WLAN Security:
Simplifying Without Compromising

Ruckus Wireless | White Paper

Striking a balance between security and cost/convenience

Executive Summary

Fundamentally there is a converse relationship between security and convenience — and in the case of WLAN security, convenience translates into IT management resources in addition to end user time and effort. Finding a balance between the right level of security for your size and type of organization is critical for cost control and end user productivity. This paper will help you determine the sweet spot for the optimal balance between your security needs and overhead cost/convenience.

Introduction

The defining characteristic of WLANs is that they do not have clear physical borders — radio waves spread. Anyone within range can potentially connect to, and certainly listen in on (packet sniff), a WLAN. Encryption is used to keep WLAN data private; encrypted data can still be overheard, but not understood. Authentication is used to identify and manage who can connect and actively use the WLAN, which at the extreme end is used in 802.1X networks that look up user credentials on an authentication server before granting network access to lesser forms of data base lookups to no authentication at all.

Although emphasis on user authentication and data privacy issues are central to WLAN security, they are only part of the story. WLAN security is part of network security, and the objective should be for the wired and wireless portions of the network to operate as a seamless whole — in other words, security redundancies are costly and inconvenient, if unnecessary for enterprises who have certain security capabilities on

BREAKING THE WIRELESS SECURITY PARADIGM

Wireless security was once considered the gating factor in implementing a wireless network — it is now quite the opposite. Although initial wireless encryption technologies were found to be crackable, the new standards have never been cracked. Traditionally, IT views the wired LAN as invulnerable; however, nothing can be farther from the truth. Less than a small fraction of users encrypt or authenticate the traffic on their LAN, and although hackers can't listen from outside the building, any physical access would be the weakest link to the wired network. By virtue of the nature of wireless frequencies leaking from the confines of a building, wireless vendors have developed encryption and authentication capabilities out of necessity, which makes the wireless traffic more secure. In reality, traffic over a wireless network is now more secure than its wired counterpart.

Case Study: At Central Utah Clinic, Erik Briggs, the IT manager, implemented Ruckus' Dynamic PSK, which is a perfect combination of security and practical usability strong enough for rigid HIPPA compliance regulations. Dynamic PSK eliminated the need for IT staff to manually configure each end device with a unique key and enabled them to simplify decrement of the AD database when a user was invalidated instead of requiring a pre-shared key change for all users, thus saving time and money.

their wired network. There are also wireless specific threats beyond eavesdropping and user access control to be concerned with, such as unauthorized 'rogue' APs allowing backdoor access to the network, or honeypot APs used in attacks that lure end users onto unsecure external networks.

Ruckus Wireless WLANs with ZoneDirector controllers have a number of innovations to help large and small organizations deploy a secure wireless LAN. Ruckus Dynamic PSK (DPSK) can provide simple encryption key administration to increase encryption strength over common WPA-PSK deployments. This is particularly valuable to organizations that are not ready for a full RADIUS based 802.1X deployment, don't have the need for such a deployment, or don't have the resources to deploy and maintain such a network in a way that will ensure productivity. DPSK is a perfect balance between the right level of security for your organization with the right level of convenience for your IT resources and end users alike.

A Brief History

Security was the IT manager's main concern in the past and the reason why WLANs were not implemented. However, as the ubiquity of wireless devices drove demand from end users, evolving wireless standards have solved these security issues to the point where a properly implemented wireless network is more secure than most wired networks (*See sidebar: Breaking the Wireless Security Paradigm*). The following is a brief summary of the previous issues and resolutions. More detail of these technologies will follow.

Wired Equivalent Privacy (WEP)

The original standard for wireless security was proven to be crackable. Now standards are more secure. With the introduction of 802.11i in 2004, encryption became effectively uncrackable in its current form; however, this can come with some complexities. 802.1X is the strongest form of authentication, but it is more expensive and difficult to set up and maintain.

Using a pre-shared key (PSK) can be strong, but using a single passphrase limits security to its weakest link — the "human factor," and requires IT managers to replace passphrases manually on a regular basis for security purposes. For best user experience and in the interest of saving IT manager time with troubleshooting and maintenance, it is important to consider a balance between strong 802.1X and PSK. Dynamic PSK or ZeroIT is the best balance for usability and security in that it does not involve IT time and removes the user from handing out their unique key.

