Cisco adaptive wips

Business, Industries

Cisco Adaptive wIPS - Introduction

An increasing number of organizations are starting to recognize the significance of the newest frontier of wireless spectrum in their business processes. However, like any other medium of system networking, this new spectrum requires strong security from possible attacks regardless to the lack of on-site deployment. Wireless intrusion prevention system (wIPS) refers to network devices which have the potential to monitor unauthorized access to radio spectrum and also take the countermeasures automatically. The wIPS therefore play a significant role in intrusion detection by checking the presence of wireless attack tools and rogue access points. They also prevent intrusion to systems by threats such as Denial of Service (DoS), Mac-Spoofing, Evil Twin Attack or Honeypot, Ad-hoc networks, Man in the Middle Attack, Client Mis-association, Mis-configured access point (AP), rogue AP and unauthorized associations. wIPS prevent any unauthorized access to local area network (LAN) as well as other data assets by means of wireless devices. The systems can be implemented as an addition to the already existing infrastructure of wireless LAN or they can also be deployed as standalone systems. As wireless spectrum increasingly introduces exciting numerous benefits to organizations the recognition of wireless security vulnerabilities and risks is critical to keep of any bottlenecks. This paper discusses mechanisms of intrusion detection and intrusion prevention drawing specific example of powerful tools provided by Cisco wIPS.

Major Detectable Wireless Threats and Vulnerability Conditions

wIPS often characterize client radios and access points by using three main classifications: infrastructure device, known device and rogue device

(Coleman & Westcott, 2006, p. 401). Classification by infrastructure device includes any access point or client station which is trusted or authenticated and not posing any security threat. Infrastructure devices are members of the organization’s wireless network. Network administrators can label all radios as infrastructure devices manually upon being detected by wIPS. At the same time, network administrators can import a list having all radio card MAC addresses owned by the organization and feed it into the system. Known devices refers to client access points or stations which are detected by wIPS but are never considered as interfering or rogue devices. After this identification, known devices are assigned to the neighboring business radio cards and are no more considered to have threats. wIPS only classifies tools as rogue devices when client access points or client stations are considered to pose some potential threat or when the device is considered to have some interference. In most cases, wIPS identify rogue devices as devices connected to the network backbone.

Wireless intrusion detection/ prevention systems (wIDS/IPS) are able to address a number of specific categories of threats including vulnerabilities, Denial of Service (DoS), general threats, and intrusions. Vulnerability alerts will always inform network administrators of any existence of settings and conditions which can cause weaknesses to WLAN and provide a swift target for hackers. Some of the weaknesses which might cause easy intrusion include the use of traffic which is not encrypted, the use of WEP and the presence of ad hoc networks (Moerschel, Carpenter & Dreger, 2007, p. 516). Denial of Service (DoS) is another threat to wireless networks. When there are DoS attacks, the DoS alerts will tend to inform the administrators about

the presence of commissions which exceed the normal thresholds and are therefore affecting the standard network operations. An example of alerts is shown below in Fig 1. 1. For instance, “ Omerta” attacks involve excessive transmission of disassociation frames meant to confuse clients and APs. Another example is the de-authentication storm which is mainly consisted of “ de-auth” frames and is normally transmitted by some sources other than the authorized WIPS sensor. These characteristics are typical signs of a man-in-the middle attack or can be signs of a general WLAN DoS attack (Moerschel, Carpenter & Dreger, 2007, p. 519). Intrusions alerts will seem to inform administrators that a certain condition which positively indicate that WLAN has been compromised

Fig. 1. 1

Unauthorized Client Detection reporting

Fig 1. 1 Example of alerts: Unauthorized client attack (Moerschel, Carpenter & Dreger, 2007, p. 518).

Among the exploits which wIPS can detect include AirJack attack which is so active to even inject fake management frames, ASLEAP attack which is able to recover PPTP or LEAP passwords, Hotspot SSID, change of MAC address, worm traffic, fakeAP that operates several SSIDs from a single station and AP Evil Twin which operated and attempts to present itself as the actual AP (Moerschel, Carpenter & Dreger, 2007, p. 519).

Fig1. 2

IP worm traffic reporting

Fig 1. 2 Example of alerts: Worm Intrusion Alert (Moerschel, Carpenter & Dreger, 2007, p. 520).

