Wireless local area networks and security mechanisms

A

WLAN– Wireless Local Area Network

LAN– Local Area Network

IEEE– Institute of Electrical and Electronics Engineers

WEP– Wired Equivalent Privacy

WPA– Wi-Fi Protected Access

NIC– Network Interface Card

MAC– Media Access Control

WAP– Wireless Access Point

AP– Access Point

NAT– Network Address Translation

SSID– Service Set Identifier

IV– Initialization Vector

IDS– Intrusion Detection Systems

Wireless local area networking (WLAN) has swiftly become very popular technology all over the world. The WLAN protocol, IEEE 802. 11, amongst other associated technologies enable secure access to a wireless network infrastructure. Before the development of wireless networking, clients had to use physical media such as wiring to connect to the network. With the rapid

increase in demand and usage of wireless networking, it is vital that secure communication is provided. Since the creation of wireless networks, the security alongside has gone through many different stages of development, from MAC address filtering, to WEP, leading to WPA/WPA2.

2. 1Wireless Communication

Wireless communication provides wireless networking between client devices, without the need for a physical connection between them (O’brien, 2008). In order to transmit via wireless signals, radio waves are used. The basic process of communication using radio waves is as follows:

A transmitter sends data by turning electrical signals into radio wavesA receiver listens for the radio waves and turns them back into electrical signals, which can create the desired output. Figure 1 below shows an illustrated example of this.

The use of this communication process enables different scenario requirements to be met, for instance short and longer distances can be achieved simply by altering the strength and size of the transmitter/reciever. It also contains various types of fixed and mobile applications including: mobile phones, two-way radios, computer hardware, GPS units, amongst others.

2. 2Wireless Internet Access

Wi-Fi is the term denoted to the functionality in which devices can be connected to the internet without the need of a physical cable. Wi-Fi technology has become the standard for internet access in homes,

workplaces and in place spaces. Regardless of the environment, the core setup consists two key components, an access point and wireless devices.

A

2. 2WLAN Components

Within WLAN, two modes of operation exist: ad-hoc and infrastructure. The ad-hoc mode enables a small wireless workgroup to be quickly setup (no access point required), whereas the infrastructure mode is utilized in cooperation with an existing LAN infrastructure; to incorporate wireless clients into the network (Netgear, 2014). Within these two operation modes there are two key components: access points and wireless clients.

2. 2. 1Access Points

An access points is used to link wireless clients into an existing traditional wired LAN (Netgear, 2014), it doesn’t however interconnect two networks (Wallace, 2011). A basic WLAN topology with a Wireless Access Point (WAP) is shown in figure 2. The topology shows an access point connected to the wired LAN, and the wireless clients that connect to the wired LAN via the access point are on the same subnet as the access point (note that no Network Address Translation (NAT) is being performed). Depending on the chosen technology (802. 11 a/b/g) and its implementation, a single access point is capable of handling up to several hundred wireless clients (Intel, 2017). The security associated with access points have some special considerations. Many traditional wired networks base the security on physical access, entrusting users currently on the network, whereas anyone

within the range of the access point can attach to the network; provided no password is attached. Another concern is if a hacker still manager to bypass the password security, the ability to packet-sniff and intercept data being sent over the wireless network. There are a few security solutions available to address these issues (see section 2. 3).

2. 2. 2Wireless Clients

A wireless client can include a range of devices, including a desktop, laptop, tablet, or mobile phone with a wireless network interface card that enables that device to communicate with an access point. For the client to communicate with the access point, it needs to be configured so that it uses the same SSID (Service Set Identifier) as the access point. An SSID is a case-sensitive alphanumeric string of up to 32 characters (Beal, 2017), and is often referred to as the network name (Intel, 2017). Most access points broadcast their SSID to “ advertise” themselves to wireless clients within its range by default.

2. 3Wireless Security

Security is a major concern in wireless networks, where the radio waves carrying the frames can propagate far beyond the confines of the desired area of the wireless access point and hosts; increasing the chances for an unwanted client to connect to the network and intercept data. Within this section, security mechanisms available to address issues surrounding wireless networking including SSID broadcasting, MAC address filtering, Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) will be covered.