FIGURE 1: Security Options

Security Option	Benefits	Drawbacks
Open Network	• Simple to use and deploy	• Completely insecure • Some client configure still required
Pre-Shared Key	• Straightforward implementation • Link layer encryption	• Easily compromised • Same key for all employees • Client configuration required
802.1X	• Robust and comprehensive framework • Strong encryption and authentication	• Expensive authentication server • Requires 802.1X supplicant on every end device • Highly complex • Time-consuming to implement
Dynamic PSK	**• Easy to use** **• Strong encryption without 802.1X** **• No admin intervention** **• Works with existing authentication without EAP**	**• Manual configuration required for handheld devices (e.g., phones, PDA) if on corporate network, however handheld devices users can use guest network**

Rogue access points (APs)

Rogue APs have long been a bane to IT. Network admins wasted countless hours tracking down unauthorized devices. Two fundamental issues drove rogue APs: lack of corporate Wi-Fi and cheap home APs that required little network knowledge to install. The later made it simple for employees to bring rogue APs to the workplace. Rogue APs are possibly the first case of consumer products critically impacting tightly controlled corporate networks. Rogue AP detection and location services in modern enterprise-class WiFi systems have given IT powerful tools to combat these devices.

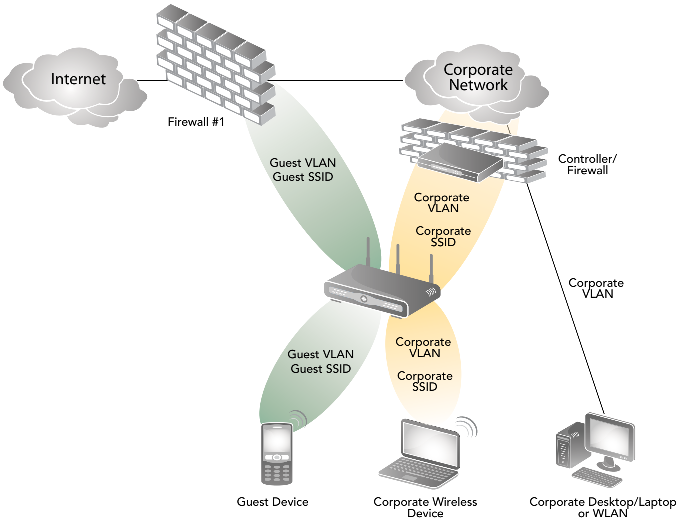
WLAN Security is part and parcel of Network Security

Wireless security is network security. The WLAN exists to provide mobile end users with access to the wired network, both for internal resources and Internet access. Whether the organization has a simple flat single subnet network connected only to an Internet gateway, or is segmented by multiple routers and firewalls, the WLAN has to integrate with the network as a whole and all WLAN traffic can be expected to wind up on the wired network.

Virtually all wired networks have a firewall implemented between the corporate network and the Internet. Some larger or more security conscious users may also have a firewall segmenting the corporate network from the rest of the user groups within the enterprise. In either case, the existing wired network security implementation can be leveraged to ensure that both the wired and wireless networks are secure.

For example, a security conscious business or larger enterprise with the resources to manage a robust security network would route all of the network traffic from the Internet into the corporate network through a firewall at the DMZ. Further, they would have another firewall segmenting the corporate network from differing end user groups on the wired network via different corporate VLANs with 802.1x authentication. Another corporate VLAN set-up would be created for the wireless network with a corporate SSID, and another SSID could be set-up for guest users wishing to only access the internet which would circumvent the internal firewall and corporate network. See the diagram below:

FIGURE 2: WLAN Implementation



In this example, the WLAN implementation layered on the existing wired network and existing security implementation negates the need for another firewall on the WLAN controller, which would simply be more software to learn and maintain without any added benefit.

Traffic segmentation

Regardless of whether a network includes a WLAN, even for very small networks, basic traffic segmentation is good security practice. In the simplest case, servers and end users, at least, should be on different segments or VLANS. Larger networks may be more complex, with users in different groups or classes and even servers grouped into logical groups. It is advisable to segment such groups by VLAN and access privileges. Policies can then be built around what kind of traffic is allowed from one segment to another.

