

The Simplicity of Attacking a Wireless Network

By Thomas Fisher

Introduction

It is well known that deploying an unencrypted wireless access point (AP) for any purpose is one quick path to a compromised network. Allowing completely anonymous, remote access to the inside of a protected computer network is not something any competent administrator would allow. However, they can often be misled by the advertising promises of the wireless device manufacturers. This article will outline the major vulnerabilities in common wireless configurations. It will simultaneously reveal the simplicity of capitalizing on these flaws and compromising a network. This article could also serve as a preliminary guide for assessing your own network's resistance to common attacks and hopefully provide some insight into the intentions and methods of attackers.

Background

The two most commonly implemented security techniques are access restrictions based on hardware Media Access Control (MAC) addresses and data encryption implementing the standard Wired Equivalent Privacy (WEP). The former is used to prevent unauthorized connections to the access point, while the latter is used to encrypt the data being transmitted by authorized users. These two techniques provide different forms of protection and are used together to help secure a wireless network. Another common wireless protection mechanism is usually referred to as ESSID hiding, where ESSID is an acronym for Extended Service Set Identifier and is synonymous with "network name." This strategy simply restricts the access point from broadcasting this information in beacon packets. Beacon packets are produced to advertise that wireless connectivity is available and conveniently provide prospective clients with the information needed to associate with the access point. The blocking of these transmissions prevents the network from being detected by most standard wireless scanning tools. Using all three of these techniques should provide reasonable security, because to gain access, an attacker would have to determine the unadvertised network name, break its encryption key, and finally thwart the MAC address filter. Unfortunately, implementing all three of these attacks is relatively simple with a few freely available tools. A compromised wireless network can have severe consequences, which will be discussed following a brief description of the attacks.

Common Attack Techniques

Assuming an organization uses all of the protection mechanisms mentioned above, the first step for an attacker is determining the hidden ESSID. Because this is not broadcast publicly, any legitimate client who wishes to

connect must know the channel and the ESSID on which the access point is operating. This means an attacker can also connect if he or she is able to determine these settings. Obviously the network itself cannot be completely hidden if it is being used, and this fact can be leveraged by periodically tuning to each wireless channel and collecting any transmitted packets. An attacker can set his or her wireless card to "monitor" mode, after which it will receive packets sent to any wireless device on the same channel, regardless of network association. A popular tool for performing this type of analysis is called Kismet (<http://www.kismetwireless.com>). This tool will read the network's Basic Service Set Identifier (BSSID) which can be found in any packet sent on that network. The BSSID, which in infrastructure networks corresponds to the MAC address of the access point, will uniquely identify a network just as the ESSID does. If traffic sniffing is the only intention of the attacker, then the BSSID is sufficient. If on the other hand the attacker wishes to establish a connection with the access point, then the ESSID of the network must be determined. The access point can be probed by clients to obtain connection information, after which Kismet can extract the ESSID from the AP's response.

The next attack must be on the WEP key, because this is needed to read any traffic or to associate with the AP. The most popular tool for attacking a WEP key is called aircrack (<http://aircrack.shmoo.com>). This tool is designed to monitor encrypted wireless networks and collect certain packets known to be "weak." A weak packet is one that can be used to guess the shared key by exploiting a mathematical shortcut found in the encryption algorithm. This must be performed many times on different weak packets to increase the probability of guessing the key correctly. For this attack to be successful, a very large number of encrypted packets (aircrack claims five to ten million) must be seen before enough weak packets will have been found. The amount of time required to collect this amount of data is heavily dependent on the network usage, and can range from around one minute to a few weeks or more. For more information on the WEP cracking process, refer to the links on aircrack's Web site. It is also worth mentioning that the vulnerability in WEP is independent of the size of the encryption key. A 128-bit WEP key will not take noticeably longer to reveal than a 64-bit WEP key.

If the goal of the attacker is to simply view the unencrypted traffic, he or she would be done at this point. Otherwise, the attacker must now focus on defeating the MAC address filter. The first step is to monitor the wireless traffic and record the MAC addresses of legitimate users' wireless network adapters. The attacker can wait until one of these users disconnects from the AP, then impersonate, or "spoof," that user's MAC address to connect to the AP. This is done by changing the hardware MAC address on the attacker's card using a tool called macchanger (<http://www.alobbs.com/macchanger>) or possibly utilities/drivers provided by the card's manufacturer. This spoofed

MAC address is known by the access point and is the only identification used to authenticate the connecting computer. The access point therefore assumes that it knows and trusts the computer and allows the connection.

Dangers of a Successful Attack

Once all three security mechanisms have been bypassed, the attacker has full access to data sent over the wireless link. Unfortunately for the administrator, wireless devices are not physically linked with the AP and can be completely passive. They therefore provide no way for the AP to determine if there is anyone spying on its network. If packet sniffing is the only intent of the attacker, then there is no need for an active technique such as ARP cache poisoning, which could be detected. This contrasts the functionality of a network switch where data can be physically directed to only one port. If the attacker's card is in monitor mode, what is seen is similar to packet sniffing on a network hub. What is even worse is that this "hub" has an undefined number of ports and can be accessed from outside most physical boundaries used to protect a wired Ethernet network.

It seems logical that a weak security mechanism is better than no security at all. It also follows that a network with a compromised security mechanism is equivalent to an unprotected network. The reasoning behind these two statements appears sound. However, investigating the specifics of each case proves them both to be completely false. From the attacker's perspective, a cracked WEP network is much more valuable than one that was intentionally deployed unencrypted. A user on an unencrypted network is more likely to be wary of what is transmitted over that link. For example, checking an e-mail account using standard unencrypted authentication mechanisms would hopefully be avoided because the login information is easily available to any passer-by with a wireless card. If the network being used was WEP-protected, the user would likely not think twice about that same action. It is also likely that a user who knows their traffic is being encrypted may overlook a secure connection type, preferring the insecure alternative for the sake of simplicity or convenience.

