TRAPEZE NETWORKS

A BELDEN BRAND

Wired and Wireless Security Best Practices

WHITE PAPER

Many wireless industry spokesmen have made the bold claim that wireless networks are more secure than most wired networks. How is this possible? This paper describes best practices for deploying stringent wireless security, using a well-defined AAA framework.

Wireless LANs can be a godsend for connectivity. Plan for a deployment of access points to provide coverage and bandwidth, connect them to your network and you're off! The flip-side is that without adequate security anyone else may be able to use that same network to gain access to your precious data.

The reality is that most wireless implementations have a diverse set of needs and implications for security. Employees of differing departments need verified and secure access to data to do their jobs, vendors and partners need restricted access to certain applications while you may wish to extend restricted, internet-only access to visiting, though validated guests or students.

While these varying requirements may seem problematic for a robust security solution, they are not. Not only can the secure access policies you already have in place be leveraged, new classes of access that come with the ease of wireless connectivity can be managed as well with proven and well-vetted standards-based approaches.

This paper outlines the different networking components and technologies available for enforcing robust security policies on both wired and wireless networks, and drills down to provide today's best practice recommendations for deploying wireless LANs with stringent security.

Know Your Enemy

Guarding from security threats is like being constantly at war. Knowing your enemy is a proven strategy for winning wars as documented from the earliest Chinese dynasty texts on the subject.[1] Your enemy will take on one of the following three forms:

1) **Thrillseekers and casual wardrivers** are those with laptops roaming around looking for networks to hop onto. They often don't do damage as they're motivated by the thrill and ease of gaining access to open networks which they map and share with friends. Simple security measures are usually enough to deter them, especially if there are other open networks in the area.

2) **Bandwidth thieves and spammers** come in various forms but the most nefarious use your network to send spam and/or deal in pirated material or porn. All of these provide a traceable path of liability back to your door and not theirs, which is their precise motivation for using your network. Because there is a profit incentive, these thieves are more willing to expend effort in overcoming casual security implementations, but like war-drivers, they will look for the path of least resistance and choose those networks that appear the least protected.

1 Sun-Tzu – The Art of War – Approximately 500BC, translated from the Chinese in 1910 by Lionel Giles

Having enemies to secure our networks from is not new, but the advent of wireless removes a user's actual location as the prime tool in determining access.

3) **Knowledgeable attackers** are rare, but what differentiates them is that you are the specific target of their efforts. They either want access to the data on your network or they are looking to cause harm. As such they are willing to expend effort and equally obvious is the severity of damage that can be wrought. There are a few attributes of the knowledgeable attacker worth noting.

   a) This type of attacker has a better chance if they can attack from the inside of your network. Of internal attacks, there is an 80% chance that an attack is done or assisted by a former or disgruntled employee, and 62% of those are planned in advance.[2]

   b) They expect or know security to be in place and will use the latest tools to gain access and do damage. One of the paths attempted will be some form of masquerade, whereby the intruder attempts to appear as a trusted individual.

   c) It's easy for bad guys to become even more evil in a hurry, and is often a function of the information they can gain access to. The more potentially damaging the information is, the greater the temptation.

One priority should be clear: you must identify precisely who is attempting access to your network. Anonymity is a useful tool to the attacker and defining access based on identity is an effective first line of defense.

AAA: A framework for LAN security

Having enemies to secure our networks from is not new, but the advent of wireless removes a user's actual location as the prime tool in determining access. In the past, network access was often determined by which port you used to gain access to the network, but this doesn't work with wireless. This is a good thing, because defining access based on identity rather than physical location is a far more robust approach even for wired networks that do not have any wireless.

There is already a well-defined and vetted framework for understanding how to approach network security called "AAA" which stands for Authentication, Authorization and Accounting. The order is important, as there is a defined flow for every user session starting with authentication, then authorization, followed by accounting and statistics associated with the session.

The first "A": Authentication

AAA also provides a lucid framework by which to view any network security design, starting with the first "A" for authentication. Authentication refers to the process of obtaining and validating the identity of the user. It is the first line of defense in separating the good guys from the bad guys. Failure to provide a good first line of defense with robust authentication places a disproportionate and inevitably 'kludgy' burden on the subsequent lines of defense, Authorization and Accounting.

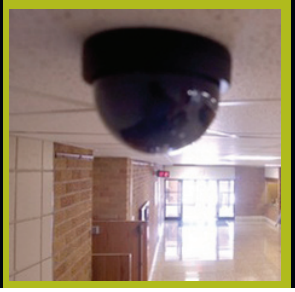
As noted previously, knowing who specifically, is attempting accessing the network is the most critical first step in securing a network. A robust authentication technique can help eliminate the most dangerous of attacks: Impersonation or Masquerading, whereby a bad guy successfully pretends to be a good guy.

By utilizing robust authentication techniques, even knowledgeable attackers with bad intentions are prevented from ever gaining access because only those with an allowed and verified identity can proceed to the next step, Authorization.

1. Examples of weak authentication

Weak authentication is the Achilles heel of any network – wired or wireless. Intruders that can authenticate to the network are effectively masquerading as a trusted user and will likely have far more ability to do damage since the user's identity is the primary determinant of access rights. The higher the level of access associated with a particular identity, the greater the damage potential. Therefore weak forms of authentication are to be either avoided completely or given minimal access. A few examples of weak authentication include:

[2] Secret Service: Inside Attacks Generally Launched By Problem Employees -- Security; Attacks from within can be worse than from without



Strong authentication techniques for wirless have a few common traits. They all leverage the IEEE's 802.1X framework which was ratified for use with wireless LANs in Dec 2004.

a) MAC authentication

Every networked device has a unique Media Access Control (MAC) address. So the thought goes, only allow authentication for those devices with a MAC address that you already know. No software on the client is required. It just has to send a packet for the network to see if the MAC address is on the list. Easy, right?

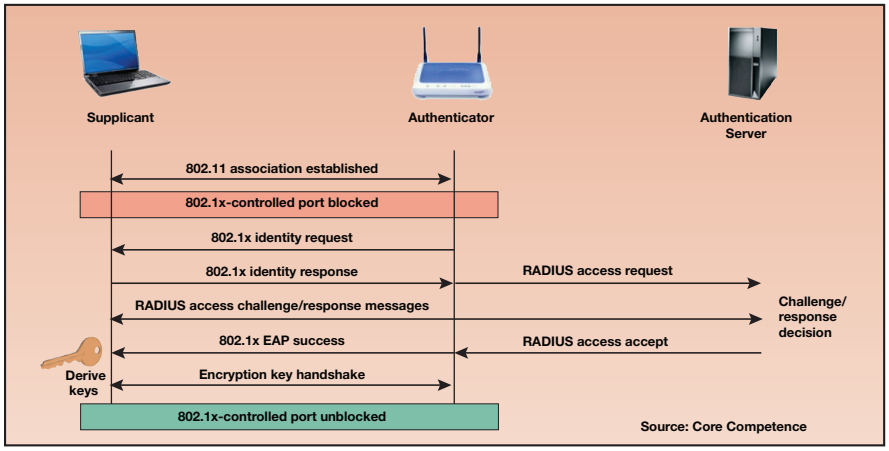
The problem is that the MAC address is sent with the header of every packet, outside any encryption that's being used so its in-the-clear over the air - and packet analyzers are widely available, as are MAC spoofing applications. It's also a hassle from the administrative end, since every new device that connects to the network has to be entered administratively. Save yourself the hassle and just avoid this form of authentication if at all possible.

b) Pre-shared Key (PSK)

Both WPA and WPA2 have an authentication mode designed for small office/home office applications. It uses a single alpha-numeric password that authenticates all users and sets up a subsequently encrypted session for each user. While the encryption is quite robust, the problem with PSK is the "Pre-Shared" part. All users of the network essentially share the same password. The more users, the greater the possibility the password can be compromised and the more difficult it is to change on a regular basis. Since only a pre-shared key is used, the network cannot resolve the identity of one individual user vs. another. It is also possible to use password-breaking software that automates thousands of access attempts.