For example, in a simple, wired only, case, a network has 4 subnets: a server subnet, an employee subnet, a guest subnet available in the conference rooms and a DMZ with an internet accessible web server. A firewall controls traffic such that the guest network is only allowed to access the internet for email and web traffic. The server subnet is only accessible from the employee subnet, and perhaps only with a proprietary database application. The DMZ is accessible by http only from the internet or http, https and SSH from the employee net, but the DMZ cannot originate traffic to any destination behind the firewall. As an organization's needs become larger and more complex, this sort of segmentation can grow in complexity as well.

In the above example, the subnets are isolated from each other by physical port isolation. A more sophisticated approach could use 802.1X enabled switches to assign VLANs according to user credentials, so that the same physical ports could service the employees after authentication, and allow guest access for those who do not authenticate.

Traffic segmentation not only helps logically structure access control, but it helps with management of other security threats. Other security systems, such as network intrusion prevention (NIPS) or internal firewalls can be placed where they will do the most good. Threats such as network worms are more easily isolated and contained.

WLAN specific traffic segmentation

WLANs primarily serve mobile devices and properly segmenting WLAN traffic will depend on the needs of the devices and their end users and the available network infrastructure. Legacy access devices may have security limitations (such as WEP only support) when compared to newer equipment. Almost all WLAN deployments include provisions for guest access. When deciding how to segment WLAN traffic, start by defining the needs of the end users and devices, and how those needs affect your network security policies.

One simple method to segment WLAN traffic is to use a different SSID for each class of device or user and map that SSID to a different VLAN — Ruckus APs support VLAN trunking. In the wired only network example above, one SSID serves the employees, while a guest SSID serves guests. The employee SSID has the most robust access control available, either Ruckus Dynamic PSK or 802.1X, but fewer controls once the network is accessed. The guest SSID may be wide open, or it may use Ruckus Guest Pass Authentication for access control.

Although multiple SSIDs are a simple method for traffic segmentation, beware of overusing them. Each SSID must send beacons, and a large number of SSIDs will reduce network bandwidth with management frame overhead. If the network requires multiple user classes, consider use of a RADIUS authentication server. All users could utilize the same SSID, but be assigned VLANs dynamically from their user profile.

Not all Ruckus APs have to service all VLANs. APs can be grouped appropriately in Zone Director. For instance, a warehouse may be using legacy WEP only inventory devices. There may be no need for APs in the offices to service the warehouse WLAN and no need for the warehouse APs to service the employee or guest WLANs, which are only needed in the office areas. In such a case, grouping the APs appropriately will allow different WLAN and security policies to be applied to each area.

Wireless Client Isolation

With a Ruckus wireless network, segmentation and its security benefits can readily be further extended to each client. End users usually do not have any need to directly access each others' machines; the network should, and usually does, have server based file shares, email or similar methods available for sharing resources.

Ruckus WLANs include an option for Wireless Client Isolation. This option prevents WLAN clients from directly communicating with another wireless device on the same VLAN. This way a disgruntled employee cannot attempt to hack into another employee's laptop over the WLAN. If a shared resource, such as a printer, has to be on the same VLAN as wireless clients, it can be 'white listed' to allow access.

WLAN Authentication and Encryption

Because radio waves cannot be isolated to a narrow location, the central concerns of WLAN security from the beginning have been access control (who can use the WLAN) and encryption (how to keep WLAN data private).

These are essentially the same concerns that came up with VPN access to secure networks over the insecure Internet. In fact, because of flaws in the original WEP security standard, many early WLAN deployments were completely separated from the primary network and used VPN connections for authentication and encryption to corporate resources. This architecture treated the WLAN as if it were an incoming Internet connection. It was and is a very secure architecture, but it required additional equipment, such as additional VPN concentrators beyond the scale required by the organizations remote access needs.

The earlier flawed WEP security standard has been replaced by 802.11i/WPA2, which is much more robust and allows for full integration of the WLAN into the LAN. Although a detailed description of encryption options follows, it boils down to, if at all possible, use WPA2 security with AES encryption.

