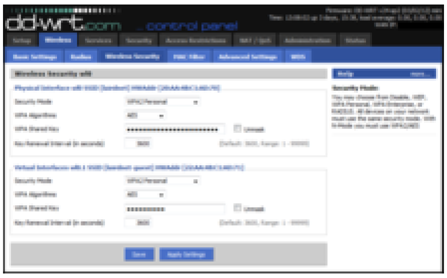
WIKIPEDIA

Wireless security

An example wireless router, that can implement **wireless security** features

Wireless security is the prevention of unauthorized access or damage to computers or data using wireless networks, which include Wi-Fi networks. The term may also refer to the protection of the wireless network itself from adversaries seeking to damage the confidentiality, integrity, or availability of the network. The most common type is **Wi-Fi security**, which includes Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is an old IEEE 802.11 standard from 1997.[1] It is a notoriously weak security standard: the password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools.[2] WEP was superseded in 2003 by WPA, a quick alternative at the time to improve security over WEP. The current standard is WPA2;[3] some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. Enterprises often enforce security using a certificate-based system to authenticate the connecting device, following the standard 802.11X.

Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks. As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources.[4] Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.



Security settings panel for a DD-WRT router

The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Hackers had not yet had time to latch on to the new technology, and wireless networks were not commonly found in the work place. However, there are many security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level.[5] Hacking methods have become much more sophisticated and innovative with wireless access. Hacking has also become much easier and more accessible with easy-to-use Windows- or Linux-based tools being made available on the web at no charge.

Some organizations that have no wireless access points installed do not feel that they need to address wireless security concerns. In-Stat MDR and META Group have estimated that 95% of all corporate laptop computers that were planned to be purchased in 2005 were equipped with wireless cards. Issues can arise in a supposedly non-wireless organization when a wireless laptop is plugged into the corporate network. A hacker could sit out in the parking lot and gather information from it through laptops and/or other devices, or even break in through this wireless card–equipped laptop and gain access to the wired network.

Contents

Background

Anyone within the geographical network range of an open, unencrypted wireless network can "sniff", or capture and record, the traffic, gain unauthorized access to internal network resources as well as to the internet, and then use the information and resources to perform disruptive or illegal acts. Such security breaches have become important concerns for both enterprise and home networks.

If router security is not activated or if the owner deactivates it for convenience, it creates a free hotspot. Since most 21st-century laptop PCs have wireless networking built in (see Intel "Centrino" technology), they don't need a third-party adapter such as a PCMCIA Card or USB dongle. Built-in wireless networking might be enabled by default, without the owner realizing it, thus broadcasting the laptop's accessibility to any computer nearby.

Modern operating systems such as Linux, macOS, or Microsoft Windows make it fairly easy to set up a PC as a wireless LAN "base station" using Internet Connection Sharing, thus allowing all the PCs in the home to access the Internet through the "base" PC. However, lack of knowledge among users about the security issues inherent in setting up such systems often may allow others nearby access to the connection. Such "piggybacking" is usually achieved without the wireless network operator's knowledge; it may even be without the knowledge of the intruding user if their computer automatically selects a nearby unsecured wireless network to use as an access point.

The threat situation

Wireless security is just an aspect of computer security; however, organizations may be particularly vulnerable to security breaches[6] caused by rogue access points.

If an employee (trusted entity) brings in a wireless router and plugs it into an unsecured switchport, the entire network can be exposed to anyone within range of the signals. Similarly, if an employee adds a wireless interface to a networked computer using an open USB port, they may create a breach in network security that would allow access to confidential materials. However, there are effective countermeasures (like disabling open switchports during switch configuration and VLAN configuration to limit network access) that are available to protect both the network and the information it contains, but such countermeasures must be applied uniformly to all network devices.

Threats and Vulnerabilites in an industrial (M2M) context

Due to its availability and low cost, the use of wireless communication technologies increases in domains beyond the originally intended usage areas, e.g. M2M communication in industrial applications. Such industrial applications often have specific security requirements. Hence, it is important to understand the characteristics of such applications and evaluate the vulnerabilities bearing the highest risk in this context. Evaluation of these vulnerabilities and the resulting vulnerability catalogs in an industrial context when considering WLAN, NFC and ZigBee are available.[7]

The mobility advantage

Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking is prone to some security issues.[8] Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks.[9] As a result, it is very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources.[4] Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) are commonly used to enforce wireless security policies.

The air interface and link corruption risk

There were relatively few dangers when wireless technology was first introduced, as the effort to maintain the communication was high and the effort to intrude is always higher. The variety of risks to users of wireless technology have increased as the service has become more popular and the technology more commonly available. Today there are a great number of security risks associated with the current wireless protocols and encryption methods, as carelessness and ignorance exists at the user and corporate IT level.[5] Hacking methods have become much more sophisticated and innovative with wireless.