2. Examples of strong authentication

Strong authentication techniques for wireless have a few common traits. They all leverage the IEEE's 802.1X framework which was ratified for use with wireless LANs in Dec 2004. This provides per-user authentication with options for the secure exchange of things like usernames and passwords over the air using the Extensible Authentication Protocol or EAP. The "E" in EAP means there are several different EAP types from which to choose.



A typical authentication process involves a device (the supplicant) trying to connect to a network; the machine that authenticates the supplicant — the authentication server — generally via Remote Dial-In User Service (RADIUS) technology; and the device that physically allows or blocks network access and handles communication between the other two elements (the authenticator). In this process, the authentication server asks the supplicant to identify itself. If satisfied with the authentication, the server informs the authenticator, which enables access and passes on the necessary encryption keys.

"It is in both Trapeze's and our customer's best interest to be at the leading edge of WLAN security issues and their standards-based solutions.

Our active participation in the standards bodies and heavy involvement in this critical area feeds directly into a more secure and interoperable product suite"

Choosing the right EAP type for your environment involves considerations for security but also the logistics of deployment. The Wi-Fi Alliance (WFA) has chosen five EAP methods in their Wi-Fi Protected Access (WPA) certification program,[3] and are due to follow with a couple more in the near future. These EAP types are determined by the WFA's Security Technical Task Group along with the compliance test suites that vendors must complete in order to obtain "WPA" and "WPA2" certification. It is worth noting that Trapeze's own CTO, Matthew Gast chairs the WFA's Security Technical Task Group, making Trapeze both aware and on the forefront of all the relevant security concerns for WLANs. As Matthew once said: "It is in both Trapeze's and our customer's best interest to be at the leading edge of WLAN security issues and their standards-based solutions. Our active participation in the standards bodies and heavy involvement in this critical area feeds directly into a more secure and interoperable product suite."

Below is a sampling of the more popular EAP choices that are part of WPA and WPA2:

a) PEAPv0/MSCHAPv2

PEAP or Protected Extensible Authentication Protocol, is perhaps the most popular choice for Microsoft Active Directory installations. It leverages your existing Active Directory usernames/passwords, without any additional client or server software to implement. It provides an encrypted transport for the username and password information in addition to setting up session-based encryption keys used for sending data. Microsoft supplies the supplicant (that's a client in 802.1X-speak) software as part of the client OS as well as the RADIUS authentication server and Active Directory integration as part of their IAS (Internet Authentication Server) server software. The benefits of using PEAP are the integration into Active Directory, the protected transport of username/password information and that each session negotiates a different set of keys used in encryption to prevent snooping or masquerading.usernames/passwords, without any additional client or server software to implement. It provides an encrypted transport for the username and password information in addition to setting up session-based encryption keys used for sending data. Microsoft supplies the supplicant (that's a client in 802.1X-speak) software as part of the client OS as well as the RADIUS authentication server and Active Directory integration as part of their IAS (Internet Authentication Server) server software. The benefits of using PEAP are the integration into Active Directory, the protected transport of username/password information and that each session negotiates a different set of keys used in encryption to prevent snooping or masquerading.

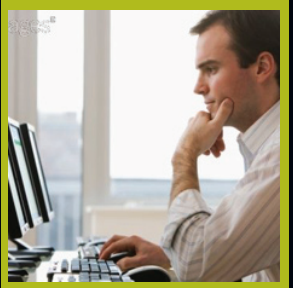
b) EAP/TLS

This EAP type provides for secure authentication and cryptographic key exchange, based on TLS (Transport Layer Security) which has been used for VPNs and secure information exchange over the internet for many years. Authentication requires valid security certificates on the supplicant (client) and authentication server (typically a server running RADIUS). Deploying and managing client certificates on a large scale can be challenging from a logistics perspective. On the plus side, it is widely standardized and supported across multiple operating systems (e.g. many flavors of Linux and Windows).

c) PEAPv1/EAP-GTC

This EAP type uses a PEAP version that is not standardized, but was developed primarily by Cisco and RSA. The GTC or Generic Token Card provides authentication using something you have (a small device or keyfob) that generates a token used in authentication. The exchange of that information is protected inside an encrypted tunnel (the PEAP part) to prevent eavesdropping.

3 See: http://www.wi-fi.org/knowledge_center_overview.php?docid=3296



Robust authentication solves a variety of security issues; this is also where wireless systems can and should differentiate themselves.

Bonded Authentication deserves a brief mention as a strong authentication technique. This refers to the ability to restrict the 802.1X authentication of a particular user if and only if the machine itself has also been authenticated using 802.1X. The value of bonded authentication is that trusted users can only use trusted machines. End Point Integrity Checking, discussed under Authorization is a related but different capability that occurs after authentication.

The second "A": Authorization

Authentication as the first step returns a yes/no response. Either the person is accepted or not and if so, several EAP types provide important session keys for subsequent encryption. But Authorization (or access control) is where, based on the identity of the person, a rich set of enforcements and conditional restrictions can be utilized. Sometimes referred to as Access Control Rules, Authorization tells us "We know who you are, now here's what we will allow you to do." Authorization is where the real power of classifying between types of users and levels of access comes in. We are restricting a user's access based on their identity and group association.

Examples of Authorization could include:

- Requiring the use of a particular encryption type
- Restricting access to certain servers based on departmental association.
- Allowing access from only those systems that are up-to-date with the enterprise's anti-virus software (end-point integrity check).
- Restricting access only to a subnet used for internet access
- Allowing/disallowing access for different groups based on time-ofday or day-of-week or even location

Robust authentication solves a variety of security issues; this is also where wireless systems can and should differentiate themselves.

1. Examples of weak authentication

In much the same way as weak authentication can jeopardize a network, weak authorization can provide vulnerable leverage points for attackers. Poor Delineation Between User Types - Most wireless networks are required to serve multiple types of users. Examples include an enterprise that wishes to provide Internet access to select guests, providing access to certain applications for select vendors and providing secure access to employees all at the same time. Mixing these types of users together, instead of segregating them, leads to significant security risks. If a guest is able to communicate to the subnets that contain internal servers, you are at risk. If a vendor, can communicate to internal servers other than the ones designated for their use, you are at risk. Even employees should have restrictions on network access based upon their role in the organization. All these are common sense, but it is necessary to provide the delineation, preferably at the network layer on the WLAN to provide simple and secure separation.

2. Examples of strong authentication

The following items demonstrate the power that a good Authorization policy can bring. The goals are to use the information on who the user is (Authentication) to further decide and enhance how they will communicate.

a) Delineation/Separation of User Types

Even though different types of users are using the same wireless access point, it is possible to separate those users in ways that they cannot eavesdrop, tamper or forge secure transactions. Typically, this starts by using different SSIDs (service set identifiers) combined with appropriate authentication and authorization that separates user groups onto different VLANs or and restricts paths through the network using differing ACLs (access control lists) based on user type/identity.