Intrusion Detection and Intrusion Prevention Mechanisms and Systems

In order to prevent such attacks, it is recommended to monitor non-encrypted traffic then divulge them to the unauthorized parties. For ad hoc networks, networks can be scanned for possible vulnerabilities and then used as potential tools for routing packets to the wiredenvironment. The use of WEP should be discouraged as it is a weak system of security. In case organizations have the infrastructure for WEP, they should consider upgrading to at least WPA security. However, for better performance, Cisco wIPS is the most recommendable system which can provide a number of security capabilities.

Upon this classification, wIPS then functions to effectively mitigate the possible threats. The commonly used methods of wireless intrusion and detection systems utilize the spoofed deauthentication frames (Coleman & Westcott, 2006, p. 402). The wIPS permit the sensors to be activated and then start transmitting the deauthentication frames. The frames then spoof the MAC address of rogue clients and rogue APs. In this mechanism, wIPS uses a known layer 2 DoS as a counterattack to make allcommunicationexchanges between the clients and the rogue APs useless (Coleman & Westcott, 2006, p. 402). This mechanism can be used to disable rogue APs, rogue ad-hoc networks and entities of client stations.

Another example of how wIPS can deal with threats management or rogue containments is the Simple Network Management Protocol (SNMP) (Coleman

& Westcott, 2006, p. 402). In this mechanism, majority of wIPS are able to determine that rouge access points are plugged to wired infrastructure and therefore wIPS may have the capacity to utilize SNMP in disabling the connected switch ports already plugged onto the rogue APs. In case the switch port is completely closed, the hackers or any malicious attacker cannot compromise the network functionality or get access to critical resources which are behind the rogue access point.

Available Tools for Intrusion Detection and Prevention

There are several vendors that have provided wIPS tools and these tools are known by their proprietary names. The commonly known tools only disable client stations and rogue access points and these tools are not normally published. In the modern state, wIPS are primarily meant for the containment and disabling rogue devices. It is expected that perhaps in the future, other wireless malicious attacks might as well be mitigated.

Several wIPS vendors sell laptops with their versions of wIPS. These tools are known as Mobile WIDS (Coleman & Westcott, 2006, p. 402). The software program that is sold together with the laptops is a protocol analyzer which has the potential of decoding frame and has layer 1 analysis capabilities which is used by attackers. Mobile WIDS software exploits the standard Wireless Fidelity (Wi-Fi) client radio and uses it as a sensor although the primary aim of the mobile WIDS software is to act as a stand-alone performance and mobile security analysis tool. Usually, mobile WIDS will retain all the policies as well as detection capacities which the vendor distributed it with. In simple terms, Mobile WIDS have servers, single sensors and consoles which are all built in one device.

Limitations of Available Options

wIPS have provided new capabilities in detecting and prevention attack activities to wireless networks. This has been seen as great advancements to WAN security as majority of threats can be kept at bay when using wIPS tools. However, wIPS will not be able to secure systems against all the known rogue devices. While wIPS provide capabilities to mitigate a number of rogue attacks, specific rogue devices will surely go undetected even when wIPS tools are used. Most of the wIPS have inbuilt radio cards with the capacity to monitor 5 GHz UNI and 2. 4 GHz ISM band frequencies (Coleman & Westcott, 2006, p. 402). However, there are other earlier versions of wireless network equipments which transmit ISM frequencies of 900 MHz and thus the equipments will not be detected posing more security threats to wireless network systems (Coleman & Westcott, 2006, p. 402).

Another limitation with wIPS is that most radio cards in the wIPS sensors use only the Orthogonal Frequency Division Multiplexing (OFDM) and direct sequence spread spectrum (DSSS) (Coleman & Westcott, 2006, p. 402). . On the other hand, there exists frequency hoping spread spectrum (FHSS) wireless network equipments which transmit in the frequencies of 2. 4 GHz ISM (Coleman & Westcott, 2006, p. 402). These devices will also go undetected by most wIPS. Perhaps the only tools that can mitigate all wireless network threats are spectrum analyzers which can detect rogue devices in all the frequencies (from 900 MHz to 2. 4 GHz) (Coleman & Westcott, 2006, p. 402).

Effective wIPS should also be able to monitor every channel that is available. Unfortunately, most wIPS tools are designed to monitor only those channels

permitted in individual organization’s country. For instance, hackers have used exploited this weakness in the united states and have used rogue devices which transmit frequencies of 2. 4GHz from channel 12 to 14 since they know that channels 12 to 14 are not acceptable in the entire United States (Coleman & Westcott, 2006, p. 402).