2. 3. 1SSID Broadcasting

As mentioned above it is very common for an access point to broadcast themselves to wireless clients within its radius. This results in clients being able to see all available access points (SSIDs) and choose which one to join, meaning users can easily attach to the network; provided no password is attached. Disabling SSID broadcasting makes it much harder for access points to be identified (Farshchi, 2003). However, this results in the clients having to remember and manually enter the SSID to join a specific access point. Whilst being the simplest security measure available, it by the most ineffective method as it provides very little protection against anything but the most casual intrusion (Ou, 2005).

2. 3. 2MAC Filtering

Another simple security feature available on many access points in MAC (Media Access Control) Address Filtering. This method utilizes the 48-bit address assigned to each network interface card (NIC) and adds them to either a whitelist or blacklist (Cisco, 2008). The restriction of network access through the use of lists is straightforward, however an individual is not identified by a MAC address, rather a device. The method means that an authorized administrator would need to whitelist or blacklist an entry for every device a client may want to use on the network. The process of specifying the approved and rejected MAC addresses can be controlled through the administrator page of the access point (provided it comes with admin tools available), see Figure 3 above. This form of security may be suitable for small home use, it isn’t practical for a business level as it

provides a massive overhead for the administrator, as they need to manually add each address. Relying on the security feature alone isn’t enough, as an individual can easily “ spoof” their MAC address to imitate another device (InfoExpress, 2017).

2. 3. 3Wired Equivalent Privacy

The IEEE 802. 11 WEP protocol was introduced as the privacy component of the original 802. 11 specification created in 1997, and was initially designed to provide confidentiality comparable to that of a traditional wired network (IEEE, 1997). Both WEP authentication and data encryption use two types of shared secret keys: 40-bit and 104-bit. To create the total encryption key is a combination of the base shared secret key and a 24-bit parameter called the Initialization vector and is used by both the client and server to decrypt the messages sent. The resulting length of the encryption key is 64-bit for the 40-bit shared key, and 128-bit for the 104-bit shared key (Schenk, 2001). The WEP protocol doesn’t provide a key management algorithm, so it assumes that the access point and client have agreed on the shared key via another prior method. With each message sent, the IV component of the encryption key can be changed. The original 802. 11 specification doesn’t standardize how the new IV should be created, with the implementation depending on the chosen algorithm. As the IV component of the key can change, it is sent as clear text with the encrypted message (cipher text), as the recipient needs to know the IV component for them to generate the new encryption key also (see figure 4 for the process overview). By having to send the IV as clear text, this means that if these packets were to be

intercepted, an unwanted user could easily gain part of the encryption key and potentially access the data.

WEP also has its own authentication process (before the data transfer process can commence) consisting of two distinct modes, Open System, and Shared Key (Qnx, 2017). The Open System mode does not require a key for the authentication process, therefore the client is always authenticated; which also means the same configuration for authentication is not required to match. An illustrated process of the Open System authentication is shown in figure 5 below.

The steps to authenticate when using Open System mode (Kurose et al, 2013):

The client sends an authentication request to the access point. The access point will then authenticate the requesting client. The client connects to the network.

The Shared Key authentication method however, requires an encryption key for the authentication process. Unlike the Open System mode, the Shared Key authentication requires both the client and access point to use the same authentication configuration. An illustrated process of the Shared Key authentication mode is shown in figure 6 below.

The following steps occur when using Shared Key Authentication (Kurose et al, 2013):

The client sends an authentication request to the access point. The access point sends challenge text to the station. The client uses the pre-configured

default key to encrypt the challenge text received, and sends the encrypted text to the access point. The access point decrypts the received text using its own pre-configured key that corresponds to the client’s key. The text is compared, and if it matches, then the client is authenticated. The client connects to the network.

When WEP was initially created, it performed the job it was designed and intended for; however as technology become more readily available and advanced; the security issues in the WEP protocol began to show. The WEP protocol was contains three major problems which make wireless networking more unsecure. The first major disadvantage is that the shared key needs to be sent to every single user on the network and this isn’t an easy task. Another disadvantage is that the encryption key size is only 40-bit or 104-bit; which is a very small size and can easily be hacked with open source software. Due to the security flaws, WEP was deprecated in 2004 with the introduction of WPA and WPA2 to more a more reliable and robust security service.

