BPG | SECURING YOUR MERU NETWORK

Meru Networks®
Powering the All-Wireless Enterprise™

Meru Best Practices Guide

Author | Thomas Lee | Technical Marketing Engineer
Date | August 2010
Version | BPG_Security_V1.0

TABLE OF CONTENTS

OVERVIEW 4
CONTROLLING ACCESS TO THE WIRELESS NETWORK 4
WIRELESS ATTACKS 6
SECURING THE LINK BETWEEN THE END DEVICE AND THE ACCESS POINT 8
AUTHENTICATING THE USER 12
PCI WIRELESS BEST PRACTICES 15
HIPPA COMPLIANCE FOR WIRELESS NETWORKS 18
SARBANES-OXLEY COMPLIANCE 19

EXECUTIVE SUMMARY

This document describes the best practices for securing the Meru wireless infrastructure. The first part of the document will discuss the importance of securing the wireless network. The next section will discuss some of the common network attacks. Subsequent parts will document the various wireless data encryption schemes, user authentication, access control lists, user separation, PCI support, HIPPA compliance, and SOX compliance.

CONTROLLING ACCESS TO THE WIRELESS NETWORK

Controlling access to the wireless network in an enterprise environment is very important. A wireless network offers the benefits of being able to be connect to networked business resources like email, databases, file servers, voice communications, and internet without having to connect to the a wired port. Just like any business controls the access to the premises for employees and guests, the wireless network as well as the wired network must be secured in the same manner. This document just addresses the wireless side of the network. The IT department must have policies and procedures in place to determine the network access for employees as well as guests.

Network security is defined by 3 terms: authentication, authorization, and accounting.

Authentication is the verification of a user by username and password, digital certificates, or multifactor authentication using token cards. Meru Networks controllers support the following methods of authentication:

- Local username and password. This requires inputting of username and passwords onto the controller.
- Username and password authentication using a RADIUS server.
- MAC address authentication via a RADIUS server. This is a common method of authentication for wireless devices like Wi-Fi phones
- Captive portal authentication. The controller will intercept an HTTP request and display a page requesting username and password when the wireless workstation invokes a web browser. The username and password will be either locally authenticated or sent to a RADIUS server
- Digital certificates.
- Two factor authentication with RSA tokens.

Depending upon the size of the IT infrastructure and resources, the recommendation is to implement RADIUS authentication with or without digital certificates. The next level of security is two factor authentication.

Authorization is the granting of access to network resources and services. Meru controllers support authorization by way of MAC filtering and QoS filter IDs. If tight controls are necessary, the recommendation is to implement MAC filtering and QoS filter IDs.

Accounting is tracking the use of network resources by the authenticated users. Meru controllers achieve this task by supporting RADIUS accounting. The following are the accounting attributes that are supported by Meru controller:

RADIUS attribute	Description
Session-ID	Client IP Address-Current Time - The session time returned from the radius server has priority. If the radius server doesn't return the session time, the configured value is used.
Status Type	Accounting Start/Accounting Stop
Authentic	Radius/Local authentication
User-Name	Username
User-Name	Station Mac Address (station info)
NAS-IP	Address Controller IP Address
NASPort	Unique value (system generated)
Called Station-ID	Controller MAC Address
Called Station-ID	Controller MAC Address:ESSID Name (Used to enforce what ESS a station can connect to)
Calling Station-ID	Station MAC address
Connect Info	Radio Band of Station
Class	Class Attribute
NAS-Identifier	Any string to identify controller (self) in Access Request Packet. Min value 3 chars.
Acct-Input-Octets	Number of octets received on this port (interface) and sent in Accounting-Request when Accounting status type is STOP
Acct-Input-Packets	Number of packets received on this port (interface) and sent in Accounting-Request when Accounting status type is STOP
Acct-Output-Packets	Number of packets sent on this port (interface) and sent in Accounting-Request when Accounting status type is STOP
Acct-Output-Octets	Number of octets sent on this port (interface) and sent in Accounting-Request when Accounting status type is STOP
Acct-Terminate-Cause	Used to get the reason for session termination and sent inAccounting-Request when Accounting status type is STOP
Acct-Delay-Time	Sent to indicate the number of seconds we have been waiting to send this record.
AP ID	Vendor specific info: the AP ID to which client connected. Sent when accounting starts
AP ID	Vendor specific info: the AP ID from which client disconnected from. Sent when accounting stops
AP Name	Vendor specific info: The AP Name to which client connected. Sent when accounting starts
AP Name	Vendor specific info: the AP ID from which client disconnected from. Sent when accounting stops
Session-Time	Number of seconds between start and stop of session

WIRELESS ATTACKS

The main function of a WLAN is to provide a portal into the wired infrastructure. The network administrator must provide strong authentication methods to guard against unauthorized access into the network. However, strong authentication methods will not guard against someone who wants to disrupt or gain unauthorized access to the wireless and wired network. This section will describe the types of attacks and how to mitigate the attacks.