The intent here is to communicate the power of Authorization by listing some of the more interesting authorization techniques.

b) End Point Integrity Checking

A laptop's mobility can be a liability. You might not know where it's been or with whom, so checking up on its safety prior to allowing it to join an internal network is just common sense. End Point Integrity checking provides a "Test and Allow or Quarantine" approach. Those devices that are up-to-date are allowed on the network while those that aren't, end up in quarantine with notification sent to the administrator.

c) Allowed Location

This refers to the ability to allow/disallow access based on a particular user's triangulated location or which access point is being used. The amount of location precision can vary, but if some user types (e.g. guests) should not be allowed to transmit/receive data from sensitive locations, this is the Authorization feature needed. Some may believe that this Authorization function is the primary tool to stop war-drivers in the parking lot from attempting access. But you now know that a good Authentication implementation would have stopped them from getting that far in the first place.

3. Other Authorization "Goodies"

The intent here is to communicate the power of Authorization by listing some of the more interesting authorization techniques. These can be combined and customized to provide the sort of strong authorization model that works well with minimal administrative intervention.

- VLAN membership – Users using the same SSID can be joined to differing VLANs based on their identity. This is done while maintaining full separation between the VLANs.
- Time-of-day / Day-of-week – Guests or students may have no business getting internet access on the weekends or after-hours. This authorization technique can automatically shut down or allow access based on time and date.
- Simultaneous logins – Perhaps Bob the vendor has no business being on two machines at the same time while Sally the V.P. is allowed to have her PDA, laptop and wireless VOIP phone running simultaneously.
- QoS Profile - This is a mechanism to map specific bandwidth control settings to a user's identity. You can also use it for dividing bandwidth between SSIDs as well (i.e. when contention happens, guests get 30% and employees gets 70%)
- Bandwidth usage – Using Dynamic Authorization (RFC 5176) it is possible to change any authorization attribute on-the-fly, even after the session is up and running. Example: perhaps you wish to 'quench' a bandwidth abuser by kicking them off entirely or by throttling down their bandwidth after they have exceeded a threshold within a certain timeframe.
- Stateful inspection - Another example of dynamic authorization involved stateful inspection of application traffic and making dynamic authorization changes accordingly. For example one might detect an employee using an application known to have vulnerabilities and divert that user's traffic to a quarantined network area.
- Firewall filters – Here, directional packet filters may be applied to individuals based on their identity or group membership. Very helpful in isolating or separating traffic such as SIP voice traffic coming from a laptop rather than a known voice device and treating it differently than other data coming from the same device.

Encryption

The encryption function provides the privacy enforcement behind Authentication and Authorization. Without it, the entire Authorization function could be compromised because it would be too easy to see and duplicate another user's identity. By stealing an identity and thus bypassing Authentication, the intruder can inherit all the Authorizations of a trusted user which equals "game over" for security. Encryption, though important, is just part of building a secure network. It cannot stand alone to provide a secure network and must be integrated into good Authentication and Authorization.

Strong accounting can record who had access when, for how long and from where and how much bandwidth was consumed.

1. Weak Encryption

Breaking encryption schemes certainly gets the most press. If an encryption is sufficiently weak it might be possible to eavesdrop and then forge packets to impersonate an authenticated session. Though WEP has long-known weaknesses and should never be used, TKIP also has known vulnerabilities (see reference).[4] TKIP was originally developed as a stopgap improvement to WEP while still preserving hardware compatibility to older wireless systems, typically shipped prior to 2003.

Additionally, the IEEE will deprecate support for TKIP as part of the 802.11 base standard due to its limited intended design life. For example, 802.11m which merges 802.11a,b,d,e,g,h,i,j with the base standard has already deprecated references to TKIP. "The use of TKIP is deprecated. The TKIP algorithm is unsuitable for the purposes of this standard"[5]

2. Strong Encryption: AES/CCMP

WPA2's AES/CCMP is a ground-up designed encryption algorithm with none of the baggage or weaknesses of WEP or TKIP and is available on most wireless gear shipped after 2003. It has been tested and approved through the U.S.'s NIST (National Institute of Standards and Technology) and is a requirement for all RSN (Robust Security Network) compliant networks. It is has also been mandatory for Wi-Fi Alliance certification since March 2006. In fact all of the latest generation products now hitting the streets support AES since the 802.11n Draft 2.0 standard mandates it.

The third "A" Accounting

In the AAA architecture, accounting is perhaps the most under-utilized part. Accounting collects and sends information used for billing, auditing, and reporting—for example, user identities, connection start and stop times, the number of packets received and sent, and the number of bytes transferred. You can track sessions by using accounting information stored locally or on a remote RADIUS server. As network users roam throughout a Mobility Domain, accounting records track them and their network usage.

1. Poor Accounting

Poor Accounting is basically no accounting at all. As a result there exists an inability to answer the question of "what happened" to a user session or the inability to research a user's use of the network. Increasingly regulatory bodies in various industries want irrefutable audit trails in the event of security intrusions or public safety issues occurring.

2. Good Accounting

Good accounting provides the infrastructure to answer "what happened". Strong accounting can record who had access when, for how long and from where and how much bandwidth was consumed. Accounting goes beyond typical network health monitoring and focuses on individual sessions; their performance and their mobility. Coupled with strong location tracking capabilities, it can be possible to literally trace the exact movements of a user or device over an extended period of time – depending on how many days history is retained. Not only can this be useful in the security war, it can be invaluable in aiding IT Troubleshooting, improving public safety and preventing theft.

[4] See articles describing known vulnerabilities of TKIP such as: http://wifinetnews.com/archives/008500.html

[5] https://mentor.ieee.org/802.11/file/08/11-08-1127-12-000m-tgmb-issues-list.xls and "TKIP has reached the end of its designed lifetime and has been deprecated in the next full release of the 802.11 standard" http://en.wikipedia.org/wiki/Temporal_Key_Integrity Protocol

Though encryption is important, it is only a small part of the more important AAA architecture of a secure network.

Current Security Issues Q&A

Is WPA or WPA2 good enough?

WPA and WPA2 refer to the Wi-Fi Alliance's branding for a compliance program focused on Wireless LAN security. They are based on the IEEE's 802.11i security initiative and define the features and components of a secure WLAN for both a home/small office and large enterprise environments. The Security Technical Task Group of the WFA which sets the standards and certification testing is chaired by Trapeze CTO, Matthew Gast.

The primary difference between WPA and WPA2 is WPA2's compliance to a ground-up designed encryption technique, AES/CCMP (Advanced Encryption Standard using Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), which has been tested by NIST (National Institute of Science and Technology) for the government's RSN (Robust Security Network) compliant networks.

By contrast, WPA utilized TKIP, which was developed as a temporary work-around on the old WEP protocol which was found by researchers to be seriously flawed in 2001.[6] TKIP (Temporal Key Integrity Protocol) was designed as a software upgrade that would be hardware-compatible with the old chipsets that supported WEP. Most devices shipped after 2003 support both TKIP and the more efficient and secure AES/CCMP. TKIP did however, inherit some known weaknesses and in 2008 researchers discovered an inherited flaw that could allow a re-injection and spoofing of short packets to a client.[7] Though the encryption was not broken it might then allow for subsequent spoofing attacks involving short packets like ARP or DNS. By no means an easy exercise, but still possible.

As TKIP was never designed as the final secure solution, but as a bridge, the Wi-Fi alliance as of early 2006 provides certification only for products that do both WPA and WPA2 and no longer provides certification for products that meet WPA only[8]. Additionally, as earlier stated, the IEEE will also deprecate TKIP entirely from the 802.11 base standard.

