wIPS Policy Alarm Encyclopedia

Security IDS/IPS Overview

The addition of WLANs to the corporate environment introduces a new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. Rogue access points installed by employees for their personal use usually do not adhere to the corporate security policy. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured and unconfigured access points and DoS (Denial of Service) attacks.

The Cisco Wireless IPS (wIPS) is designed to help manage against security threats by validating proper security configurations and detecting possible intrusions. With the comprehensive suite of security monitoring technologies, the wIPS alerts the user on more than 100 different threat conditions in the following categories:

- User authentication and traffic encryption
- Rogue and ad-hoc mode devices
- Configuration vulnerabilities
- Intrusion detection on security penetration
- Intrusion detection on DoS attacks
- Performance Violation

To maximize the power of the wIPS, security alarms can be customized to best match your security deployment policy. For example, if your WLAN deployment includes access points made by a specific vendor, the product can be customized to generate the rogue access point alarm when an access point made by another vendor is detected by the access point or sensor.

User Authentication and Encryption

The first line of defense for WLAN security is user authentication and wireless traffic encryption. Centralized WLAN user authentication based on the IEEE 802.1x standard with a RADIUS server at the back-end is a flexible and strong mechanism. Other authentication methods such as VPN may also be used to achieve the same goals.

User authentication blocks out unauthorized access to the wired and wireless resources. Traffic encryption goes hand-in-hand with user authentication during which the encryption secrets are exchanged between AP and authorized users. Traffic encryption prevents intruders from eavesdropping into the wireless traffic. Cisco wIPS validates your WLAN security deployment by monitoring on the authentication transactions and traffic encryption methods against the specified security deployment policy, which Cisco wIPS learns from the policy configuration. For example, the Cisco wIPS generates the **Device unprotected by PEAP** alarm if the **802.1x EAP** type-**PEAP** is the enterprise standardized authentication protocol. Common security violations in this category (authentication and encryption) include mis-configurations, out-of-date software/firmware, and suboptimal choice of corporate security policy. Cisco wIPS alerts the administrator on these issues and provides counter measures.

User Authentication and Encryption includes the following two subcategories:

Static WEP Encryption

Static WEP encryption was specified in the IEEE 802.11 standard in 1999. For security sensitive WLAN deployments, other alternatives such as WPA (Wireless Protected Access - TKIP and 802.1x) and 802.11i exist to address the encryption tasks.

Statistics show that more than 50 percent of WLANs do not implement any encryption method. Even with the potential vulnerability of static WEP, it is still safer than no encryption at all. If you decide to use static WEP, there are ways to keep it as secure as WEP can provide. Cisco wIPS assists you in accomplishing this goal by monitoring on static WEP usage and identifying security holes such as crackable WEP key usage, shared-key authentication, and detecting devices that do not use WEP.

Static WEP Encryption include the following types:

AP with Encryption Disabled

Alarm Description and Possible Causes

Cisco wIPS alerts the administrator on any AP operating without any WLAN layer 2 data encryption mechanisms such as **WEP, TKIP,** or **AES**. **VPN** technologies at layer three and above are the most commonly used alternative to the WLAN layer 2 data encryption mechanisms . If neither of the encryption mechanisms are used, data exchanged between an AP and its client stations is subject to eavesdropping by intruders. For an AP that is operating without any sort of encryption mechanism, there can be unauthorized clients without encryption keys that can associate with the AP and obtain access to the enterprise wired network. This puts at risk not only the user data privacy but also exposes the corporate wired network access. This alarm may be turned off for the enterprise guest WLAN network or for hot spot deployments where encryption is not required. You can turn on the Publicly Secure Packet Forwarding (**PSPF**-term generally used by Cisco Aironet access points. Other vendors may call this differently) alarm to protect your wireless network operating without any encryption. **PSPF** is a feature implemented on the WLAN Access Points to block wireless clients from communicating with other wireless clients. PSPF protects public networks by prohibiting wireless traffic between wireless clients.

wIPS Solution

Cisco wIPS detects wireless clients communicating with other wireless clients and alerts the administrator on a possible Publicly Secure Packet Forwarding (PSPF) violation. For most WLAN environments, the wireless clients mostly communicate only with devices such as web servers on the wired network. Enabling the PSPF feature on an Access Point, the administrator can protect wireless clients from being hacked by another wireless intruder. PSPF is very effective when implemented at wireless public networks (hotspots) such as airports, hotels, coffee shops, college campuses, etc. where there is no authentication and any one can associate with the APs. PSPF prevents client devices from inadvertently sharing files with other client devices on the wireless network.

Client with Encryption Disabled

Alarm Description and Possible Causes

Cisco wIPS alerts the administrator on any client station operating without any WLAN layer 2 data encryption mechanisms such as WEP, TKIP, or AES. VPN technologies at layer three and above are the most commonly used alternative to the WLAN layer 2 data encryption mechanisms . If neither of the encryption mechanism is used, data exchanged between an AP and its client stations is subject to eavesdropping by intruders. Clients with WEP disabled put at risk their file system that may contain confidential corporate information from wireless intruders. These clients can then act as an entry point for the intruders into the corporate network. This alarm may be turned off for the enterprise guest WLAN network or for hot spot deployments where encryption is generally not required. It is advisable to turn on the PSPF (Publicly Secure Packet Forwarding-term generally used by Cisco Aironet access points. Other vendors may call this differently) alarm to protect your wireless network operating without any encryption. PSPF is a feature implemented on the WLAN Access Points to block wireless clients from communicating with other wireless clients.

wIPS Solution

Cisco wIPS detects wireless clients communicating with other wireless clients and alerts the administrator on a possible PSPF violation. For most WLAN environments, the wireless clients mostly communicate only with devices such as web servers on the wired network. Enabling the PSPF feature on an Access Point, the administrator can protect wireless clients from being hacked by another wireless intruder. PSPF is very effective when implemented at wireless public networks (hotspots) such as airports, hotels, coffee shops, college campuses, etc. where there is no authentication and any one can associate with the APs. PSPF prevents client devices from inadvertently sharing files with other client devices on the wireless network.

Crackable WEP IV key used

Alarm Description and Possible Causes

WLAN devices using static WEP key for encryption are vulnerable to WEP key cracking attack. The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key which is in 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key specified by the user concatenated with the 24-bit IV (Initialization Vector). The IV that is determined by the transmitting station can be reused frequently or in consecutive frames, thus increasing the possibility of the secret key to be recovered by wireless intruders. By excluding certain IV values that would create "weak keys," the weakness of WEP is avoided.

wIPS Solution

Cisco wIPS alerts on weak WEP implementations and recommends a device firmware upgrade if available from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN networks can protect against WEP vulnerability by using the Temporal Key Integrity Protocol (TKIP) encryption mechanism,

which is supported by most enterprise level wireless equipment. TKIP enabled devices are not subject to any WEP key attacks.

Device Using Open Authentication

Alarm Description and Possible Causes

802.11 Open Authentication (as opposed to Shared-key authentication) is widely used today in conjunction with a higher level authentication protocol such as 802.1x to secure a WLAN. In some deployments, Shared-key Authentication is used instead of Open Authentication where a static WEP key is used to challenge client stations attempting to associate with the AP. Open Authentication on the other hand accepts associations from any client and there is no verification of the identity of the client. Shared-key authentication appears to be more secure but has been proven to be vulnerable to WEP key cracking by wireless intruders because the challenge text and response are both clear and unencrypted.

wIPS Solution

It is always recommended to use 802.11 Open Authentication with some higher level authentication mechanisms such as the 802.1x/EAP framework or VPN. In case your deployment chooses to use Shared-key Authentication or something other than Open Authentication, you can enable this alarm . Cisco wIPS alerts you on any device that violates the deployment policy of not using Open Authentication.

Device Using Shared Key Authentication

Alarm Description and Possible Causes

The IEEE 802.11 standard designed the Shared-key Authentication protocol to work with static WEP key encryption to lock out unauthorized WLAN devices from associating with an AP or ad-hoc station. The Shared key authentication uses a standard challenge and response approach for authentication between the 802.11 client and the access point. The challenge text is unencrypted and in clear text. The algorithm (not the shared secret key) for the challenge response is standard and public knowledge. It has been proven that shared key authentication can be easily exploited through a passive attack by eavesdropping. An attacker can use brute force to compute the challenge response off-line after capturing challenge text, which is in clear text. Once the match is found, the attacker has acquired the shared secret key.

wIPS Solution

Cisco wIPS detects the use of Shared Key Authentication and advises alternatives. Many enterprises today deploy 802.11 WLANs using Open Authentication instead of Shared Key Authentication with a higher level authentication mechanism provided by 802.1x and EAP methods such as LEAP, PEAP and TLS .

WEP IV Key Reused

Alarm Description and Possible Causes

The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key which in most cases is 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key specified by the user concatenated with the 24-bit IV (Initialization Vector). The IV that is determined by the transmitting station can be reused frequently in consecutive frames, thus increasing the possibility of the secret key to be recovered by wireless intruders.

wIPS Solution

Cisco wIPS alerts on weak WEP implementations and recommends a device firmware upgrade if available from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN networks can protect against WEP vulnerability by using the Temporal Key Integrity Protocol (TKIP) encryption mechanism,

which is now supported by most enterprise level wireless equipment. TKIP enabled devices are not subject to any such WEP key attacks.

WPA and 802.11i

The Wi-Fi published Wireless Protected Access (**WPA**) specification identifies a feature subset of the IEEE **802.11i** standard. WPA is one of the answers to the well publicized vulnerability of static WEP as specified by the original IEEE 802.11 specification. Most wireless vendors supports **WPA** and consider it to be a more secure alternative to static **WEP**.

There are three major end user benefits provided by the **WPA** products:

- **802.1x** allows user based authentication instead of the vulnerable global encryption key method.
- Temporal Key Integrity Protocol (**TKIP**) enhances industrial strength encryption with dynamic keying.
- Pre-shared Master Key (**PMK**) offers small and medium size deployment to use **802.1x** and **TKIP** without complex infrastructure back-end servers such as **RADIUS**

The wIPS server monitors **WPA** transactions and alerts the administrator when it detects non-compliant devices and weak configurations.

WPA and 802.11i include the following types:

Device Unprotected by EAP-TTLS

Alarm Description and Possible Causes

The Extensible Authentication Protocol (EAP) is a basic security framework which provides a means for improving the encryption of 802.11 transactions. This framework can be paired with a wide variety of different types of authentication mechanisms, including a version known as Tunneled Transport Layer Security (TTLS). EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends Transport Layer Security (TLS). EAP-TTLS provides security that is as strong as EAP-TLS but doesn't require the clients to be issued certificates. User authentication is still performed via passwords, but the credentials are tunneled. Devices configured to use the EAP protocol but not the TTLS authentication mechanism can represent potential insecure connections to the wireless network. Although such mechanisms make it easier for end-users to get connected quickly, wireless attackers may also be able to gain access to critical corporate data . EAP exchanges that are not secured by TTLS authentication can be easier for attackers to intercept and decode, potentially resulting in sensitive leakage of data sent from a valid user.

wIPS Solution

Cisco wIPS monitors EAP transactions to detect any devices that are not implementing the EAP-TTLS mechanism and triggers an alarm to notify administrators of the vulnerability. The alarm text provided on the AirWISE screen will identify the problematic device as well as the alternative authentication mechanism in use. It is recommended that IT personnel locate the device triggering the alarm and configure it to use the EAP-TTLS mechanism.

Device Unprotected by 802.1X

Alarm Description and Possible Causes

If your WLAN security deployment requires the use of 802.1x for authentication and encryption, Cisco wIPS alerts you on devices that are not configured to use 802.1x protection. Wireless Protected Access (**WPA**) specified 802.1x as one of the requirements. The 802.1x framework provides centralized user authentication

and encryption key management. The 802.1x is used with a variety of Extensible Authentication Protocol (**EAP**) types such as Lightweight Extensible Authentication Protocol(**LEAP**),Transport Layer Security(**TLS**),Tunneled Transport Layer Security(**TTLS**), Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (**EAP-FAST**) and Protected Extensible Authentication Protocol (**PEAP**) to implement an authentication and encryption mechanism. If your WLAN security relies on WPA or 802.1x, APs not configured for 802.1x weaken your WLAN security by allowing non-compliant users to falsely authenticate and enter your wired network. Mis-configured client stations without 802.1x protection also introduce security risks. For example, it would not have the mutual authentication mechanism provided by 802.1x framework and therefore be vulnerable to accidentally associate with an intruder's fake AP.

wIPS Solution

Cisco wIPS recognizes all 802.1x **EAP** types including **PEAP, TLS, TTLS, LEAP, EAP-FAST**, Cisco wIPS detects APs and client stations unprotected by 802.1x by observing rejected 802.1x authentication challenges.