Rogue Wireless Devices

Rogue wireless device is any device that has an Ethernet port and a wireless card in it and is not under the supervision of the company's IT department. Any low priced SOHO (small office, home office) wireless router can be plugged into a company's live Ethernet port. Due to the lack of authorization and authentication security on the rogue device, any hacker can use this router to gain access to the company's network.

Another type of rogue wireless device is an ad-hoc workstation. This type of workstation can be a laptop or desktop computer with an Ethernet connection and a wireless card. The computer is then configured to bridge network traffic between the Ethernet adapter and the wireless card. This configuration will provide anyone access to the company network.

There are a couple of ways of mitigating rogue wireless devices: one, utilize Meru's rogue access point detection and mitigation services and two, implement 802.1x authentication on all wired ports. Meru's rogue AP detection and mitigation feature can detect and mitigate rogue APs over the air.

Refer to the Meru System Director user guide for information on configuring rogue AP detection and mitigation.

Implementing 802.1x authentication on all wired ports is a good way of preventing rogue APs from gaining access the network. Typically, when layer 1 link is established, the port is put into a quarantined state until 802.1x authentication successfully performed. One temporary IP address is allocated on the port for communication purposes. Rogue APs do not have the ability to negotiate 802.1x authentication. Therefore, the wired port is never placed into a VLAN with access to the rest of the network.

Peer to Peer attacks

Peer to peer attacks can occur when a workstation associates to an ad hoc network and launches at DOS (denial of service) attack or the DOS attack occurs between workstations in the same wireless VLAN. Typically, wireless clients communicate only with devices on a wired network. Therefore, peer to peer communication is not needed. Meru controllers can be configured with QoS rules to block peer to peer communications. Refer to the Meru System Director user guide for information on blocking peer to peer communication.

Eavesdropping

802.11 wireless networks operate in license free frequency bands and all data transmissions occur in the open air. Therefore, access to the wireless network is available as long as the wireless device is within range of the nearest AP. There are two type of eavesdropping: casual eavesdropping and malicious eavesdropping. Casual eavesdropping (AKA wardriving) involves using wireless utilities like NetStumbler to find SSIDs to associate to. Another way is to use the MS windows zero configuration utility to detect SSIDs as the

person is walking or driving down the street. Most of the time, wardrivers are just looking for free internet access.

Malicious eavesdropping is the unauthorized use of network protocol analyzers to capture wireless frames. Without any kind of strong wireless encryption, valuable data like personal information, email, passwords, credit card numbers, bank account numbers and other types of account numbers can be extracted from the data portion of the wireless frames. One of the most common targets of malicious eavesdropping is public hotspots where wireless security is virtually non-existent. If one is using a computer in this type of wireless environment, then using VPN (virtual private network) software is imperative towards guarding wireless data transmission.

To guard against either type of eavesdropping, encryption schemes like CCMP/AES and to a lesser extent TKIP should be enabled on the wireless network. Do not use WEP encryption as the data can be cracked with WEP-cracking software. The WEP-cracking software can derive the WEP key within minutes. Once the key is derived, the key can then be used to decrypt the data. Also, do not use MAC authentication with MAC filtering as the MAC address can be seen with a wireless packet sniffer. This is different from MAC authentication using an 802.1x server. Meru Networks support WPA2 TKIP and AES.

Authentication Attacks

Authentication attacks involves executing offline dictionary attacks to determine the preshared key in a WPA/WPA2 preshared key encryption or 802.1x LEAP hashed password. Once this is done, a hacker can use the preshared key to decrypt data gathered from a wireless protocol analyzer as well as gain access to the wireless network. The recommendation is to use WPA with 802.1x authentication. If it is necessary to use a preshared key, then the preshared key should be 20 characters or longer. Meru controllers allow the administrator to configure preshared keys up to 65 characters. In an 802.1x LEAP environment, the username is not encrypted. Therefore, a hacker can access the network with the stolen username and password. The recommendation is to implement EAP type of TLS or TTLS. TLS and TTLS are not susceptible to offline dictionary attacks. Meru controllers support all forms of EAP.

MAC spoofing

MAC spoofing is taking the MAC address of a legitimate device and using that MAC address on another workstation. MAC addresses can be changed within the configuration utility of a workstation. MAC filtering at the access point or controller can be bypassed if MAC spoofing is occurring. To prevent a hacker from using MAC spoofing as a way to getting into a network, one must use a layered approach to security. Start with MAC filtering to limit the device access to the network. Next implement WPA2 with 802.1x authentication. In 802.1x authentication, implement TLS or TTLS EAP.