Modes of unauthorized access

The modes of unauthorised access to links, to functions and to data is as variable as the respective entities make use of program code. There does not exist a full scope model of such threat. To some extent the prevention relies on known modes and methods of attack and relevant methods for suppression of the applied methods. However, each new mode of operation will create new options of threatening. Hence prevention requires a steady drive for improvement. The described modes of attack are just a snapshot of typical methods and scenarios where to apply.

Accidental association

Violation of the security perimeter of a corporate network can come from a number of different methods and intents. One of these methods is referred to as “accidental association”. When a user turns on a computer and it latches on to a wireless access point from a neighboring company's overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.

Accidental association is a case of wireless vulnerability called as "mis-association".[10] Mis-association can be accidental, deliberate (for example, done to bypass corporate firewall) or it can result from deliberate attempts on wireless clients to lure them into connecting to attacker's APs.

Malicious association

“Malicious associations” are when wireless devices can be actively made by attackers to connect to a company network through their laptop instead of a company access point (AP). These types of laptops are known as “soft APs” and are created when a cyber criminal runs some software that makes his/her wireless network card look like a legitimate access point. Once the thief has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans. Since wireless networks operate at the

Layer 2 level, Layer 3 protections such as network authentication and virtual private networks (VPNs) offer no barrier. Wireless 802.1X authentications do help with some protection but are still vulnerable to hacking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the criminal is just trying to take over the client at the Layer 2 level.

Ad hoc networks

Ad hoc networks can pose a security threat. Ad hoc networks are defined as [peer to peer] networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.[11]

The security hole provided by Ad hoc networking is not the Ad hoc network itself but the bridge it provides into other networks, usually in the corporate environment, and the unfortunate default settings in most versions of Microsoft Windows to have this feature turned on unless explicitly disabled. Thus the user may not even know they have an unsecured Ad hoc network in operation on their computer. If they are also using a wired or wireless infrastructure network at the same time, they are providing a bridge to the secured organizational network through the unsecured Ad hoc connection. Bridging is in two forms. A direct bridge, which requires the user actually configure a bridge between the two connections and is thus unlikely to be initiated unless explicitly desired, and an indirect bridge which is the shared resources on the user computer. The indirect bridge may expose private data that is shared from the user's computer to LAN connections, such as shared folders or private Network Attached Storage, making no distinction between authenticated or private connections and unauthenticated Ad-Hoc networks. This presents no threats not already familiar to open/public or unsecured wifi access points, but firewall rules may be circumvented in the case of poorly configured operating systems or local settings.[12]

Non-traditional networks

Non-traditional networks such as personal network Bluetooth devices are not safe from hacking and should be regarded as a security risk.[13] Even barcode readers, handheld PDAs, and wireless printers and copiers should be secured. These non-traditional networks can be easily overlooked by IT personnel who have narrowly focused on laptops and access points.

Identity theft (MAC spoofing)

Identity theft (or MAC spoofing) occurs when a hacker is able to listen in on network traffic and identify the MAC address of a computer with network privileges. Most wireless systems allow some kind of MAC filtering to allow only authorized computers with specific MAC IDs to gain access and utilize the network. However, programs exist that have network “sniffing” capabilities. Combine these programs with other software that allow a computer to pretend it has any MAC address that the hacker desires,[14] and the hacker can easily get around that hurdle.

MAC filtering is effective only for small residential (SOHO) networks, since it provides protection only when the wireless device is "off the air". Any 802.11 device "on the air" freely transmits its unencrypted MAC address in its 802.11 headers, and it requires no special equipment or software to detect it. Anyone with an 802.11 receiver (laptop and wireless adapter) and a freeware wireless packet analyzer can obtain the MAC address of any transmitting 802.11 within range. In an organizational environment, where most wireless devices are "on the air" throughout the active working shift, MAC filtering provides only a false sense of security since it prevents only "casual" or unintended connections to the organizational infrastructure and does nothing to prevent a directed attack.

Man-in-the-middle attacks

A man-in-the-middle attacker entices computers to log into a computer which is set up as a soft AP (Access Point). Once this is done, the hacker connects to a real access point through another wireless card offering a steady flow of traffic through the transparent hacking computer to the real network. The hacker can then sniff the traffic. One type of man-in-the-middle attack relies on security faults in challenge and handshake protocols to execute a “de-authentication attack”. This attack forces AP-connected computers to drop their connections and reconnect with the hacker's soft AP (disconnects the user from the modem so they have to connect again using their password which one can extract from the recording of the event). Man-in-the-middle attacks are enhanced by software such as LANjack and AirJack which automate multiple steps of the process, meaning what once required some skill can now be done by script kiddies. Hotspots are particularly vulnerable to any attack since there is little to no security on these networks.

Denial of service

A Denial-of-service attack (DoS) occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash. These attacks rely on the abuse of protocols such as the Extensible Authentication Protocol (EAP).