Device Unprotected by any Selected Authentication Methods

Alarm Description and Possible Causes

Cisco wIPS monitors on 802.1x transactions and their specific Extensible Authentication Protocol (EAP) methods. When a specific EAP method is not used, Cisco wIPS will trigger an alarm. Cisco wIPS supports the following EAP methods for this alarm:

- Leap - This is a proprietary EAP method developed by Cisco. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys and configurable WEP session key time out.
- PEAP - The Protected Extensible Authentication Protocol, is also known as Protected EAP. It is a protocol that encapsulates EAP within a potentially encrypted and authenticated Transport Layer Security (TLS) tunnel.
- EAP-TLS - EAP-Transport Layer Security (EAP-TLS). The EAP-TLS mechanism provides additional security over standard shared-key password authentication sessions by creating a new key on a per-session basis.
- EAP-TTLS - EAP-Tunneled Transport Layer Security (EAP-TTLS) is an EAP protocol that extends TLS. EAP-TTLS provides security that is as strong as EAP-TLS but doesn't require the clients to be issued certificates. User authentication is still performed via passwords, but the credentials are tunneled.
- EAP-FAST - Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials.
- EAP-MD5 - This is a password based authentication method that offers minimal security. EAP-MD5 differs from other EAP methods by providing authentication of the EAP peer to the EAP server but not the mutual authentication.

wIPS Solution

Cisco wIPS monitors EAP transactions to detect any devices that are not implementing the enabled authentication methods and triggers an alarm to notify administrators of the vulnerability. The alarm text provided on the AirWISE screen will identify the problematic device. It is recommended that IT personnel locate the device triggering the alarm and configure it to use the correct authentication method.

802.1 X Unencrypted Broadcast or Multicast

Alarm Description and Possible Causes

802.1x has a framework allowing a system to use per-session encryption keys to defend against the weakness inherited from the global static WEP key mechanism. 802.1x provide per-session encryption keys and also facilitates the session key rotation mechanism there by ensuring that the encryption keys are updated periodically. This enhances security by eliminating the use of static encryption keys and preventing attacks that require the collection of large amounts of data encrypted with a single static key. For multicast and broadcast packets, where there are multiple recipients, per-session encryption key cannot be applied. In order to secure multicast and broadcast communication, a shared encryption key and re-key mechanism has to be implemented. It has been found that very few wireless devices implement the multicast and broadcast encryption key mechanism correctly. In reality, multicast and broadcast packets are not encrypted. To make matters more complicated, enterprise grade APs with multiple SSIDs are frequently deployed with 802.1x security for one SSID (corporate WLAN) and no encryption for another SSID (guest WLAN). This deployment scenario is usually coupled with the VLAN configuration so that client devices using the guest SSID can only access the Internet but not the corporate wired network. An AP supporting multiple SSIDs transmits broadcast and multicast frames thus making the encryption option selection (802.1x or no encryption) , an implementation challenge.

wIPS Solution

Cisco wIPS detects unencrypted multicast and broadcast frames caused by mis-configuration or vendor implementation errors. Cisco recommends that the user should use APs that implement the encryption of multicast and broadcast frames in a proper manner.

802.1 X Rekey Timeout Too Long

Alarm Description and Possible Causes

A cracked WEP secret key results in no encryption protection so, data privacy will have to be compromised. Dynamic encryption key or key rotation mechanisms such as Temporal Key Integrity Protocol (TKIP) resolves such vulnerabilities by periodically changing the encryption key even within a single session. Managing key rotation for multicast and broadcast traffic is challenging technically because multiple devices have to update to the new key synchronously. Vendors' implementations of multicast or broadcast key rotation varies from null to complete. When the multicast and broadcast key is not rotated or rotated infrequently, it is as weak as static WEP, which is subject to key recovery attacks. By continuously monitoring on the WLAN 802.1x authentication and encryption transactions, Cisco wIPS can detect an AP configured without encryption key rotation or configured with a long key rotation timeout. It is important for WLAN 802.1x configurations to include a reasonable encryption rekey timeout . A staled encryption key makes your encryption static and as vulnerable as static WEP key encryption. A rekey mechanism should be applied to unicast, multicast, and broadcast data streams. TKIP enabled devices implement a WEP key hashing algorithm and typically rotate keys on their unicast data streams but not always on the multicast or broadcast data streams.

wIPS Solution

This Cisco wIPS alarm assists you in enforcing rekey mechanism for all data streams. Take appropriate steps including the checking of the AP configuration for this setting to tackle the issue.

Device Not Protected by EAP-TLS

Alarm Description and Possible Causes

The Extensible Authentication Protocol (EAP) is a basic security framework which provides a means for improving the encryption of 802.11 transactions. This framework can be paired with a wide variety of different types of authentication mechanisms, including a version known as Transport Layer Security (TLS), a certificate-based protocol. The EAP-TLS mechanism provides additional security over standard shared-key password authentication sessions by creating a new key on a per-session basis. This means that every active connection to an AP utilizing EAP-TLS authentication creates a new shared key specific to that connection. This makes the protocol significantly stronger than the standard shared-key mechanisms against wireless attackers. Devices configured to use the EAP protocol and not the TLS authentication mechanism, can represent potential insecure connections to the wireless network. There are a number of alternative mechanisms that may be used (such as EAP-TTLS or EAP-FAST) which generally provide greater convenience than EAP-TLS at the cost of reduced security for the network. Although such mechanisms make it easier for end-users to get connected quickly, wireless attackers may also be able to gain access to critical corporate data. EAP exchanges that are not secured by TLS authentication can be easier for attackers to intercept and decode, resulting in sensitive data leakage sent from a valid user.

wIPS Solution

Cisco wIPS monitors EAP transactions to detect devices that are not implementing the TLS mechanism and triggers an alarm to notify administrators of the vulnerability. The alarm text provided on the AirWISE screen will identify the problematic device as well as the alternative authentication mechanism in use. It is recommended that IT personnel locate the device triggering the alarm and configure it to use the EAP-TLS mechanism.

Device Unprotected by IEEE 802.11i/AES

Alarm Description and Possible Causes

The new 802.11i standard provides three critical network security capabilities:- authentication and privacy. Cisco wIPS alerts on detecting devices that are not using the IEEE 802.11i standard. Devices that are not using this security standard could be vulnerable to various attacks, compromising the enterprise network's security. When the IEEE 802.11 standard was ratified it suggested the implementation of the 64-bit WEP key as a security standard. Later it was increased to 128 bit keys. Some implementations were using upto 256 bit WEP keys. Since then, Static WEP has been proved to be flawed with respect to authentication, encryption and integrity checks. Soon the Wi-Fi alliance realized the importance of having an alternative to the WEP standard. The IEEE 802.11i standard was introduced to mitigate all the security issues that have been plaguing the wireless networks in the enterprise environment. This standard creates Robust Secure Networks (RSN). As the 802.11i standard would not be ratified in time, the Wi-FI Alliance created a subset of the IEEE 802.11i standard called Wi-Fi Protected Access (WPA).WPA/802.11i implements 802.1x for user authentication and key distribution. 802.1x is used with a variety of**EAP** (Extensible Authentication Protocol) types such as **LEAP, TLS, TTLS, EAP-FAST** and **PEAP** to implement an authentication and encryption mechanism. The IEEE 802.11i standard leaves it upto the user to select the authentication scheme.

The IEEE 802.11i standard provides a pre-shared key (PSK) mechanism and the 802.1x-server based key management schemes. The server based mechanism requires an authentication server such as a RADIUS server to securely and dynamically distribute session keys (Pairwise Master Key or PMK). When PSK is used instead of 802.1x, the passphrase PSK is converted via a formula into a 256-bit value needed for the PMK. In the PSK mode, the 802.11i defined 4-way handshake is used for encryption key management, with no EAP exchange. As there is no RADIUS server and no EAP methods (EAP-TLS, LEAP) involved, the PSK mode is less secure. There are two encryption standards defined in the IEEE 802.11i standard- Temporal Key

Integrity Protocol (TKIP) and Advanced Encryption Standard-Counter Mode-CBC MAC Protocol. WLAN traffic encrypted with TKIP and MIC defeats packet forgery, and replay attack. TKIP is most importantly immune to the weakness introduced by a static WEP key and attacks stemming from key reuses. Along with MIC, TKIP also provides per packet key mixing which helps prevent many keystream attacks.

The implementation of AES-CCMP is mandatory for the IEEE 802.11i standard. The IEEE standard supports only the 128-bit AES. As AES is supposed to work on 128-bit blocks, CCMP provides the padding necessary to increase the bit size for the data block. This padding is added before encryption and is discarded after the decryption. AES-CCMP mode provides authentication and encryption using the AES block cipher. CCMP is a combination of the Counter (CTR) mode encryption for data privacy, and Cipher Block Chaining Message Authentication Code (CBC-MAC) authentication, for an authenticate-and-encrypt security process for each data block processed. CCMP computes the CBC-MAC over the IEEE 802.11 header length, selected parts of the IEEE 802.11 MAC Payload Data Unit (MPDU) header, and the plaintext MPDU data, whereas the old IEEE 802.11 WEP mechanism provided no protection to the MPDU header. Second, both CCMP encryption and decryption use only the forward AES block cipher function leading to significant savings in code and hardware size.

wIPS Solution

Cisco wIPS detects devices that are not using the IEEE 802.11i standard and compromising the security of the wireless network. Cisco wIPS recommends the user to take the appropriate steps to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard. Once such device is identified and reported by Cisco wIPS, the WLAN administrator may use the device locator feature provided on the Cisco wIPS Console to locate the device if it is a rogue device. Known devices can be marked as Monitored node and then located using the Triangulation feature.

Device Unprotected By EAP-FAST

Alarm Description and Possible Causes

Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol which will stop these dictionary attacks. EAP-FAST helps prevent Man-in-the-middle attacks, dictionary attacks, packet and authentication forgery attacks. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials. Some of the major advantages of EAP-FAST are that it is not proprietary, is compliant with the IEEE 802.11i standard, supports TKIP and WPA, does not use certificates thus avoiding complex PKI infrastructures and supports multiple Operating Systems on the PCs and the Pocket PCs.

wIPS Solution

Cisco wIPS alerts the wireless administrator on devices that are using the 802.1x authentication mechanism but are not using the EAP-FAST protocol. It is recommended that EAP-FAST be implemented in the wireless environment.

Device Unprotected by PEAP

Alarm Description and Possible Causes

Cisco wIPS monitors on **802.1x** transactions and their specific Extensible Authentication Protocol (**EAP**) types. By adopting Protected EAP (**PEAP**) as your authentication method, your 802.1x security authentication protocol will be further wrapped and protected by TLS (Transport Layer Security). EAP methods running within PEAP are provided with built-in advantages on the following:

- Identity protection

- Dictionary attack resistance
- Protected negotiation from replay attack
- Header protection
- Protected termination from packet spoofing, flooding, and denial-of-service attack
- Fragmentation and re-assembly
- Fast reconnect
- Proven and method independent key management

Many WLAN equipment vendors including Cisco have recently added support for PEAP with a firmware upgrade.

wIPS Solution

This Cisco wIPS alarm alerts you on devices that are not using Protected Extensible Authentication Protocol (**PEAP**). Ensure that the PEAP authentication method is implemented on various devices in the wireless environment.

Device Unprotected by TKIP

Alarm Description and Possible Causes

The latest **IEEE 802.11i** standard includes Temporal Key Integrity Protocol (**TKIP**) and Message Integrity Checksum(**MIC**) as one of the recommended data privacy protocols. WiFi Alliance also recommends **TKIP** and **MIC** in its (Wireless Protected Access (**WPA**) specification. WLAN traffic encrypted with **TKIP** and **MIC** defeats packet forgery, and replay attack. **TKIP** is immune to the weakness introduced by a static WEP key and attacks stemming from key reuses. Along with **MIC, TKIP** also provides per packet key mixing which helps prevent many keystream attacks. Unlike **AES** based **CCMP** encryption, TKIP typically does not require a hardware upgrade. Many WLAN equipment vendors including Cisco have added TKIP and MIC support in their latest firmware and driver.

wIPS Solution

Cisco wIPS detects WLAN traffic that is not protected by TKIP encryption and raises an alarm for attention. Cisco wIPS advises updating these devices to the latest firmware and re-configuring them to include TKIP encryption.

WPA or 802.11i Pre-Shared Key Used

Alarm Description and Possible Causes

WPA and the **802.11i** standard provide a pre-shared key (**PSK**) mechanism as an alternative to using the IEEE 802.1x-based key establishment. 802.1x-based key management requires an authentication server such as a **RADIUS** server to securely and dynamically distribute session keys (Pairwise Master Key or **PMK**). When **PSK** is used instead of 802.1x, the passphrase **PSK** is converted via a formula into a 256-bit value needed for the Pairwise Master Key. In the **PSK** mode, the 802.11i defined 4-way handshake is used for encryption key management, with no **EAP** exchange. As there is no **RADIUS** server and no **EAP** methods (EAP-TLS, LEAP) involved, the PSK mode is less secure. **PSK** is used to eliminate the need to set up an authentication server (RADIUS) but at the cost of reduced security. The 802.11i specification specifies that security can be considered weak if the pass phrase is less than 20 characters as it can be easily broken via an off-line dictionary attack once the 4-way handshake is captured. The problem is that vendors do not provide any easy-to-use tool that can generate and manage 20 character passphrases.

wIPS Solution

Cisco wIPS detects the use of the pre-shared key (**PSK**) mode and recommends switching to the more secure 802.1x EAP based key management and authentication system. If you decide to stay with **PSK** mode key management, please make sure your choice of the pass phrase is longer than 20 characters and does not comprise of words from a dictionary, thus preventing possible attacks.

