Wireless Security with Cyberoam

Robust, fault-tolerant security is a must for companies sporting wireless networks. Cyberoam UTM strengthens the existing Wireless Security Architecture of these companies and overcomes most challenges of securing their legacy IEEE 802.11 wireless local area networks (WLAN).
Contents

Need For Wireless Security ................................................................. 3
Challenges of Securing Wireless LANs ............................................... 3
Existing Wireless LAN Security Architectures ..................................... 5
The Cyberoam Edge ........................................................................... 7
Conclusion .......................................................................................... 8
References .......................................................................................... 8
Need For Wireless Security

While security is important for all networks, wireless LANs deserve special consideration since they are subject to a much heightened level of risk. First, since wireless networks extend beyond the walls of an organization, physical security is far less effective than with wired networks. Secondly, wireless network abuse has become more common with tools that assist wireless hacking being widely available, resulting in companies increasingly falling at risk from targeted attacks. Finally, 802.11 protocols operating on unlicensed spectrum use well-understood protocols, resulting in a proliferation of devices that are able to access corporate networks.

Wireless networks are also subject to several regulations that mandate high security networks including PCI, HIPAA, and SOX. The credit card industry requires those processing credit card transactions to comply with PCI standards in order to mitigate the chances of card number theft and fraud. All merchants using payment cards must build and maintain a secure network to protect and encrypt cardholder data, and regularly monitor and test their networks including wireless networks.

The Health Insurance Portability and Accountability Act (HIPAA), was enacted by the U.S. Congress in 1996. Many health care institutions are covered by it and required to maintain administrative, technical and physical safeguards to ensure integrity and confidentiality of patient data. Wireless networks are potentially vulnerable and must be secured in order to comply.

Finally, public companies are subject to the Sarbanes-Oxley act (SOX) and similar measures outside the U.S. SOX requires companies to maintain and assess internal control structures and procedures for financial reporting and to assess the effectiveness of these internal control structures. Network security is typically part of the control review. Thus, a combination of regulatory requirements as well as common sense make wireless security an important consideration.

Challenges of Securing Wireless LANs

In this section, we would look at the “Security Objectives” of Wireless LAN along with some of the challenges in achieving them.

Like every other Information system, Wireless LAN needs to support the basic “security objectives”. They are:

- **Confidentiality**: Ensures that communication cannot be read by unauthorized parties
- **Integrity**: Detect any intentional or unintentional changes to data that occur in transit
- **Availability**: Ensure that devices and individuals can access WLAN and its resources whenever needed.
Wireless LANs also face all major high level threat categories like every other information system. The threats are summarized below:

<table>
<thead>
<tr>
<th>Threat Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of Service</td>
<td>Attacker prevents or limits the normal use or management of networks or network devices.</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Attacker passively monitors network communications for data, including authentication credentials.</td>
</tr>
<tr>
<td>Man-in-the-Middle</td>
<td>Attacker actively impersonates multiple legitimate parties, such as appearing as a client to an AP and appearing as an AP to a client. Allows attacker to intercept communications between an AP and a client, thereby obtaining authentication credentials and data.</td>
</tr>
<tr>
<td>Masquerading</td>
<td>Attacker impersonates an authorized user and gains certain unauthorized privileges.</td>
</tr>
<tr>
<td>Message Modification</td>
<td>Attacker alters a legitimate message by deleting, adding to, changing, or reordering it.</td>
</tr>
<tr>
<td>Message Replay</td>
<td>Attacker passively monitors transmissions and retransmits messages, acting as if the attacker were a legitimate user.</td>
</tr>
<tr>
<td>Misappropriation</td>
<td>Attacker steals or makes unauthorized use of a service.</td>
</tr>
<tr>
<td>Traffic Analysis</td>
<td>Attacker passively monitors transmissions to identify communication patterns and participants.</td>
</tr>
</tbody>
</table>

The most significant difference between wireless and wired networks is the relative ease of intercepting wireless network transmissions and inserting new or altered transmissions from what is presumed to be the authentic source.

Most threats against wireless networks involve an attacker with access to the radio link between wireless devices. Several threats listed in the table above rely on an attacker’s ability to intercept and inject network communications. This highlights the most significant difference between protecting wireless and wired networks: the relative ease of intercepting wireless network transmissions and inserting new or altered transmissions from what is presumed to be the authentic source. To breach a wired network, an attacker would need to gain physical access to the network or remotely compromise systems in there; for a wireless network, an attacker simply needs to be within the range of the wireless transmissions, making eavesdropping a particularly prevalent threat. (Some attackers use highly sensitive directional antennas, which can greatly extend the effective range of attack on wireless networks beyond the standard range.) Another consideration in threats against wireless networks is that in many cases, a wireless network is logically connected to a wired network, so the wireless network should be secured against both threats that wired networks typically face and the threats that are specific to wireless networks.

In addition to eavesdropping, another common threat against wireless networks is the deployment of rogue wireless devices. For example, an attacker could deploy a wireless access point (AP) that has been configured to appear as part of the organization’s wireless network infrastructure. This provides a backdoor into the wired network, bypassing perimeter security mechanisms such as firewalls. In addition, if clients inadvertently connect to the rogue device, the attacker can view and manipulate the clients’ communications.
Denial of service (DoS) situations are another threat against wireless networks. Examples are flooding (an attacker sends large numbers of messages at a high rate to prevent the wireless network from processing legitimate traffic) and jamming (a device emits electromagnetic energy on the wireless network’s frequency to make it unusable). Jamming often occurs unintentionally; for example, microwave ovens, cordless telephones, and other devices share bandwidth with certain wireless technologies and the devices' operation can inadvertently make wireless networks in proximity unusable. Denial of service conditions can also be caused through protocol manipulation such as improper requests or responses that cause devices to enter abnormal states.