The DoS attack in itself does little to expose organizational data to a malicious attacker, since the interruption of the network prevents the flow of data and actually indirectly protects data by preventing it from being transmitted. The usual reason for performing a DoS attack is to observe the recovery of the wireless network, during which all of the initial handshake codes are re-transmitted by all devices, providing an opportunity for the malicious attacker to record these codes and use various cracking tools to analyze security weaknesses and exploit them to gain unauthorized access to the system. This works best on weakly encrypted systems such as WEP, where there are a number of tools available which can launch a dictionary style attack of "possibly accepted" security keys based on the "model" security key captured during the network recovery.

Network injection

In a network injection attack, a hacker can make use of access points that are exposed to non-filtered network traffic, specifically broadcasting network traffic such as “Spanning Tree” (802.1D), OSPF, RIP, and HSRP. The hacker injects bogus networking re-configuration commands that affect routers, switches, and intelligent hubs. A whole network can be brought down in this manner and require rebooting or even reprogramming of all intelligent networking devices.

Caffe Latte attack

The Caffe Latte attack is another way to defeat WEP. It is not necessary for the attacker to be in the area of the network using this exploit. By using a process that targets the Windows wireless stack, it is possible to obtain the WEP key from a remote client.[15] By sending a flood of encrypted ARP requests, the assailant takes advantage of the shared key authentication and the message modification flaws in 802.11 WEP. The attacker uses the ARP responses to obtain the WEP key in less than 6 minutes.[16]

Wireless intrusion prevention concepts

There are three principal ways to secure a wireless network.

- For closed networks (like home users and organizations) the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. Wireless Intrusion Prevention Systems can be used to provide wireless LAN security in this network model.
- For commercial providers, hotspots, and large organizations, the preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN.
- Wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it is also often possible for remote intruders to gain access to the network through backdoors like Back Orifice. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

There is no ready designed system to prevent from fraudulent usage of wireless communication or to protect data and functions with wirelessly communicating computers and other entities. However, there is a system of qualifying the taken measures as a whole according to a common understanding what shall be seen as state of the art. The system of qualifying is an international consensus as specified in ISO/IEC 15408.

A wireless intrusion prevention system

A Wireless Intrusion Prevention System (WIPS) is a concept for the most robust way to counteract wireless security risks.[17] However such WIPS does not exist as a ready designed solution to implement as a software package. A WIPS is typically implemented as an overlay to an existing Wireless LAN infrastructure, although it may be deployed standalone to enforce no-wireless policies within an organization. WIPS is considered so important to wireless security that in July 2009, the Payment Card Industry Security Standards Council published wireless guidelines[18] for PCI DSS recommending the use of WIPS to automate wireless scanning and protection for large organizations.

Security measures

There are a range of wireless security measures, of varying effectiveness and practicality.

SSID hiding

A simple but ineffective method to attempt to secure a wireless network is to hide the SSID (Service Set Identifier).[19] This provides very little protection against anything but the most casual intrusion efforts.

MAC ID filtering

One of the simplest techniques is to only allow access from known, pre-approved MAC addresses. Most wireless access points contain some type of MAC ID filtering. However, an attacker can simply sniff the MAC address of an authorized client and spoof this address.

Static IP addressing

Typical wireless access points provide IP addresses to clients via DHCP. Requiring clients to set their own addresses makes it more difficult for a casual or unsophisticated intruder to log onto the network, but provides little protection against a sophisticated attacker.[19]

802.11 security

IEEE 802.1X is the IEEE Standard authentication mechanisms to devices wishing to attach to a Wireless LAN.

Regular WEP

The Wired Equivalent Privacy (WEP) encryption standard was the original encryption standard for wireless, but since 2004 with the ratification WPA2 the IEEE has declared it "deprecated",[20] and while often supported, it is seldom or never the default on modern equipment.

Concerns were raised about its security as early as 2001,[21] dramatically demonstrated in 2005 by the FBI,[22] yet in 2007 T.J. Maxx admitted a massive security breach due in part to a reliance on WEP[23] and the Payment Card Industry took until 2008 to prohibit its use – and even then allowed existing use to continue until June 2010.[24]

WPAv1

The Wi-Fi Protected Access (WPA and WPA2) security protocols were later created to address the problems with WEP. If a weak password, such as a dictionary word or short character string is used, WPA and WPA2 can be cracked. Using a long enough random password (e.g. 14 random letters) or passphrase (e.g. 5 randomly chosen words) makes pre-shared key WPA virtually uncrackable. The second generation of the WPA security protocol (WPA2) is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance. With all those encryption schemes, any client in the network that knows the keys can read all the traffic.

Wi-Fi Protected Access (WPA) is a software/firmware improvement over WEP. All regular WLAN-equipment that worked with WEP are able to be simply upgraded and no new equipment needs to be bought. WPA is a trimmed-down version of the 802.11i security standard that was developed by the IEEE 802.11 to replace WEP. The TKIP encryption algorithm was developed for WPA to provide improvements to WEP that could be fielded as firmware upgrades to existing 802.11 devices. The WPA profile also provides optional support for the AES-CCMP algorithm that is the preferred algorithm in 802.11i and WPA2.