Cisco Adaptive Wireless Intrusion Prevention System (Cisco Adaptive wIPS)

Cisco Adaptive wIPS delivers the industry’s most accurate, cost effective and comprehensive solutions to wireless security issues. Cisco Adaptive wIPS is incorporated into the infrastructure of Cisco Unified Wireless Network to offer detection and mitigation capabilities against security vulnerabilities, malicious attacks and disruption performance sources specific to wireless network security (Cisco. com, 2010). Cisco Adaptive wIPS has the potential of detecting, analyzing and identifying a number of threats related to wireless network security and can centrally manage all functions of threat mitigations and threat resolution. Apart from security issues, Cisco Adaptive wIPS resolves issues related to system performance and this makes Cisco Adaptive wIPS to be the sole modern option for organizations that care about system securities and user satisfaction (Cisco. com, 2010).

Cisco Adaptive wIPS delivers the most modern capabilities for proactive threat prevention as opposed to other tools which provide reactive IDS (AirTight Networks, 2009). In its capabilities, Cisco Adaptive wIPS employs a multiple approach for threat detections such as network traffic, air monitoring, anomaly analysis, network configuration analysis and real-time network topology and device information which other tools don’t provide. The proactive threat prevention tools provided by Cisco grants a hardened

core of wireless network which is hard to be penetrated by wireless hackers. Cisco Adaptive wIPS collaborates with a robust security portfolio from Cisco Self-Defending Network to offer an advanced set of layered mechanism of threat detection for wireless and wired interconnections (Cisco. com, 2010).

Why Choose Cisco Tools?

Integrated Network Infrastructure

Cisco Adaptive wIPS exploits wireless network infrastructure integration power for cost efficiency, enhanced security and performance. Unlike other typical wIPS, Cisco Adaptive wIPS is directly integrated into Cisco Unified Wireless Network infrastructure components including Cisco AP, Cisco wireless LAN controllers, Cisco Wireless Control System and Cisco Mobility Services Engine (Cisco. com, 2010). The integration of wIPS with WLAN infrastructure provides not only cost efficiency but also efficiencies in operations which are granted by only a single infrastructure for WLAN and wireless IPS at the same time. The need for separate infrastructure in other wIPS makes it more expensive for organizations to afford (Cisco. com, 2010). The general features that male Cisco Adaptive wIPS superior features can be understood from table 1. 1 below

Table 1. 1 Technical Overview of Cisco Adaptive wIPS Functions and Usage

Technical Function	Usage Scenario
Rogue threat Detection and Mitigation	Detection and mitigation of rogue clients and APs
Over-the-air attack detection	

Detect external thieves and hackers	
Assessment of security vulnerability	
Robust network security	
Self-healing and performance monitoring	
Consistent WLAN performance	
Proactive prevention of threats	
Internal security audit and reporting	
Compliance and security reporting	
External audit and compliance reporting	

Table 1. 1 Overview if technical capabilities offered by Cisco Adaptive wIPS (Cisco. com, 2010)

Accurate Detection and Comprehensive Protection

With Cisco Adaptive wIPS, clients gain a comprehensive protection and accurate real-time detection. Cisco has an advanced approach to detecting threats by integrating capabilities such as network anomaly and traffic analysis, air monitoring, real-time topology and network device information, as well as real-time analysis of network configuration. This combination brings to Cisco Adaptive wIPS analysis engine a comprehensive viewing of the event capabilities and thus enabling Cisco Adaptive wIPS to detect events rarely or not easily traceable using purely over-the-air signatures (Table 1. 2). Not only does this make Cisco Adaptive wIPS to detect these signatures but also makes Cisco Adaptive wIPS tools to make accurate detections decisions hence reducing false positives and increasing effectiveness (Cisco. com, 2010).