Another dangerous aspect of standard WEP-protected 802.11 networks is the use of shared key encryption. The most common complaint of this scheme is that it offers no way to individually authenticate users, nor does it allow users to protect data from one another. If an attacker has cracked the WEP key, he or she can impersonate any legitimate user of the network by spoofing their MAC address. Similarly, once the key is known, the transmissions of all users on the network are exposed, even though they still believe that they are communicating across secured channels. This can also be seen by considering the example of public "hot spots" like an Internet café or coffee shop where anyone is allowed to use the wireless service. In order for customers to connect, the WEP key would need to be given to everyone who requested access. If a malicious person wanted to monitor the unencrypted traffic, he or she could simply request access and be given the key without hesitation. This setup would simply complicate the access procedure for non-technical customers and at the same time provide them the assumption that their connection is secure. The only situation worse than wireless users transmitting unencrypted data is having them transmit data that they only believe is secure.

Options for Better Protection

As mentioned previously, there is no way to completely hide a wireless network from detection. With this fact in mind, it becomes apparent that securing any network well is of utmost importance. The next generation of wireless security has been standardized by the IEEE as 802.11i. This new

standard includes a different approach to authentication and encryption. It has support for forwarding authentication requests to separate, dedicated servers including the commonly used RADIUS system. This would make the MAC-based restriction currently used unnecessary and therefore attacking it would become irrelevant. The new Wi-Fi Protected Access (WPA) encryption no longer uses the vulnerable key scheduling algorithm used in WEP and instead implements a rotating key system known as the Temporal Key Integrity Protocol, or TKIP. WPA also uses the newer Advanced Encryption Standard (AES), which uses much larger keys than the previous Data Encryption Standard (DES) used by WEP. Using the new 802.11i techniques will successfully prevent all of the attacks outlined in this article. However this should not be accepted as a single solution. The weaknesses of the WEP scheme were not known immediately after the release of the standard; it took some time for its discovery. While WPA may currently appear to be completely secure, no administrator should assume that vulnerabilities will never be found in the future.

Rogue Access Points


Administrators who recognize all of these concerns may have deployed wireless networks using the newer WPA encryption scheme that is not susceptible to these simple attacks. Even if the current WEP technologies must be used, more secure connections should be made using an encrypted tunnel such as a Virtual Private Network (VPN) inside the WEP-protected connection. For the most sensitive networks, administrators may have refused to implement wireless at any level. These administrators, however, must still be concerned with the aforementioned attack techniques because another major threat is that of a rogue access point. With the low price tag and tempting convenience of home-use wireless access points, those companies implementing a strict wireless-free environment may be the most at risk.

The setup of home-use "Wireless Routers" has become unbelievably simple. Driven by MAC address restrictions enforced by many Internet providers, these devices often have the option of cloning the address of the network card that is configuring them. Consider the scenario where a network administrator has set up company employees, each with a network jack and Ethernet connectivity. In addition, network access is only granted if originating from the MAC address of the computer with which that employee was provided. The intention is to prevent the employee from attaching a different device, in this case a wireless access point, because the MAC filter on the network will see a new address and prevent it from obtaining connectivity. If the MAC cloning option is used, without even understanding the purpose of the MAC filter or the implications of bypassing it, the employee can have his or her wireless router connected to the company's network despite the efforts of the administrator. This access point can provide outside attackers with a back door into the network that is more dangerous than a legitimately deployed wireless network that has been compromised. Even if the employee secures the access point properly, it would still be vulnerable to all the attacks outlined above because most home-use wireless devices do not fully support the new 802.11i standards yet. Again, the severity of this is derived from the belief that the network is secure. Regardless of their actual origin, all packets entering the wired Ethernet from the employee's network jack are modified by the wireless router to contain the employee's MAC address as their source. The router handles all address translations internally, therefore being transparent to the attacker, the employee and the administered Ethernet network (including its MAC address filter). Any individual residing nearby who has infiltrated this access point has then gained exactly the same network

privileges as the employee. These are the same privileges that were granted under the assumption that the network jack was being used by a single computer physically protected inside the employee's office.

A solution to this is using a wireless network detection tool to monitor the air for the appearance of new BSSIDs in the vicinity. However, even if a new access point is detected, the physical location could be difficult to track down, nor is it apparent that it even belongs to the same company. While the location can be found with some degree of precision, it will take some time and effort on the administrator's part. If monitoring the air is not done, it is possible that these likely unsecured and remotely configurable rogue access points can appear without notice. It is also possible that a rogue access point may not even be detected by a monitoring administrator because there could be an object blocking the signal or it was installed just out of range. The best tactic for preventing unauthorized access point deployment is educating employees on why they are being restricted and ensuring that they understand the risks involved in a compromise.

Summary

If there is a wireless network in your organization, whether it has been authorized or not, any attacker can find it. Extending your network to allow wireless clients should not be done unless there is very strong encryption in place. Standard protection methods are unacceptable, regardless of what the advertisements on the product packaging may claim. While the newer WPA techniques are becoming available on many devices and platforms, they should still be implemented with caution. Secure connection protocols should always be used, even if other protections (like WEP) are in place. If your organization provides wireless access, ensure that it is properly audited. If you are not the administrator of your network, this is most likely not your responsibility. If there is a break-in, however, it could very well be your problem. Remember that your data is at risk if any malicious individual breaks into your network. 

Thomas Fisher is with Sytex, Inc., a leading provider of quality services, integrated systems and solutions for the government and military sectors.