WIPS Wireless Security in Enterprise Network

C.Monika¹, S. Sakhthi priya², D.Sumihra³, Mr. V. Shanmugam, M. Tech⁴
Student¹,²,³, Assistant Professor⁴
Department of Information technology
Kingston Engineering College, India

Abstract:
In the current world there exists many security protocols. The technical advancement also developed to duplicate or malfunction one’s documents and data. In this paper the enhancement in enterprise level security is proposed using WIPS. Many protocols are using in day by day work for wireless security like WEP, WPA and WPA2. But with use of rogue and inference access points the hacker can interrupt a signal and collect the client’s data from the controller. Here introducing the security protocol WIPS in the AP controller. This WIPS-Wireless intrusion prevention detects and prevents the rouge AP from entering the secured network system. Once the rogue is detected the rogue containment is performed and it prevents the client from connecting to wrong AP by giving warning message to every client in that network area till they disconnect from the AP. Thus it will disconnect every client who gets connected to that rogue AP. Thus, this WIPS is the proposed idea to be used along with the Aruba access point it is well suited for large scale enterprise.

Keywords: Rogue access point, WIPS and WIDS, alarm, air monitor, airwave, WLAN, Aps, RF licence.

I. INTRODUCTION

It is important to specific the rules at the top of the directory and that generic catch-all rule are at the bottom. If a neighboring APs signal strength is weak so it would fall to the ‘Detected wirelessly’ rule and get classified as a suspect neighbour Wireless Local Area Networks (WLANs) succeed in providing wireless network access at acceptable data charge. The association of Electrical and Electronics Engineering (IEEE) has set standards and specifications for data communications in wireless environment, IEEE802.11 is the driving technology for WLANs. WLANs are deployed as an extension to the existing fixed LANs and due to the nature of WLANs are different from their wired counterparts, it is important to raise the security of WLANs to closer or equal to the wired LANs. In the infrastructure topology, wireless stations (STAs) communicate wirelessly to a network access point (AP) which is connected to the wired network, this setup forms a WLAN. The establishments of connections between STAs and AP have three phases; probing, validation and association. In probing phase, the STA can either listen in passively to AP signal and automatically attempt to join the access point or can actively request to join an AP. Next is the authentication phase, the station here is authenticated by the access point using some authentication mechanism. After successfully authenticating, the station will send an association request to the access point, when approved, the access point adds the STA to its table of associated wireless devices. The ACCESS POINT can associate many STAs but an STA can be associated to one access point only at a time. There are many issues about the security of WLANs like with Radio Frequency (RF) as a middle of transmitting information and the fact that all messages are broadcasted to wherever the coverage of that WLAN can reach. The propagation of air waves cannot be blocked or locked in a room so there is a big risk. When dealing with WLANs it is important to keep three security goals in brains, Authentication to the WLAN, Confidentiality and Integrity of the data transmit. Confidentiality means hiding high sensitive data during information transmission between STAs and access point So, there is a need to centralize and handle security issue in small WLANs as well as large ones and a need to develop techniques to counter security threats. As WLANs application like wireless Internet and wireless e-commerce increase very fast, there is a need to assure the security of such applications. WLANs security problem in both physical and logical aspect and discusses the current existing solutions to these troubles. The following sections will therefore discuss major threats affecting WLANs security. The configuration and features of the Wireless Intrusion Protection solution are available from Aruba Network. For simplicity, this document assumes that the Controller, RF Protect license and Air Wave are used. In most cases, functionality is similar to what is in the Controller is available in Aruba Instant.

<table>
<thead>
<tr>
<th>TABLE 1. ARUBA SOFTWARE VERSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Product</strong></td>
</tr>
<tr>
<td>ArubaOS™ (Mobility Controllers)</td>
</tr>
<tr>
<td>AirWave®</td>
</tr>
</tbody>
</table>
In the past, wired networks were considered to be far more secure than wireless networks. Today, however, wireless networks are as secure as wired networks as long as they are properly configured. Wired networks use cables connected to Ethernet ports on the network router on one end and to a computer or other device on the cable's opposite end. A wired network is simply a collection of two or more computers, printers, and other devices linked by ether cables.