WPA Enterprise provides RADIUS based authentication using 802.1X. WPA Personal uses a pre-shared Shared Key (PSK) to establish the security using an 8 to 63 character passphrase. The PSK may also be entered as a 64 character hexadecimal string. Weak PSK passphrases can be broken using off-line dictionary attacks by capturing the messages in the four-way exchange when the client reconnects after being deauthenticated. Wireless suites such as aircrack-ng can crack a weak passphrase in less than a minute. Other WEP/WPA crackers are AirSnort and Auditor Security Collection.[25] Still, WPA Personal is secure when used with ‘good’ passphrases or a full 64-character hexadecimal key.

There was information, however, that Erik Tews (the man who created the fragmentation attack against WEP) was going to reveal a way of breaking the WPA TKIP implementation at Tokyo's PacSec security conference in November 2008, cracking the encryption on a packet in between 12–15 minutes.[26] Still, the announcement of this 'crack' was somewhat overblown by the media, because as of August, 2009, the best attack on WPA (the Beck-Tews attack) is only partially successful in that it only works on short data packets, it cannot decipher the WPA key, and it requires very specific WPA implementations in order to work.[27]

Additions to WPAv1

In addition to WPAv1, TKIP, WIDS and EAP may be added alongside. Also, VPN-networks (non-continuous secure network connections) may be set up under the 802.11-standard. VPN implementations include PPTP, L2TP, IPsec and SSH. However, this extra layer of security may also be cracked with tools such as Anger, Deceit and Ettercap for PPTP;[28] and ike-scan, IKEProbe, ipsectrace, and IKEcrack for IPsec-connections.

TKIP

This stands for Temporal Key Integrity Protocol and the acronym is pronounced as tee-kip. This is part of the IEEE 802.11i standard. TKIP implements per-packet key mixing with a re-keying system and also provides a message integrity check. These avoid the problems of WEP.

EAP

The WPA-improvement over the IEEE 802.1X standard already improved the authentication and authorization for access of wireless and wired LANs. In addition to this, extra measures such as the Extensible Authentication Protocol (EAP) have initiated an even greater amount of security. This, as EAP uses a central authentication server. Unfortunately, during 2002 a Maryland professor discovered some shortcomings. Over the next few years these shortcomings were addressed with the use of TLS and other enhancements.[29] This new version of EAP is now called Extended EAP and is available in several versions; these include: EAP-MD5, PEAPv0, PEAPv1, EAP-MSCHAPv2, LEAP, EAP-FAST, EAP-TLS, EAP-TTLS, MSCHAPv2, and EAP-SIM.

EAP-versions

EAP-versions include LEAP, PEAP and other EAP's.

LEAP

This stands for the Lightweight Extensible Authentication Protocol. This protocol is based on 802.1X and helps minimize the original security flaws by using WEP and a sophisticated key management system. This EAP-version is safer than EAP-MD5. This also uses MAC address authentication. LEAP is not secure; THC-LeapCracker can be used to break Cisco’s version of LEAP and be used against computers connected to an access point in the form of a dictionary attack. Anwrap and asleap finally are other crackers capable of breaking LEAP.[25]

PEAP

This stands for Protected Extensible Authentication Protocol. This protocol allows for a secure transport of data, passwords, and encryption keys without the need of a certificate server. This was developed by Cisco, Microsoft, and RSA Security.

Other EAPs There are other types of Extensible Authentication Protocol implementations that are based on the EAP framework. The framework that was established supports existing EAP types as well as future authentication methods.[30] EAP-TLS offers very good protection because of its mutual authentication. Both the client and the network are authenticated using certificates and per-session WEP keys.[31] EAP-FAST also offers good protection. EAP-TTLS is another alternative made by Certicom and Funk Software. It is more convenient as one does not need to distribute certificates to users, yet offers slightly less protection than EAP-TLS.[32]

Restricted access networks

Solutions include a newer system for authentication, IEEE 802.1X, that promises to enhance security on both wired and wireless networks. Wireless access points that incorporate technologies like these often also have routers built in, thus becoming wireless gateways.

End-to-end encryption

One can argue that both layer 2 and layer 3 encryption methods are not good enough for protecting valuable data like passwords and personal emails. Those technologies add encryption only to parts of the communication path, still allowing people to spy on the traffic if they have gained access to the wired network somehow. The solution may be encryption and authorization in the application layer, using technologies like SSL, SSH, GnuPG, PGP and similar.

The disadvantage with the end-to-end method is, it may fail to cover all traffic. With encryption on the router level or VPN, a single switch encrypts all traffic, even UDP and DNS lookups. With end-to-end encryption on the other hand, each service to be secured must have its encryption "turned on", and often every connection must also be "turned on" separately. For sending emails, every recipient must support the encryption method, and must exchange keys correctly. For Web, not all web sites offer https, and even if they do, the browser sends out IP addresses in clear text.

