CYBER ATTACKS EXPLAINED: WIRELESS ATTACKS

Wireless networks are everywhere, from the home to corporate data centres. They make our lives easier by avoiding bulky cables and related problems. But with these benefits comes a threat: wireless networks are prone to attacks. This article discusses techniques to protect FOSS networks, which systems administrators can implement to achieve adequate security.

Before we talk about wireless security and vulnerability attacks, we must understand the basic radio transmissions, and the IEEE 802.11 protocol, also commonly known as the WLAN protocol. This protocol links two or more devices over a short distance, using spread spectrum signals. Spread spectrum, at its core, is based on radio communication frequencies to establish point-to-point wireless communication between a transmitter and a receiver, while achieving resistance to signal jamming and signal fading. As shown in Figure 1, to establish a wireless network, you need a wireless access point (AP) and also a wireless adaptor for each node to be connected. The AP is also called a hot-spot; it hosts a radio transceiver similar to a walkie-talkie. It also contains hardware to convert digital data into radio signals and vice-versa.

The AP has a unique feature called a beacon transmission, whereby it keeps transmitting a digitised signal, typically, a few times every second. This signal contains the network identification data, the service set identifier (SSID) and some trivial error-correction information. Nodes such as laptops or other wireless devices detect this signal in order to show it in the list of available wireless networks. It also detects whether or not the AP is using any security, the level of the security protocol, etc.

The AP contains a TCP/IP stack, which responds to ARP requests when a node tries to connect to it. Since wireless networks can allow multiple nodes, it is essential to have an authentication layer prior to letting data transfer take place. It is the APs responsibility to ensure this security, as well as to monitor packet transmission and data integrity.

Wi-Fi security

Since wireless networks don't have built-in security mechanisms, a secure layer on top of the wireless protocol stack is achieved by encryption and authentication techniques such as WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access). This is especially important because, unlike a wired network, wireless signals can be easily intercepted using a signal-trapping device. Let's discuss how these encryption techniques work, in detail.

To establish a secure channel, the client first sends an authentication request to the AP, and receives a challenge from it in text form. The client encrypts this text using the preconfigured key and sends it back. The AP decrypts it, and when it succeeds, replies to the client. If the keys don't match, the request is dropped, and the client cannot connect to the AP. This method is called pre-shared authentication. In an improved version, the shared key is combined with the SSID of the wireless AP, to further toughen the encryption key logic. WEP encryption uses the RC4 algorithm on all packets that travel between the AP and the node. Unfortunately, these security mechanisms are either flawed by design, or are not adequate for IT infrastructures where data carried on wireless channels is sensitive.

With this basic understanding of Wi-Fi security, let us now discuss a few security attacks. In general, there are four categories of possible attacks.

Passive attacks: In this type, the attacker listens or eavesdrops on an open wireless channel by using a wireless modem rigged to work in a promiscuous mode. All traffic packets that contain important information, such as MAC addresses, packet sequences, etc, are stored. Passive attacks may not necessarily be malicious in nature, but help provide information for active attacks. Since passive attacks take place silently, they are almost impossible to detect and stop. Attackers using passive methods usually capture and store data, and use a packet-deciphering tool to decrypt it and steal information. This is especially true in case of the WEP protocol, due to its inherent lack of security. Passive attacks are also called wireless war-driving.

Active attacks: Once an attacker gets sufficient information by passive attacks, an active attack can be tried. Common examples are denial of service, IP spoofing, etc. In case of spoofing, the attacker gains access to an unauthorised wireless station, and performs packet crafting to impersonate a valid and authorised station. Wireless nodes are incapable of detecting this, and end up connecting to the attacker's station and revealing information. By extending this technique, the attacker can now plant a denial of service attack on a particular node in order to disrupt its services. Typically, a SYN flood method is used, because it is sufficient to generate a packet storm on the given wireless connection bandwidth.

MITM attacks: We did explore man in the middle (MITM) attacks in one of the previous articles and most of that applies to wireless networks as well. The only technical difference here is that the attacker gains information of an actively used SSID of an AP, instead of an on-the-wire session. As shown in Figure 2, a dummy AP with exactly the same name is created by the attacker, and the signal power is raised to such an extent that the nodes are fooled into believing that it is the AP they should connect to. This creates an MITM situation. These dummy APs, also called rogue points, are usually set up close to the nodes to be hacked.

Signal-jamming attacks: Unlike the above techniques, this method uses wireless radio transmission techniques to create an attack. In this type, the attacker uses a powerful antenna and a signal generator, and creates frequency patterns in the same range as wireless signals. The frequency patterns are modulated with powerful radio frequency ripples, to create a wireless signal storm. This results in the jamming of the APs as well as the nodes, thus disabling their connectivity. While such an attack was just a theory previously, with a growing number of wireless networks these attacks have now occurred more often than earlier.

Besides these, there are a few other types of attacks, some of which make use of one or more of the attacks mentioned above.