1. Good Encryption Isn't Enough

Though encryption is important, it is only a small part of the more important AAA architecture of a secure network. The IEEE (and therefore WPA and WPA2) make specific recommendations for secure Authentication which must also be followed properly. We refer here to an enterprise deployment of 802.1X with an EAP type that matches your vendor compatibility and administrative needs (see "Strong Authentication" earlier).

2. 802.1X vs. PSK

802.1X in combination with EAP is the standard for authentication that is designed around authentication requirements of large networks and offers several key elements needed when scaling secure network access control (NAC). Just a few of these include:

- Per-user authentication – The ability to authenticate and preserve for accounting purposes, the identity of the user.
- Per-session encryption – The EAP functions allow each session to have unique encryption keys and thus disallow snooping, even by other authenticated users.
- Integration to existing NAC equipment & standards – Using RADIUS servers that either already exist or are easily deployed.

The PSK (Pre-shared Key) authentication technique has none of these key elements. In the PSK scenario, any device with the key (password) can gain access to the network. PSK is easy to deploy but absolutely not a secure authentication technique for anything larger than the smallest enterprises. Due to the nature of pre-shared keys, with more users it is 16 too easy for the key to get into the wrong hands and too difficult to propagate a change if the key becomes compromised.

[6] See Nikita Borisov, Ian Goldberg, David Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11 http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

[7] "Battered, but not broken: understanding the WPA crack". Ars Technica (2008-11-06).

[8] See "WPA2 Security Now Mandatory for Wi-Fi CERTIFIED™ Products" http://www.wifi.org/pressroom_overview.php?newsid=16

FIPS 140 (Federal Information Processing Standard) are a series of publications numbered 140 that specify requirements for cryptography modules related to computer security and data communications for the U.S. government.

As such an enterprise should avoid utilizing the PSK authentication technique that is intended only for home office/small office by the Wi-Fi Alliance. There are unfortunately many older devices and wireless phone sets that are only capable of PSK. In this case, we must resort to substituting more Authorization restrictions in an attempt to make up for weak Authentication. For example, if PSK must be used, it should be restricted and isolated to its own network, with restrictive access control lists, etc,

In summary, WPA's TKIP is showing its age and though useful for devices with old chipsets, the use of WPA2 and its AES/CCMP encryption has been and remains the only choice for the U.S. government's most secure wireless networks. For authentication, there is a wide choice of robust 802.1X/EAP implementations approved as part of WPA2 which provide a scalable and secure authentication technique appropriate for the enterprise in contrast to PSK, whose focus is for simple home and small business networks.

What is FIPS 140-2 and why should I care?

FIPS 140 (Federal Information Processing Standard) are a series of publications numbered 140 that specify requirements for cryptography modules related to computer security and data communications for the U.S. government. The current version is FIPS 140-2. FIPS 140 is intended to coordinate both hardware and software requirements and standards for use by any/all departments and agencies of the U.S. government. Being certified at a particular level of the FIPS 140 requirements is not sufficient for building a secure network, but is thought to be necessary by government entities.

In addition to the agencies themselves, it is often necessary that private contractors to the U.S. government are required to comply with aspects of FIPS 140 as part of carrying out the government contract. This can affect the contractor's internal and external design and operation of their network.

A FIPS 140-2 certification demonstrates that the product's relevant security features have been thoroughly validated and documented in terms of its hardware and software design. These are done to four specific "levels" of security that various agencies can call out as a requirement.

1. Rigorous FIPS requirements in 11 areas

FIPS 140-2 imposes software and hardware requirements across 11 different areas and based on capabilities are placed on four different levels. The 11 areas are:

- Cryptographic module specification and documentation
- Cryptographic module parts and interfaces (flow of sensitive information, how secure/insecure information is segregated in both hardware and software)
- Roles, services and authentication (who can do what administratively, and how this is checked)
- Finite state model (documentation of the various states the cryptographic module can be in, and how transitions occur)
- Physical security (primarily tamper evidence and resistance)
- Operational environment (the operating system the module uses and is used by)
- Cryptographic key management (generation, entry, display, storage, deletion of crypto keys)
- EMI/EMC
- Self-tests of crypto modules (what must be tested and when, how failures are handled)
- Design assurance (documentation demonstrating good design and implementation)
- Mitigation of other attacks (if a module's function is designed to mitigate an attack, how is this done?)

There has been debate, though some would call it a red-herring, on where the encryption and decryption boundaries should occur in a WLAN for client data.

2. Four FIPS Certification Levels

- FIPS 140-2 Level 1 the lowest, imposes very limited requirements; loosely, all components must be "production-grade" and various common forms of insecurity must be absent.
- FIPS 140-2 Level 2 adds significantly more documentation requirements for cryptography and describing state models. It also adds requirements for physical tamper-evidence and role-based authentication. This is the most commonly required FIPS level for government agencies. This is the level of certification attained by the few WLAN vendors which have valitaded FIPS 140 solutions.
- FIPS 140-2 Level 3 adds requirements for physical tamper-resistance, identity-based authentication, and for a physical or logical separation between the interfaces by which "critical security parameters" enter and leave the module, and its other interfaces.
- FIPS 140-2 Level 4 makes the physical security requirements more stringent, and requires robustness against environmental attacks.

3. Examples of FIPS certifications

To see examples of the various reports involved with FIPS certifications, go to NIST's "Cryptographic Module Validation Program" at http://csrc.nist.gov/groups/STM/cmvp/ . You can then view examples of "Security Policy" summary documents and the actual certifications for various products. You can also find the validation certificates for the Trapeze MP_422F access point at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm#933 and for the MX-200F and MX216F WLAN controllers at: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm#954

Where should encryption occur in WLANs?

There has been debate, though some would call it a red-herring, on where the encryption and decryption boundaries should occur in a WLAN for client data. The most obvious answer is "over the wireless part", between the client and the access point which is where it was intended to be used. Some vendors however argue that it's somehow better to extend the encrypted session of the user back through the wired network and terminate it on a controller located somewhere on the wired network (centralized encryption model). Traffic would then be decrypted at the controller placed back onto the same wired network in order to reach its destination.

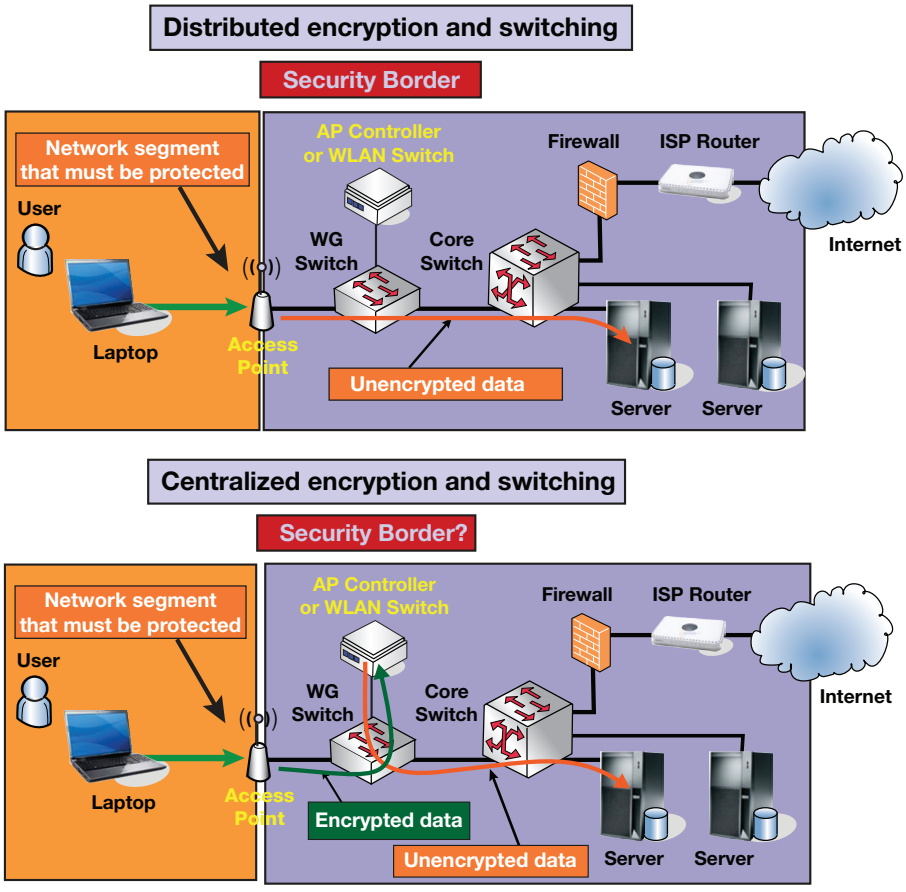
The FIPS 140 Tamper Evidence seal on a Trapeze MP-422F Access Point.