Existing Wireless LAN Security Architectures
In this section, we will look at the existing security architectures for Wireless LAN and their limitations. This section described WEP and WPA which are designed to protect link-level data during wireless transmission between clients and APs. As figure below shows, WLAN standards cannot provide end-to-end security because they are only used for the wireless link between the AP and STA.

Security is Provided Through Other Means

IEEE 802.11 Security

Wired Equivalent Privacy (WEP)
Designed for Wireless Local Area Networks (WLANs), WEP provides wireless security equivalent to that of a wired LAN. While it is still considered to be a basic deterrent, it has several known flaws that any moderately skilled hacker could exploit with just a little time and a few tools.

At the March 2005 meeting of the Information Systems Security Association (ISSA) in Los Angeles, a team of FBI agents were easily able to hack into a WEP-protected network in approximately three minutes.
While WEP is regarded as the baseline from which subsequent, WEP has several significant security problems, most of them cannot be solved by reconfiguration of WEP itself. For example, increasing the length of the WEP key would only marginally increase the time needed to decrypt packets. WEP does not provide an acceptable level of wireless transmission security, so it should not be the sole security mechanism used in legacy IEEE 802.11 WLAN deployments.

**Wi-Fi Protected Access (WPA)**
Built upon the foundation of WEP, WPA was created in 2002 to bring enhanced LAN security to the wireless market. WPA uses Temporal Key Integrity Protocol (TKIP) encryption using the same RC4 algorithm as WEP for encryption, but adding sophisticated key management and effective message integrity checking. Developed in conjunction with the IEEE 802.11 Standards Working Group for WLANs, WPA effectively replaced WEP and the other security features of the original 802.11 standard.

WPA offers dynamic key encryption and mutual authentication. It secures both email packet headers and their payloads, and provides a deterrent to replay attacks. WPA’s enhanced encryption is an ideal solution for wireless networks that deal with many different types of 802.11 radio Message Integrity Checks (MICs) such as public hotspots. Most leading wireless access point and chip set vendors have lent their support to WPA.

WPA is not a miracle cure however, and as with any new solution that addresses existing issues, new issues have emerged as a result. Like its predecessor WEP, WPA has been found to have weaknesses that can be used to bring down a network. Two attack techniques adept at exploiting WPA vulnerabilities are dictionary attacks and Denial of Service (DoS) attacks.

Though Wi-Fi protected access (WPA) is currently the most commonly used mechanism for protecting users of wireless networks, protection is afforded by authenticating users of the network and encrypting communication which travels through the wireless medium. However, WPA is limited in the amount of protection offered in networks which use a pre-shared key (WPA-PSK) for authentication, as anyone holding the PSK may eavesdrop on other authorized users. Hence, **WPA is most effective when supplemented with other wireless security precautions.**

**Wi-Fi Protected Access 2 (WPA2)**
The second generation of WPA, known as WPA2, replaced TKIP encryption with 128-bit Advanced Encryption Standard (AES) encryption for compliance with FIPS140-2 government security requirements.

With each successive generation of standards, there are new issues to address. WPA2 requires a dedicated chip to handle the encryption and decryption which for many will mean a hardware upgrade in order to take advantage of the benefits.

To summarize it all, the existing wireless security architectures are either expensive or do not provide security in a real sense. The Wireless Administrator is not able to create a roaming profile for a wireless user. Also, none of the existing technologies take rogue access point into consideration and protect the wireless users’ data from being compromised.
The Cyberoam Edge

We discussed the challenges of securing Wireless LANs and along with the existing Wireless LAN security architectures. Cyberoam does include each and every security architecture discussed in the previous section. In this section though, we would concentrate on how Cyberoam’s Layer-8 “Identity Based Firewall” helps fortify existing Wireless LAN security architectures.

Cyberoam’s Layer-8 “Identity based firewall” technology was developed out of the need for a more robust technology to secure LANs. This functionality is extended to Wireless LANs as well. Cyberoam provides user identity as a matching criteria within the firewall rules. This takes organizations a step ahead of conventional security appliances which bind security to IP addresses. This is depicted below:

Cyberoam’s “Identity Based Firewall” acts as the functional core of the appliance ensuring that you can segment the wireless network for employees and guest. Using this technology, the administrator is able to create a “roaming profile” for every user in the Wireless LAN. Also, he can define access to the wired LANs and extranet servers/DMZ based on user identity.

Cyberoam incorporates integration with various directory services like the Active Directory, LDAP and RADIUS to ensure that its “identity based firewall” does not hamper the flexibility with which businesses are run. Moreover, it includes flexible modes of authentication like the “Single Sign On” to have users identify themselves to the appliance transparently.

Cyberoam has a Wireless IDS/IPS system which can identify rogue Access points on the LAN and prevent “man in the middle” attacks. This can also detect ad hoc networks and other possible violators of the enterprise Wireless security policy. With an integrated IPS system, identity-based alerts and reports are generated every time DoS/DDoS attack, malicious code transmission, backdoor activity or blended threats occur due to the wireless user activities.

Cyberoam’s identity based content filter ensures that the Wireless users are compliant with the organization’s Internet Access Policy. It also takes application filtering into consideration. The “application filter” can recognize various bandwidth hungry applications and prevent the users from accessing that.
Conclusion
Cyberoam UTM offers high performance, layer 8 based security over WLAN networks in order to secure wireless network to the same extent as wired networks. Cyberoam offers strong user authentication, Internet access controls and reports with an identity approach and offers a separate Guest and Employee Network Access. With this, it has the ability to trace user specific activities while reducing the risk of information theft and liability of Cyberoam terrorism attacks.