireless networks. WPA handles security keys differently and the users are authorized in such a way that it provides better security than WEP. For an encrypted data transfer to work, both systems on the beginning and end of a data transfer must use the same encryption/decryption key (Arash habibi lashkari *et al.*, 2009). WPA uses the temporal key integrity protocol (TKIP), which dynamically changes the key that the systems use. Thus preventing the intruders from creating their own encryption key to match the one used by the secure network. WPA also implements something called as Extensible Authentication Protocol (EAP) for authorizing users. Instead of authorizing computers based only on their MAC address, WPA can use several other methods to verify each computer's

***Corresponding author: Arnaja Sen,**
K. J. Somaiya College of Engineering, Mumbai, Maharashtra, India.

identity. Thus making it more difficult for unauthorized systems to gain access to the wireless network.

WPA2 (Wi-Fi Protected Access version 2)

WPA2 is an improvement of the WPA protocol. One of the most significant changes between WPA and WPA2 was the mandatory use of AES (Advanced Encryption Standard) algorithms and the introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a restoration for TKIP (Arash habibi lashkari *et al.,* 2009).Currently, the primary security weakness of the actual WPA2 system is an obscure one (and requires the attacker to already have access to the secured Wi-Fi network in order to gain access to certain keys and then attack other devices on the network). As such, the security implications of the known WPA2 vulnerabilities are limited almost completely to enterprise level networks and deserve little to no practical consideration regarding home network security.

Wireless security issues

There are several issues related to the present wireless security systems. In this paper, we explore some of these issues such as creating rogue access points, sniffing, denial of service, bluesnarfing and blujacking and presence of elvin twin.

Creating Rogue access points

Rogue access points are created within the range of existing wireless local area networks. These create an illusion to a node of the network that rogue point is a part of the network and associates with such point (David Frankk, 2012). These are short duration attacks and they are vulnerable for a short period of time. Once the attacker associates itself with the physical port of network, they can extend the period of vulnerability (Min-kyu Choi *et al.*, 2008).

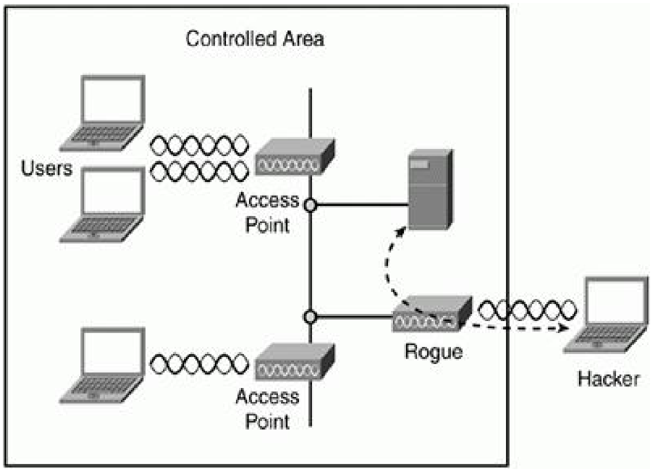

Fig. 1. rogue access points

Sniffing

Sniffing involves capturing, decoding, inspecting and interpreting the information inside a network packet on a TCP/IP network. Attackers or hackers use a software called Sniffer, which allows them to scan the traffic and different access points in a location having many wireless networks (David Frankk, 2012). Sniffer helps the hackers to find an open network, which they use to latch themselves with. Sniffing is possible at every layer of the OSI model.

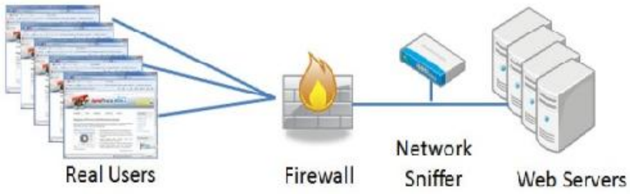

Fig. 2. Sniffing

Denial of Service

It is a renowned security issue in network technology. It need not access any port or any location in the server of company. The attacker overloads the network of the company by sending large packets of data so as to slow down the processing capabilities of server (Arockiam and Vani, 2011). This forces the server to deny the service to be provided to the user. In wireless networks, this is achieved by interfering with the frequency of operation of any wireless network (David Frankk, 2012).

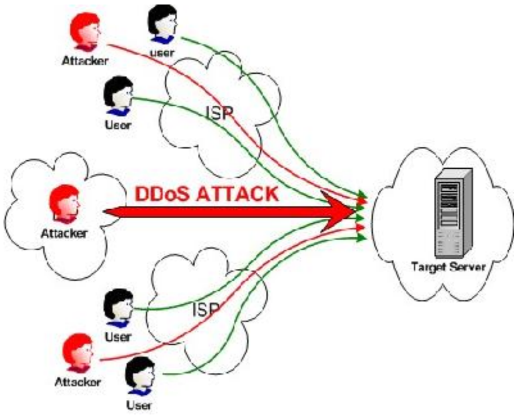

Fig. 3. Dos attack

Bluesnarfing and bluejacking

Along with conventional local area networks, the Bluetooth is also used with the intention of data manipulation .Bluejacking allows any device accessed by unauthorized users to send messages to the device, which could be malicious in nature. Bluesnarfers can hack the data from the device and manipulate it (David Frankk, 2012). The most dangerous aspect of this technique is that it cannot be found if some bluesnarfer hacks data from the device.

Elvin Twin

The Elvin Twin creates a replica of the authorized host at attacker’s point. The authorized access point is obstructed by the attacker and user is redirected through another access point under the authority of the attacker (David Frankk, 2012). This allows the attacker to control, manipulate and analyse all the traffic from the user, including the keystrokes.

Existing solutions

To reduce the threats of such attacks, three main types of tools are used on a wireless network system.