2. 3. 4Wi-Fi Protected Access 2

The 802. 11i WPA2 protocol was introduced in 2004, as an improvement upon the intermediate WPA protocol and original WEP protocol. The WPA protocol increases security by introducing two new protocols: 4-way handshake, and the group key handshake. The two protocols use authentication and port access services in WPA2 to create and alter the encryption keys (IEEE, 2004).

The four-way handshake is an authentication process that occurs between an access point and the client. It is method used for them both to prove to one another that they both know the Pairwise Master Key (PMK), without ever needing to disclose any part of the key; already providing more security over WEP. The process of sending encrypted message between the client and access point is still adopted from the WEP protocol, and if they successfully decrypt the message; then it proves they are knowledgeable of the PMK (Chaudhary, 2014). This process is vital in protecting the PMK from malicious and unwanted users, even if an attackers network id (SSID) was impersonating a real access point, the PMK would still never have to be disclosed.

Amongst the content in the aforementioned sections, there are other aspects that also relate to both wireless networking and wireless security. The most relevant aspect to consider is operational security, which includes three sub components: firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS). These systems provide an extra layer of security to attempt to block, detect and resolve security issues.

3. 1Firewalls

A firewall is a combination of software and hardware that isolates an organizations internal network from the internet, controlling which packets are allowed to pass through, and those that are blocked (Boudriga, 2010), by scanning the header fields of each packet to check if it passes the defined criteria. Figure 8 shows an illustrated example of where a physical firewall would sit within a networking infrastructure.

Firewalls are often categorized as either network firewalls or host-based firewalls (Vacca, 2009). A network firewall controls the traffic flow between two or more networks, and are typically the form of a software application, but dedicated physical devices are also used. Host-based firewalls on the other hand only controls the traffic for an individual machine (PersonalFirewall, 2017). Both types of firewalls use a set of pre-defined rules that are defined by an administrator through the use of either built in or third party software (see figure 9).

Utilizing a firewall as an extra layer of security is a must for many individual computers and networks, as they provide many strengths including: enforcing security and policies for an organization’s infrastructure, restricting access to specific services, removes the need to compromise between usability and security, and provides the ability for an administrator to monitor the traffic that flows through the network. Whilst providing many strengths, it does however also have some weaknesses including: only being capable of stopping the traffic that passes through the firewall itself, no ability to protect against an approved item, and they cannot protect against issues created from within the network.

3. 2Intrusion Detection Systems

Intrusion Detection Systems (IDS) are another method used to detect network activity. These systems can take the form of either a device or software application that monitors networks/systems for malicious and/or policy violations (Kurose. 2013); and is logged and handled by management

software. IDS systems can be categorized into two types: signature-based and anomaly-based.

A signature based IDS maintains a database of known attack signatures. Each signature is simply a set of rules retaining characteristics about a known packet(s), such as port numbers, protocol types, string of bits. Signatures are normally created by network security engineers, however customizations and additions can be made. Despite Signature-based IDS systems being widely deployed, they do have limitations. Most notably, they require previous knowledge of the attack to generate an accurate signature. An anomaly based IDS on the other hand creates a traffic profile as it observes during normal operation, seeking packets that are unusual statistically. The one major benefit about anomaly-based IDS systems is that they don’t rely on previous knowledge about existing attacks, as they can potentially detect new attacks on the go. On the other hand, it is an extremely challenging problem to distinguish between normal traffic and simply unusual traffic.

In conclusion, it is clear from the literature reviewed that wireless networking has become an extremely popular and sophisticated technology, but brings many security issues along with its use over traditional wired connectivity. As wireless networks utilize electromagnetic waves to transfer data, it is much easier for unwanted users to gain access to the data being transferred between a client and access point. Therefore, resulting in a combination of security features being required, including encrypted authentication and data transfer; along with extra layers such as a firewall and intrusion detection/prevention systems. With new technologies being developed and

standards updated, it is vital that these technologies are used to provide the best security when using wireless networking.

Al Tamimi, A. (2006). Security in Wireless Data Networks : A Survey Paper. [online] Cs. wustl. edu. Available at: http://www. cs. wustl. edu/~jain/cse574-06/ftp/wireless_security/index. html

Boudriga, N. and Boudriga, N. (2010). Security of mobile communications. Boca Raton: CRC Press.