Intrusion Detection—Denial of Service Attack

Wireless DoS (denial of service) attacks aim to disrupt wireless services by taking advantage of various vulnerabilities of WLAN at Layer one and two. DoS attacks may target the physical RF environment, access points, client stations, or the back-end authentication RADIUS servers. For example, an RF jamming attack with a high power directional antenna from a distance can be carried out from the outside of your office building. Attack tools used by intruders leverage hacking techniques such as spoofed 802.11 management frames, spoofed 802.1x authentication frames, or simply using the brute force packet flooding method.

The nature and protocol standards for wireless are subject to some of these attacks. Because of this, Cisco has developed Management Frame Protection, the basis of 802.11i, to proactively prevent many of these attacks. (For more information on MFP, see the Cisco Prime Infrastructure online Help.) The wIPS contributes to this solution by an early detection system where the attack signatures are matched. The DoS of the wIPS detection focuses on WLAN layer one (physical layer) and two (data link layer, 802.11, 802.1x). When strong WLAN authentication and encryption mechanisms are used, higher layer (IP layer and above) DoS attacks are difficult to execute. The wIPS server tightens your WLAN defense by validating strong authentication and encryption policies. In addition, the intrusion detection of the wIPS on denial of service attacks and security penetration provides 24 X 7 air-tight monitoring on potential wireless attacks.

Denial of service attacks include the following three subcategories:

- Denial of Service Attack Against Access Points, on page 11
- Denial of Service Attack Against Infrastructure, on page 16
- Denial of Service Attacks Against Client Station, on page 20

Denial of Service Attack Against Access Points

DoS attacks against access points are typically carried out on the basis of the following assumptions:

- Access points have limited resources. For example, the per-client association state table.
- WLAN management frames and authentication protocols 802.11 and 802.1x have no encryption mechanisms.

Wireless intruders can exhaust access point resources, most importantly the client association table, by emulating large number of wireless clients with spoofed MAC addresses. Each one of these emulated clients attempts association and authentication with the target access point but leaves the protocol transaction mid-way. When the access points resources and the client association table is filled up with these emulated clients and their incomplete authentication states, legitimate clients can no longer be serviced by the attacked access point. This creates a denial of service attack.

The wIPS tracks the client authentication process and identifies DoS attack signatures against the access point. Incomplete authentication and association transactions trigger the attack detection and statistical signature

matching process. Detected DoS attack results in setting off wIPS alarms, which includes the usual alarm detail description and target device information.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, see the Prime Infrastructure online Help.

DoS attacks against access points include the following types:

Alarm Description and Possible Causes

A form of DoS (denial-of-service) attack is to exhaust the access point's resources, particularly the client association table, by flooding the access point with a large number of emulated and spoofed client associations. At the 802.11 layer, Shared-key authentication is flawed and rarely used. The other alternative is Open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker leveraging such a vulnerability can emulate a large number of clients to flood a target access point's client association table by creating many clients reaching State 3 as illustrated below. Once the client association table overflows, legitimate clients are not able to get associated thus a denial-of-serve attack is committed.

wIPS Solution

The Cisco Adaptive Wireless IPS detects spoofed MAC addresses and tracks the follow-up 802.1x actions and data communication after a successful client association to detect this form of DoS attack. After this attack is reported by the Cisco Adaptive Wireless IPS, you may log on to this access point to inspect its association table for the number of client associations.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, refer to the Cisco Prime Infrastructure Configuration Guide or the Online help.

-

Denial of Service Attack: Association Table Overflow

Alarm Description and Possible Causes

Wireless intruders can exhaust access point resources, most importantly the client association table, by imitating a large number of wireless clients with spoofed MAC addresses. Each one of these imitated clients attempts association and authentication with the target access point. The 802.11 authentication typically completes because most deployments use 802.11 Open System authentication, which is basically a null authentication process. Association with these imitated clients follows the authentication process. These imitated clients do not, however, follow up with higher level authentication such as 802.1x or VPN, which would leave the protocol transaction half-finished. At this point, the attacked access point maintains a state in the client association table for each imitated client. Once the access point's resources and client association table is filled with these imitated clients and their state information, legitimate clients can no longer be serviced by the attacked access point. This creates a DoS (denial of service) attack.

wIPS Solution

The Cisco Adaptive Wireless IPS tracks the client authentication process and identifies a DoS attack signature against an access point. Incomplete authentication and association transaction trigger the Cisco Adaptive Wireless IPS's attack detection and statistical signature matching process.

Denial of Service Attack: Authentication Flood

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement such a state machine according to the IEEE standard (see illustration below). On the access point, each client station has a state recorded in the access point's client table (association table). This recorded state has a size limit that can either be a hard-coded number or a number based on the physical memory constraint.

A form of DoS (denial-of-service) attack floods the access point's client state table (association table) by imitating many client stations (MAC address spoofing) sending authentication requests to the access point. Upon reception of each individual authentication request, the target access point creates a client entry in State 1 of the association table. If Open System authentication is used for the access point, the access point returns an *authentication success* frame and moves the client to State 2. If Shared-key authentication is used for the access point, the access point sends an *authentication challenge* to the attacker's imitated client which does not respond. In this case, the access point keeps the client in State 1. In either case, the access point contains multiple clients hanging in either State 1 or State 2 which fills up the access point association table. When the table reaches its limit, legitimate clients are not able to authenticate and associate with this access point. This results in a DoS attack.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form a DoS attack by tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log on to the access point to check the current association table status.

Denial of Service Attack: EAPOL-Start Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP (Extensible Authentication Protocol) over LANs, or EAPOL. The 802.1x protocol starts with a EAPOL-Start frame sent by the client station to begin the authentication transaction. The access point responds to an EAPOL-Start frame with a EAP-Identity-Request and some internal resource allocation.

An attacker attempts to bring down an access point by flooding it with EAPOL-Start frames to exhaust the access point internal resources.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS (denial-of-service) attack by tracking the 802.1x authentication state transition and particular attack signature.

Denial of Service Attack: PS Poll Flood Attack

Alarm Description and Possible Causes

Power management is probably one of the most critical features of wireless LAN devices. Power management helps to conserve power by enabling stations to remain in power saving state mode for longer periods of time and to receive data from the access point only at specified intervals. The wireless client device must inform the access point of the length of time that it will be in the sleep mode (power save mode). At the end of the time period, the client wakes up and checks for waiting data frames. After it completes a handshake with the access point, it receives the data frames. The beacons from the access point also include the Delivery Traffic Indication Map (DTIM) to inform the client when it needs to wake up to accept multicast traffic.

The access point continues to buffer data frames for the sleeping wireless clients. Using the Traffic Indication Map (TIM), the access point notifies the wireless client that it has buffered data buffered. Multicast frames are sent after the beacon that announces the DTIM.

The client requests the delivery of the buffered frames using PS-Poll frames to the access point. For every PS-Poll frame, the access point responds with a data frame. If there are more frames buffered for the wireless client, the access point sets the data bit in the frame response. The client then sends another PS-Poll frame to get the next data frame. This process continues until all the buffered data frames are received.

A potential hacker could spoof the MAC address of the wireless client and send out a flood of PS-Poll frames. The access point then sends out the buffered data frames to the wireless client. In reality, the client could be in the power safe mode and would miss the data frames.

wIPS Solution

The Cisco Adaptive Wireless IPS can detect this DoS (denial-of-service) attack that can cause the wireless client to lose legitimate data. Locate the device and take appropriate steps to remove it from the wireless environment. Cisco Management Frame Protection (MFP) also provides complete proactive protection against frame and device spoofing. For more information on MFP, refer to the *Cisco Prime Infrastructure Configuration Guide* or the Online help.

Denial of Service Attack: Probe Request Flood

Alarm Description and Possible Causes

A form of Denial of Service attack allows the attacker to force the target AP into a constant stream of wireless packets intended to serve nonexistent clients. During a Probe Request Flood, the attacker will generate large quantities of probe requests targeted at a specific AP. Typical wireless design specifies that an AP will respond to a probe request by sending a probe response, which contains information about the corporate network. Due to the volume of probe requests transmitted during a flood attack, the AP will be stuck continuously responding, thus resulting in a denial of service for all clients depending on that AP.

wIPS Solution

The wIPS server monitors the levels of probe request frames detected and will trigger a Probe Request Flood alarm when the threshold is exceeded. Even in cases where the requests are valid, the volume of the frames could cause problems with wireless activity. Consequently, the source(s) of the offending frames should be located and removed from the enterprise environment.

Denial of Service Attack: Re-association Request Flood

Alarm Description and Possible Causes

A form of Denial-of-service attack is to exhaust the AP's resources, particularly the client association table, by flooding the AP with a large number of emulated and spoofed client re-associations. At the 802.11 layer, Shared-key authentication is flawed and rarely used any more. The only other alternative is Open authentication (null authentication) that relies on higher level authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker leveraging such a vulnerability can emulate a large number of clients to flood a target AP's client association table by creating many clients reaching State 3 as illustrated below. Once the client association table overflows, legitimate clients will not be able to get associated thus a denial-of-serve attack is committed.

wIPS Solution

The wIPS server monitors the levels of re-association requests on the network and triggers this alarm if the threshold is exceeded.

Denial of Service Attack: Unauthenticated Association

Alarm Description and Possible Causes

A form of DoS (denial-of-service) attack is to exhaust the access point's resources, particularly the client association table, by flooding the access point with a large number of imitated and spoofed client associations. At the 802.11 layer, Shared-key authentication is flawed and rarely used. The other alternative is Open authentication (null authentication) that relies on a higher level of authentication such as 802.1x or VPN. Open authentication allows any client to authenticate and then associate. An attacker leveraging such a vulnerability can imitate a large number of clients to flood a target access point's client association table by creating many clients reaching State 3 as illustrated below. Once the client association table overflows, legitimate clients are not able to get associated causing a DoS attack.

wIPS Solution

Denial of Service (DoS) attacks are unique in that most ways to contain them will not work. Unauthenticated Association Attack is no different. You have an attacker that is randomly generating hundreds if not thousands of MAC addresses and crafting those as Association frames and sending them as fast as possible to the target Access Point. Wireless containment on this type of attack is clearly not possible. What are your options?

Locating the source of the attack is your best option

- Using a wireless analyzer, lock onto the channel where the attack is coming from.

- Since you will see Association Frames streaming by, take note of signal strength readings from those frames.
- Using these signal strength numbers, try to locate the source of the attack by walking around the area where you think the attack is being generated from.

Denial of Service Attack Against Infrastructure

In addition to attacking access points or client stations, the wireless intruder may target the RF spectrum or the back-end authentication RADIUS server for DoS (denial of service) attacks. The RF spectrum can be easily disrupted by injecting RF noise generated by a high power antenna from a distance. Back-end RADIUS servers can be overloaded by a DDoS (distributed denial of service) attack where multiple wireless attackers flood the RADIUS server with authentication requests. This attack does not require a successful authentication to perform the attack.

DoS attacks against infrastructure include the following types:

Denial of Service Attack: Beacon Flood

Alarm Description and Possible Causes

A form of Denial of Service attack allows an attacker to inhibit wireless activity for the entire enterprise infrastructure by preventing new associations between valid APs and stations. Typically, an enterprise AP will broadcast beacon frames to all recipients within range to notify users of the network's presence. Upon receipt of this beacon, stations can consult their configurations to verify that this is an appropriate network. During a beacon flood attack, stations that are actively seeking a network are bombarded with beacons from networks generated using different MAC addresses and SSIDs. This flood can prevent the valid client from detecting the beacons sent by the corporate APs, and thus a denial of service attack is initiated.

wIPS Solution

The wIPS server monitors the levels of beacon frames detected and will trigger a Beacon Flood alarm when the threshold is exceeded. Even in cases where the beacons are valid, the volume of the frames could cause problems with wireless activity. Consequently, the sources of the offending frames should be located and removed from the enterprise environment.

Denial of Service Attack: CTS Flood

Attack tool: CTS Jack

Alarm Description and Possible Causes

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (Request-To-Send/Clear-To-Send) functionality to control the station access to the RF medium. The wireless device ready for transmission sends a RTS frame in order to acquire the right to the RF medium for a specified time duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same time duration. All wireless devices observing the CTS frame should yield the media to the transmitter for transmission without contention.