Problems in wired network

Mobility: The disadvantage of wired technology is that it lacks the mobility that wireless technology provides. You are physically limited to the make of the cable, where wireless technology allows users to move great distances freely and without hassle. Moving equipment that is even within the series of the cables may be tricky if you select to mount the cables rather than have them dangling.

Damage: Another physical constraint of wired technology is that it can be easily damaged. This is not as large of a concern with wireless technology. Exposed cables are vulnerable to everyday abuse from things such as cleaning. Wires that are uncovered and not properly laid may also pose a tripping risk. Not only damaging the cable but also potentially sending someone to the emergency room. Damaged wires may have to be completely replaced.

Expansion: The scalability of wired technology is costly and time consuming. It may even interrupt workflow as crews rewire areas within the office. In comparison, wireless networks can be set up cheaply using multiple access points without the need for significant alterations in the building.

A. Solutions

1. Properly configure network

2. Run cables underneath carpets or mats

3. Keep network up to date

4. It was very difficult to pinpoint the fault location on those days.

5. But later using the impedance of the wire, they can find the location.

III. PROPOSED SYSTEM

A. Wireless scanning

The Radios in an Aruba access point can be configured to run in different Modes: Access point mode, Air Monitor (AM) mode, or Spectrum Monitor (SM) mode. Each mode is designed to work on different tasks but will perform some level of all of them. Access point mode radios focus on serving clients and pushing wireless traffic but they also perform IDS detection, rascal detection and spectrum study. The information provided by the access point is the base for detection. Most customers only need access points and do not need to deploy any air monitor mode. IDS detection occurs 100% of the time that the access point is serving clients. This means you will have full attack detection against your deployed network. The off-channel scanning will find rogue policy and IDS attacks outer of your network. Typically, an Access point will perform off channel scan for every 10 seconds for slightly less than 100 milliseconds. This allows the Access point to see what is occurring around it, without causing problems for clients. A lot of logic has been built into the Aruba scanning algorithm. It will pause scanning for any similar detected voice or video on a particular radio to ensure the best quality for the clients. These settings can be configured using the VoIP Aware Scan, Video Aware Scan and Power Save Aware Scan options in the Adaptive Radio Management profile. PEF firewall rules can also be defined to pause scanning based on a type of traffic running through the network. This typically is not needed but can be useful to ensure QoS for specific latency sensitive applications. It is important to note that the off-channel scanning is used for more than just WIP. It is also a key piece of Aruba's ARM. All Aruba access points ship with scanning enabled by default. All published Aruba performance has scanning enabled unless otherwise noted. The Access point mode can be configured to scan different sets of channels by changing the Scan Mode setting in the scanning section of the Adaptive Radio Management profile. Scanning all the domain channels is recommended. That will include any channel valid in any regulatory domain, not just the regulatory domain of the access point. This step is recommended since attackers normally don’t feel the have to to follow the law. Please note that the access point cannot perform containment on the channels outside of its regulatory domain. The set of channels can be restricted to use those within the access point’s regulatory domain but that is not recommended for security conscious customers. The access point uses a bucketing based algorithm for channel scanning. The access boots channels are divided into 2 different buckets, regulatory channels and non-regulatory channels. The regulatory channels are scanned more frequently than the non-regulatory channel. The third channel container, active channels, is populated as the access point scans and detects channels with wireless traffic. The active bucket is scanned more frequently than all the others. This allows the access point to spend most of its time on channels where threats is likely and the least amount of time on channels that are not
expected to see attacks. Because of the adaptive nature of the scan algorithm it is very difficult to give an answer to the question ‘how long does it take to scan all channels’. Typically, all channels will be scan at least once in fewer than an hour with active channels getting scanned much more frequently. Starting in AOS 6.4.3, the 2x2 series APs will scan 80 MHz in the 5 GHz spectrum when feasible. This significantly decrease the amount of time it takes for an AP to detect rogue devices in the 5 GHz band. Access point mode can perform wireless containment but they will prioritize close to client traffic over containment. This is a very key distinction and the reason why Air Monitor mode are recommended if wireless containment is enabled. If the access point mode is serving clients on channel 1 and the rogue is on channel 6, the access point mode will not change channels to contain the rogue. If the rogue happens to be on channel 1, the access point mode will perform wireless containment while serving clients. If there are no clients on the access point mode, it can be configured to change channel to contain the rogue device by enabling the ‘Rogue access point Aware’ setting in the Adaptive Radio Management profile. Access points can also perform spectrum analysis on the channel where they are serving clients. This gives the access point the ability to detect and classify non-Wi-Fi interferers that are impacting the deployed wireless network. Access points are not able to scan and process spectrum data off the home channel due to the short dwell times and relatively infrequent visit to other channels. Spectrum monitor are designed to scan each channel within 1 second. Air monitor are dedicated to wireless security. They do not serve clients. Air monitor typically do not need to be deployed at the same density an access point would since they do not serve clients. In most cases a 4 to 1 or 5 to 1 ratio of access points to Air monitor is recommended, but that varies heavily based on access point density and environment. AMs use a channel scanning algorithm that is similar as an access point but has an extra bucket for ‘Rare’ channel. In raw MHz that is 2412-2484 and 4900 during 5895 in 5 MHz increment. Rare channels include the 4.9 GHz spectrum which is a licensed public safety band in many countries. AMs will also scan the 5 GHz spectrum in 5 MHz increments. Due to the equivalent nature of wireless, we have found that the natural bleed through of radio frequency signals will allow us to find rogue that are configured in among channels by scanning each 5 MHz the channels scanned by an air monitor are configured in the air monitor scanning profile which is part of the radio profile.