From a pure security perspective, we defer to the Department of Defense's view on whether there is any requirement or benefit to the centralized approach.

This approach is manifest from the early days of wireless in which the old WEP protocol was broken and only way to secure the network over the air was to run a VPN on every client which then all terminated to a centralized VPN controller. The data traffic was then sent unencrypted from the controller over the same wired network. This unintended consequence has several problems, not the least of which is capacity and scaling.

This is in contrast to the intended Distributed Encryption model in which encryption occurs between the clients and the several access points that serve them. The approach scales and secures the wireless medium. The resultant data flows over the wire don't have the burden of encryption/decryption which is why nearly all WLAN vendors take this same approach.[9]

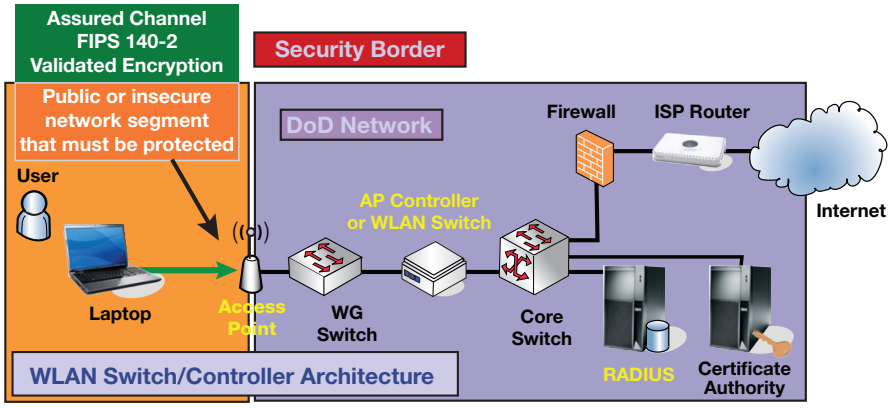
From a pure security perspective, we defer to the Department of Defense's view on whether there is any requirement or benefit to the centralized approach. The DoD, when directing how to use WLANs[10] uses three fundamental elements in defining a security solution: End-to-End, Assured Channel and Security Border to refer to where the network boundary of control ends and then traverses a medium subject to eavesdropping (e.g. wireless) to the client. Capt. Jon Kennedy of the DoD states "....if it were a WLAN located on a DoD base, where an end-user was connecting to the base through a WLAN AP, then the end-to-end concept would only span the following [end-user --> air interface --> AP]; since the AP is directly connected to a DoD owned and operated network, thereby representing the end with the 802.11i encryption protecting the insecure section (i.e. the wireless air interface)."



[9] Vendors include Trapeze, Cisco, Nortel, Motorola, Meru

10 DoDD 8100.2 - Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GiG)

The additional load and overhead placed on the controller in the centralized encryption model can become a significant scalability barrier, which is even more acute with the deployment of 802.11n.



From the DoD's point of view there is no incremental security value in performing encryption/decryption somewhere behind the security border. In fact it only serves to blur the security border which can cause mistakes later. But what about the trade-offs to the wireless system, especially to a more typical Enterprise? Here things get a bit more clear:

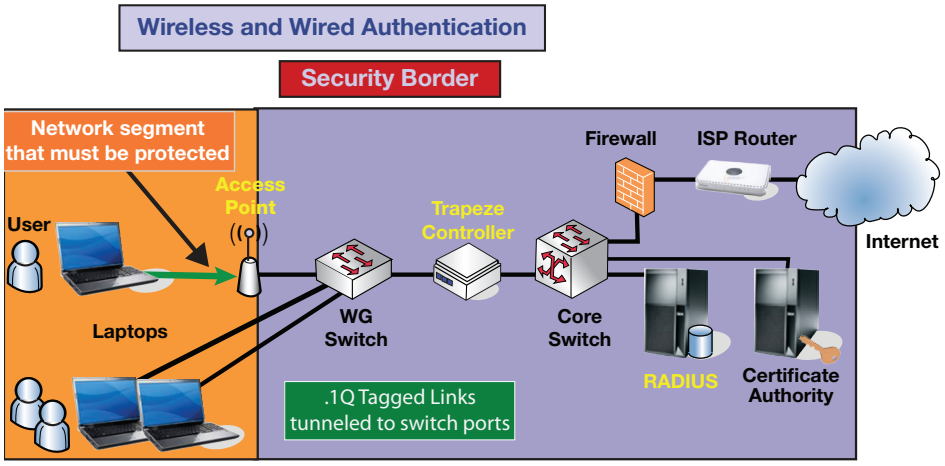
The additional load and overhead placed on the controller in the centralized encryption model can become a significant scalability barrier, which is even more acute with the deployment of 802.11n. Whereas the distributed encryption model leverages the additive processing power of each AP that is added to the network – since the encryption is included in the chipset.

	Centralized Encryption Model	Distributed Encryption Model
Where is the "Security Border"?	"Fuzzy" not at AP, not at WLAN controller, some wires can have both encrypted/decrypted data	"Clear" precisely where the controlled network ends at the Access Point
Does this architecture comply with DODD 8100.2 guidelines?	No	Yes
Does this architecture comply with FIPS 140-2 requirements	Yes	Yes
How does performance scale as more APs are added?	Since all data forwarding and encryption/decryption must flow through the switch CPU, capacity is increased only by adding more controllers.	With encryption/decryption distributed to APs, each AP adds more than enough cryptographic computing power to match the additional traffic load.
Can the AP forward data as anything but the controller?	No - with all encrypted traffic terminating at the controller, the controller must also forward the traffic to its destination.	Yes- some vendors support distributed forwarding at the AP, relieving controllers of the forwarding load.
Is it possible to preserve sessions in redundant fail-over scenarios?	No- if a controller fails all all encrypted sessions will be lost, and all clients will need to re-authenticate to the backup controller.	Yes - if a controller fails all active sessons can be preserved in real time by switching them over to another active controller.

Wired clients can be authenticated and authorized under an AAA architecture using 802.1X through the controller in order to gain access to the network. Wireless clients can do the same and APs themselves can authenticate to their respective controllers as well.

Can Wired LANs learn from Wireless?