The most prized resource is often access to the Internet. An office LAN owner seeking to restrict such access will face the nontrivial enforcement task of having each user authenticate themselves for the router.

802.11i security

The newest and most rigorous security to implement into WLAN's today is the 802.11i RSN-standard. This full-fledged 802.11i standard (which uses WPAv2) however does require the newest hardware (unlike WPAv1), thus potentially requiring the purchase of new equipment. This new hardware required may be either AES-WRAP (an early version of 802.11i) or the newer and better AES-CCMP-equipment. One should make sure one needs WRAP or CCMP-equipment, as the 2 hardware standards are not compatible.

WPAv2

WPA2 is a WiFi Alliance branded version of the final 802.11i standard.[33] The primary enhancement over WPA is the inclusion of the AES-CCMP algorithm as a mandatory feature. Both WPA and WPA2 support EAP authentication methods using RADIUS servers and preshared key (PSK).

The number of WPA and WPA2 networks are increasing, while the number of WEP networks are decreasing,[34] because of the security vulnerabilities in WEP.

WPA2 has been found to have at least one security vulnerability, nicknamed Hole196. The vulnerability uses the WPA2 Group Temporal Key (GTK), which is a shared key among all users of the same BSSID, to launch attacks on other users of the same BSSID. It is named after page 196 of the IEEE 802.11i specification, where the vulnerability is discussed. In order for this exploit to be performed, the GTK must be known by the attacker.[35]

Additions to WPAv2

Unlike 802.1X, 802.11i already has most other additional security-services such as TKIP. Just as with WPAv1, WPAv2 may work in cooperation with EAP and a WIDS.

WAPI

This stands for WLAN Authentication and Privacy Infrastructure. This is a wireless security standard defined by the Chinese government.

Smart cards, USB tokens, and software tokens

Security token use is a method of authentication relying upon only authorized users possessing the requisite token. Smart cards are physical tokens in the cards that utilize an embedded integrated circuit chip for authentication, requiring a card reader.[36] USB Tokens are physical tokens that connect via USB port to authenticate the user.[37]

RF shielding

It's practical in some cases to apply specialized wall paint and window film to a room or building to significantly attenuate wireless signals, which keeps the signals from propagating outside a facility. This can significantly improve wireless security because it's difficult for hackers to receive the signals beyond the controlled area of a facility, such as from a parking lot.[38]

Denial of service defense

Most DoS attacks are easy to detect. However, a lot of them are difficult to stop even after detection. Here are three of the most common ways to stop a DoS attack.

Black holing

Black holing is one possible way of stopping a DoS attack. This is a situation where we drop all IP packets from an attacker. This is not a very good long-term strategy because attackers can change their source address very quickly.

This may have negative effects if done automatically. An attacker could knowingly spoof attack packets with the IP address of a corporate partner. Automated defenses could block legitimate traffic from that partner and cause additional problems.

Validating the handshake

Validating the handshake involves creating false opens, and not setting aside resources until the sender acknowledges. Some firewalls address SYN floods by pre-validating the TCP handshake. This is done by creating false opens. Whenever a SYN segment arrives, the firewall sends back a SYN/ACK segment, without passing the SYN segment on to the target server.

Only when the firewall gets back an ACK, which would happen only in a legitimate connection, would the firewall send the original SYN segment on to the server for which it was originally intended. The firewall doesn't set aside resources for a connection when a SYN segment arrives, so handling a large number of false SYN segments is only a small burden.

Rate limiting

Rate limiting can be used to reduce a certain type of traffic down to an amount the can be reasonably dealt with. Broadcasting to the internal network could still be used, but only at a limited rate for example. This is for more subtle DoS attacks. This is good if an attack is aimed at a single server because it keeps transmission lines at least partially open for other communication.

Rate limiting frustrates both the attacker, and the legitimate users. This helps but does not fully solve the problem. Once DoS traffic clogs the access line going to the internet, there is nothing a border firewall can do to help the situation. Most DoS attacks are problems of the community which can only be stopped with the help of ISP's and organizations whose computers are taken over as bots and used to attack other firms.

Mobile devices

With increasing number of mobile devices with 802.1X interfaces, security of such mobile devices becomes a concern. While open standards such as Kismet are targeted towards securing laptops,[39] access points solutions should extend towards covering mobile devices also. Host based solutions for mobile handsets and PDA's with 802.1X interface.

Security within mobile devices fall under three categories:

1. Protecting against ad hoc networks
2. Connecting to rogue access points
3. Mutual authentication schemes such as WPA2 as described above

Wireless IPS solutions now offer wireless security for mobile devices.

