Cisco Wireless Security Solutions – External Threats

The Challenge of Wireless Security

Implementation of wireless systems presents a unique security concern in that wireless is an uncontained medium. Two primary concern arise from this, unauthorized access, and “eves dropping”. Wireless networks can be segregated into separate network so unauthorized access to proprietary information would not be possible however; this then limits the usefulness of the system. In order to achieve versatile yet secure access via the wireless system, comprehensive security mechanisms must be put into place.

Cisco’s Approach to Wireless Security

Comprehensive security requires a multi-tiered approach:

- Layer 1, Surveillance
- Layer 2 and 3 Authentication, Encryption, Detection
- Layer 4-7 Encryption and Assessment.
- Mitigation at all levels

Cisco provides a comprehensive approach to wireless security, offering enterprises the ability to address the threats of access and eves dropping. This at-a-glance focuses on the external threats that a WLAN will encounter and the mechanisms to detect and mitigate these threats. This capability will assist the enterprise in preventing both unwanted access and disruption.

External Threats

Threats in the network can come from intentional attackers trying to gain access to a network or to render that network unusable (attacks). It can also come from well meaning employees trying to provide access to simplify their efforts (rouges). A comprehensive strategy involves both detecting and classifying attacks as they occur as well as taking action to mitigate the threats.

Protecting Your Network

The Cisco Adaptive Wireless Intrusion Protections provides the detection, classification, location and mitigation of wireless threats. Unintentional threats such as rouge APs can provide serious security threats. More sophisticated threats exist with readily available software to allow the rouge device to work off-channel making it undetectable for many wireless systems. These rouge devices present backdoor access to the network and put company assets at risk. Cisco’s Wireless IDS along with Clean Air technology can detect, classify, and locate these threats.

Protecting Your Network (Continued)

Clean Air is a technology that processes the incoming signal while it is still at the AP. Processing at the AP allows for distributing the processing. More important, it allows the centralized system to focus on correlating, locating, and mitigating these threats without the constant attention of the network administrator.

Intentional attackers also pose a serious risk to any wireless system. One of the most common types of attacks on a network is Denial of Service (DoS) attack. Wireless attackers can emulate large numbers of clients, consuming the resources of the AP. Attackers can do similar actions against the RADIUS servers or even other clients. Left unattended, this can make the network unusable and force clients to continue to try to re-authenticate giving attackers an opportunity to detect passwords and ultimately gain access into the system. In order to do this, a specific type of attack is employed that a form of ARP flooding. All of these attacks present certain “signatures” in layer 2 or layer 3 traffic. The Wireless IDS system recognizes these signatures and will alert and recommend or take action. This provides the operator with contextual visibility into the vulnerability and provides this visibility without the constant vigilance of someone watching or roaming the area with detection devices.

These threats (and other similar threats) have driven the Department of Defense to issue STIG 8420.01: www.dtic.mil/whs/directives/corres/pdf/842001p.pdf

This states that “DoD Components shall ensure that a wIDS is implemented that allows for monitoring of WLAN activity and the detection of WLAN-related policy violations on all unclassified and classified DoD wired and wireless LANs."

Cisco’s APs, Controllers, and WCS have built in wIDS capability that meets the needs of this requirement. However, for comprehensive wIPS Cisco provides “Adaptive” wIPS which adds the capability to add a Mobility Services Engine, providing location, history, classification, correlation, and mitigation. The AwIPS capability allows the operator to provide preset responses so that the detection, notification and mitigation are all done autonomously. This greatly reduces the operations time and cost. More information is available at this site: www.cisco.com/go/wips

Cisco’s Solution for Wireless Security

While detecting and mitigating network intrusion is vital to having a secure wireless network, there are many parts to wireless security. Cisco uses a comprehensive approach to providing security.

Cisco Wireless LAN Controllers and Access Points

Secure over the air communication:

- Management Frame Protection
- FIPS Validated 802.11i data encryption
- Port based 802.1x over the air authentication enforced at the Access Point

Secure Wireless Infrastructure:

- All components, APs & WLAN Controllers installed with x.509 Certificates to ensure only trusted APs communicate to WLAN Controller
- IETF Standards based CAPWAP protocol between AP and WLAN controller ensures secure, publically vetted protocol
- FIPS Validated AES 256 encryption of all CAPWAP control and data traffic.

Provides Wireless Intrusion Detection and Protection:

- Detect, alert and mitigate for any unauthorized Wi-Fi device
- Detect and alert over the air wireless attacks and exploits
- Identify and track the location of the unauthorized devices

Supports Clean Air technology:

- Identification of non-WiFi threats
- Location of those threats
- Rapid adaptation of the network to the threats

Cisco Adaptive Security Appliance 5500 Series & AnyConnect

Secure supplicant for wireless devices:

- PC
- Apple OS and iOS
- Android (including CIUS and Samsung Galaxy)
- Windows Mobile

VPN connectivity can be layered on top of wireless security.

Includes firewall and posture for status of anti-virus, anti-spyware, and firewall on devices.

Cisco Access Control System

Delivers an 802.1X authentication server, VLAN override capability and Secure Authentication of Management.

Cisco Catalyst Switches

Integrates 802.1X authentication of access points and VLAN separation of traffic.

Learn More

For more information, please go to the following website: www.cisco.com/go/cyber