**B.802.11ac Rogue Detection**

802.11ac devices are backwards companionable with 802.11a/b/g/n devices. For 11ac devices to be backwards Companionable, the management frames, like beacons, will go out at 20 MHz That way non-11ac clients can detect the access point and connect to them. This means that legacy a/b/g/n access point can also wirelessly detect rogue 11ac access points. But the legacy Access points won’t necessarily have visibility into the data coming out of a rogue 11ac access point. If the rogue is communicating with an 11ac client, the data frame may have a channel that is too large, or a accent that the legacy access point cannot decode. That means legacy access points are unable to always determine if a client is related to the rogue. That recognition is critical for more advanced skin tone such as wireless containment and wired rogue detection. If an access point can’t hear the client on the rogue, then it cannot contain it. Earlier it was mentioned that the wired rogue detection was based on the source MAC address of frames coming out of the rogue access point. Those are the data frames. With an 11ac rogue and an 11ac client, they will not be visible to 11a/b/g/n devices. If a legacy client connects to the 11ac rogue, then it will be detected by the legacy access point since the legacy radio can understand the traffic. Because of such limitations, an 11ac overlay or 11ac network is recommended for high security customers. 11ac is required to detect all potential threat.

**Level-1CLASSIFYING ROGUE ACCESS POINTS:**

Rogue classification should happen in Airwave. The controller can perform basic device classification but Airwave provides a more robust and configurable solution. The heart of the Aruba classification system is configured on the Rapids Rules page in Airwave. The rules are displayed in a list form. They act like firewall rules. The first rule in the list that is matched is the classification a device will receive. If a device does not match any rule, it will get the default classification specified in the drop down above the rules list. Devices will get continuously reclassified as new information. If a week later the device suddenly had strong signal strength of -60 dB, it would be promoted up to a suspect rogue. At that point an alert could fire, but alerts in the alerting and reporting chapter. Now if that device were to be detected on the wire a day later, it would be classified by the ‘Detected wirelessly and on local area network’ rule and reclassified as a rogue. Threat level is an optional additional bucketing system within a single classification. It has no set definition. A threat level of 1 or 10 can be considered the most dangerous. However, be sure to keep the rules in sync so that a specific threat level is always considered the most dangerous. The threat level can be used to change the alerting options within Airwave. The rules above are pretty much the default rules you will see in RAPIDS. The rules should be customized for your unique environment. They should be updated based on the security policies implemented by your enterprise. It is a recommended best practice to make sure that anything classified into the ‘Rogue’ categorization is considered a major security threat and will be investigate by the security team right away. It is important to focus that classification down into things that need to be investigate so that the true threats don’t get lost in a flood of neighbouring devices. Once the customized security policy rules are in place, it is recommended that you look at the classified devices. You can often find sets of devices that can be reclassified into the neighbour classification without creating any security risk. It is both common and recommended to create general rules to match neighbouring devices so that they can be pushed down the danger meter into less threatening classifications. A common example is 2Wire ACCESS POINTS. 2Wire makes home DSL routers that are often used by AT&T or SBC for wireless. If you have a campus near an apartment building or residential area, you will see a lot of 2Wire devices. Within RAPIDS you can create a rule that will reclassify any 2Wire device to be a neighbour without manually inspecting it. This can save a great deal of time and make it much easier to keep up with the wirelessly detect devices in your RF environment. The general 2Wire rule is to classify any device manufactured by 2Wire with a 2Wire SSID, running encryption,
heard with weak signal strength and not connected to the local area network as a neighbour.