One additional best-practice aspect of the security boundary concept we can borrow from the DoD is that the infrastructure devices on the boundary should authenticate themselves to the network. For WLANs, this means the Access Points as well as wireless clients should authenticate themselves. For LANs this means wired clients should also authenticate themselves since they are outside the security boundary (the cubicles and offices vs. the locked wiring closets).



Interestingly, the Trapeze architecture does "all of the above". Wired clients can be authenticated and authorized under an AAA architecture using 802.1X through the controller in order to gain access to the network. Wireless clients can do the same and APs themselves can authenticate to their respective controllers as well. It should be noted that while APs are not encrypting client data over the wire, the management and control traffic between AP and Controller is typically encrypted, following AP Authentication during the AP boot sequence.

Can Guest Access Be Easy but Secure?

Many enterprises have guests and vendor partners they regularly host on their premise. They recognize that allowing their visitors to connect to their respective company email and application servers means productivity benefits for all parties concerned. But what kind of a threat to network integrity does this represent?

Being 'easy to do business with' doesn't have to mean you sacrifice your corporation's security.

So, what are the considerations for deployment of guest and vendor access to ensure that they don't impact or threaten corporate security?

1) **It should be easy and compatible.**

You don't know what laptop your guest is bringing in through the door, so the solution needs to be vendor independent with zero training requirements while not allow ing any viruses or worms they have to threaten your internal network.

2) **You need to be a real guest,** and not some war-driver in the parking lot – remember you don't want someone spamming the world through your IP address. Just like issuing a visitor badge, you must have some modicum of authentication through a receptionist to grant the minimal authorized access required with the ability to account for who, what and where. In other words, you still need an effective Authentication, Authorization and Accounting (AAA) architecture for guests.

3) **Low overhead.** Given the transient nature of guests, this needs to happen without day- to-day interaction from IT staff. Using the visitor badge analogy, there needs to be a supervised granting (e.g. a receptionist) for restricted access and automatic revocation (e.g. only good for that business day) of guest privileges with a logging of who, when and where they went.

Much noise was made of wireless intrusion detection and protection in the earlier days of Wi-Fi networks.

The best way to address the first requirement of "easy and compatible" is a web portal that blocks traffic to the network during authentication. The second and third requirements, making sure your guest is "real" but without a lot of IT overhead, is often seen as more difficult but doesn't have to be if you have the right application and infrastructure. Here's how it can work:

- As part of the usual guest sign-in process, Authentication can be supervised and granted through the receptionist ondemand using a web-based application. This can produce an individually generated username and password for the guest to use with the wireless web portal, and can even be included with their printed name badge.
- Authorization policies for different types guests or visitors can be set up by IT in advance, so that the receptionist only has to assign the appropriate group policy to a guest.
- Through policies, guest traffic may be tunneled through the corporate network to be placed on the DMZ making it impossible for a guest to have any direct communications with the internal network, while still allowing them access to the outside world. Along with some Time-of-day, QoS attributes for bandwidth, disallowing simultaneous logins and any custom filters you may wish to impose, you're set.
- Because Authentication and Authorization was done correctly, Accounting can now be performed down to an individual guest's identity, including name, roaming history and data sent/received.
- The AAA architecture used for guests can run simultaneously but independently of the AAA used for employees, which might be desirable for IT management and separation of NAC functions.

Trapeze's solution for guest access is SmartPass which meets and exceeds all these requirements with ease. The key is to provide all the same AAA security infrastructure with identity-based network access, but integrated into a typical guest sign-in process that can be managed by a receptionist. That's a guest access security architecture that IT staff can control but doesn't need to baby-sit.

Do You Need WIPS/WIDS?

Much noise was made of wireless intrusion detection and protection in the earlier days of Wi-Fi networks. Indeed, this made sense as robust AAA implementations were difficult to deploy and had some missing pieces, and as we all quickly learned, the de-facto security protocols such as WEP, later turned out to be not as secure as we thought. You had to rely on dedicated IDS/IPS systems to stop intruders because there wasn't a strong enough Authentication and Authorization architecture in place to stop them from trying. But today, this market is not keeping pace with WLAN deployments and in many cases declining. Further, the principal intrusion threats such as Rogue Access points, DoS attacks and the like are now easily detected with the base-level IDS/IPS feature set built into most Access Points as standard.

Today, most dedicated wireless IDS and IPS solutions are deployed where:

1) **There is no intention of supplying a WLAN,** yet wired services do exist. In this case the IDS/IPS system is deployed solely to prevent the unauthorized creation of a WLAN to keep employees or intruders from installing "Rogue" APs or creating an "ad-hoc" network that attaches to the internal wired network, thus allowing a back door in.
2) **The wireless devices are old** legacy devices with outdated security capabilities, thus limiting the AAA architecture that can be deployed. In this case the open path to the internal network required by the legacy devices must be augmented to prevent intruders. The most common environment for this is Retail, in which the recent PCI DSS (Payment Card Industry, Data Security Standards) v1.2 standards mandates not deploying WEP and "... using strong encryption technologies for wireless networks, for both authentication and transmission". But many retailers are loath to replace lots of hand held terminals, barcode scanners and the like in order to comply. The alternative of extending their life a few more years by augmenting their existing solution with WEP

Trapeze WLAN equipment is fully capable of identifying, alerting, locating and automatically combating Rogue APs and their users.

cloaking schemes offered by dedicated IPS/IDS infrastructure vendors, seems more attractive in the short term.

Dedicated IDS/IPS systems are typically not installed where the customer is already running or planning to run a WLAN with WPA/WPA2 capable devices. This is because they offer very limited incremental value. Most WLAN vendors, in addition to a strong approach to AAA using WPA2, provide much of the primary functionality for Denial of Service (DoS) and Intrusion Detection formerly found only in IDS/IPS systems. For example, Trapeze WLAN equipment is fully capable of identifying, alerting, locating and automatically combating Rogue APs and their users. There are additionally over 40 different IDS and DoS detection functions "built-in" to the existing equipment. These include detecting flooding techniques using de-authentication, disassociation and decryption error frames, use of RF jamming, "Fake AP" flooding, Spoofed AP and SSID masquerading, detecting the use of popular sniffing/spoofing applications, presence of a wireless bridge and use of weak encryption keys to name a few.

Dedicated systems are too pricy for most enterprises, but they do have additional IDS/IPS features beyond a 'built-in' solution. However, a strong implementation of AAA combined with included rogue-detection, IDS and DoS functions often offsets the real need and management overhead of dealing with the many "false positives" that standalone IDS/IPS systems tend to produce. This, and the complexity of integrating and maintaining security policies across two separate wireless systems is often more trouble than its worth.

Does Location, Location, Location Matter?

This real estate mantra has much in common with security requirements in managing a network that gives users mobility. With the mobility that WLANs provide, you are free to be anywhere and have the access that you need. That's both a great freedom and potential problem – because the traditional benefits of physical security can be bypassed. With a wired network nobody in the parking lot can get on the network, but now with wireless you might. Or, it may be that from certain locations even within the building, certain types of users have no business accessing the network – but with wireless they might. Or knowing where an expensive mobile asset is could be really important. The classic example is the $100,000 crash-cart in a hospital. Knowing where the carts are is not only critical to who needs them but lets you make better use of the carts you have, thereby enabling fewer of them. There are also critical security reasons for being able to know where someone is. It's great to provide users the convenience of wireless but you shouldn't be giving them the ability to hide.