Mobile patient monitoring devices are becoming an integral part of healthcare industry and these devices will eventually become the method of choice for accessing and implementing health checks for patients located in remote areas. For these types of patient monitoring systems, security and reliability are critical, because they can influence the condition of patients, and could leave medical professionals in the dark about the condition of the patient if compromised.[40]

Implementing network encryption

In order to implement 802.11i, one must first make sure both that the router/access point(s), as well as all client devices are indeed equipped to support the network encryption. If this is done, a server such as RADIUS, ADS, NDS, or LDAP needs to be integrated. This server can be a computer on the local network, an access point / router with integrated authentication server, or a remote server. AP's/routers with integrated authentication servers are often very expensive and specifically an option for commercial usage like hot spots. Hosted 802.1X servers via the Internet require a monthly fee; running a private server is free yet has the disadvantage that one must set it up and that the server needs to be on continuously.[41]

To set up a server, server and client software must be installed. Server software required is an enterprise authentication server such as RADIUS, ADS, NDS, or LDAP. The required software can be picked from various suppliers as Microsoft, Cisco, Funk Software, Meetinghouse Data, and from some open-source projects. Software includes:

- Aradial RADIUS Server
- Cisco Secure Access Control Software
- freeRADIUS (open-source)
- Funk Software Steel Belted RADIUS (Odyssey)
- Microsoft Internet Authentication Service
- Meetinghouse Data EAGIS
- SkyFriendz (free cloud solution based on freeRADIUS)

Client software comes built-in with Windows XP and may be integrated into other OS's using any of following software:

- AEGIS-client
- Cisco ACU-client
- Intel PROSet/Wireless Software
- Odyssey client
- Xsupplicant (open1X)-project

RADIUS

Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization and accounting) protocol used for remote network access. RADIUS, developed in 1991, was originally proprietary but then published in 1997 under ISOC documents RFC 2138 and RFC 2139.[42][43] The idea is to have an inside server act as a gatekeeper by verifying identities through a username and password that is already pre-determined by the user. A RADIUS server can also be configured to enforce user policies and restrictions as well as record accounting information such as connection time for purposes such as billing.

Open access points

Today, there is almost full wireless network coverage in many urban areas – the infrastructure for the wireless community network (which some consider to be the future of the internet) is already in place. One could roam around and always be connected to Internet if the nodes were open to the public, but due to security concerns, most nodes are encrypted and the users don't know how to disable encryption. Many people consider it proper etiquette to leave access points open to the public, allowing free access to Internet. Others think the default encryption provides substantial protection at small inconvenience, against dangers of open access that they fear may be substantial even on a home DSL router.

The density of access points can even be a problem – there are a limited number of channels available, and they partly overlap. Each channel can handle multiple networks, but places with many private wireless networks (for example, apartment complexes), the limited number of Wi-Fi radio channels might cause slowness and other problems.

According to the advocates of Open Access Points, it shouldn't involve any significant risks to open up wireless networks for the public:

- The wireless network is after all confined to a small geographical area. A computer connected to the Internet and having improper configurations or other security problems can be exploited by anyone from anywhere in the world, while only clients in a small geographical range can exploit an open wireless access point. Thus the exposure is low with an open wireless access point, and the risks with having an open wireless network are small. However, one should be aware that an open wireless router will give access to the local network, often including access to file shares and printers.
- The only way to keep communication truly secure is to use end-to-end encryption. For example, when accessing an internet bank, one would almost always use strong encryption from the web browser and all the way to the bank – thus it shouldn't be risky to do banking over an unencrypted wireless network. The argument is that anyone can sniff the traffic applies to wired networks too, where system administrators and possible hackers have access to the links and can read the traffic. Also, anyone knowing the keys for an encrypted wireless network can gain access to the data being transferred over the network.
- If services like file shares, access to printers etc. are available on the local net, it is advisable to have authentication (i.e. by password) for accessing it (one should never assume that the private network is not accessible from the outside). Correctly set up, it should be safe to allow access to the local network to outsiders.
- With the most popular encryption algorithms today, a sniffer will usually be able to compute the network key in a few minutes.
- It is very common to pay a fixed monthly fee for the Internet connection, and not for the traffic – thus extra traffic will not be detrimental.
- Where Internet connections are plentiful and cheap, freeloaders will seldom be a prominent nuisance.

On the other hand, in some countries including Germany,[44] persons providing an open access point may be made (partially) liable for any illegal activity conducted via this access point. Also, many contracts with ISPs specify that the connection may not be shared with other persons.