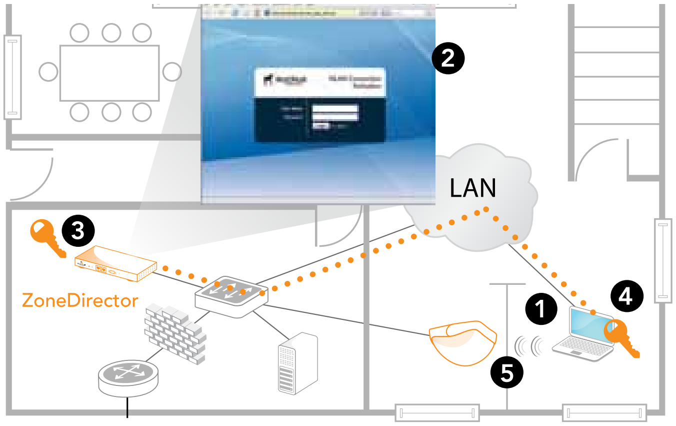
WPA2 options – PSK, Ruckus Dynamic PSK and Enterprise (802.1X)

Simplify Your Security with DPSK

The 802.11i standard defines two authentication methods, commonly called by their Wi-Fi alliance certifications: WPA2-Enterprise and WPA2-Personal (or WPA2-PSK for 'pre-shared key'). WPA2-Enterprise is extremely secure and is built around the 802.1X port authentication standard. Note that even though 802.1X frequently comes up in discussion of Wi-Fi networks, it is a port based authentication protocol and was originally designed for wired networks.

WPA2-Enterprise requires a RADIUS server (or RADIUS proxy) and a database of users with their corresponding credentials. However, 802.1X can be challenging to deploy, as discussed in detail below.

FIGURE 3: Dynamic PSK



1. User attaches to wired LAN (or open a dedicated provisioning WLAN)
2. User challenged to authenticate at captive portal page
3. Upon authentication, a unique encryption key is dynamically generated for user by the ZoneDirector
4. Key is passed to user device where it is automatically configured within the wireless configuration
5. User detaches from the LAN and can now safely connect to the WLAN

For less complex WLAN deployments, WPA2-PSK uses a single passphrase, the Pre Shared Key, or PSK, to access the WLAN. From an end user point of view, and even a deployment point of view, it is virtually the same as WEP — the user chooses the SSID of the WLAN and is asked for the passphrase, which will be cached by the OS for future automatic connections. However, unlike WEP, WPA2-PSK corrects implementation weaknesses, can use AES encryption and cannot be broken unless a weak passphrase was chosen.

The security concerns with WPA2-PSK do not stem from the quality of the encryption implementation, but from issues of managing the passphrase. Because the passphrase is shared, all users of the WLAN must know it. The more people that know a secret, the less secret it is. Well meaning folks tend to give the PSK to visitors who wish to check their email. Key rotation (periodically changing the passphrase) almost never happens, even when someone leaves the organization, because it is so cumbersome. When it does happen, informing users of the new PSK may wind up being by email or posted signs – not great ways to preserve a secret. Although the encryption is strong, a poorly chosen or weak passphrase is subject to brute-force dictionary attacks that attempt to guess the passphrase.

How serious these concerns are depends on the security needs of the organization. Even a relatively large but tight knit organization with limited security concerns may find this acceptable, while a very small organization with significant privacy concerns such as a legal firm or a medical office may find this unacceptable.

If only there were an option more secure than PSK that was not as complex as an 802.1X implementation…

Ruckus Dynamic PSK and Zero-IT Configuration

Ruckus has introduced two valuable innovations to enable more robust security on a WLAN without the need for a RADIUS server or other additional infrastructure — significantly reducing the administration burdens on IT. Dynamic PSK, and its companion, Zero-IT Configuration, only require ZoneDirector to implement.

Dynamic PSK creates a unique 63-byte encryption key for each user, while Zero-IT Configuration automatically configures the end-user's WLAN profile with their personal key. No end users share a key, so if one leaves the organization, only that key needs to be deleted from the ZoneDirector. The key is 63 bytes long and effectively random, making it superior to any PSK a human can be expected to remember. A 63 byte random PSK is immune to dictionary attacks and effectively uncrackable. It is also unshareable in a practical sense: thanks to Zero-IT Configuration the end users do not even know what their passphrases are.

With Zero-IT enabled, a new user simply connects to a wired port on the LAN and authenticates via a captive portal (web page) hosted on the Ruckus ZoneDirector. The user's credentials (user name and password) can be checked against a user database on the ZoneDirector or for that matter, any existing standard back-end authentication (AAA) server such as Active Directory, RADIUS, LDAP, etc.