1. Considerations for Location Services

In the modern enterprise, Location services are fast becoming a 'musthave', both for security reasons, asset tracking purposes, and day-to-day troubleshooting assistance. The primary considerations generally are around integration and ease of use, and here are some of the more relevant aspects to consider for these location services:

a) It should be possible to graphically display where a user is on a floorplan of the building

b) This function should be integrated with your existing network infrastructure as your eyes and ears for location.

c) There should be multiple options to consider based on need: from on-demand rudimentary location search with a moderate degree of accuracy, all the way up to 3-4 meter accuracy for thousands of devices in real time.

For example:

Using Trapeze's RingMaster management application you can have an integrated solution that provides on-demand graphical displays of a user's predicted location. The same access points used for the WLAN can be queried to determine the likely location of a specific device – but its only doing it for ne device at a time.

For an advanced location services capability however, you will need to deploy a location appliance that continuously records the current locations of hundreds of devices in real-time, without taxing the WLAN controllers. With a dedicated location appliance, you can track devices instantly with increased accuracy, maintain history, and also leverage advanced features of asset identity tags from companies like Newbury Networks (now owned by Trapeze

Most NAC systems address Authentication and Authorization in various ways and for WLANs this is well covered using standards, such as 802.1X and WPA2. But NACs can also offer powerful Authorization capabilities including endpoint integrity checking.

Networks), Pango, AeroScout and Ekahau to name a few. Further, through published APIs, you can easily integrate location awareness with both your business applications and your physical security systems such as key cards.

2. RF Jamming

One approach getting discussion is focused on the security aspect of location and utilizes RF noise generators ('jamming') to prevent access from certain locations. The theory is that anyone inside the RF borders is "OK" and anyone outside is not. The primary benefit being to discourage "war-driving" (access by unauthorized persons from the parking lot of a building). This should not be confused with location services, rather it's about using strategically placed directional antennas to emit a jamming signal in locations from which you want to prevent access. This approach has some serious obstacles:

a) **Possibly illegal, certainly un-neighborly.** While use of the RF spectrum utilized by WLANs is defined to be unlicensed in most countries, the use of RF jamming devices that might interfere with a neighbor or the Starbucks across the street would be seen as abuse. You probably don't want to go there.

b) **Highly in-accurate.** It's neither easy nor accurate to combine RF Jamming techniques for the areas where you don't want coverage with the RF coverage where you do want it. While multiple Access Points from a WLAN can play nice with each other and provide overlapping, simultaneous coverage to users, being anywhere near an RF jamming device isn't so nice. In order to be effective it must jam on multiple frequencies, and the nature of RF is that boundaries of coverage can be 'fuzzy' and imprecise such that clear-boundaries of access and non-access are really not attainable.

c) **Not really needed.** If you're paying attention to your security architecture, you won't need this approach. A WLAN system such as the Trapeze Smart Mobile® solution combined with a robust standards-based implementation of AAA using WPA2 and 802.1X will prevent unauthorized access. Trapeze also allows the combination of sophisticated location-aware policies that will further prevent certain users from accessing the network while allowing others, unlike the "all-or none" approach of RF Jamming.

In summary, the RF jamming approach is like using a shotgun that doesn't aim well to protect a circle of wagons, whereas a security implementation that embraces AAA using standards like WPA2 and 802.1X is like using a laser-targeted rifle from a reinforced concrete fortress.

Is End Point Integrity Checking Useful?

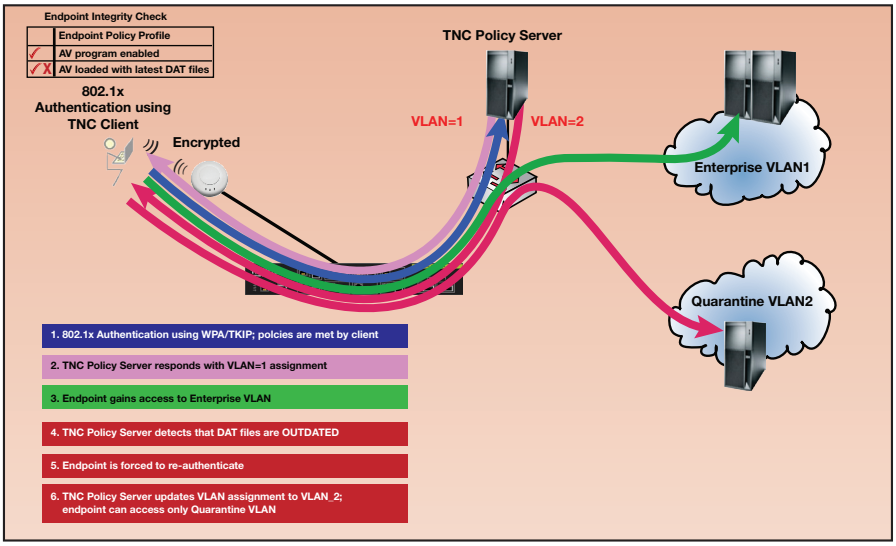
In the context of a WLAN that has implemented a standards-based, robust AAA architecture, the two terms, Network Access Control and endpoint integrity checking are nearly one in the same. Most NAC systems address Authentication and Authorization in various ways and for WLANs this is well covered using standards, such as 802.1X and WPA2. But NACs can also offer powerful Authorization capabilities including endpoint integrity checking. This capability allows a device that is attempting access to the network to be process through a health-check and validation policy before gaining access to the actual network. Failure to pass these checks puts the client in a "quarantine" network that is isolated and sends alerts to the administrator.

A capability like this requires cooperative functioning across multiple applications and networking gear to ensure that the checking, notification and isolation function properly. Much of the approach to this capability has been defined through a cooperative industry group called the "Trusted Computing Group" or TCG which created the "Trusted Network Connect" or TNC specification. Trapeze, being a member of the TCG, has followed the TNC specification which ensures that the Trapeze elements work properly across a variety of other vendor's TNC compliant solutions.

TNC-compliant network elements will determine whether each client that accesses the wireless LAN have been inspected before they are granted full access to the network.

For example, TNC-compliant network elements will determine whether each client that accesses the wireless LAN have been inspected before they are granted full access to the network. If a client is determined a security risk, it can be allowed limited access to a quarantined segment of the corporate network. Another example of a TNC-deployment is preventing misconfigured or infected devices from accessing the network by checking for the latest security patches and service packs, firewalls, antivirus software, and anti-spyware. This can help prevent the spread of new viruses and provide the network or IT administrators' time to correct a suspect clien device.

A Note about LDAP and NAC – LDAP: (Lightweight Directory Access Protocol) is often used by educational institutions as a centralized directory lookup to a persons name, phone #, etc. which can then be bound to Authentication based on username and password. Though WLAN standards provide no direct interaction with LDAP, many NAC systems can provide an interoperability bridge between standard WLAN AAA mechanisms and LDAP.



As you might imagine, what matters is reliable interaction and compatibility with NAC vendors. Though by no means the only NAC vendors, Trapeze has field-proven interoperability with these:

NAC Vendors
Juniper (UAC)
Bradford Networks
Lockdown Networks
Mirage Networks
Microsoft (NAP)
Cisco (via ACS products)

What are HIPAA Security Requirements?

The Health Insurance Portability & Accountability Act (HIPAA) is a federal law creating security standards to ensure the privacy of patients' medical records and personal health information. It is intended primarily for anyone who has access to a patient's medical data such as hospitals, healthcare providers and insurance companies. Therefore any network, including a WLAN used by these enterprises, must comply with HIPAA security standards. Also, any "business associate" which is a broad term applying to any equipment or services utilized in the transfer of confidential information would be considered subject to HIPAA requirements. As such, Trapeze Networks would be considered a "business associate".