Management Interface infiltration

If the network has a RADIUS server, then enable RADIUS authentication for access to the Meru controller. As a last resort, the network administrator can control access to the Meru interface (command line, GUI) by changing the default passwords for the admin and guest users to a long password composed of different types of characters like: upper and lower case characters, numbers, and symbols.

Hole 196 attack

Security experts at AirTight Networks have discovered a hole in the WPA2 Wi-Fi security protocol. The security hole was named as Hole 196 after the number of the relevant page in the IEEE 802.11 (2007) standard document. At the bottom of page 196, the IEEE standard introduces the keys used by WPA2: the PTK (Pair-wise Transient Key), which is unique for every WiFi client and used for unicast traffic, and the GTK (Group Temporal Key) used for broadcasts. While data forgeries and spoofed MAC addresses can be detected with the PTK, the GTK does not offer this functionality.

The AirTight experts say that this is the crux of the matter, because it allows a client to generate arbitrary broadcast packets which other clients respond to with information about their secret PTKs which can be decrypted by attackers. AirTight reportedly only needed to add 10 extra lines of code to the freely available open source Madwifi driver to make a PC with an off-the-shelf WiFi client card spoof the MAC address of the Access Point and pretend to be the gateway for sending out traffic. Attackers could exploit this to cause damage on the network, for instance via denial-of-service (DoS) attacks. The experts say that the only factor mitigating the attack potential is that attackers need to be internal and authorized WiFi users. They do not anticipate that a patch will become available because "Hole 196" is written into the standard.

Each client has a “Unicast” key (or a key based on a unique ID) and a “Broadcast” key that is set on a per BSSID basis and is common to every client associated with that BSSID. This is the crux of the issue. It is possible for a nefarious client to exploit that broadcast key to damage the network or potentially steal information.

In a microcell architecture, the AP acts as an Ethernet hub and everyone associates with that AP is associated with the same BSSID and is now vulnerable to the “Hole 196” vulnerability.

Since connections to Meru are controlled via Virtual Port each station has a unique BSSID generated and controlled by System Director. This means that each client now has a unique broadcast key for WPA2. This is the element of virtualization makes it impossible for a nefarious client to spoof the AP’s MAC address and exploit the broadcast key to launch security attacks (because there are no other clients with the same broadcast key and therefore no one will be exposed to the attack).

So the nefarious client will use the broadcast key based on the BSSID that Meru’s Virtual Port generates thinking it’s going out to everyone. In reality, the actual broadcast is not seen by anyone other than the Meru system and the attacker never has access directly to the other clients. The recommendation is to ensure virtual port is enabled on the Meru controller(s).

SECURING THE LINK BETWEEN THE END DEVICE AND THE ACCESS POINT

Securing the link between the end device and the access point is important because any hacker with a laptop, wireless card, and network analyzing software such as Airopeek, AirPCAP, etc. can capture packets and look into the data portion of the packet for sensitive application data. The sections below will outline the different ways of encrypting the data in the packets between the wireless end device and AP starting from the most unsecured method to the most secure method.

No security at all

There are wireless networks that you will encounter that are unsecured. At most, a splash screen will appear when you bring up your internet browser requesting acceptance of terms of conditions for usage of the wireless network. Data that flows between the wireless end station and the access point can be easily captured with wireless network analyzers. The following information can be seen by the network analyzers:

1. Source and destination addresses: MAC addresses and IP addresses
2. Packet types: UDP or TCP.
3. Unencrypted data in the data portion of the packet such as email conversations.
4. Wireless beacon frames.

The information above could be used for network attacks.

Any security in terms of encryption would be based upon the security settings of the destination website. For example, bank transaction websites offer a secure connection in which sensitive data is encrypted at the end station and decrypted at the website.

Unsecured networks are good for environments where ease-of-use is more important than security. It is not recommended for most enterprise environments.

Meru Networks controllers do provide support for unsecured wireless support. Use the default security profile when creating ESS profiles. Refer to the Meru System Director user guide for further information.

WEP security

Wired Equivalent Privacy (WEP64 and WEP128) is a Layer 2 security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11. WEP is designed to provide a wireless LAN with comparable level of security and privacy to what is usually expected of a wired LAN. A wired LAN is generally protected by physical security mechanisms, such as controlled access to a building, that are effective for a controlled physical environment. However, such security mechanisms do not apply to WLANs because the walls containing the network do not necessarily bind radio waves. WEP seeks to establish protection similar to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. Data encryption protects the vulnerable wireless link between clients and access points. Once this measure has been taken, other typical LAN security mechanisms such as authentication, password protection, and end-to-end encryption, can be put in place to protect privacy. With the WEP protocol, all access points and client radio NICs on a particular wireless LAN must use the same encryption key. Each sending station encrypts the body of each frame with a WEP key before transmission, and the receiving station decrypts it using an identical key. This process reduces the risk of someone passively monitoring the transmission and gaining access to the information contained within the frames. The WEP implementation allows the Security Profile configuration to specify one of four possible WEP keys that can be configured by a user station key management program.