Read also about Threshold Capabilities

Table 1. 2 Rogue Detection and Mitigation

Functional Feature	Specific Technical Features	Benefits
Rogue Detection	Scanning of On/Off-Channeling	Detection of rogue APs, spoofed clients, rogue clients and client ad hoc connections on each channel related to 802. 11 spectrum
	Network analysis based and signature-based threat detection	Increase rogue, spoofing detection, and ad hoc accuracy and breadth hence decreasing manual threat investigation
Spectrum Intelligence	Detection of all rogue devices and DoS in non-802. 11 frequencies like radar, Bluetooth and microwave	
Event Classification	Personalized auto-classification of rogue events	Auto classifies threats according to levels defined by user classification rules and thus reducing interventions by staff
Tracing of rogue-port switch	Identifies customer-side rogue devices and reduces manual investigations	
Identify rogue physical location	Plotting of rogue AP and clients on floor maps to facilitate removal	
Threat Mitigation	Disabling of rogue switch-Port	Disables Ethernet port remotely to which the rogue AP is plugged and thus

speeding the mitigation process

Over-the-air mitigation

Mitigates all clients, rogue APs and ad hoc over-the-air connections by employing any deployed Cisco AP and thus scaling and speeding mitigation process

Manual or automatic mitigation

Flexible actions of mitigation enable tailoring to the client operational and risk environment model

Table 1. 2 Technical overview of Cisco Adaptive wIPS Features and Benefits of Rogue Detection and Mitigation (Cisco. com, 2010)

Cisco Adaptive wIPS also provides detailed attack classification and thus providing the users with easy to implement rules for automatic threat classification and security mitigation. The automatic classification combined with the inherent accuracy of the system highly reduces operational costs incurred while using manual investigation methods of threat detections. Cisco therefore integrates the advanced techniques in classifying and detecting threats with extensive vulnerability, extensive attack and a library of performance detection. Cisco Adaptive wIPS can detect several threats including DoS attack, man-in-the middle attacks like relay attacks and identity/address spoofing, hacker access points like evil twins and honeypots, ad hoc connections, network reconnaissance, protocol attacks, encryption and authentication cracking, over-the –air vulnerabilities of network security, as well as performance related issues such as coverage holes and interference of co channel (Cisco. com, 2010).

Cisco Adaptive wIPS is complemented with Proactive Prevention of Threats Capabilities

Network security is better achieved when threats can be prevented before damages are done to the system. There are rich tools embedded in Cisco Unified Wireless Network which complements the Cisco Adaptive wIPS and thus providing critical techniques for preventing threats. An example of these techniques includes 802. 1x wired port authentication which is in all Cisco access points and it locks out all rogue access points (Cisco. com, 2010). Strong Wi-Fi Protected Access 2 (WPA2) and user authentication and 802. 11 i standards of encryption prevent data from traversing the WLAN and access to the network (Cisco. com, 2010). These features protect against theft of network resources. IEEE 802. 11w in Cisco Management Frame Protection authenticates and encrypts WLAN management frames in order to protect against over-the-air attacks (Table 1. 3). The policies for client exclusion can automatically respond to high-level failures in user authentication and spoofing of IP address.

Table 1. 3 Over-the-air Attack Detection

Functional Feature

Specific Technical Features

Benefits

Breath of Attack Detection

Network reconnaissance and detection profiling

Analyzes the behavior of traffic and matches patterns to detect techniques and tools like Kismet, Netstumbler and honeypot thus providing timely alerts that the hacker is seeking loose avenues

Encryption and authentication cracking

Analyzes traffic and matches pattern to detect tools such as AirCrack, Chop-Chop, Airsnarf and ASLEAP

Inadvertent or malicious DoS

Analyze traffic and match patterns to detect techniques and tools such as AirJack, 802. 11 protocol abuse, resource starvation and RF jamming

Detection of man-in-the middle

Detect techniques and tools such as replay attacks, 802. 11 protocol manipulation and fake APs to avoid theft of network resources

Detection of spoofing and impersonation

Detect techniques and tools such as fake APs, MAC/IP spoofing, evil twin APs and spoiling of Dynamic Host Configuration Protocol (DHCP)

Detection of Zero-Day attack

Detect uncategorized and new threats which other wIPS cannot detect

Continued research in threat detection

Research to discover new attack tools and techniques

Classification and tuning of events

Detection profiles set by default

Detects tuning profiles by default

Tuning driven by knowledge base

Gives operators description of attack types in plain language

Table 1. 3 Technical overview of Cisco Adaptive wIPS Features and Benefits of over-the air attack Detection (Cisco. com, 2010)