Once the user is authenticated, the ZoneDirector generates a unique encryption key for that user. A temporary applet with the unique user key and other wireless configuration information is then pushed to the client. This applet automatically configures the user's device without any human intervention.

The user then detaches from the LAN and connects to the wireless network. Once associated, the Dynamic PSK is bound to the specific user and the end device being used.

The Dynamic PSK has a configurable lifetime. After the key expires, users can repeat the configuration process.

Another deployment option is to use an open WLAN that only allows access to the captive portal, possibly running on a single AP, which could serve as the initial configuration connection, rather than a wired port.

From an overworked IT staff perspective, end users can easily self-service. New users can be provided with an instruction sheet for first time connection.

DPSK with Web Authentication

Dynamic PSK authenticates the user's machine rather than the user. A unique key is installed on the client machine and that key is tied to the wireless MAC address in ZoneDirector. Spoofing the MAC address does an attacker no good, because the attacker does not have the pre-shared key.

However, it is the machine that is authenticated rather than the user. If an organization was concerned with this, it could easily add user authentication through a web portal login to the WLAN for two factor authentication. In the Zone Director WLAN configuration screen, simply click "Web Authentication" and choose the authentication server from the drop down box. The user will be presented with a login screen when accessing the WLAN. Authentication has become a two-step process — Dynamic PSK to access the WLAN, followed by web authentication to access network resources.

Note that Web authentication can be used without encryption for circumstances where user authentication is a concern but not data privacy or machine authentication, a circumstance more common in guest networks (see below).

PSK vs. Ruckus DPSK with Zero-IT Configuration

The right balance between security and convenience

In almost any circumstance you would use WPA2-PSK, Ruckus DPSK is a better choice. It provides significant security improvement for little effort. Ruckus DPSK builds on WPA2-PSK and works with Zero-IT configuration to allow end users to easily configure their wireless settings on Windows 7, Windows Vista, Windows XP/SP2 or later and MAC OS X.

For devices with non-standard operating systems, such as Linux of Voice over Wi-Fi phones, dynamic PSKs can be generated in batches and stored in a spreadsheet for manual device configuration. On connection to the WLAN, the DPSK will be bound to that device in ZoneDirector.

In cases where a Pre-Shared Key is unavoidable, one option gaining popularity in some security circles is to rely on greater length rather than complexity in designing passwords, by using 'pass-phrases.' This does not necessarily have to be difficult to remember, because actual phrases are not much more difficult to type than complex passwords. For Example: TommyTutoneCallJenny8675309 is surprisingly easy to remember for people of a certain age, and yet it is very strong even without the addition of special characters.

802.1X/EAP — WPA2-Enterprise

The 802.1X standard is, in fact, not a wireless specific standard. It is a port based access control standard, and can be and is applied to access network ports of most any type. In the case of a WLAN, each client connection to an AP is a 'virtual port,' analogous to a wired Ethernet port. In an 802.1X context, APs and Ethernet switches may act as an Authenticator.

802.1X defines three components. A Supplicant is client software that provides the user's credentials and runs on the client machine (laptop, Wi-Fi phone, etc.). An Authenticator is the device that grants or blocks network access — a switch or an AP. An Authentication Server is the sever and database that validates the user's credentials, instructing the AP or switch to grant access to the network.

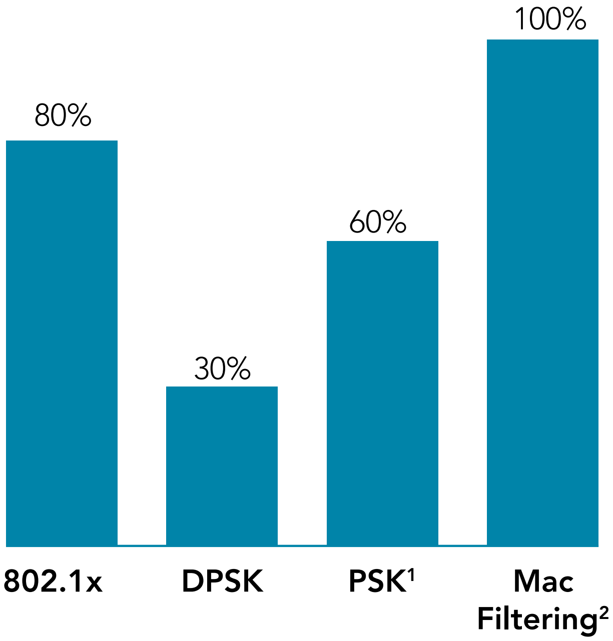
In a WLAN context, a laptop associates to an AP. Initially, the AP will only accept the user's credentials. The credentials may be username and password, but depend on what EAP method is used; more on EAP below. The AP (in conjunction with ZoneDirector) is a pass through for the username and password, or other credentials. The credentials are sent to a RADIUS server (or proxy server) that looks up the credential and tells the AP to grant access or reject the laptop connection. Before authentication, all IP/Layer 3 communication is restricted to the Authenticator (AP) and the Authentication server (RADIUS).