A wireless denial-of-service attacker may take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back CTS frames, an attacker can force other wireless devices sharing the RF medium to hold back their transmission until the attacker stops transmitting the CTS frames.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the abuse of CTS frames for a DoS attack.

Denial of Service Attack: Destruction Attack

Alarm Description and Possible Causes

MDK3 is a suite of hacking tools that allows users to utilize a number of different security penetration methods against corporate infrastructures. MDK3-Destruction mode is a specific implementation of the suit that uses an array of the tools to effectively completely shut down a wireless deployment. During an MDK-Destruction attack, the tool simultaneously:

- Initiates a beacon flood attack, which creates fake APs within the environment,
- Triggers an authentication flood attack against valid corporate APs, preventing them from servicing clients, and kicks all active connections with valid clients.

Additional enhancements allow for the tool to be used to connect the valid clients to the fake APs generated with the beacon flood, causing further confusion in the environment.

wIPS Solution

The wIPS server monitors for the combination of symptoms of an MDK3-Destruction attack and triggers an alarm when they are detected. Due to the dramatic impact that this attack can have on a wireless deployment, it is strongly recommended that the source of the attack be identified and removed immediately in order to resume normal network operations.

Denial of Service Attack: Queensland University of Technology Exploit

Denial of Service Vulnerability in IEEE 802.11 Wireless Devices: US-CERT VU#106678 & Aus-CERT AA-2004.02

Alarm Description and Possible Causes

802.11 WLAN devices use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) as the basic access mechanism in which the WLAN device listens to the medium before starting any transmission and backs-off when it detects any existing transmission taking place. Collision avoidance combines the physical sensing mechanism and the virtual sense mechanism that includes the Network Allocation Vector (NAV), the time before which the medium is available for transmission. Clear Channel Assessment (CCA) in the DSSS protocol determines whether a WLAN channel is clear so an 802.11b device can transmit on it.

Mark Looi, Christian Wullems, Kevin Tham and Jason Smith from the Information Security Research Centre, Queensland University of Technology, Brisbane, Australia, have recently discovered a flaw in the 802.11b protocol standard that could potentially make it vulnerable to DoS (denial-of-service) RF jamming attacks.

This attack specifically attacks the CCA functionality. According to the AusCERT bulletin, "an attack against this vulnerability exploits the CCA function at the physical layer and causes all WLAN nodes within range, both clients and access points, to defer transmission of data for the duration of the attack. When under attack, the device behaves as if the channel is always busy, preventing the transmission of any data over the wireless network."

This DoS attack affects DSSS WLAN devices including IEEE 802.11, 802.11b, and low-speed (below 20Mbps) 802.11g wireless devices. IEEE 802.11a (using OFDM), high-speed (above 20Mbps using OFDM) 802.11g wireless devices are not affected by this attack. Devices that use FHSS are also not affected.

Any attacker using a PDA or a laptop equipped with a WLAN card can launch this attack on SOHO and enterprise WLANs. Switching to the 802.11a protocol is the only solution or known protection against this DoS attack.

For more information on this DoS attack refer to :

- http://www.auscert.org.au/render.html?it=4091
- http://www.qut.edu.au/institute-for-future-environments
- http://www.kb.cert.org/vuls/id/106678

wIPS Solution

The Cisco Adaptive Wireless IPS detects this DoS attack and sets off the alarm. Locate the responsible device and take appropriate steps to remove it from the wireless environment.

Denial of Service attack: RF Jamming Attack

Alarm Description and Possible Causes

Note RF Jamming Attack is a channel alarm and does not contain alarm source or destination MAC address and hence no location will be generated for such alarms.

RF Jamming Attack does not populate attacker mac address. RF jamming is an attack against a particular channel. The attacker may send thousands of frames per second to jam the channel, and the frames are sent with different MAC addresses. Hence, you do not have a unique MAC address to identify the attacker.

WLAN reliability and efficiency depend on the quality of the RF media. Each RF is susceptible to RF noise impact. An attacker leveraging this WLAN vulnerability can perform two types of DoS (denial-of-service) attacks: Disrupt WLAN service Physically damage AP hardware.

- Disrupt WLAN service —At the 2.4GHz unlicensed spectrum, the attack may be unintentional. A cordless phone, Bluetooth devices, microwave, wireless surveillance video camera, or baby monitor can all emit RF energy to disrupt WLAN service. Malicious attacks can manipulate the RF power at 2.4GHz or 5GHz spectrum with a high gain directional antenna to amplify the attack impact from a distance. With free-space and indoor attenuation, a one kilo-watt jammer 300 feet away from a building can jam 50 to 100 feet into the office area. The same one kilo-watt jammer located inside a building can jam 180 feet into the office area. During the attack, WLAN devices in the target area are out of wireless service.
- Physically damage AP hardware— An attacker using a high output transmitter with directional high gain antenna 30 yards away from an access point can pulse enough high energy RF power to damage

electronics in the access point resulting in it being permanently out of service. Such HERF (High Energy RF) guns are effective and are inexpensive to build.

wIPS Solution

Like any RF based disturbance, your best way to resolve this would be to physically locate the device that is triggering the RF Jamming alarm and take it offline. Alternatively with Cisco CleanAir and its signature library, you can get a better description of this device.

- Find out the wIPS Access Point that triggered this alarm.
- Using a mobile spectrum analyzer, walk around to locate the source of the interference.
- Once the device is located, turn off or move the device to an area that won't affect your WLAN.

Denial of Service: RTS Flood

Alarm Description and Possible Causes

As an optional feature, the IEEE 802.11 standard includes the RTS/CTS (Request-To-Send/Clear-To-Send) functionality to control access to the RF medium by stations. The wireless device ready for transmission sends an RTS frame to acquire the right to the RF medium for a specified duration. The receiver grants the right to the RF medium to the transmitter by sending a CTS frame of the same duration. All wireless devices observing the CTS frame should yield the RF medium to the transmitter for transmission without contention.

A wireless denial of service attacker may take advantage of the privilege granted to the CTS frame to reserve the RF medium for transmission. By transmitting back-to-back RTS frames with a large transmission duration text box, an attacker reserves the wireless medium and force other wireless devices sharing the RF medium to hold back their transmissions.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the abuse of RTS frames for denial-of-service attacks.

Denial of Service Attack: Virtual Carrier Attack

Alarm Description and Possible Causes

The virtual carrier-sense attack is implemented by modifying the 802.11 MAC layer implementation to allow random duration values to be sent periodically. This attack can be carried out on the ACK, data, RTS, and CTS frame types by using large duration values. By doing this the attacker can prevent channel access to legitimate users. Under normal circumstances, the only time a ACK frame carries a large duration value is when the ACK is part of a fragmented packet sequence. A data frame legitimately carries a large duration value only when it is a subframe in a fragmented packet exchange.

One approach to deal with this attack is to place a limit on the duration values accepted by nodes. Any packet containing a larger duration value is truncated to the maximum allowed value. Low cap and high cap values can be used. The low cap has a value equal to the amount of time required to send an ACK frame, plus media access backoffs for that frame. The low cap is used when the only packet that can follow the observed packet

is an ACK or CTS. This includes RTS and all management (association, etc) frames. The high cap is used when it is valid for a data packet to follow the observed frame. The limit in this case needs to include the time required to send the largest data frame, plus the media access backoffs for that frame. The high cap must be used in two places: when observing an ACK (because the ACK my be part of a MAC level fragmented packet) and when observing a CTS.

A station that receives an RTS frame also receives the data frame. The IEEE 802.11 standard specifies the exact times for the subsequent CTS and data frames. The duration value of RTS is respected until the following data frame is received or not received. Either the observed CTS is unsolicited or the observing node is a hidden terminal. If this CTS is addressed to a valid in-range station, the valid station can nullify this by sending a zero duration null function frame. If this CTS is addressed to an out-of-range station, one method of defense is to introduce authenticated CTS frames containing cryptographically signed copies of the preceding RTS. With this method, there is a possibility of overhead and feasibility issues.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this DoS (denial-of-service) attack. Locate the device and take appropriate steps to remove it from the wireless environment.

Denial of Service Attacks Against Client Station

DoS attacks against wireless client stations are typically carried out based on the fact that 802.11 management frames and 802.1x authentication protocols have no encryption mechanism and thus can be spoofed. For example, wireless intruders can disrupt the service to a client station by continuously spoofing a 802.11 disassociation or deauthentication frame from the access point to the client station.

Besides the 802.11 authentication and association state attack, there are similar attack scenarios for 802.1x authentication. For example, 802.1x EAP-Failure or EAP-logoff messages are not encrypted and can be spoofed to disrupt the 802.1x authenticated state to disrupt wireless service.

Cisco Adaptive Wireless IPS tracks the client authentication process and identifies DoS attack signatures. Incomplete authentication and association transactions trigger the attack detection and statistical signature matching process. Detected DoS attack results in setting off wIPS alarms that include the usual alarm detail description and target device information.

DoS attacks against client station include the following types:

Denial of Service Attack: Authentication Failure Attack

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this client state machine based on the IEEE standard (see illustration below). A successfully associated client station remains in State 3 in order to continue wireless communication. A client station in State 1 and in State 2 cannot participate in the WLAN data communication process until it is authenticated and associated to State 3. IEEE 802.11 defines two authentication services: Open System Authentication and Shared Key Authentication. Wireless clients go through one of these authentication processes to associate with an access point.

A denial-of-service (DoS) attack spoofs invalid authentication request frames (with bad authentication service and status codes) from an associated client in State 3 to an access point. Upon reception of the invalid authentication requests, the access point updates the client to State 1, which disconnects its wireless service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of a DoS attack by monitoring for spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an access point, the server raises this alarm to indicate a potential intruder's attempt to breach security.

Note This alarm focuses on 802.11 authentication methods, such as Open System and Shared Key. 802.1x and EAP based authentications are monitored by other alarms.

Denial of Service Attack: Block ACK Flood

Alarm Description and Possible Causes

A form of Denial of Service attack allows an attacker to prevent an 802.11n AP from receiving frames from a specific valid corporate client. With the introduction of the 802.11n standard, a transaction mechanism was introduced which allows a client to transmit a large block of frames at once, rather than dividing them up into segments. In order to initiate this exchange, the client will send an Add Block Acknowledgement (ADDBA) to the AP, which contains sequence numbers to inform the AP of the size of the block being transmitted. The AP will then accept all frames that fall within the specified sequence (consequently dropping any frames that fall outside of the range) and transmit a BlockACK message back to the client when the transaction has been completed.

In order to exploit this process, an attacker can transmit an invalid ADDBA frame while spoofing the valid client's MAC address. This process will cause the AP to ignore any valid traffic transmitted from the client until the invalid frame range has been reached.

wIPS Solution

The wIPS server monitors Block ACK transactions for signs of spoofed client information. When an attacker is detected attempting to initiate a Block ACK attack, an alarm is triggered. It is recommended that users locate the offending device and eliminate it from the wireless environment as soon as possible.

Denial of Service Attack: Deauthentication Broadcast

Attack tool: WLAN Jack, Void11, Hunter Killer

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client station remains in State 3 to continue wireless communication. A client station in State 1

and State 2 can not participate in WLAN data communication until it is authenticated and associated to State 3.

A form of DoS (denial-of-service) attack aims to send all clients of an access point to the unassociated or unauthenticated State 1 by spoofing de-authentication frames from the access point to the broadcast address. With today's client adapter implementation, this form of attack is very effective and immediate in terms of disrupting wireless services against multiple clients. Typically, client stations re-associate and re-authenticate to regain service until the attacker sends another de-authentication frame.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed de-authentication frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security analyst can log on to the access point to check the current association table status.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MAC spoofing. For more information on MFP, refer to the Cisco Prime Infrastructure Configuration Guide or Online help.

Denial of Service Attack: Deauthentication Flood

Attack tool: WLAN Jack, Void11

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client station stays in State 3 in order to continue wireless communication. A client station in State 1 and State 2 can not participate in WLAN data communication until it is authenticated and associated to State 3.

A form of DoS (denial-of-service) attack aims to send an access point's client to the unassociated or unauthenticated State 1 by spoofing de-authentication frames from the access point to the client unicast address. With today's client adapter implementations, this form of attack is very effective and immediate in terms of disrupting wireless services against the client. Typically, client stations re-associate and re-authenticate to regain service until the attacker sends another de-authentication frame. An attacker repeatedly spoofs the de-authentication frames to keep all clients out of service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed dis-association frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log on to the access point to check the current association table status.

Denial of Service Attack: Disassociation Flood

Alarm Description and Possible Causes

IEEE 802.11 defines a client state machine for tracking the station authentication and association status. Wireless clients and access points implement this state machine according to the IEEE standard. A successfully associated client station stays in State 3 in order to continue wireless communication. A client station in State 1 and State 2 can not participate in WLAN data communication until it is authenticated and associated to State 3.