Critical Monitoring, Reporting and Overall Management

What makes Cisco Adaptive wIPS stand out is the type of management, monitoring and reporting it provides. Cisco Adaptive wIPS offers critical monitoring, reporting and management tools which is integrated into Cisco WCS thus providing a single and unified capability for all wireless security operations and wireless network. The integration of wireless security and wireless network management greatly reduces the security challenges by keeping all APs and security policies and client device inventories aligned. This also simplifies the reporting and management of events (Cisco. com, 2010). The features offered by Cisco to provide ease in network security and managed can be understood from Table 1. 4 and 1. 5 below

Table 1. 4 Auto-optimization and Performance Monitoring

Functional	Feature
Benefits	
Persistent network monitoring of performance and networkhealth	
Protect against accidental, malicious or over-the-air interference	
Automatic problem fixing of problems in RF Domain	
Solve remedial issues like RF-based DoS without the intervention of an administration	
RF management with no special skill required	
Reduces operation staff overburdening	

Table 1. 4 Auto-optimization and Performance Monitoring (Cisco. com, 2010)

Table 1. 5 Monitoring Of Security Vulnerability

Functional	Feature
Benefits	

Automated analysis of configurations round the clock
Analyze wireless APs, controllers, and all management interfaces
Analyze on the Best Practices and Customer-Based Security Policies
Clients can use WCS Config Audit capabilities to analyze all configurations using their individual security policies
Wide identifications of vulnerabilities
Identify data theft, DoS attack, man-in-the-middle, unauthorized network access and protocol attacks

Table 1. 5 Monitoring Of Security Vulnerability (Cisco. com. 2010)

Recommendations and Future Directions

Security auditing can help fix the possible network security bottlenecks that exist in using various wIPS tools (Coleman, Westcott, Harkin & Jackman, 2010, p. 350). As a good practice, organizations should have wIPS security audit to always maintain their wireless networks at secure levels. It is not unusual to find several organizations running without wIPS and this can be dangerous in terms of network security (AirTight Networks, 2009). However, majority of wIPS vendors always perform the initial security audit without any charges. Upon taking wIPS security audit, the vendor will then show the client possible loose security points and make recommendations. Afterwards, the vendor will sell to the client a distributed wIPS solution which can monitor WLAN security in full- time basis (Coleman, et al, 2010, 350).

Wireless IDS/IPS products in the future are expected to evolve and include enhanced analysis of layer protocol. However, with the availability of WLAN encryption, this functionality may be seen futile. At the same time, the encryption of payloads may see the wIPS capabilities useless as wIPS do not

understand the language of encryption used in encrypted payloads (Cisco. com, 2010). This dangerous limitation can be equated to the inability of wired IPS to properly analyze a number of unauthorized attack actions which can possibly be present in the VPN traffic. However, there is an ongoing Threat and Vulnerability Research and Detection Development at Cisco comprised of a dedicated team with the main objective of mapping and discovering new attack techniques (Cisco. com, 2010). The team at Cisco endeavors to analyze all network vulnerabilities which can be exploited in developing new tools to mitigate the merging threats.

Conclusion

As businesses persistently rely on the new frontier of wireless network spectrum, new attacks continue to be crafted by attackers which pose challenges to the vendors developing network security devices. Manufacturers of mobile phones, laptops, iPhones and other gadgets which utilize wireless network should invest in research to identify the emerging tools and techniques which the hackers use in gaining unauthorized access to networks. However, a few companies have taken this initiative. Cisco continues to improve their products of wireless security monitoring and management by identifying the existing and the emerging threats. Cisco then integrates functionalities under a single infrastructure thus making clients to significantly reduce costs of operations and redesigning wireless network infrastructure.

Reference:

AirTight Networks (2009). Walk around wireless security audit-the end is near! Retrieved August 13, 2010 from, http://www. airtightnetworks. com/fileadmin/pdf/whitepaper/WP_WalkAroundWir eless. pdf

Coleman, et al. (2010). CWSP: Certified Wireless Security Professional Official Guide. Indianapolis, Indiana: Wiley Publishers

Cisco. com. (2010). Cisco Adaptive Wireless Intrusion Prevention System. Retrieved August 12, 2010 from, http://www. cisco. com/en/US/prod/collateral/wireless/ps9733/ps9817/data_sheet_ c78- 501388. html

Coleman, D. D., & Westcott, D. A. (2006). CWNA: Certified Wireless Network Administrator Study Guide. Indianapolis, Indiana: Wiley Publishers.

Moerschel, Carpenter & Dreger. (2007). CWSP Certified Wireless Security Professional: Official Study Guide (2nd Ed). New York: McGraw-Hill Companies.