802.11 injection attacks: Modern attackers tend to go deep into the protocol stack in order to plant an attack. For wireless networks, an attacker can first perform a passive attack to understand the protocol frame structure, and then create 802.11 protocol datagram frames and insert those into the network. This is usually done either to create a false packet stream as a hindrance for a wireless network, or to sniff the network further in an active mode. The response 802.11 frames are then captured again, interpreted and modified to perform an MITM attack. Since this attack happens at Layer 2, it is very tough to detect.

Wireless packet injection: Here, passive attacks are used to capture traffic, which is then analysed. However, there can be situations in which there won’t be enough traffic to generate sufficient data, which can lead to time-consuming or futile hacking efforts. Hence, attackers use wireless packet injection techniques whereby, besides the 802.11 frames, IP datagrams are sent to the target AP. Though the AP will drop such packets as unauthorised, this gives the attacker the necessary amount of traffic, which is captured and fed into key-cracking utilities. Since the attacker controls the packet-generator utility, specific data patterns are intentionally created to map the APs behaviour in terms of response packets, which further helps in reducing the cracking time.

PSK guessing: As we learnt earlier, a pre-shared key is used between the wireless AP and node to encrypt communication. Typically, administrators setting up Wi-Fi networks tend to leave the vendor-provided default key in place. Smart attackers usually first try to detect the manufacturer of wireless APs, and if that information is not available, they try to guess it and attempt to break the key.

Key cracking: Usually a pre-shared key should be enough to establish security. However, in case of WEP-based Wi-Fi networks, attackers can use passive methods to sniff and capture a lot of data, and subject it to key-cracking algorithms. As we saw earlier, WEP is a simple RC4 XOR type of encryption, and it only takes some amount of time to break into it. It had been demonstrated by attackers that a packet capture of more than 40000 can be sufficient data to crack a WEP key in minutes. With the introduction of WPA security features in a wireless AP, it became tough to break the key. However other brute-force attacks, such as statistical key guessing, dictionary attacks, etc, can be used to crack it.

Wireless attack detection

Before we talk about protecting the infrastructure, it is imperative to understand a few detection techniques. Unlike wired networks, a wireless network signal can be compromised easily, which makes detection difficult but certainly not impossible.

AP monitoring: As we learnt, securing the SSID of an AP or wireless router is very important. In a large organisation, keeping track of SSIDs can be a challenge; hence, this information should be programmatically stored in a secure database. Other crucial details, such as the MAC ID, IP restrictions, the wireless channel used, the beacon settings, wireless signal strength and bandwidth type are stored for each corresponding SSID. A wireless monitoring device, or a mobile device running monitoring software, is used to detect all stations and APs periodically, and the results are compared with the baseline database created earlier. Such routine audits ensure the integrity of router settings and thus the overall wireless network security.

Wi-Fi node monitoring: Along with the APs, each node needs to be monitored too. The technique is a bit different, though. For the nodes, a MAC-based security on the APs can be configured, whereby a particular AP would support only a set of MAC addresses. This ensures that the wireless client node cannot roam around beyond the configured zone, and if such a need arises the request can be fulfilled via an authorisation and approval process. For large organisations, this can result in systems administration overhead, in which case the nodes can be allowed to connect to all APs; however, each connection and disconnection can be logged and parsed for anomalous behaviour.

Traffic monitoring: Besides the above techniques, network administrators can periodically take samples of data from each AP, and check for denial of service and SYN flood attacks. Multiple connections and disconnections on a particular AP from one or more client nodes should also trigger a warning. As for Layer 2 attacks, a signal spectrum detection tool can be incorporated too, to detect signal-jamming situations.

Protecting FOSS systems

Along with the monitoring techniques, additional security measures are essential. For small networks, changing the default password and SSID of the AP is a must. Modern routers are equipped with a feature to disable the broadcasting of SSID, which should be turned on to ensure that passive sniffing attacks are thwarted to some extent. Periodically changing SSIDs is highly recommended, though it can be a tough task for a large number of wireless APs. To protect a Linux server farm hosted in a data-centre, the wireless signal strength of APs should be adjusted in such a way that it should be adequate for client nodes to connect and transfer data seamlessly, but at the same time it should not cross physical building boundaries, whereby it can be detected by a drive-by attacker.

Using WPA2 security instead of WEP is recommended. Besides, the shared key of WPA security should be long and complex enough to stop directory brute-force attacks. For large corporations, the Layer-7 wireless security software should be installed on client nodes as well as APs, to further strengthen the encryption process. For FOSS systems, using an X.509 certificate on either end of the wireless communication can help achieve cheaper yet effective security. Most famous flavours, such as Debian and Ubuntu, support WPA2 security with trimmings such as AES, TKIP and LEAP. Configuring those, along with MAC address filtering, and enabling firewall features can protect a serious server farm, yet let it enjoy the benefits of wireless networks.

Wireless attacks are, unfortunately, easy to carry out and difficult to detect. Modern data centres allow the presence of wireless networks connected to the product server farms, thus requiring the implementation of security measures. While there is no single solution to protect wireless networks, an appropriate combination of the techniques mentioned above can achieve adequate security. Wireless monitoring audits are an important activity that needs to be done by network administrators at regular intervals.

Source : http://www.opensourceforu.com/2013/04/cyber-attacks-explained-wireless-attacks/