Operation of the WEP Protocol

If a user activates WEP, the NIC encrypts the payload, which consists of the frame body and cyclic redundancy check (CRC), of each 802.11 frame before transmission using an RC4 stream cipher provided by RSA Security. The receiving station, such as an access point or another radio NIC, performs decryption when it receives the frame. As a result, 802.11 WEP only encrypts data between 802.11 stations. Once the frame enters the wired side of the network, such as between access points, WEP no longer applies. As part of the encryption process, WEP prepares a key schedule (“seed”) by concatenating the shared secret key

supplied by the user of the sending station with a randomly-generated 24-bit initialization vector (IV). The IV lengthens the life of the secret key because the station can change the IV for each frame transmission. WEP inputs the resulting "seed" into a pseudo-random number generator that produces a key stream equal to the length of the frame's payload plus a 32-bit integrity check value (ICV). The ICV is a checksum that the receiving station later recalculates and compares to the one sent by the sending station to determine whether the transmitted data underwent any form of tampering while in transit. In the case of a mismatch, the receiving station can reject the frame or flag the user for potential security violations. With WEP, the sending and receiving stations use the same key for encryption and decryption. WEP specifies a shared 40- or 104-bit key to encrypt and decrypt data (once the 24-bit IV is added in, this matches System Director's 64- or 128-bit WEP specification, respectively). Each radio NIC and access point, therefore, must be manually configured with the same key. Before transmission takes place, WEP combines the key stream with the payload and ICV through a bit-wise XOR process, which produces cipher text (encrypted data). WEP includes the IV in the clear (unencrypted) within the first few bytes of the frame body. The receiving station uses this IV along with the shared secret key supplied by the user of the receiving station to decrypt the payload portion of the frame body.

Limitations of the WEP Protocol

WEP is vulnerable because the relatively short IVs and keys remain static. Within a short amount of time, WEP eventually uses the same IV for different data packets. For a large busy network, the same IVs can be used within an hour or so. This result in transmitted frames having key streams that are similar. If a hacker collects enough frames based on the same IV, the hacker can determine the shared values among them (the key stream or the shared secret key). This can allow to the hacker to decrypt any of the 802.11 frames. A major underlying problem with the existing 802.11 standard is that the keys are cumbersome to change. The 802.11 standard does not provide any functions that support the exchange of keys among stations. To use different keys, an administrator must manually configure each access point and radio NIC with a new common key. If the WEP keys are not updated continuously, an unauthorized person with a sniffing tool can monitor your network and decode encrypted frames. Despite the flaws, the network administrator should enable WEP as a minimum level of security. Many hackers are capable of detecting wireless LANs where WEP is not in use and then use a laptop to gain access to resources located on the associated network. By activating WEP, however, the network administrator can at least minimize this from happening. WEP does a good job of keeping most honest people out.

Refer to the System Director user guide to implement WEP security. The recommendation is to only implement WEP security if the end device only supports WEP.

WPA encryption

WPA (Wi-Fi Protected Access) resolves the issue of weak WEP headers, which are called initialization vectors (IV), and provides a way of insuring the integrity of the messages passed through MIC (called Michael or message integrity check) using TKIP (the Temporal Key Integrity Protocol) to enhance data encryption. WPA-PSK is a special mode of WPA for home users without an enterprise authentication server and provides the same strong encryption protection.

In simple terms, WPA-PSK is extra-strong encryption where encryption keys are automatically changed (called rekeying) and authenticated between devices after a specified period of time, or after a specified number of packets has been transmitted. This is called the rekey interval. WPA-PSK is far superior to WEP and provides stronger protection for the home/SOHO user

for two reasons. The process used to generate the encryption key is very rigorous and the rekeying (or key changing) is done very quickly. This stops even the most determined hacker from gathering enough data to break the encryption.

WPA-PSK employs a consistent, easy to use method to secure your network. This method uses a passphrase (also called a shared secret) that must be entered in both the wireless access point/router and the WPA clients. This shared secret can technically be between 8 and 63 characters and can include special characters and spaces. The WPA preshared key should be a random sequence of either keyboard characters (upper and lowercase letters, numbers, and punctuation) at least 20 characters long or hexadecimal digits (numbers 0-9 and letters A-F) at least 24 hexadecimal digits long. The more random your WPA preshared key, the safer it is to use.