**Level-2 Rouge Containment:**

Not all customers are comfortable running rogue containment. Some types of rogue containment may impact neighbouring networks while others will only protect your network and pose no threat to neighbours. Just like IDS, containment is most easily configured through the wizard. Containment may also be referred to as shield in or mitigation. They all mean the same thing. Breaking the rogue’s or client’s ability to connect to the network. There are two main types of containment, wired and wireless. Wired containment is performed by ARP poisoning the default gateway of a rogue device connected to the wire. The detecting AP or AM will perform the containment. The wirelessly detecting device needs to be on the same VLAN as the rogue for the wired containment to be successful. There are two types of wireless containment, death and tar-pitting. Both start out the same way. The Aruba AP will send de-authentication packets to the AP and the client device. Most client devices will automatically try to reconnect to the network. When death is selected, the AP will send another deauth packet once the client is connected to the network. With modern clients that can happen as quickly as every 15 milliseconds. Tar-pitting will behave a little differently. When the client device attempts to reconnect to the network; the Aruba AP will respond with a probe response that has some fake data in it to induce the client device to connect to the Aruba AP rather than the rogue device. The client device then takes some time to realize the connection isn’t going anywhere. At that point it disconnects and starts over. The important thing is that realization can take anywhere from 500 milliseconds to requiring user intervention. This makes tar-pitting a significantly more efficient mechanism to contain rogue devices. AMs are always recommended when wireless containment is enabled. APs will perform containment, but only if the rogue device or client is on the same channel as the AP. APs may change channel to include a rogue if there are no clients on the AP and ‘Rogue AP Aware’ is enabled in the ARM profile. AMs will mark a channel for DOS and will alternate between it and the channels it is scanning. This allows an AM to spend a lot more time containing rogues. There are a lot of automatic rogue containment options that go beyond ‘contain if the device is classified as a rogue’. The safest and most common options are ‘Protect Valid Stations’ and ‘Protect SSID’. Any station that has authenticated to the Aruba network with encryption will be automatically classified as valid. Once this happens, the Aruba network will not allow them to connect to any other network if Protect Valid Stations is enabled. This protects the network by preventing users with sensitive data from connecting to neighboring networks that may be snooping the data. Protect SSID will automatically contain any non-valid APs that are broadcasting the SSIDs on the controller. This can be very effective and preventing honey pot attacks and poor network experience caused by connecting to non-approved APs.

**IV. SCOPE AND CONCLUSION**

Thus, the rogue and inference access points are detected and prevented from network. It also used in wired network from the wireless signal from making traffic in the wired network connection. The WIPS is the security protocol using that the rogue is avoided and WIPS is mostly used in AP but Aruba is the one which has WIPS feature after getting RF License. Thus, rogue containment is done and data are protected. The warning message lasts till the clients get disconnect from that AP. This is the proposed idea and scope of this project with a correct output it is implemented. Surely this idea will bring a great revolution in enterprise level security and it will overcome all issues and enhance a good security system to enterprises.

**V. REFERENCE**


[2]. Autonomic 802.11 wireless LAN security auditing J. W. Branch; N. L. Petroni; L. Van Doorn; D. Safford Privacy Year: 2004, Volume:2, Issue: Pages: 56 - 65, DOI: 10.1109/MSP.