A form of DoS (denial-of-service) attack aims to send an access point's client to the unassociated or unauthenticated State 2 by spoofing dis-association frames from the access point to the broadcast address (all clients). With today's client adapter implementations, this form of attack is effective and immediate in terms of disrupting wireless services against multiple clients. Typically, client stations re-associate to regain service until the attacker sends another dis-association frame. An attacker repeatedly spoofs the dis-association frames to keep all clients out of service.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by detecting spoofed dis-association frames and tracking client authentication and association states. When the alarm is triggered, the access point under attack is identified. The WLAN security officer can log on to the access point to check the current association table status.

Denial of Service Attack: EAPOL Logoff Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP (Extensible Authentication Protocol) over LANs, or EAPOL. The 802.1x protocol starts with a EAPOL-Start frame to begin the authentication transaction. At the end of an authenticated session when a client station wishes to log off, the client station sends an 802.1x EAPOL-Logoff frame to terminate the session with the access point.

Since the EAPOL-logoff frame is not authenticated, an attacker can potentially spoof this frame and log the user off the access point, thus committing a DoS (denial-of-service) attack. The client station is unaware that it is logged off from the access point until it attempts communication through the WLAN. Typically, the client station discovers the disrupted connection status and re-associates and authenticates automatically to regain the wireless connection. The attacker can continuously transmit the spoofed EAPOL-Logoff frames to be effective on this attack.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the use of FATA-jack by monitoring on spoofed MAC addresses and authentication failures. This alarm may also indicate an intrusion attempt. When a wireless client fails too many times in authenticating with an access point, the Cisco Adaptive Wireless IPS raises this alarm to indicate a potential intruder's attempt to breach security.

Note This alarm focuses on 802.11 authentication methods (Open System, Shared Key, etc). EAP and 802.1x based authentications are monitored by other alarms.

Denial of Service Attack: FATA Jack Tool Detected

Alarm Description and Possible Causes

EEE 802.11 defines a client state machine for tracking station authentication and association status. Wireless clients and access points implement this state machine based on the IEEE standard. A successfully associated client station stays in State 3 in order to continue wireless communication. A client station in State 1 and in State 2 cannot participate in the WLAN data communication process until it is authenticated and associated to State 3. IEEE 802.11 defines two authentication services: Open System Authentication and Shared Key Authentication. Wireless clients go through one of these authentication processes to associate with an access point.

A form of DoS (denial-of-service) attack spoofs invalid authentication request frames (with bad authentication service and status codes) from an associated client in State 3 to an access point. Upon reception of the invalid authentication requests, the access point updates the client to State 1, which disconnects its wireless service.

FATA-jack is one of the commonly used tools to run a similar attack. It is a modified version of WLAN-jack and it sends authentication-failed packets along with the reason code of the previous authentication failure to the wireless station. This occurs after it spoofs the MAC address of the access point. FATA-jack closes most active connections and at times forces the user to reboot the station to continue normal activities.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking the spoofed pre-mature EAP-Failure frames and the 802.1x authentication states for each client station and access point. Locate the device and take appropriate steps to remove it from the wireless environment.

Denial of Service Attack: Premature EAP Failure Attack

Alarm Description and Possible Causes

The IEEE 802.1x standard defines the authentication protocol using EAP (Extensible Authentication Protocol) over LANs, or EAPOL. The 802.1x protocol starts with a EAPOL-Start frame to begin the authentication transaction. When the 802.1x authentication packet exchange is complete with the back-end RADIUS server, the access point sends an EAP-Success or EAP-Failure frame to the client to indicate authentication success or failure.

The IEEE 802.1X specification prohibits a client from displaying its interface when the required mutual authentication is not complete. This enables a well-implemented 802.1x client station to avoid being fooled by a fake access point sending premature EAP-Success packets.

An attacker keeps the client interface from displaying (therefore Denial-of-Service) by continuously spoofing pre-mature EAP-Failure frames from the access point to the client to disrupt the authentication state on the client.

wIPS Solution

The Cisco Adaptive Wireless IPS detects this form of DoS attack by tracking spoofed premature EAP-Success frames and the 802.1x authentication states for each client station and access point. Locate the device and take appropriate steps to remove it from the wireless environment.

Intrusion Detection—Security Penetration

A form of wireless intrusion is to breach the WLAN authentication mechanism to gain access to the wired network or the wireless devices. Dictionary attacks on the authentication method is a common attack against an access point. The intruder can also attack the wireless client station during its association process with an access point. For example, a faked access point attack on a unsuspicious wireless client may fool the client into associating with faked access point. This attack allows the intruder to gain network access to the wireless station and potentially hack into its file system. The intruder can then use the station to access the wired enterprise network.

These security threats can be prevented if mutual authentication and strong encryption techniques are used. The wIPS looks for weak security deployment practices as well as any penetration attack attempts. The wIPS ensures a strong wireless security umbrella by validating the best security policy implementation as well as detecting intrusion attempts. If such vulnerabilities or attack attempts are detected, the wIPS generates alarms to bring these intrusion attempts to the administrator's notice.

Security penetration attacks include the following types:

ASLEAP Tool Detected

Alarm Description and Possible Causes

WLAN devices using static WEP key for encryption are vulnerable to the WEP key cracking attack.

Cisco Systems introduced LEAP (Lightweight Extensible Authentication Protocol) to leverage the existing 802.1x framework to avoid such WEP key attacks. The Cisco LEAP solution provides mutual authentication, dynamic per session and per user keys, and configurable WEP session key time out. The LEAP solution was considered a stable security solution and is easy to configure.

There are hacking tools that compromise wireless LAN networks running LEAP by using off-line dictionary attacks to break LEAP passwords After detecting WLAN networks that use LEAP, this tool de-authenticates users which forces them to reconnect and provide their user name and password credentials. The hacker captures packets of legitimate users trying to re-access the network. The attacker can then analyze the traffic off-line and guess the password by testing values from a dictionary.

The main features of the ASLEAP tool include:

- Reading live from any wireless interface in RFMON mode with libpcap
- Monitoring a single channel or performing channel hopping to look for target networks running LEAP.
- Actively deauthenticating users on LEAP networks, forcing them to reauthenticate. This allows quick LEAP password captures.
- Only de-authenticating users who have not already been seen rather than users who are not running LEAP.

- Reading from stored libpcap files.
- Using a dynamic database table and index to allow quick lookups on large files. This reduces the worst-case search time to .0015% as opposed to lookups in a flat file.
- Writing only the LEAP exchange information to a libpcap file.

This could be used to capture LEAP credentials with a device short on disk space (like an iPaq); the LEAP credentials are then stored in the libpcap file on a system with more storage resources to mount the dictionary attack.

The source and Win32 binary distribution for the tool are available at http://asleap.sourceforge.net.

Cisco Systems has developed the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) protocol which stops these dictionary attacks. EAP-FAST helps prevent man-in-the-middle attacks, dictionary attacks, and packet and authentication forgery attacks. In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is then authenticated using the user-name and password credentials.

Some advantages of EAP-FAST include:

- It is not proprietary.
- It is compliant with the IEEE 802.11i standard.
- It supports TKIP and WPA.
- It does not use certificates and avoids complex PKI infrastructures.
- It supports multiple Operating Systems on PCs and Pocket PCs.

wIPS Solution

The Cisco Adaptive Wireless IPS detects the de-authentication signature of the ASLEAP tool. Once detected, the server alerts the wireless administrator. The user of the attacked station should reset the password. The best solution to counter the ASLEAP tool is to replace LEAP with EAP-FAST in the corporate WLAN environment.

Cisco WCS also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, refer to Cisco WCS online help.

Airdrop Session Detected

Alarm and Possible Causes

Starting with Apple OSX Lion, Apple has a new feature called AirDrop. This new feature is supported on "newer" MacBook, MacBook Pro and iMac. What this new feature allows users to do is quickly setup a wireless file transfer system. To achieve this, both of the users that want to share files need to open their finder and click on the AirDrop link. Once both of the systems are in range of each other and the link is setup, the users will see the other user's login icon in the AirDrop window. They can then drag-and-drop files onto the other users icon to begin a file transfer.

This could potentially create a security risk due to unauthorized Peer-to-Peer networks being dynamically created in your WLAN environment. File sharing is also a concern here.

wIPS Solution

The system monitors the wireless network for traffic consistent with an AirDrop session. Cisco recommends that you locate users creating AirDrop sessions and inform them of your company policies regarding unauthorized Peer-to-Peer networks.

AirPwn

Alarm Description and Possible Causes

Airpwn is a framework for 802.11 packet injection. Airpwn listens to incoming wireless packets, and if the data matches a pattern specified in the config files, custom content is injected (spoofed) from the wireless access point. Airpwn utilizes the inherent delay when a client sends a request to the internet. Since the Airpwn attacker is closer, it will be able to quickly respond. As an example, the hacker might replace all images on a website that the visitor is trying to view, showing only what the hacker wants the visitor to see.

Airpwn only works on open wireless networks and WEP encrypted networks when the attacker knows the WEP key.

wIPS Solution

Cisco Enterprise monitors the wireless network for potential traffic that is consistent with an Airpwn attack against Open or WEP decrypted Access Points and notifies the WLAN administrator. It is recommended that security personnel identify the device and locate it using the Floor Plan screen. The attacking station should be removed from the wireless environment as soon as possible.

Airsnarf Attack Detected

Alarm Description and Possible Causes

wIPS Solution

The Cisco Adaptive Wireless IPS detects the wireless device running the AirSnarf tool. Appropriate action must be taken by the administrator to remove the AirSnarf tool from the WLAN environment.

Bad EAP-TLS Frames

Alarm Description and Possible Causes

Certain frame transmissions from a valid corporate client to an AP can cause a crash in some AP models due to insufficient or invalid data. A wireless attacker can take advantage of this vulnerability by transmitting the defective frames in order to bring down a corporate AP. By sending EAP-TLS packets with flags set to 'c0' and no TLS message length or data, APs from some vendors can be rendered inoperable until they are rebooted. During this reboot process, attackers may have a brief opportunity to gain access to the corporate network, resulting in a potential security leak.

wIPS Solution

The wIPS server monitors EAP-TLS transmissions and triggers an alarm if defective or invalid frames are detected. Although this issue may not always represent a wireless attack, it is an issue that should be remedied in order to maintain the health of the overall wireless deployment.

Beacon Fuzzed Frame Detected

Alarm Description and Possible Causes

802.11 Fuzzing is the process of introducing invalid, unexpected or random data into the 802.11 frames and then replaying those modified frames into the air. This can cause unexpected behavior to the destination device including driver crashes, operating system crashes and stack based overflows which would allow execution of arbitrary code on the affected system. The CVE website (http://cve.mitre.org/index.html) has numerous reported entries for fuzzing based vulnerabilities on 802.11 frames.

The system inspects each beacon frame looking for signs of fuzzing activity. Most common forms of beacon fuzzing involve expanding the SSID field beyond the limit of 32 bytes and changing the supported data rates to invalid rates. The system looks for these anomalies and will generate the Beacon Fuzzing alarm when the field values are beyond the 802.11 specification.

wIPS Solution

The system monitors the wireless network for traffic consistent with Beacon Fuzzing. It is recommended to locate the device and take it offline.

Brute Force Hidden SSID

Alarm Description and Possible Causes

A common practice amongst WLAN Administrators is to disable broadcasting of the SSID for an Access Point. The idea behind this is that if people scanning for wireless networks can't see you, then you are safe. Basically you would need to know the SSID in order to connect to that wireless network. This protects your

wireless network from casual drive by users who don't have the tools to extract the SSID from hidden networks. But hackers are a different story. They have the tools, the time and energy to extract the SSID from hidden networks. There are many tools to perform this type of snooping. If a hidden SSID is not found through normal methods, hackers can use a brute force method using the tool mdk3. With the tool mdk3, they can perform a Dictionary attack or a word list attack on the hidden network to extract the SSID.

wIPS Solution

Cisco Enterprise monitors the wireless network for potential traffic that is consistent with a brute force attack against a hidden SSID and notifies the WLAN administrator. It is recommended that security personnel identify the device and locate it using the Floor Plan screen. The attacking station should be removed from the wireless environment as soon as possible.

ChopChop Attack

Alarm Description and Possible Causes

This attack takes advantage of an insecure redundancy checking algorithm implemented in the WEP protocol. By compromising a few known properties, an attacker is able to take an encrypted packet and decrypt it while retrieving the keystream used to encrypt the packet.

The way the attack works, is the attacker captures a packet and chops one byte off the end of the packet before the ICV.

The attacker will then append a "guess" to the decrypted value of the byte. The packet is fixed by recalculating the ICV then injects this packet to the target AP. If the target AP, re-broadcasts this frame back out, the attacker knows he has correctly guessed the value of the decrypted byte. The attacker then moves onto the next byte. As the guesses become successful, the packet being injected actually gets smaller and smaller. If the packet doesn't get re-broadcasted, then the attacker changes the guess and repeats the process, he or she has 256 possible choices to try and guess. Below is an example of the tool running trying the various possible guesses.