Mutual authentication

Mutual authentication should be used between the client and Access Point. The authentication process uses a secret password, called a key, on both the client and the AP. By using mathematical algorithms, the AP can verify that the client does know the right key value. Similarly, the client can confirm that the AP also has the right key value. This process never sends the key through the air, so even if the attacker is using a network analysis tool to copy every frame inside the wireless network, the attacker is unable to get the key value. Also by allowing mutual authentication, the client can make confirmation that the AP knows the right key, thus preventing a connection to an AP.

Encryption

Encryption uses a secret key along with mathematical formula to encrypt the contents of the wireless network system. The device at the receiving side uses another formula to decrypt the data. Here, without the secret encryption key, an attacker may be able to intercept the frame inside the wireless network, but he or she will not be able read the contents.

Intrusion tools

The Intrusion tools include Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), and WLAN-specific tools. It includes many tools, some of which explicitly address the issue of detecting and identifying rogue APs, and whether they represent threats.

Solutions for above stated issues

In this paper, we discuss the solutions which are not only efficient but also feasible.

Preventing Wireless Sniffer Attacks

There are several measures that organizations should take to lessen wireless packet sniffer attacks. Firstly, organizations and individual users should refrain from using insecure protocols. Insecure protocols that are commonly used include basic HTTP authentication, File Transfer Protocol (FTP), and Telnet. Secure protocols such as HTTPS, Secure File Transfer Protocol (SFTP), and Secure Shell (SSH) should be used instead of their insecure alternatives wherever possible. Secure protocols makes sure that any information transmitted will automatically be encrypted. Organizations themselves need to encrypt the data, if an insecure protocol is used. Virtual Private Networks (VPNs) can be used to encrypt internet traffic .It is a widely used tool for organizations today. In addition to encrypting information and using secure protocols, companies can inhibit attacks by using wireless sniffer software to detect their own networks. This allows security teams to view their networks from an attacker’s point of view and discover sniffing vulnerabilities and attacks in progress. It is possible to detect sniffers in promiscuous mode (the preferred mode for attackers) by sniffing your own network whenever this method is not effective in discovering wireless network in monitor mode.

Protection from Elvin twin

Virtual private networks or end-to-end encryption (such as TLS/SSL/HTTPS) may be used to protect passwords, e-mail and other information that are sensitive. Most existing evil twin detection solutions can be classified into two categories. The first approach monitors Radio Frequency (RF) airwaves and/or additional information gathered at routers/switches and then compares with a known authorized list. The second approach monitors traffic at the wired side and determines whether a system uses wired or wireless connections. This information is then compared with an authorization list to detect if the associated AP is a rogue one. The limitation of the above approaches is that they require the knowledge of an authorization list of APs and/or users/hosts.

Preventing Bluesnarfing and Bluejacking

Any device with its Bluetooth connection turned on and set to "discoverable" may be susceptible to Bluejacking and possibly to Bluesnarfing if there is vulnerability in the vendor's software. By turning off this feature, the victim can be safe from the possibility of being Bluesnarfed; The device that is set to "hidden" may also be Bluesnarfable by guessing the device's MAC (media access control) address via a brute force attack. As with all brute force attacks, the main obstacle to this approach is the sheer number of possible MAC addresses. Bluetooth uses a 48-bit unique MAC Address, out of which the first 24 bits are common to a manufacturer. The remaining 24 bits have approximately 16.8 million possible combinations which requires an average of 8.4 million attempts to guess by brute force.

Security from denial of service

Central Manager, back end server, is one of the available solution that takes the responsibility of Authenticated Server (AS). It detects and avoids DoS (Denial of Service) attacks based on three tables and a timer. The next solution in existence is Traffic Pattern Filtering (TPF).In this, AP will stop processing authentication request frame if it receives certain number of frames per second. A normal AP can receive around five 802.11 frames per second and process it. Traffic Pattern Filtering (TPF) is implemented after checking the authentication state of the sender of the received association request frame (Sachin Shetty *et al.*, 2007). If the sender exists, the request is processed. If in case of the sender does not exist, TPF is used (Arockiam and Vani, 2011). If the number of authentication or association request frames received per second is greater than 5, it will be aborted or else the frames sent will be processed.

Conclusion

Wireless network systems provide several opportunities to increase productivity and reduce expenditures. It also alters an organization's overall computer security risk profile. Although it is impossible to totally eliminate all risks associated with wireless network systems, it is possible to achieve a reasonable level of overall security by adopting a systematic approach to assessing and managing risk. The threats and vulnerabilities associated with the wireless networks (clients, access points, and the transmission medium) and commonly available countermeasures that could be used to mitigate those risks have been discussed in this paper.

REFERENCES

Arash habibi lashkari, Mir Mohammad Seyed Danesh, Behrang Samadi, 2009. "A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i)", *International Conference on Computer Science and Information Technology*.

Arockiam, L. and Vani, B. 2011. "A Comparative Study of the Available Solutions to Minimize Denial of Service Attacks in Wireless LAN," *International Journal of Computer Technology and Applications*, Volume 2 Issue 3.

David Frankk. (2012, May 25) Important Security Issues in Wireless Networks[Online]. Available: http://www.examiner.com/article/security-issues-wireless-networks.

Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, 2008. "Wireless Network Security: Vulnerabilities, Threats and Countermeasures," *International Journal of Multimedia and Ubiquitous Engineering*, Volume 3 Issue 3 July.

Sachin Shetty, Min Song, Liran Ma, 2007. "Rogue Access Point Detection by Analyzing Network Traffic Characteristics", IEEE Military Communications Conference, October, pp 1-7.

Yang Xiao, Xuemin (Sherman) Shen, Ding-Zhu Du, 2007. " Wireless Network Security", 3rd Edition.

****