The Temporal Key Integrity Protocol (TKIP) takes over after the initial shared secret is entered in your wireless devices and handles the encryption and automatic rekeying. WPA is not an official IEEE standard, but is based on and is expected to be compatible with the upcoming 802.11i security standard, sometimes referred to as WPA2. WPA is designed to be a software upgrade. The 802.11i standard will likely require a hardware upgrade. However, wireless vendors and security professionals expect today's WPA and WPA-PSK to be useful for a very long time.

As of late 2008, two German researchers found a way to break TKIP. In summary, an attacker, who has about 12-15 minutes access to the network, is then able to decrypt an ARP request or response and send 7 packets with custom content to network. The encryption key has not been discovered however. This brings to light that WPA was just an interim solution for older hardware that did not support WPA2. If at all possible, the solution is to convert to WPA2. If it is not possible to convert to WPA2, then the best practice is to make the preshared key 21 bytes or longer.

Refer to the Meru Networks System Director user guide to configure a security profile for WPA encryption.

WPA2 encryption

WPA2 (Wi-Fi Protected Access 2) provides network administrators with a high level of assurance that only authorized users can access the network. Based on the ratified IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm. WPA2 can be enabled in two versions - WPA2 - Personal and WPA2 - Enterprise. WPA2 - Personal protects unauthorized network access by utilizing a set-up password. WPA2 - Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.

In WPA2, the WPA Message Integrity Code (MIC) algorithm is replaced by a message authentication code, CCMP, that is considered fully secure and the RC4 cipher is replaced by the Advanced Encryption Standard (AES). AES is the Advanced Encryption Standard and is used by the US Department of Defense as a replacement for older encryption standards. As such, it is very secure. AES can be used in several modes, and CCMP is the mode used by WPA2. Both terms are commonly used interchangeably.

On a Meru Networks controller, WPA2 & WPA2/PSK can be configured in the security profile. WPA2 is coupled with a RADIUS server. WPA2/PSK requires a preshared key be entered. The

longer the preshared key, the better. Refer to the Meru Networks System Director user guide to configure a security profile for WPA2 encryption.

AUTHENTICATING THE USER

Now that we have determined that WPA2 is the best encryption scheme, we will now address security as it pertains to access to the network. In the section above, a user only had to know the pre-shared key or WEP key to gain access to the network. However, network administrators will want to know who is granted access to the network. The section below will address 802.1x authentication and 2 factor authentication with RSA tokens.

802.1x authentication

The IEEE 802.1x standard is the next step in security. Up to this point, data encryption schemes have been discussed. WEP, WPA, and WPA2 require the user to have knowledge of the key. Once the AP association and DHCP address has been assigned, the user has access to the network. 802.1x is a port-based access control standard. 802.1x provides an authorization framework that allows or disallows access to the network and its resources. User name and password is required to gain access to the network and its resources. Of course, you can have selected resources such as databases with further username and password protection.

In 802.1x authentication, there are 3 components: supplicant, authenticator, and authentication server. The supplicant is the end device that is requesting the authentication. The authenticator is the device that either blocks or allows the end device onto the network. In Meru terms, the authenticator is the Meru controller. The authentication server is the server that validates the user credentials and notifies the authenticator that the supplicant has been authorized.

The reasons for implementing 802.1x authentication are:

- Scalable – An 802.1x-based WLAN deployment easily accommodates a growing number of WLAN users.
- Distributable – It's easy to distribute 802.1x-based WLAN access to separate departments, floors, branch offices or other off-site locations, with very little administrative overhead.
- Cost-effective – An 802.1x-based WLAN deployment may be significantly less expensive.

Meru supports the following EAP types: MD5, TLS, TTLS, PEAP, and LEAP. If strongest security is paramount, then Meru recommends implement EAP-TLS. EAP-TLS requires a digital certificate to be downloaded to the supplicant (i.e. workstation) before the workstation is allow onto the network.

Refer to the System Director user guide to implement 802.1x security.

2 Factor Authentication with RSA

There are a number of reasons to justify the need for stronger security and to help build the case for investing in two-factor authentication:

- Movement of new business applications online. Organizations continue to recognize the opportunities and cost efficiencies associated with providing access to

information online. As a result, more web-based applications are being launched to help facilitate the demand for instant access to information.

- Increased demand for remote access. The global nature of business and employee mobility has forced many organizations to provide anytime, anywhere access to enable employee productivity.
- Access privileges to new user populations. Contractors, partners and suppliers now require on-demand access to proprietary information such as sales forecasts, competitive intelligence, pricing charts, inventory, and customer data.
- Increase in customer-facing portals. There is an increased demand by customers to provide real-time access to information and the self-service options that enable them to manage their accounts online.
- Regulatory compliance. Numerous regulations have been issued in the last few years requiring organizations to enact security measures that prevent unauthorized access to information.
- Advanced threats. Threats to information continue to evolve and are becoming more challenging to contain. From the inside, employees engage in poor password management practices and work around established security policies to make their jobs easier. From the outside, phishing and malware are become an increasingly nefarious threat and fraudsters are beginning to recognize the value of enterprise credentials.