Once complete, the attacker will have decrypted the entire WEP packet byte by byte, which can then be XORed with the original encrypted packet to produce the plaintext data.

wIPS Solution

The ChopChop Attack is targeted at WEP based Access Points to break the WEP key and gain direct access to the wireless network. Since this particular attack can take less than 5 minutes to perform, there is a good chance the attacker has already gained access to your wireless network. If possible, migrate your WLAN off WEP. WPA2-AES is recommended. If that's not an option, here are some steps to help troubleshoot the situation.

- Turn off the radios for the affected AP. This will disconnect all clients that are currently connected.
- Change the WEP key
- Turn the radios back on
- You will need to change the WEP key on all of the devices that were currently connected to the new WEP key that was just set.
- Monitor NCS to see if the ChopChop alarm happens again.

DHCP Starvation Attack Detected (ID:215)

Alarm Description and Possible Causes

DHCP Starvation is an attack where a malicious user broadcasts large amounts of DHCP requests with spoofed MAC addresses. If enough DHCP request frames flood the network, the attacker could use up all of the remaining DHCP IP addresses that are available for valid users. This would create a DoS condition on the network. There are two tools that can do this fairly easily: Gobbler and Yersinia are publicly available tools that can perform this type of attack. This type of attack is especially harmful on guest networks or hotspot networks where the user is allowed to get an IP address before the authentication happens.

Mitigation options for this type of attack can be handled at the switch level. For Cisco IOS switches, enable DHCP Snooping. For Cisco CatOS, enable port security.

wIPS Solution

The system monitors the wireless network for traffic consistent with a DHCP Starvation attack. Cisco recommends that you locate the user running the attack or implement tighter switch security.

Alarm Description and Possible Causes

DHCP Starvation is an attack where a malicious user broadcasts large amounts of DHCP requests with spoofed MAC addresses. If enough DHCP request frames flood the network, the attacker could use up all of the remaining DHCP IP addresses that are available for valid users. This would create a DoS condition on the network. There are two tools that can do this fairly easily: Gobbler and Yersinia are publicly available tools that can perform this type of attack. This type of attack is especially harmful on guest networks or hotspot networks where the user is allowed to get an IP address before the authentication happens.

Mitigation options for this type of attack can be handled at the switch level. For Cisco IOS switches, enable DHCP Snooping. For Cisco CatOS, enable port security.

wIPS Solution

The system monitors the wireless network for traffic consistent with a DHCP Starvation attack. Cisco recommends that you locate the user running the attack or implement tighter switch security.

Day-0 Attack by WLAN Security Anomaly

wIPS Solution

The Cisco Adaptive Wireless IPS has detected a single Security IDS/IPS policy violation on a large number of devices in the wireless network. Either the number of devices violating the specific policy in the time period specified are observed or there is a sudden percentage increase in the number of devices as specified in the threshold settings for the alarm. Depending on the Security IDS/IPS violation, it is suggested that the violation be monitored individually to determine the source and destination of this attack. If this is an increase in the number of rogue devices, it may indicate an attack against the network.

If there is a sudden increase in the number of client devices with encryption disabled, it may be necessary to revisit the Corporate Security Policy and enforce users to use the highest level of encryption and authentication according to the policy rules.

Day-0 Attack by Device Security Anomaly

wIPS Solution

The Cisco Adaptive Wireless IPS detects a device violating a large number of Security IDS/IPS policies. This device has either generated a number of Security IDS/IPS violations in the time period specified or there is a sudden percentage increase as specified in the threshold settings for the various alarms. The device should be monitored and located to carry out further analysis to check if this device is compromising the Enterprise Wireless Network in any way (attack or vulnerability). If this is a rogue device, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find it.

Device Broadcasting XSS SSID

Alarm Description and Possible Causes

Cross-Site scripting vulnerabilities are well known and consist of publicized attacks that target web applications to gain access to the underlying server or the web application itself. It does this by injecting a client-side script into web pages viewed by the user.

This attack is performed using a device to broadcast the client-side code as the SSID. Once a WLAN monitoring system picks up the malicious SSID and records it, if the system is web based and there are Cross-Site Scripting vulnerabilities, then that system will be exploited once the device with the malicious SSID is clicked.

wIPS Solution

Cisco Enterprise monitors the wireless network for Access Points and Ad-hoc devices broadcasting malicious Cross-site scripting (XSS) traffic. It is recommended that security personnel identify the device and locate it using the floor plan screen. The device should then be removed from the wireless environment as soon as possible.

Device Probing for Access Points

Some commonly used scan tools include: NetStumbler (newer versions), MiniStumbler (newer versions), MACStumbler, WaveStumbler, PrismStumbler, dStumbler, iStumbler, Aerosol, Boingo Scans, WiNc, AP Hopper, NetChaser, Microsoft Windows XP scans.

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects wireless devices probing the WLAN and attempting association (i.e. association request for an access point with any SSID).

Such devices could pose potential security threats in one of the following ways:

- War-driving, WiLDing (Wireless LAN Discovery), war-chalking, war-walking, war cycling, war-lightrailing, war-busing, and war-flying.
- Legitimate wireless client attempting risky promiscuous association.

War-driving, war-chalking, war-walking, and war-flying activities include:

- War-driving- A wireless hacker uses war-driving tools to discover access points and publishes information such as MAC address, SSID, and security implemented on the Internet with the access points' geographical location information.
- War-chalking- War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols
- War-flying-War-flying refers to sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet relay chat sessions from an altitude of 1,500 feet on a war-flying trip.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your the access points to not broadcast SSIDs. Use the Cisco Adaptive Wireless IPS to see which access points are broadcasting (announcing) their SSID in the beacons.

Dictionary Attack on EAP Methods

Alarm Description and Possible Causes

IEEE 802.1x provides an EAP (Extensible Authentication Protocol) framework for wired or wireless LAN authentication. An EAP framework allows flexible authentication protocol implementation. Some implementations of 802.1x or WPA use authentication protocols such as LEAP, MD5, OTP (one-time-password), TLS, and TTLS. Some of these authentication protocols are based upon the user name and password mechanism, where the user name is transmitted clear without encryption and the password is used to answer authentication challenges.

Most password-based authentication algorithms are susceptible to dictionary attacks. During a dictionary attack, an attacker gains the user name from the unencrypted 802.1x identifier protocol exchange. The attacker then tries to guess a user's password to gain network access by using every "word" in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on the fact that a password is often a common word, name, or combination of both with a minor modification such as a trailing digit or two.

A dictionary attack can take place actively online, where an attacker repeatedly tries all the possible password combinations. Online dictionary attacks can be prevented using lock-out mechanisms available on the authentication server (RADIUS servers) to lock out the user after a certain number of invalid login attempts. A dictionary attack can also take place off-line, where an attacker captures a successful authentication challenge protocol exchange and then tries to match the challenge response with all possible password combinations off-line. Unlike online attacks, off-line attacks are not easily detected. Using a strong password policy and periodically expiring user passwords significantly reduces an off-line attack tool's success.

wIPS Solution

The Cisco Adaptive Wireless IPS detects online dictionary attacks by tracking 802.1x authentication protocol exchange and the user identifier usages. Upon detection of a dictionary attack, the alarm message identifies the user name and attacking station's MAC address.

The Cisco Adaptive Wireless IPS advises switching user name and password based authentication methods to encrypted tunnel based authentication methods such as PEAP and EAP-FAST, which are supported by many vendors including Cisco.

Fake Access Points Detected

Alarm Description and Possible Causes

The Fake AP tool is meant to protect your WLAN acting as a decoy to confuse war-drivers using NetStumbler, Wellenreiter, MiniStumbler, Kismet, etc. The tool generates beacon frames imitating thousands of counterfeit 802.11b access points. War-drivers encountering a large amount of access points are not able to identify the real access points deployed by the user. This tool, although very effective in fending off war-drivers, poses other disadvantages such as bandwidth consumption, misleading legitimate client stations, and interference with the WLAN management tools. The Cisco Adaptive Wireless IPS does not recommend running the Fake AP tool in your WLAN.

wIPS Solution

The Cisco Adaptive Wireless IPS recommends that the administrator locate the device running the Fake AP tool and take appropriate steps to remove it from the wireless environment.

Fake DHCP Server Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects such wireless STAs running the DHCP service and providing IP addresses to unaware users.

Once the client is identified and reported, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the device.

wIPS Solution

The Cisco Adaptive Wireless IPS detects such wireless STAs running the DHCP service and providing IP addresses to unaware users.

Once the client is identified and reported, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the device.

Fast WEP Crack (ARP Replay) Detected

Alarm Description and Possible Causes

It is well publicized that WLAN devices using static WEP key for encryption are vulnerable to WEP key cracking attack (Refer to Weaknesses in the Key Scheduling Algorithm of RC4 - I by Scott Fluhrer, Itsik Mantin, and Adi Shamir).

The WEP secret key that has been cracked by any intruder results in no encryption protection, thus leading to compromised data privacy. The WEP key that is in most cases 64-bit or 128-bit (few vendors also offer 152-bit encryption) consists of the secret key specified by the user linked with the 24-bit IV (Initialization Vector). The IV that is determined by the transmitting station can be reused frequently or in consecutive frames, thus increasing the possibility of the secret key to be recovered by wireless intruders.

The most important factor in any attack against the WEP key is the key size. For 64-bit WEP keys, around 150K unique IVs and for 128-bit WEP keys around 500k to a million unique IVs should be enough. With insufficient traffic, hackers have created a unique way of generating sufficient traffic to perform such an attack. This is called the replay attack based on arp-request packets. Such packets have a fixed length and can be spotted easily. By capturing one legitimate arp-request packet and resending them repeatedly, the other host responds with encrypted replies, providing new and possibly weak IVs.

wIPS Solution

The Cisco Adaptive Wireless IPS alerts on weak WEP implementations and recommends a device firmware upgrade if available from the device vendor to correct the IV usage problem. Ideally, enterprise WLAN networks can protect against WEP vulnerability by using the TKIP (Temporal Key Integrity Protocol) encryption mechanism, which is now supported by most enterprise level wireless equipment. TKIP enabled devices are not subject to any such WEP key attacks.

Cisco WCS also provides automated security vulnerability scanning that proactively reports any access points configured to utilize weak encryption or authentication. For more information on automated security vulnerability scanning, refer to the Cisco WCS online help.

Fragmentation Attack

Alarm Description and Possible Causes

It is well publicized that a WLAN device using a static WEP key for encryption is vulnerable to various WEP cracking attacks. Refer to Weaknesses in the Key Scheduling Algorithm of RC4 - I, by Scott Fluhrer, Itsik Mantin, and Adi Shamir for more information.

wIPS Solution

The Cisco Adaptive Wireless IPS alerts on detecting a potential fragmentation attack in progress, and recommends that WEP not be used in the corporate environment and that appropriate measures be taken to avoid any security holes in the network and upgrade the wireless network infrastructure and devices to use the more secure IEEE 802.11i standard.

HT Intolerant Degradation Services

Alarm Description and Possible Causes

While 802.11n deployments provide the potential for dramatically increased wireless range and speed over legacy implementations, these benefits can be easily lost or offset if a single legacy device is introduced to the network. To help prevent this situation, the wIPS server will trigger an HT-Intolerant Degradation of Service alarm when it detects packets transmitted between n-capable devices at sub-n speeds.

Alarm Description and Possible Causes

While 802.11n deployments provide the potential for dramatically increased wireless range and speed over legacy implementations, these benefits can be easily lost or offset if a single legacy device is introduced to the network. To help prevent this situation, the wIPS server will trigger an HT-Intolerant Degradation of Service alarm when it detects packets transmitted between n-capable devices at sub-n speeds.

Honeypot AP Detected

Alarm Description and Possible Causes

The addition of WLANs in the corporate environment introduces a whole new class of threats for network security. RF signals that penetrate walls and extend beyond intended boundaries can expose the network to unauthorized users. A rogue access point can put the entire corporate network at risk for outside penetration and attack. Not to understate the threat of the rogue access point, there are many other wireless security risks and intrusions such as mis-configured access points, unconfigured access points, and DoS (denial-of-service) attacks.

One of the most effective attacks facing enterprise networks implementing wireless is the use of a "honey pot" access point. An intruder uses tools such as NetStumbler, Wellenreiter, and MiniStumbler to discover the SSID of the corporate access point. Then the intruder sets up an access point outside the building premises or, if possible, within the premises and broadcasts the discovered corporate SSID. An unsuspecting client then connects to this "honey pot" access point with a higher signal strength. Once associated, the intruder performs attacks against the client station because traffic is diverted through the "honey pot" access point.

wIPS Solution

Once a "honey pot" access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Hot-Spotter Tool Detected (Potential Wireless Phishing)

Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access available for the general public. Hotspots are often found in airports, hotels, coffee shops, and other places where business people tend to congregate. It is currently one of the most important network access service for business travelers. The customer requires a wireless-enabled laptop or handheld to connect to the legitimate access point and to receive service. Most hotspots do not require the user to have an advanced authentication mechanism to connect to the access point, other than using a web page to log in. The criterion for entry is only dependent on whether or not the subscriber has paid subscription fees. In a wireless hotspot environment, no one should trust anyone else. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.