See also

- Aircrack-ng
- Electromagnetic shielding
- Kismet
- KRACK
- List of router firmware projects
- Mobile security
- Payment Card Industry Data Security Standard
- Stealth wallpaper
- Tempest (codename)
- Wireless intrusion prevention system
- Wireless Public Key Infrastructure (WPKI)

- Exploits of wireless networks (https://en.wikipedia.org/w/index.php?title=Special:Search&search=deepcat%3A%22Computer+security+exploits%22+deepcat%3A%22Wireless+networking%22&ns0=1&fulltext=Search)

References

1. *IEEE 802.11-1997 Information Technology- telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications*. 1997. doi:10.1109/IEEESTD.1997.85951 (https://doi.org/10.1109%2FIEEESTD.1997.85951). ISBN 978-0-7381-3044-6.
2. "Definition of WEP" (https://www.pcmag.com/encyclopedia/term/wep). *PCMAG*. Retrieved 2021-06-04.
3. LinkedIn. "How Can You Secure a Wi-Fi Network With WPA2?" (https://www.lifewire.com/what-is-wpa2-818352). *Lifewire*. Retrieved 2021-06-04.
4. "How to: Define Wireless Network Security Policies" (http://www.wireless-nets.com/resources/tutorials/define_wireless_security_policies.html). Retrieved 2008-10-09.
5. "Wireless Security Primer (Part II)" (http://www.windowsecurity.com/articles/Wireless_Security_Primer_Part_II.html). windowsecurity.com. 2003-04-23. Retrieved 2008-04-27.
6. "Fitting the WLAN Security pieces together" (https://www.pcworld.com/article/144647/guide_to_wireless_lan_security.html). pcworld.com. 2008-10-30. Retrieved 2008-10-30.
7. "SECURITY VULNERABILITIES AND RISKS IN INDUSTRIAL USAGE OF WIRELESS COMMUNICATION" (https://www.researchgate.net/publication/264436422). IEEE ETFA 2014 – 19th IEEE International Conference on Emerging Technology and Factory Automation. Retrieved 2014-08-04.
8. "Network Security Tips" (http://www.linksysbycisco.com/EU/en/learningcenter/HowtoSecureYourNetwork). Cisco. Retrieved 2011-04-19.
9. "The Hidden Downside Of Wireless Networking" (https://www.districtadministration.com/article/hidden-downside-wireless-networking). Retrieved 2010-10-28.
10. "Top reasons why corporate WiFi clients connect to unauthorized networks" (http://www.infosecurity-us.com/view/7410/comment-top-reasons-why-corporate-wifi-clients-connect-to-unauthorized-networks-/). InfoSecurity. 2010-02-17. Retrieved 2010-03-22.
11. Margaret Rouse. "Encryption" (http://searchsecurity.techtarget.com/definition/encryption). TechTarget. Retrieved 26 May 2015.
12. Bradely Mitchell. "What is Ad-Hoc Mode in Wireless Networking?" (http://compnetworking.about.com/cs/wirelessfaqs/f/adhocwireless.htm). about tech. Retrieved 26 May 2015.
13. Browning, Dennis; Kessler, Gary (2009). "Bluetooth Hacking: A Case Study" (https://dx.doi.org/10.15394/jdfsl.2009.1058). *Journal of Digital Forensics, Security and Law*. doi:10.15394/jdfsl.2009.1058 (https://doi.org/10.15394%2Fjdfsl.2009.1058). ISSN 1558-7223 (https://www.worldcat.org/issn/1558-7223).
14. "SMAC 2.0 MAC Address Changer" (http://www.klcconsulting.net/smac/). klcconsulting.com. Retrieved 2008-03-17.
15. Lisa Phifer. "The Caffe Latte Attack: How It Works—and How to Block It" (http://www.wi-fiplanet.com/tutorials/article.php/10724_3716241_1). wi-fiplanet.com. Retrieved 2008-03-21.
16. "Caffe Latte with a Free Topping of Cracked WEP: Retrieving WEP Keys from Road-Warriors" (http://www.airtightnetworks.com/home/news/pr/select_category/14/article/123/airtight-wireless-security-researcher-reveals-wep-can-be-cracked-without-an-access-point.html). Retrieved 2008-03-21.