2 factor authentication requires 2 items for a user to gain access to the wireless network: something they have like a SecureID card with rotating numbers and a passcode. Meru wireless controllers support the RSA 2 factor authentication scheme. The security components for RSA 2 factor authentication are:

- RSA SecurID Authenticator token (hardware based or software based) that generates a unique authentication code
- RSA SecurID Server (Authentication Manager)
- RSA Authentication Agent

RSA SecurID Authenticator Token and Code

Each RSA SecurID token includes a factory-encoded, unique 'seed.' The token uses this unique seed to generate an authentication code at fixed intervals (for example 60 seconds). By utilizing the built-in-clock time and the unique seed, the authentication code keeps changing at fixed intervals. Since the token's clock and the server's clock are synchronized. The server generates authentication codes at the same fixed intervals as the token. Possession of the resulting code is then combined with knowledge of a PIN number to produce secure authentication.

RSA SecurID Server

Users are authenticated against the RSA SecurID Server with the username and the passcode, which is the combination of the authentication code generated/displayed by the token and the PIN (see above). The first time a user uses the token, they are asked to choose a new PIN. The server also requests a new time-synchronous PIN regularly or whenever the timing between a token and a server 'drifts.' If the drift is more than 3 minutes, then the Server requests the user to enter the next authentication code generated by the token in the next interval to verify the possession of the token. If the next authentication mode has the same clock drift, then token is assumed valid by the Server.

RSA SecurID Agent

This authentication is similar to the standard username-passcode authentication, but the passcode is not a single word. It is a numeric combination of the authentication code in the token and the PIN known to the user.
The RSA SecurID can be achieved two ways:

- EAP-RSA based authentication - implemented currently
- Native SecurID Authentication - not in use at this time

Although 2 factor authentication is more expensive and requires more work to implement, it is the most secure authentication scheme that Meru supports. Refer to System Director user guide to configure the Meru controller for RSA 2 factor authentication.

Access control lists

Access control lists allow the administrator to control access to network resources by way of IP address, protocol port number, and MAC address. Access control list are implemented in 2 different ways: Per user firewall and MAC filtering.

Per user firewall

Per user firewall is used to limit access to users either on an ESS basis or individual basis. If the network administrator implements a RADIUS server, then access can be limited on a per-user basis. This is done by returning a value for the filter-id attribute. If you do not use a RADIUS server, then anyone that gets authenticated on the specific ESS will have access limited based upon the filter ID specified in the ESS. Refer to the System Director user guide on implementing per-user firewalls.

MAC filtering

MAC filtering allows you to filter devices with matching MAC addresses to either permit or deny access to the network.

Implementing VLANs

VLAN (virtual LANs) is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain regardless of their physical location. On a Meru controller, a VLAN is assigned to an ESS profile. VLANs are a way of segmenting traffic based upon departments or other group entities. Therefore, you can keep a device from accessing resources that reside on another VLAN. The only way that resources on another VLAN can be accessed is by way of a routed interface. When a VLAN is configured on a Meru controller, packets to and from this ESS will have 802.1q/802.1p fields in the packet. This is also known as a tagged frame.

Authenticating phones and wireless monitors

Some phones and wireless cameras have 802.1x authentication capability. Typically, these devices will send its MAC address as the username and password to the 802.1x server. This prevents unauthorized devices from gaining access to the network. Meru recommends placing these devices into a separate ESS with a RADIUS profile that has the password type set to MAC address. Refer to the System Director user guide and reference guide for instructions on implementing 802.1x authentication.

Disabling AP during non use

In some enterprise environments, wireless access to the network is not needed on a 24x7 basis. A good way of securing the wireless network during off hours is to shutdown the AP. This can be done at the wired switch level by disabling the PoE function on the switch or can be done by taking the AP out of the ESS from the controller CLI or GUI. An added benefit to shutting off the AP is energy savings.

Cloaking SSIDs

Cloaking SSIDs is not broadcasting the SSID from the APs. This means that end devices will have to be statically configured to associate to an AP that supports that SSID. If the end device can only scan for an SSID to attach, then this end device will not be able see the SSID when scanning.

Cloaking SSIDs is not a good way of totally securing the wireless network. Cloak should be a part of a layered approach to securing the wireless network. Any wireless network analyzer can detect the SSID once an end device sends out a probe request for the cloaked SSID. The SSID is in the probe request and probe response frames and is in clear text.