The four components of a basic hotspot network are:

- Hotspot Subscribers-Valid users with a wireless enabled laptop or handheld and valid login for accessing the hotspot network.
- WLAN Access Points-SOHO gateways or enterprise level access points depending upon the hotspot implementation.
- Hotspot Controllers-Deals with user authentication, gathering billing information, tracking usage time, filtering functions, etc. This can be an independent machine or can be incorporated in the access point itself.
- Authentication Server-Contains the login credentials for the subscribers. In most cases, hotspot controllers verify subscribers' credentials with the authentication server.

Hotspotter automates a method of penetration against wireless clients, independent of the encryption mechanism used. Using the Hotspotter tool, the intruder can passively monitors the wireless network for probe request frames to identify the SSIDs of the networks of the Windows XP clients.

After it acquires the preferred network information, the intruder compares the network name (SSID) to a supplied list of commonly used hotspot network names. Once a match is found, the Hotspotter client acts as an access point. The clients then authenticate and associate unknowingly to this fake access point.

Once the client gets associated, the Hotspotter tool can be configured to run a command such as a script to kick off a DHCP daemon and other scanning against the new victim.

Clients are also susceptible to this kind of attack when they are operating in different environments (home and office) while they are still configured to include the hotspot SSID in the Windows XP wireless connection settings. The clients send out probe requests using that SSID and make themselves vulnerable to the tool.

wIPS Solution

Once the rogue access point is identified and reported by the Cisco Adaptive Wireless IPS, the WLAN administrator may use the integrated over-the-air physical location capabilities, or trace device on the wired network using rogue location discovery protocol (RLDP) or switchport tracing to find the rogue device.

Identical Send and Receive Address

Alarm Description and Possible Causes

In order to inhibit wireless activity in a corporate network, attackers will often modify wireless packets to emulate various different characteristics, including changes to the packets' Source and Destination MAC information. In cases where these fields are identical, the Identical Send and Receive Address alarm will be triggered in order to alert IT personnel of a potential attack.

wIPS Solution

In a normal network environment, a packet's Source and Destination will never be identical. As such, the enterprise administrators should take immediate steps to locate the root cause of the modified packets.

Improper Broadcast Frames

Alarm Description and Possible Causes

Standard 802.11 deployments allow for certain frames to be transmitted to individual destinations (also known as unicast frames, such as an ACK) and other frames to be 'broadcast' to all recipients in the wireless deployment. In general, these two categories should not overlap, e.g., an Association Request frame should not be sent out as a broadcast to all listening devices. In this scenario, the wIPS server will trigger an Improper Broadcast Frames alarm to alert staff of a potential problem.

Improper Broadcast Frames

Karma Tool Detected

Alarm Description and Possible Causes

The Karma tool allows a wireless attacker to configure a client as a soft AP that will respond to any probe request detected. This implementation is designed to respond to queries from stations configured to connect to multiple different networks, e.g., SSID "Corporate" for work and SSID "Home" for home use. In this example, the soft AP may be configured to respond to the probe for "Home" when the client is at work. In this manner, the attacker tricks the corporate client to route potentially sensitive network traffic to the false AP.

wIPS Solution

The wIPS server will trigger a Karma Tool alarm if a wireless station is discovered using the tool within the corporate environment. Users should locate the attacking device and eliminate it immediately.

Man-in-the-Middle Attack Detected

Alarm Description and Possible Causes

Man-in-the-Middle (MITM) attack is one of the most common 802.11 attacks that can lead to confidential corporate and private information being leaked to hackers. In a MITM attack, the hacker can use a 802.11 wireless analyzer and monitor 802.11 frames sent over the WLAN. By capturing the wireless frames during the association phase, the hacker gets IP and MAC address information about the wireless client card and access point, association ID for the client, and the SSID of the wireless network.

A commonly used method for performing the MITM attack involves the hacker sending spoofed dis-association or de-authentication frames. The hacker station then spoofs the MAC address of the client to continue an association with the access point. At the same time, the hacker sets up a spoofed access point in another channel to keep the client associated. This allows all traffic between the valid client and access point to pass through the hacker's station.

One of the most commonly used MITM attack tools is Monkey-Jack.

wIPS Solution

The Cisco Adaptive Wireless IPS recommends the use of strong encryption and authentication mechanisms to thwart any MITM attacks by hackers. One way to avoid such an attack is to prevent MAC spoofing by using MAC address exclusion lists and monitoring the RF channel environment.

Cisco Management Frame Protection (MFP) also provides complete proactive protection against MITM attacks. For more information on MFP, refer to the Cisco Wireless Control System Configuration Guide or the WCS online help.

NetStumbler Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (such as an association request for an access point with any SSID) using the NetStumbler tool. The Device probing for Access Point alarm is generated when hackers use recent versions of the NetStumbler tool. For older versions, the Cisco Adaptive Wireless IPS generates the NetStumbler detected alarm.

NetStumbler is the most widely used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover access points and to publish their information (MAC address, SSID, security implemented, etc.) on the Internet with the access points' geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similiar to war-driving, but the hacker is on foot instead of a car. It can run on a machine running Windows 2000, Windows XP, or better. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers like to use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up email and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which of your access points is broadcasting an SSID in the beacons.

Cisco WCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, refer to the WCS online help.

NetStumbler Victim Detected

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which access point is broadcasting its SSID in the beacons.

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (i.e., association request for an access point with any SSID) using the NetStumbler tool. The Device probing for access point alarm is generated when hackers more recent versions of the NetStumbler tool. For older versions, the Cisco Adaptive Wireless IPS generates the NetStumbler detected alarm.

NetStumbler is the most widely used tool for war-driving, war-walking, and war-chalking. A wireless hacker uses war-driving tools to discover access points and publish their information (MAC address, SSID, security implemented, etc.) on the Internet with the access points' geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker conducts the illegal operation on foot instead of by car. The NetStumbler web site (http://www.netstumbler.com/) offers MiniStumbler software for use on Pocket PC hardware, saving war-walkers from carrying heavy laptops. It can run on a machine running Windows 2000, Windows XP, or later. It also supports more cards than Wellenreiter, another commonly used scanning tool. War-walkers typically use MiniStumbler and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used, but from a low-flying private plane with high-power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

The Cisco Adaptive Wireless IPS alerts the user when it observes that a station running Netstumbler is associated to a corporate access point.

Publicly Secure Packet Forwarding (PSPF) Violation

Alarm Description and Possible Causes

Publicly Secure Packet Forwarding (PSPF) is a feature implemented on WLAN access points to block wireless clients from communicating with other wireless clients. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network.

For most WLAN environments, wireless clients communicate only with devices such as web servers on the wired network. By enabling PSPF it protects wireless clients from being hacked by a wireless intruder. PSPF is effective in protecting wireless clients especially at wireless public networks (hotspots) such as airports, hotels, coffee shops, and college campuses where authentication is null and anyone can associate with the access points. The PSPF feature prevents client devices from inadvertently sharing files with other client devices on the wireless network.

wIPS Solution

The Cisco Adaptive Wireless IPS detects PSPF violations. If a wireless client attempts to communicate with another wireless client, the Cisco Adaptive Wireless IPS raises an alarm for a potential intrusion attack. This alarm does not apply if your WLAN deploys wireless printers or VoWLAN applications because these applications rely on wireless client-to-client communication

Probe Request Fuzzed Frame Detected

Alarm Description and Possible Causes

802.11 Fuzzing is the process of introducing invalid, unexpected or random data into the 802.11 frames and then replaying those modified frames into the air. This can cause unexpected behavior to the destination device including driver crashes, operating system crashes and stack based overflows which would allow execution of arbitrary code on the affected system. The CVE website (http://cve.mitre.org/index.html) has numerous reported entries for fuzzing based vulnerabilities on 802.11 frames.

The system inspects each Probe Request frame looking for signs of fuzzing activity. Most common forms of Probe Request fuzzing involve expanding the SSID field beyond the limit of 32 bytes and changing the supported data rates to invalid rates. The system looks for these anomalies and will generate the Probe Request Fuzzing alarm when the field values are beyond the 802.11 specification.

Probe Response Fuzzed Frame Detected

Alarm Description and Possible Causes

802.11 Fuzzing is the process of introducing invalid, unexpected or random data into the 802.11 frames and then replaying those modified frames into the air. This can cause unexpected behavior to the destination device including driver crashes, operating system crashes and stack based overflows which would allow execution

of arbitrary code on the affected system. The CVE website (http://cve.mitre.org/index.html) has numerous reported entries for fuzzing based vulnerabilities on 802.11 frames.

The system inspects each Probe Response frame looking for signs of fuzzing activity. Most common forms of Probe Response fuzzing involve expanding the SSID field beyond the limit of 32 bytes and changing the supported data rates to invalid rates. The system looks for these anomalies and will generate the Probe Response Fuzzing alarm when the field values are beyond the 802.11 specification.

wIPS Solution

The system monitors the wireless network for traffic consistent with Probe Response Fuzzing. It is recommended to locate the device and take it offline.

Soft AP or Host AP Detected

Host AP tools: Cqure AP

Alarm Description and Possible Causes

A hotspot is any location where Wi-Fi network access available for the general public. Hotspots are often found in airports, hotels, coffee shops, and other places where business people tend to congregate. It is currently one of the most important network access service for business travelers. The customer requires a wireless-enabled laptop or handheld to connect to the legitimate access point and to receive service. Most hotspots do not require the user to have an advanced authentication mechanism to connect to the access point, other than using a web page to log in. The criterion for entry is only dependent on whether or not the subscriber has paid subscription fees. In a wireless hotspot environment, no one should trust anyone else. Due to current security concerns, some WLAN hotspot vendors are using 802.1x or higher authentication mechanisms to validate the identity of the user.

Basic components of a WLAN Hotspot network

The four components of a basic hotspot network are as follows:

- Hotspot Subscribers—Valid users with a wireless enabled laptop or handheld and valid log in for accessing the hotspot network.
- WLAN Access Points—SOHO gateways or enterprise level access points depending upon the hotspot implementation.
- Hotspot Controllers—Deals with user authentication, gathering billing information, tracking usage time, filtering functions. This can be an independent machine or can be incorporated in the access point itself.
- Authentication Server—Contains the log in credentials for the subscribers. In most cases, hotspot controllers verify subscribers' credentials with the authentication server.

Hotspotter automates a method of penetration against wireless clients, independent of the encryption mechanism used. Using the Hotspotter tool, the intruder can passively monitor the wireless network for probe request frames to identify the SSIDs of the networks of the Windows XP clients.

After it acquires the preferred network information, the intruder compares the network name (SSID) to a supplied list of commonly used hotspot network names. When a match is found, the Hotspotter client acts as an access point. The clients then authenticate and associate unknowingly to this fake access point.

When the client gets associated, the Hotspotter tool can be configured to run a command such as a script to kick off a DHCP daemon and other scanning against the new victim.

Clients are also susceptible to this kind of attack when they are operating in different environments (home and office) while they are still configured to include the hotspot SSID in the Windows XP wireless connection settings. The clients send out probe requests using that SSID and make themselves vulnerable to the tool.

wIPS Solution

Soft APs or Software Access points should be treated as a Rogue device. The following steps should help eliminate this threat.

- Use integrated over-the-air physical location capabilities to locate the Rogue device
- Wireless Containment to prevent any devices from connecting to the Soft AP
- Trace the device on the wired network using rogue location discovery protocol (RLDP) or switch port tracing to find the rogue device

Spoofed MAC Address Detected

Alarm Description and Possible Causes

Spoofed mac address detected is a type of attack where a hacker will change their factory assigned wireless mac address to either gain access to a restricted wireless network by impersonating a valid connected user or to hide their presence on the wireless network.

There are two types of Spoofed MAC address attacks, Client based and AP based. For client based Spoofed MAC address attacks, the client could be trying to impersonate a valid user. An example of this would be a wireless hacker trying to get onto an access controlled hotspot by spoofing their wireless mac address of a client that is already connected, in effect "piggybacking" on the connection. Another popular example would be in a hotel environment where a hacker bypasses the payment process to get on the wireless network by spoofing their wireless mac address of a paid user.

Another type of Spoofed MAC address attack is AP based. In this case, the hacker is trying to hide their presence on the wireless network by spoofing the mac address of a corporate access point. This is a typical rogue scenario.