Beal, V. (2017). What is Service Set Identifier (SSID)? Webopedia Definition. [online] Webopedia. com. Available at: http://www. webopedia. com/TERM/S/SSID. html

Cisco. (2008). Network Virtualization–Access Control Design Guide. [online] Available at: http://www. cisco. com/c/en/us/td/docs/solutions/Enterprise/Network_Virtualization/AccContr. html

Cisco. (2008). Authentication Types for Wireless Devices. [online] Available at: http://www. cisco. com/c/en/us/td/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes. html

Farshchi, J. (2003) “ The Essential Components of a Wireless Policy. “ Wireless Network Policy Development. Part Two. Symantec Corp. 10 October 2003. URL: http://www. securityfocus. com/printable/infocus/1735

IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11. (1997). [Place of publication not identified]: [publisher not identified].

IEEE 802. 11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements (pdf), IEEE Standards

Intel. 2017. Wireless Ethernet LAN (WLAN). (2017). 1st ed. [ebook] Intel. Available at: http://www. intel. com/content/dam/www/public/us/en/documents/faqs/wireless-ethernet-lan-faq1. pdf

InfoExpress. (2017). Detecting and Preventing MAC Spoofing. [online] Available at: https://infoexpress. com/content/practical/142

Kurose, J. and Ross, K. (2013). Computer networking. Boston: Pearson

Mitchell, B. (2016) Wireless Internet Service: An Introduction

Microsoft. (2003). How 802. 11 Wireless Works. [online] Available at: https://technet. microsoft. com/en-us/library/cc757419(v= ws. 10). aspx

Netgear. 2014. Wireless Access Points. [ONLINE] Available at: https://kb. netgear. com/235/What-is-a-wireless-access-point? cid= wmt_netgear_organic

Netgear. (2016). How to configure Access Control or MAC Filtering (Smart Wizard routers) | Answer | NETGEAR Support. [online] Available at: https://kb.

netgear. com/13112/How-to-configure-Access-Control-or-MAC-Filtering-Smart-Wizard-routers? cid= wmt_netgear_organic

Netgear. (2017). WEP Open System Authentication. [online] Available at: http://documentation. netgear. com/reference/nld/wireless/WirelessNetworkingBasics-3-08. html

Ou, G. (2005). The six dumbest ways to secure a wireless LAN | ZDNet. [online] ZDNet. Available at: http://www. zdnet. com/article/the-six-dumbest-ways-to-secure-a-wireless-lan/

O'Brien, J. & Marakas, G. M.(2008) Management Information Systems

PersonalFirewall. (2017). What is a Firewall? | How does a Firewall Protect your Computer. [online] Available at: https://personalfirewall. comodo. com/what-is-firewall. html

Qnx. com. (2017). Help – QNX SDP 6. 6 Documentation. [online] Available at: http://www. qnx. com/developers/docs/660/index. jsp? topic=%2Fcom. qnx. doc. core_networking%2Ftopic%2Fwpa_background_Connecting_WEP. html

Schenk, R. Garcia, A. Iwanchuk, R. " Wireless LAN Deployment and Security Basics." (2001). ExtremeTech. com. URL: http://www. extremetech. com/article2/0, 3973, 1073, 00. asp

Sheridan (2017). Printing Services – Optimizing Client Printing at Sheridan. [online] Available at: https://it. sheridancollege. ca/service-catalogue/printing/printing-optimization. html

Chaudhary, S. (2014). Hack WPA/WPA2 PSK Capturing the Handshake. [online] Kali Linux Hacking Tutorials. Available at: http://www. kalitutorials. net/2014/06/hack-wpa-2-psk-capturing-handshake. html

Vacca, J. (2009). Computer and information security handbook. Amsterdam: Elsevier.

Wallace, K. (2011). CompTIA Network+ Cert Guide: Connecting Wirelessly | Foundation Topics | Pearson IT Certification. [online] Pearsonitcertification. com. Available at: http://www. pearsonitcertification. com/articles/article. aspx? p= 1773082

NIST, 2007 – Guide to Intrusion Detection and Prevention Systems (IDPS)" (PDF).