Captive Portal

Captive portal isolates unauthenticated users to a sign-on portal until a user provides the necessary identification credentials. Captive portal is enabled or disabled from a security profile which is then assigned to an ESS. User authentication and authorization for web authentication is provided by the site's RADIUS server.

If a Captive Portal is enabled, the HTTP protocol over Secure Socket Layer (SSL, also known as HTTPS) provides an encrypted login interchange with the RADIUS server until the user is authenticated and authorized. During this interchange, all traffic from the client station except DHCP, ARP, and DNS packets are dropped until access is granted. If access is not granted, the user is unable to leave the captive portal. If access is granted, the user is released from the captive portal and is allowed to enter the WLAN.

Captive portal is commonly used for guest access. If possible, it is recommended the guest access should be implemented as a totally separate network that connects to a separate ISP (internet service provider). A common practice in enterprise networks is to use the current network infrastructure and create a guest VLAN for guest traffic. This means all traffic from guest and internal users going to and from the Internet must go through a NAT (network address translation router or a router if the enterprise has a large block of registered internet addresses which is rare. In extreme cases, a hacker can generate so much SPAM traffic that an ISP can shutdown the allocated addresses for the specific enterprise network. This action would mean the enterprise would not have any communication to the internet.

Another best practice for guest access is to configure a time limit for guest users. Refer to the Meru System Director user guide for more information.

Rogue AP detection and mitigation

A rogue access point is any Wi-Fi device that is connected to the wired infrastructure but is not under the management of network administrator. Often enterprise users will bring their own wireless router to gain access to the network. Meru APs can detect such devices and mitigate them (support by System Director 4.0) using AP300s. An AP that does not have the Meru OUI (i.e. 00:0C:E6) in its MAC address is considered a rogue AP by default. Any

broadcasted BSSID that does not have the Meru OUI is considered a rogue AP by default. Meru System Director software allows for creating access lists to allow non-Meru APs to coexist. It is a good practice to have rogue AP detection and mitigation. Refer to the System Director user guide for more information.

PCI WIRELESS BEST PRACTICES

Credit card theft is costing retailers an estimated $500 million annually. As a constant reminder, new stories continue to emerge, with the most recent involving inadequate security at a top retailer which resulted in the exposure of 45.7 million customers' personal information. In another incident, hackers obtained credit-card account data and personal information for approximately 19,000 customers at an e-commerce site. In an effort to address some of the root causes of the problem, the top five payment card brands—American Express, Discover Financial Services, JCB, MasterCard Worldwide and VISA International—formed the Payment Card Industry (PCI) standards council. This council has created the PCI Data Security Standard (DSS), which defines global security guidelines that applies to all merchants and service providers who store, process and transmit credit card data.

The PCI DSS standard, which went into effect in June 2005, consists of "a set of comprehensive requirements for enhancing payment account data security" that includes twelve major security requirements to secure payment account information and testing methodologies to ensure these requirements are met.

Meru Guidelines for PCI Compliance

The following guidelines provide the recommendations for assuring that Meru Networks wireless networks are part of an end-to-end communications infrastructure that meet or exceed the PCI DSS requirements.

Install and maintain a firewall configuration to protect cardholder data

PCI DSS section 1.3.8 states:

> Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes).

This requirement calls on a formal process in establishing internal firewall standards and on installing a firewall at each Internet connection and between any demilitarized zone (DMZ) and in the internal network zone. It is worth noting that a general purpose application firewall helps to meet a minimum requirement; however, with the spread of more sophisticated attacks through attack vectors such as email and IM, it is best to augment the firewall with a specialist vendor solution. Meru's per user firewall offers a superior solution and meets the requirement, and in combination with a third party firewall from Checkpoint, Juniper or others, provides wired and wireless integrity.

Meru's application firewall offers the protection that wired application firewalls can't. Meru's WLAN per-user, per-application firewall allows network administrators to centrally and precisely enforce a set of security and QoS policies for each wireless user and device. Access to applications can be defined and controlled by location and time of day, giving the administrator complete control over the types of traffic carried over the wireless network. Bandwidth can also be policed based on application and user, which allows administrators to rate-limit some applications, such as FTP traffic, while giving full bandwidth to more mission-critical applications like wireless point of sale.

Install and maintain a personal firewall for any mobile device with access to the retailer's network

PCI DSS section 1.3.9 states:

> Installing personal firewall software on any mobile and employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.

Meru meets these requirements by defining best practices with their technology partners. By working with partners and testing mobile clients with personal firewall solutions, Meru assures that the individual components brought together for joint end-to-end solutions maintain the integrity and continuity within the overall solution.

Do not use vendor supplied defaults for system passwords and other security parameters

PCI DSS section 2.1.1 states:

> For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable WiFi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable.

This requirement deals with changing the default passwords on all wireless equipment.

It is recommended to change vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords and SNMP community strings.