Suspicious After Hours Traffic Detected

Alarm Description and Possible Causes

One way to detect a wireless security penetration attempt is to match wireless usage against the time when there is not supposed to be any wireless traffic. The wIPS server monitors traffic patterns against the office-hours configured for this alarm to generate alerts when an abnormality is found. Specific suspicious wireless usage sought after by the wIPS server during after-office hours include the following:

- Client station initiating authentication or association requests to the office WLAN that may indicate security breach attempts.

- Wireless data traffic that may indicate suspicious download or upload over the wireless network.

wIPS Solution

For global wIPS deployment, the configurable office-hour range is defined in local time. The access point or sensor can be configured with a time zone to facilitate management. For the office and manufacturing floor mixed WLAN, one can define one set of office hours for the office WLAN SSID and another (for example, 6am to 9pm) for the manufacturing floor WLAN SSID. If this alarm is triggered, the administrator should look for devices responsible for the suspicious traffic and take appropriate steps to locate it and remove it from the wireless environment.

Unauthorized Association By Vendor List

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS enables network administrators to include vendor information in a policy profile to allow the system to effectively detect stations on the WLAN that are not made by approved vendors. Once such a policy profile is created, the system generates an alarm whenever an access point is associating with a station by an unapproved vendor. See the diagram below.

As the diagram shows, the access points in ACL-1 should only associate with stations made by Cisco and the access points in ACL-2 can only associate with stations manufactured by Intel. This information is entered in the wIPS system's policy profile. Any association between the access points and non-Cisco or non-Intel stations is unauthorized and triggers an alarm.

In the enterprise WLAN environment, rogue stations cause security concerns and undermine network performance. They take up air space and compete for network bandwidth. Since an access point can only accommodate a limited number of stations, it rejects association requests from stations once its capacity is reached. An access point laden with rogue stations denies legitimate stations the access to the network. Common problems caused by rogue stations include connectivity problems and degraded performance.

wIPS Solution

The Cisco Adaptive Wireless IPS automatically alerts network administrators to any unauthorized access point-station association involving non-conforming stations using this alarm. Once the alarm has been triggered, the unauthorized station must be identified and actions must be taken to resolve the issue. One way is to block it using the rogue containment.

Unauthorized Association Detected

Alarm Description and Possible Causes

In an enterprise network environment, rogue access points installed by employees do not usually follow the network's standard deployment practice and therefore compromise the integrity of the network. They are loopholes in network security and make it easy for intruders to hack into the enterprise wired network. One of the major concerns that most wireless network administrators face is unauthorized associations between

stations in an ACL and a rogue access point. Since data to and from the stations flows through the rogue access point, it leaves the door open for hackers to obtain sensitive information.

Rogue stations cause security concerns and undermine network performance. They take up air space and compete for bandwidths on the network. Since an access point can only serve a certain number of stations, it rejects association requests from stations once its capacity is reached. An access point laden with rogue stations denies legitimate stations access to the network. Common problems caused by rogue stations include disrupted connections and degraded performance.

wIPS Solution

The Cisco Adaptive Wireless IPS can automatically alert network administrators to any unauthorized access point-station association it has detected on the network through this alarm. The WLC new feature "MAC Address Learning" will prevent this violation from happening, it is recommended to enable this feature.

Wellenreiter Detected

Alarm Description and Possible Causes

The Cisco Adaptive Wireless IPS detects a wireless client station probing the WLAN for an anonymous association (i.e. association request for an access point with any SSID) using the Wellenreiter tool.

Wellenreiter is a commonly used tool for war-driving and war-chalking. A wireless hacker uses war-driving tools to discover access points and to publish their information (MAC address, SSID, security implemented, etc.) on the Internet with the access points' geographical location information. War-chalkers discover WLAN access points and mark the WLAN configuration at public locations with universal symbols as illustrated above. War-walking is similar to war-driving, but the hacker is on foot instead of a car. War-walkers like to use Wellenreiter and similar products to sniff shopping malls and big-box retail stores. War-flying is sniffing for wireless networks from the air. The same equipment is used, but from a low flying private plane with high power antennas. It has been reported that a Perth, Australia-based war-flier picked up e-mail and Internet Relay Chat sessions from an altitude of 1,500 feet on a war-flying trip.

The tool supports Prism2, Lucent, and Cisco based cards. The tool can discover infrastructure and ad-hoc networks that are broadcasting SSIDs, their WEP capabilities, and can provide vendor information automatically. It also creates an ethereal/tcpdump-compatible dumpfile and an Application savefile. It also has GPS support. Users can download the tool from Wellenreiter website.

wIPS Solution

To prevent your access points from being discovered by these hacking tools, configure your access points to not broadcast its SSID. You can use the Cisco Adaptive Wireless IPS to see which of your access points is broadcasting an SSID in the beacons.

Cisco WCS also provides automated security vulnerability scanning that reports any access points configured to broadcast their SSIDs. For more information on automated security vulnerability scanning, refer to the WCS online help.

WiFi Protected Setup Pin Brute Force

Alarm Description and Possible Causes

WiFi Protected Setup is a feature on most consumer grade Access Points that allows for easy device setup without the need for complex passwords. The feature allows the user to either use the push button method or enter in the pin found on the bottom of the Access Point to connect. A vulnerability was announced in December 2011 by Stefan Viehböck and independently discovered by Craig Heffner. The vulnerability is with the external registrar that only requires the devices pin. This mode is susceptible to brute force attacks against the pin. There are currently 2 active tools in the wild exploiting this.

The basic idea behind the attack is when a pin authentication fails, the access point sends back an EAP-NACK message to the client. With this EAP-NACK message, the attacker is able to determine if the first half of the pin is correct. The last digit of the pin is known since it is a checksum for the pin. This reduces the attempts to brute force the pin down to 11,000.

It is recommended to disable the external registrar feature of WiFi Protected Setup on your Access Point. Most manufacturers have this feature on by default.

wIPS Solution

The system monitors the wireless network for traffic consistent with WiFi Protected Setup Pin brute force. It is recommended to locate the device and take it offline.

WiFi Tap Tool Detected

Alarm Description and Possible Causes

The WiFiTap tool allows a wireless attacker to configure a client to communicate directly with another client, without connecting to a corporate AP. This implementation allows the intruder to target an attack against the individual client, bypassing any security measures configured on the corporate network. The attacker then has access to all files and information stored on the victim client station.

wIPS Solution

The wIPS server monitors for use of the WiFiTap tool and triggers an alarm if it is detected. Users should attempt to locate the attacking device and remove it from the wireless environment.

Performance Violation

WLAN performance efficiency is constantly challenged by the dynamics of the RF environment and the mobility of client devices. A closely monitored and well tuned WLAN system can achieve a higher throughput than a poorly managed one. Cisco wIPS ensures WLAN performance and efficiency by monitoring the WLAN on a continued basis and alerting the wireless administrator on early warning signs for trouble.

To maximize the power of Cisco wIPS, performance alarms can be customized to best match your WLAN deployment specification.

Performance Violation include the following subcategory:

Channel or Device Overload

WLAN technologies use the radio frequency spectrum as a shared physical media similar to the original 10 Mbps Ethernet technology. Even for the latest WLAN standards for 802.11a and 802.11g, there is still a 54 Mbps shared media bandwidth ceiling. In reality, the ceiling is much lower considering the necessary MAC protocol overhead, inter-frame spacing, collision, and random transmission back-offs.

The radio medium has its own bandwidth limitations. WLAN Access Points have limitations that can be overloaded by heavy traffic or a large number of associated clients. Like the wired LAN, excessive multicast and broadcast frames can put extra burden on the WLAN devices. Overloaded devices suffer from degraded performance and cause connectivity problems. For example, AP association table overflowed by large number of clients.

Be it channel bandwidth limitation or the WLAN device resource capacity, Cisco wIPS, monitors and tracks the load to ensure smooth operation. Cisco wIPS raises alarms and offers specific details in scenarios where WLAN's performance is not satisfactory due to under-provisioning or over-growth. RF has no boundaries that lead to your WLAN channel utilization, to increase significantly even when your neighbor installs new WLAN devices in an adjoining channel. Cisco wIPS monitors your WLAN to ensure proper bandwidth and resource provisioning.

Performance Violation include the following types:

AP Association Capacity Full

Alarm Description and Possible Causes

All WLAN Access Points have a resource limit for the number of client stations that can associate to it ,to receive wireless services. Usually, this limit is a user configurable number on the AP. After an AP reaches this limit, it will not accept any more new client association requests.

wIPS Solution

Cisco wIPS monitors on rejected association requests and responses to determine the cause of failed associations. This alarm is generated when Cisco wIPS concludes that it is caused due to AP association capacity overflow problem. This alarm indicates under-provisioning or failed load balancing for the WLAN deployment.

AP Overloaded by Stations

Alarm Description and Possible Causes

A WLAN Access Point can service only a limited number of clients due to limited resources . When the limit is reached, additional clients are rejected in service, or degraded performance for the existing clients. When designing a WLAN equipment deployment and provisioning for service, this limitation should be considered.

After deployment, the limitation may be challenged by the growing number of users and thereby requires constant monitoring for under-provisioned deployment.

wIPS Solution

Cisco wIPS monitors the AP work load by tracking its active client stations. You can configure the system to generate alarms of different severity levels by the work load threshold (active client session count).For example, warning alarm for 64 active client sessions and urgent alarms for 128 active client sessions.

AP Overloaded by Utilization

Alarm Description and Possible Causes

A WLAN design for deployment includes an expectation for the maximum clients an AP can support. Similarly, there is an expectation for the maximum bandwidth utilization supported by an AP. Such expectations can be used to monitor on sufficient WLAN provisioning and effective load-balancing.

wIPS Solution

Cisco wIPS tracks AP bandwidth utilization (the sum of outgoing and incoming traffic combined) and raises an alarm when the sustained utilization exceeds the user configured threshold.

Excessive Bandwidth Usage

Alarm Description and Possible Causes

The WLAN spectrum is a shared medium with a limitation on bandwidth. Be it 802.11b at 11 mbps or 802.11a/g at 54 mbps, bandwidth utilization should be closely monitored on a per channel and per device basis to ensure sufficient WLAN provisioning for all client devices. Please note that high bandwidth consumption does not mean high WLAN throughput. The problem lies in the low speed transmission, and could also be due to an authorized user who is downloading music or movies from the Internet causing the bandwidth of the corporate network to choke. Cisco wIPS tracks WLAN bandwidth utilization on a per channel and per device basis

wIPS Solution

Cisco wIPS tracks bandwidth utilization based on channel and wireless device. The bandwidth calculation includes the PLCP header, preamble, and the actual frame payload. Because of the CSMA collision avoidance protocol, it is practically impossible to get even close to 100% utilization. 60 to 70% of utilization should be considered extremely high and requires better provisioning or improved efficiency such as strict high speed transmission. When the user defined threshold (in percentage of utilization) is exceeded, Cisco wIPS raises this alarm. Take appropriate steps to tackle this problem. This could include finding users who may be causing this due to excessive file downloading from the Internet.

Excessive Multicast/Broadcast on Channel

Alarm Description and Possible Causes

Like the wired network, excessive broadcast and multicast frames on the WLAN impose an extra load on all devices on the WLAN. WLAN is more sensitive to multicast and broadcast frames than the wired networks because all multicast and broadcast frames are transmitted at low speed (for example, 1 or 2 mbps for 802.11b WLAN). Such low speed transmissions consume more WLAN bandwidth. Besides bandwidth inefficiency, low speed multicast and broadcast frames take longer to complete the transmission process thus introducing higher delays for other devices waiting for the wireless medium to be free. Excessive multicast and broadcast frames introduce jitters to delay-sensitive WLAN applications such as **VoIP**. For example, a 1000-byte broadcast frame would take at least 8 milliseconds to transmit at 1 mpbs, which is a considerable delay for a voice application.

wIPS Solution

Cisco wIPS tracks multicast and broadcast frame usage on a per channel and per device basis to report abuse. The alarm threshold is the percentage of multicast and broadcast frames to total frames by the device or channel.

Excessive Multicast/Broadcast on Node

Alarm Description and Possible Causes

Just like the wired network, excessive broadcast and multicast frames on the WLAN impose an extra load on all devices on the WLAN. WLAN is sensitive to multicast and broadcast frames than the wired networks because of the low speed at which all the multicast and broadcast frames are transmitted (for example, 1 or 2 mbps for 802.11b WLAN). Such low speed transmissions consume more WLAN bandwidth. Besides bandwidth inefficiency, low speed multicast and broadcast frames take longer to complete the transmission process thus introducing higher delays for other devices waiting for the wireless medium to be free. Excessive multicast and broadcast frames introduce jitters to delay-sensitive WLAN applications such as **VoIP**. For example, a 1000-byte broadcast frame would take at least 8 milliseconds to transmit at 1 mpbs, which is a considerable delay for a voice application.

wIPS Solution

Cisco wIPS tracks multicast and broadcast frame usage on a per channel and per device basis to report abuse. The alarm threshold is the percentage of multicast and broadcast frames to total frames by the device or channel.