EAP stands for Extensible Authentication Protocol. 802.1X is designed to work with a lot of authentication credentials and there are many types of EAP protocols. Some EAP types are built around usernames and passwords, and others are built around certificates. It is beyond the scope of this paper to discuss all the variations of EAP, but we will outline the deployment of one of the most common — Microsoft's PEAP-MS-CHAP v2.

The PEAP portion of PEAP-MS-CHAP v2 stands for Protected EAP. PEAP sets up an encrypted tunnel using the TLS standard between the laptop (supplicant) and the Ruckus AP (authenticator). MS-CHAP v2 is a username and password credential scheme that was designed for use with Microsoft's Active Directory, and has since been implemented in most every common operating system and access network device. MS-CHAP v2 does not provide encryption itself, but the PEAP portion of the scheme provides the encryption that ensures the user credentials cannot be overheard.

The summary charts below are based on interviews with wireless security experts and customer references.

FIGURE 4: Comparative level of combined IT resources + user effort to implement security protocols



[1] *Must update everyone on network routinely, and after personnel changes*

[2] *Manual management and maintenance of Mac address list of all devices on network*

In a Microsoft and Ruckus only environment, Windows clients from Windows XP to Windows 7 include supplicant software that supports PEAP-MS-CHAP v2. Naturally, Ruckus APs and Zone Directors support this environment as authenticators. Windows 2008 Server includes Active Directory Domain Services to store all user accounts and their credentials. Windows 2008 Server also includes Network Policy Server (Authentication Server), which acts as the RADIUS server (or Proxy server). For a full Microsoft 802.1X deployment, you would have to implement both the active Directory Domain Services and the Network Policy server.

One additional consideration is the authentication of the server by the clients. In PEAP-MS-CHAP v2, the clients are authenticated by the server using the username and passwords stored in the Active Directory database, but the option for the clients to authenticate the server (confirming the server's identity before sending credentials) requires the use of a server certificate and a Certificate Authority trusted by the client computers.

Deploying a certificate supporting Public Key Infrastructure can be daunting in complexity. The simplest way to include server authentication is to not deploy your own PKI, but rely on an established, public one, such as Verisign, by purchasing and installing a certificate for the Windows 2008 Server. Microsoft client operating systems such as Windows 7 come equipped to trust certificates issued from the major Certificate Authorities. See Microsoft's website for detailed implementation information.

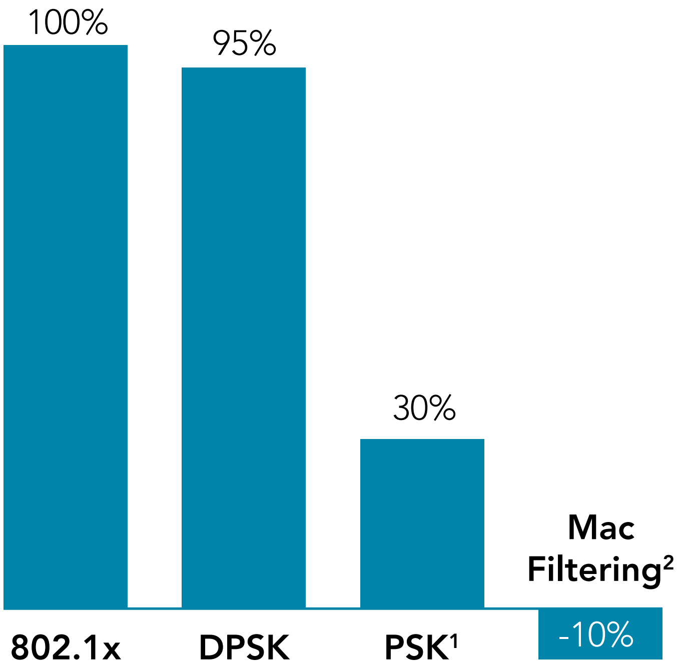
Dynamic VLANs and 802.1X — traffic segmentation