Encrypt wireless link carrying payment card information

PCI DSS v1.1 section 4.1.1 states:

> For wireless networks transmitting cardholder data, encrypt the transmissions by using WiFi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If using WEP, follow the instructions below:
>
> - Use with a minimum 104-bit encryption key and 24 bit-initialization values.
> - Use ONLY in conjunction with WiFi protected access (WPA or WPA2) technology, VPN, or SSL/TLS.
> - Rotate shared WEP keys quarterly (or automatically if the technology permits).
> - Rotate shared WEP keys whenever there are changes in personnel with access to keys.

Meru meets these requirements through the following security measures via the authentication and encryption security layer:

- WPA (802.1x authentication with TKIP encryption).
- WPA2 (802.1x authentication with AES-CCM encryption).
- IPSec (3DES encryption).

It is recommended to disable SSID broadcasts and enable Wi-Fi protected access (WPA and WPA2) technology for encryption and authentication.

Use and regularly update anti-virus software

PCI DSS v1.1 section 5.1 & 5.2 state:

- 5.1 Deploy anti-virus software on all systems commonly affected by viruses.
- 5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

Retailers need to assure that their WLAN solution is deployed with the endpoint security client that checks for a variety of conditions, including the presence and configuration of antivirus and personal firewall software; operating system patches and updates; registry settings and system configuration.

Maintain secure systems

PCI DSS v1.1 section 6.1 states:

> Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.

Meru E(z)RF™ Network Manager checks the latest software version and simplifies the process by centralizing all versions, configuration and management in the mobility controller.

Users need to have a unique ID

PCI DSS v1.1 section 8.1 states:

> Identify all users with a unique user name before allowing them to access system components or cardholder data.

Meru meets this requirement. Users can be assigned unique login credentials and these credentials are verified during authentication against Radius or RSA SecurID.

Use wireless analyzers periodically

PCI DSS v1.1 section 11.1 states:

> Test security controls, limitations, network connections and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.

It is recommended to use a wireless protocol analyzer like AirPCAP or Airopeek to scan for all wireless devices in use.

Run internal and external network vulnerability scans periodically

PCI DSS v1.1 section 11.2

> Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).

PC DSS v1.1 section 11.4

> Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.

To aid meeting requirements 11.2 and 11.4, Meru recommends that companies implement wireless security policies and test them on a regular basis. Security solutions, such as ArcSight SIEM can be used to monitor security systems in real time. Meru also recommends that all security systems are tested using third party certified PCI testers including McAfee Foundstone on a regular basis. Meru itself goes through such testing to assure that its solutions are built from the ground up with security.

For more information go to the following link PCI wireless standards document: https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

HIPPA COMPLIANCE FOR WIRELESS NETWORKS

The Meru Wireless LAN System provides a wide range of security options and controls to ensure healthcare institutions are HIPAA-compliant. A wireless LAN network can be implemented with confidence, allowing the institution to reap the enormous benefits of a converged voice and data wireless LAN.

Access Controls (Section 164.312a1)

- Unique User Identification: Username and password through WPA-based IEEE 802.1x authentication. Can be supplemented with MAC Address ACLs for additional control.
- Encryption and Decryption: TKIP. Dynamic re-keying via WPA-capable RADIUS server.

Audit Controls (Section 164.312b)

- Via SNMP through WPA-compliant RADIUS server.

Integrity (Section 164.312c1)

- TKIP implements a Message Integrity Check to ensure data has not been compromised.

Person or Entity Authentication (Section 164.312d)

- Using WPA with 802.1x authentication, each user must enter a unique user name and password to gain access to the network.

Transmission Security

- Integrity Controls: TKIP implements a Message Integrity Check to ensure data has not been compromised.
- Encryption: TKIP encryption and dynamic re-keying via WPA-capable RADIUS server.

Security Management (Section 164.308a1)

- Risk Analysis: Continuous monitoring of air waves for security violations including rogue access points, ad hoc stations, improper configurations, accidental associations. Provides a continuous review of security policy and vulnerability assessment of the wireless LAN.
- Risk Management: Implementation of a 24 x 7 wireless monitoring system mitigates potential risks due to wireless threats.

Incident Reporting Procedures (Section 164.308a6)

- Immediate detection of intruders with alerts to security managers of type of event, time and event resolution.

SARBANES-OXLEY COMPLIANCE

The Sarbanes-Oxley Act of 2002 (SOX) addresses financial reporting and corporate governance in publicly held companies. The section of the act that is relevant to the wireless network is section 404. Section 404 requires businesses to document their financial reporting controls and procedures. Part of the financial reporting controls and procedures is network security; how secure is the network from unauthorized access and usage? Utilizing the security technologies discussed previously, a Meru wireless network can be configured to contribute to the SOX compliance.