17. "Official PCI Security Standards Council Site – Verify PCI Compliance, Download Data Security and Credit Card Security Standards" (https://www.pcisecuritystandards.org).
18. "PCI DSS Wireless Guidelines" (https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf) (PDF). Retrieved 2009-07-16.
19. Ou, George (March 2005). "The six dumbest ways to secure a wireless LAN" (https://www.zdnet.com/blog/ou/the-six-dumbest-ways-to-secure-a-wireless-lan/43). *ZDNet*.
20. "What is a WEP key?" (http://lirent.net/wifi/what-is-a-wep-key.html). lirent.net. Retrieved 2008-03-11.
21. [e.g. "Weaknesses in the Key Scheduling Algorithm of RC4" by Fluhrer, Mantin and Shamir
22. "FBI Teaches Lesson In How To Break Into Wi-Fi Networks" (http://www.informationweek.com/news/160502612). *informationweek.com*.
23. "Analyzing the TJ Maxx Data Security Fiasco" (http://www.nysscpa.org/cpajournal/2008/808/essentials/p34.htm). *New York State Society of CPAs*.
24. "PCI DSS 1.2" (http://www.infosecstuff.com/pci-dss-12/).
25. *Hacking Wireless Networks for Dummies*. ISBN 9780764597305.
26. Robert McMillan. "Once thought safe, WPA Wi-Fi encryption is cracked" (http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9119258). IDG. Retrieved 2008-11-06.
27. Nate Anderson (2009). "One-minute WiFi crack puts further pressure on WPA" (https://arstechnica.com/tech-policy/news/2009/08/one-minute-wifi-crack-puts-further-pressure-on-wpa.ars). Ars Technica. Retrieved 2010-06-05.
28. Kevin Beaver; Peter T. Davis; Devin K. Akin (2011-05-09). *Hacking Wireless Networks For Dummies* (https://books.google.com/books?id=i0Edxmcly1oC&pg=PA295). p. 295. ISBN 978-1-118-08492-2.
29. "Extensible Authentication Protocol Overview" (https://technet.microsoft.com/en-us/library/bb457039.aspx). TechNet. Retrieved 26 May 2015.
30. "Extensible Authentication Protocol Overview" (http://www.microsoft.com/technet/network/eap/eap.mspx). Microsoft TechNet. Retrieved 2008-10-02.
31. Joshua Bardwell; Devin Akin (2005). *CWNA Official Study Guide* (Third ed.). McGraw-Hill. p. 435. ISBN 978-0-07-225538-6.
32. George Ou. "Ultimate wireless security guide: A primer on Cisco EAP-FAST authentication" (https://archive.today/Htb0). TechRepublic. Archived from the original (http://articles.techrepublic.com.com/5100-10878_11-6148557.html) on 2012-07-07. Retrieved 2008-10-02.
33. "Wi-Fi Protected Access" (https://web.archive.org/web/20070521092851/http://www.wifialliance.org/knowledge_center_overview.php?docid=4486). Wi-Fi Alliance. Archived from the original (http://www.wifialliance.org/knowledge_center_overview.php?docid=4486) on May 21, 2007. Retrieved 2008-02-06.
34. "WiGLE – Wireless Geographic Logging Engine – Stats" (https://wigle.net/gps/gps/main/stats).
35. "WPA2 Hole196 Vulnerability" (http://www.airtightnetworks.com/WPA2-Hole196). 2019-01-28.
36. "Secure Technology Alliance" (https://www.securetechalliance.org/smart-cards-intro-primer/). Retrieved 23 April 2021.
37. Etienne, Stefan (2019-02-22). "The best hardware security keys for two-factor authentication" (https://www.theverge.com/2019/2/22/18235173/the-best-hardware-security-keys-yubico-titan-key-u2f). *The Verge*. Retrieved 2021-06-03.
38. "How to: Improve Wireless Security with Shielding" (http://www.wireless-nets.com/resources/tutorials/rf_shielding.html). Retrieved 2008-10-09.

39. "What is Kismet?" (http://www.kismetwireless.net/). kismetwireless.net. Retrieved 2008-02-06.
40. Khamish Malhotra; Stephen Gardner; Will Mepham. "A novel implementation of signature, encryption and authentication (SEA) protocol on mobile patient monitoring devices" (http://iospress.metapress.com/content/12j78x26151wu377/). IOS Press. Retrieved 2010-03-11.
41. Briere, Danny; Hurley, Pat (30 September 2005). *Wireless Networks, Hacks and Mods for Dummies*. ISBN 9780764595837.
42. Jonathan Hassell (2003). *RADIUS: Securing Public Access to Private Resources*. O'Reilly Media. pp. 15–16. ISBN 9780596003227.
43. John Vollbrecht (2006). "The Beginnings and History of RADIUS" (http://www.interlinknetworks.com/app_notes/History%20of%20RADIUS.pdf) (PDF). Interlink Networks. Retrieved 2009-04-15.
44. "Offene Netzwerke auch für Deutschland!" (http://netzpolitik.org/2006/offene-netzwerke-auch-fuer-deutschland/). *netzpolitik.org*. 2006-09-15.

- *Wi-Foo: The Secrets of Wireless Hacking* (2004) – ISBN 978-0-321-20217-8
- *Real 802.11 Security: Wi-Fi Protected Access and 802.11i* (2003) – ISBN 978-0-321-13620-6
- *Design and Implementation of WLAN Authentication and Security*(2010) – ISBN 978-3-8383-7226-6
- "The Evolution of 802.11 Wireless Security" (https://benton.pub/research/benton_wireless.pdf) (PDF). ITFFROC. 2010-04-18.
- Boyle, Randall, Panko, Raymond. Corporate Computer Security. Upper Saddle River, New Jersey. 2015

External links

- Wireless security (https://curlie.org/Computers/Data_Communications/Wireless/Security) at Curlie
- How to Secure Your Wireless Home Network (https://www.wikihow.com/Secure-Your-Wireless-Home-Network) at wikiHow

Retrieved from "https://en.wikipedia.org/w/index.php?title=Wireless_security&oldid=1107978472"

This page was last edited on 1 September 2022, at 21:37 (UTC).