When using 802.1X, the RADIUS server database can include a VLAN ID attribute in the user's profile. ZoneDirector can dynamically assign the VLAN to the user according to the returned RADIUS attribute, allowing traffic segmentation of multiple user groups using a single SSID. Three RADIUS attributes would have to be configured in the RADIUS sever — Tunnel-Type (set to VLAN), Tunnel-Media-Type (IEEE-802) and Tunnel-Private-Group-Id (the desired VLAN ID).

ZoneDirector EAP Server

ZoneDirector also includes a local user database that can be configured. A WLAN can use the local database as an authentication server and can use certificate based authentication. In the case of an authentication server failure or network outage which precludes successful authentication, having a small number of critical users can be invaluable to disaster recovery execution. User certificates can be generated by the ZoneDirector and distributed using Zero-IT activation. Users simply follow the instructions provided during the Zero IT Wireless Activation process to complete this task. Once it is done, users can connect to the internal WLAN using 802.1X/EAP authentication. User IDs will have to be preconfigured on the ZD and VLANs cannot be assigned with this method.

FIGURE 5: Security level for selected security protocols



[1] *Depending on how often IT changes key*

[2] *Negative since Mac filtering gives false sense of security while requiring significant effort*

Guest WLANs

Guest WLANs are often deployed to provide Internet access for visitors. How to configure one depends on what makes the most sense for your user base.

Segmentation is a vital concern with Guest WLANs. By definition, they are not being used by the organization's users. Ruckus Guest WLAN configuration will automatically prevent Guests from accessing subnets/VLANs that ZoneDirector and its APs are connected to. It is good practice in the Zone Director Guest Access configuration to explicitly add any additional subnets guests should not access. If possible, isolate the Guest VLAN with a firewall. It would be good practice to configure the firewall to only allow Internet and Email access from the Guest VLAN — see your firewall's documentation for details.

Similarly, Wireless Client Isolation should certainly be enabled on Guest WLANs. Guest clients should not need to connect directly to each other.

Ruckus Guest Pass Authentication

Guest WLANs can be open with access for anyone. However, many organizations want some control over their guest WLAN, and Ruckus ZoneDirector includes the option of issuing passes to the guest network. Ruckus Guest passes are unique pass keys that can be issued to guests, contractors and other temporary users, providing control of access times, privileges and bandwidth consumption.

A Guest Pass administrator can be configured under 'users' and enabled to generate passes from a web page hosted on the ZoneDirector. It is common for this function to be handled by an office administrator, who simply goes to the guest pass URL, types in the guest's name and chooses duration, then generates the pass and prints it out. It is also possible to configure guest pass duration to begin on first login and to generate and print out guest passes ahead of time. This would allow an admin to simply hand a guest a pre-printed sheet with the pass and instructions. Guest Passes bind to a specific client MAC address upon successful authentication. If desired, a single pass key can also be shared among many users.

Guest Network Encryption

Guest passes provide control over network access, but do not provide for data privacy. If privacy is a concern for the guest network, it can be setup with as a WPA2 PSK network. The guest user would have to be given the PSK as well as the guest pass. The guest would enter the PSK before being able to access the web portal to enter the guest pass.

Note that Guest Pass policies are set globally in ZoneDirector in Guest Access configuration. However, guest WLANs are created in WLAN configuration. When creating the WLAN, simply choose the type as Guest Access.

Rogue APs and Wireless Threats

"Rogue AP" is an unfortunately vague term. Generally any AP not controlled by the ZoneDirector controller is considered a rogue. However, neighbor network's APs are not generally a threat, while unauthorized APs connected to your wired network are a huge security issue.

Ruckus APs will scan for and detect other 802.11 APs in range and list them (along with clients advertising ad hoc networks) as rogue devices in the rogue devices screen. The best way to determine if these are a threat is to use location tracking to determine if they are in your location or are in fact a neighbor's device.