Perhaps the most challenging aspect will be the implementation of the new standard by retailers reluctant to change out very old equipment that is still functioning but cannot be made compliant — remember those old "Symbol" wireless bar code readers?

The main thrust of the security requirement is simple. Access to electronic medical information must document the individuals who accessed the files, when they accessed it, and for what purpose they accessed it. HIPAA identifies 5 key areas for secure electronic transfer of patient records:

1) **Authentication –** The first A in AAA. Ensuring the system knows who you are.

2) **Authorization –** The second A in AAA. Ensures that authenticated individuals access the network based on a defined set of priviledges.

3) **Confidentiality –** In AAA-speak you can think of this as using robust Authorization. Confidentiality ensures that only persons authorized to access records are allowed to do so. Conversely, users that are not properly authenticated and authorized cannot gain access to private patient data.

4) **Integrity –** Ensure the data hasn't been manipulated en-route. This again can be thought of as using robust Authorization and can be ensured through the use of session-based encryption keys (e.g. WPA2 using 802.1X).

5) **Non-repudiation –** Once access is granted, neither the sender nor receiver can deny it took place. Here there is an implied requirement for the final A of AAA which is Accounting. Only by doing the first two A's properly (Authentication and Authorization), can good Accounting occur which can track access to the network. In HIPAA networks both network and the database application accounting are needed to identify what particular records are accessed by whom.

It is noteworthy that though the thrust of HIPAA is access to patient data, the requirements can extend to discussion of patient data that might occur. For example using VOIP to discuss a patient should follow the same HIPAA compliance requirements. In this case the network and call application software are needed to do proper accounting for who is talking when and to whom.

In summary, the HIPAA security requirements, like any other security requirements, can be thought of within the context of the AAA architecture and that for WLANs, using WPA2 along with 802.1X in our toolkit allows us to easily comply with the five areas of Authentication, Authorization, Confidentiality, Integrity and Non-repudiation.

What is the PCI Standard about?

After some disturbing early implementations of wireless networks by retailers that resulted in "war drivers" being able to pick up credit card numbers by simply being in the parking lot and using a wireless sniffer, the Payment Card Industry (PCI) extended its Data Security Standards to include wireless. They are currently up to v1.2[11] and have notably required their members to discontinue the use of WEP and mandate requirements for "strong encryption technologies for wireless networks, for both authentication and transmission" such as WPA2 with 802.1X. This is a further recognition that the AAA architecture using the Wi-Fi Alliance's standards matters. Trapeze Networks is of course, fully compliant with PCI DSS v1.2.

Perhaps the most challenging aspect will be the implementation of the new standard by retailers reluctant to change out very old equipment that is still functioning but cannot be made compliant (remember those old "Symbol" wireless bar code readers?).

[11] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Too often, voice handsets that can only use a weak Authentication technique, such as MAC authentication, combined with a weak Authorization, like utilizing WEP encryption, will undermine the entire security infrastructure of the enterprise WLAN.

Is Voice over Wireless secure?

Voice conversations need the same attention to detail when it comes to security that data does. There is in fact, a higher expectation of privacy between two parties. The same AAA architecture can and should be used for understanding the security implementation of Voice over Wireless to ensure proper Authentication, Authorization and Accounting.

Here again, using a standards-based approach like WPA2 utilizing 802.1X is the ideal. The special QoS requirements for voice can be handled in multiple ways, either through the standards-based WMM[12] or through QoS attributes assigned via the Authorization step of AAA.

Voice traffic can also be placed on its own VLAN with wired VoIP phones, leveraging the existing QoS configuration over the wired network.

But beware of letting the tail wag the dog, or in this case letting the limited security capability of a particular handset determine your security architecture. In order to utilize a high security implementation like WPA2, the clients, or in this case the Wi-Fi handsets must also support WPA2. Not supporting this implies some other, likely less secure, approach to AAA. Too often, voice handsets that can only use a weak Authentication technique, such as MAC authentication, combined with a weak Authorization, like utilizing WEP encryption, will undermine the entire security infrastructure of the enterprise WLAN. Though additional Authorization attributes can be used to restrict access of these weaker handsets (or a device pretending to be a handset), this is a stop-gap approach to shore up security holes that can only be resolved by using handsets with robust AAA capabilities such as WPA2 and 802.1X.

Conclusion

We can conclude that regardless of the security issues at hand, defining the problem through the lens of standards not only provides clarity but actual solutions. Understanding security challenges through AAA (Authentication, Authorization and Accounting) provides the basis for understanding who is on the network, how and what they have access to and a recording of when it happened. We then compared weak AAA implementations with robust AAA implementations and their associated characteristics. Most importantly, we found that following the Wi-Fi alliance's 'WPA2' enterprise recommendations (802.1X combined with AES/CCMP encryption), which are based on IEEE standards efforts continues to deliver time-tested, resilient security, and are an integral part of the Federal Government's own requirements (through NIST) for their most secure WLAN implementations.

In fact, every new security scare to date associated with WLANs involves something older or lesser than the use of the Wi-Fi alliance's WPA2 enterprise recommendations, yet nearly every enterprise vendor has had these capabilities for some time. So since WPA2 is simple "table stakes" and every vendor has it, is there any useful differentiation between vendors on their implementation of WPA2? Perhaps, but this should to be evaluated based on needs which may or may not be strictly related to security.

[12] Wireless Multimedia Extensions (WME), also known as Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification, based on the IEEE 802.11e draft standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four Access Categories (AC) - voice, video, best effort, and background. It is suitable for simple applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones

Additional vendor differentiation beyond WPA2 can be useful but these need to be understood within the context of a particular enterprise's needs.

For example:

- If 802.11n and scaling is an important issue, then look to avoid WPA2 implementations that have centralized encryption/decryption. According to NIST, there is no incremental security benefit from a centralized model and it's obvious that the centralized encryption model cannot scale as well as the distributed encryption model favored by the majority of vendors for restricting and categorizing access that may be useful. This is an area worth investigating because it uses a standards-based approach, yet vendors will differ greatly in capability and implementation.
- Wireless Voice. Here the standard WPA2 implementation is fine for security purposes, but must be combined with

  Authorization techniques to ensure users of voice handsets get the right QoS that is properly differentiated from normal data usage occurring simultaneously.
- Guest Access. Generally guest access by definition cannot follow a WPA2 recommendation for AAA since the users are not integrated into the hosting enterprise's native security architecture. A guest solution must therefore provide a strong AAA architecture with individual web-based authentication; particularly strong authorization restrictions for isolating guests from critical resources while preventing use in the wrong time and place and the accounting functions to ensure you know which guest accessed the network and when. All of this must be integrated with how guests normally obtain a guest badge and without burdening the day-to-day tasks of IT (e.g. SmartPass).
- Basic IDS/IPS (intrusion detection/prevention) capabilities are useful if integrated into the WLAN solution, though dedicated equipment is generally only useful if the network is forced to use a weak AAA architecture due to supporting older technology clients. This path is more of a "finger in the dike" approach where older devices that are incapable of WPA2 are supplemented in an attempt to keep them in use. The real solution is to move to devices capable of WPA2.
- FIPS 140-2 is a useful certification if you are a U.S. government entity or government contractor, otherwise it just serves as peace of mind that if correctly configured, the system is capable of secure operation.

And so we see that the Wi-Fi Alliance's WPA2 enterprise recommendations provide a standards-based platform for secure WLAN implementations that most vendors have. Additional vendor differentiation beyond WPA2 can be useful but these need to be understood within the context of a particular enterprise's needs.