To enable this function, you will need to import maps of your location into Zone Director Map View and then place your controlled Ruckus APs on the maps to enable location tracking. Once location tracking is enabled, any rogue device can be checked against the map. If it is clearly outside your building, it can be ignored and marked as a 'known' device.' If it is inside your building, it should be investigated further and most likely physically removed once located.

With any new deployment, there will be a shakeout period while all neighbor APs are identified as such and then marked as 'known' in ZoneDirector. After that, best practices dictate regular checking of new rogues as they appear.

The real threat concern is with Rogue APs that are connected to your wired network. The bad news is that there is no 100% effective way of determining if an AP is on your wired network other than finding it and checking it manually. The good news is that rogues attached to your network are much less common once a sanctioned WLAN is deployed. Rogues are placed to enable wireless access, often by well-meaning but naive end users. Once they have legitimate wireless access, the motivation for adding a personal AP disappears.

ZoneDirector detects and alarms when a Rogue AP is found connected on your wired network. This is very reliable alarm and should be taken seriously. Positive detection of wired rogues is difficult even for specialized Wireless Intrusion Prevention Systems (WIPS) such as those available from Ruckus Partners AirMagnet and AirTight Networks. There is no guarantee that the rogue's BSSID matches its Ethernet MAC, or that a crafty installer hasn't placed behind a NAT boundary or personal firewall, which makes it exceedingly difficult to guarantee the rouge's isolation regardless of the level of integration between the WIPS and switching or routing infrastructure systems. There is no substitute for periodic rogue checks using location tracking such as is available in ZoneDirector.

Honeypot, Evil Twin and Man-in-the-Middle threats

Wireless introduces not only new concerns with preventing unauthorized access to the network, but concerns with keeping the clients on the correct network. Some threats are attempts to lure end users off of the corporate network.

In general, Man-in-the-Middle attacks involve an attacker inserting himself in a legitimate transaction to gain information, and redirecting the traffic to its original destination. The redirection is necessary for the end user to continue using the network. Terminology varies, but Honeypot APs generally copy an SSID to lure end users. The more sophisticated Evil

Twin will copy the MAC address of a legitimate AP. If an Evil twin then redirects traffic to the internet, the end user may be unaware of being on the wrong AP.

ZoneDirector will alert when a rogue AP is using one of the organizations SSIDs, or when an AP is spoofing one of the legitimate AP MAC addresses. These alerts indicate definite attacks — SSID and MAC spoofing do not happen accidentally.

Denial of Service

Ruckus APs will temporarily block clients that make excessive wireless requests or authentication attempts. DoS attacks may be used in conjunction with Man-in-the-Middle attacks described above. The attacker may try to wirelessly interfere with the AP being impersonated in order to get better results on the attacking Evil Twin AP.

Ad hoc networks

The ZoneDirector rogue AP list will also list ad hoc networks. End users are not generally sophisticated enough to clear the cache of networks they have connected to. Clients advertising ad hoc networks can be attacked by using the ad hoc connection. When performing regular rogue checks, location-track the ad hoc networks as well. Common ad hoc SSIDs include HPSETUP and Free Public Wi-Fi. The Free Public Wi-Fi is amusing — people see it in airports, try to connect (not noting or understanding it is an ad hoc network), get nowhere, but now have the cached profile for someone else to connect to. Thus, it propagates virally, leaving a potentially exploitable ad hoc connection running on laptops all over the world.

Summary

Clearly, WLAN security can be complicated and this paper only scratches the surface of some of the gory details. But, security doesn't have to be complicated. Achieving the sweet spot between the right level of security with the right level of implementation, ongoing management, and usability is key for all sizes of organization — and that means using Ruckus' patented Dynamic PSK. If you are extremely security conscious with resources to implement and manage an 802.1x infrastructure — Ruckus can support that as well.

KEY SECURITY CAPABILITIES / RECOMMENDATIONS

- Wireless Client Isolation
- Multiple SSIDs
- Wi-Fi Protected Access 2 (WPA2)
  – DPSK
  – 802.1x EAP
- Advanced Encryption Standard (AES)
- Guess Pass Authentication with encryption
- Location Tracking for Periodic Rogue AP Checking
- Alerts for Rogue AP MAC Address Spoofing Threats
  – Honeypot
  – Evil Twin
  – Man-in-the-Middle
- Denial of Service (DoS) Blocking
- Removal of Broadcast Ad-hoc Networks