Cisco Networking Acade
Mind Wide

obility Series
odule 4 – Wireless LAN Security

liam H. Wolfe II

sco Certified Networking Academy Instructor Trainer

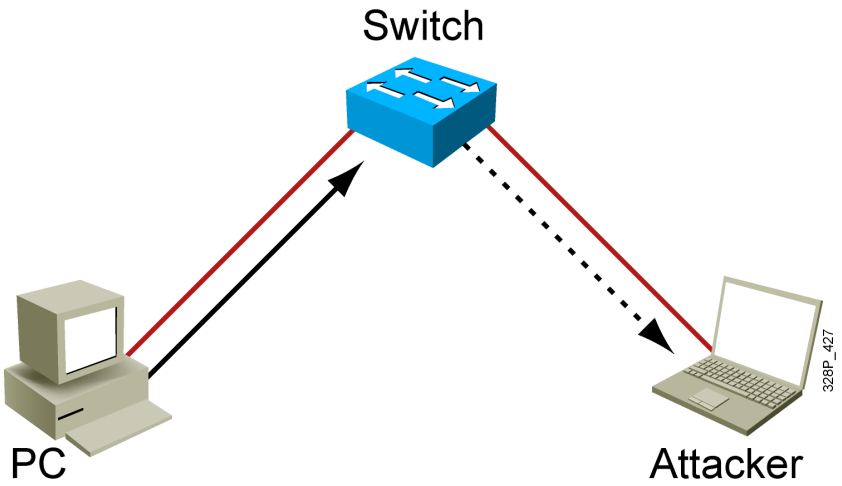
o now you need wireless AND security…

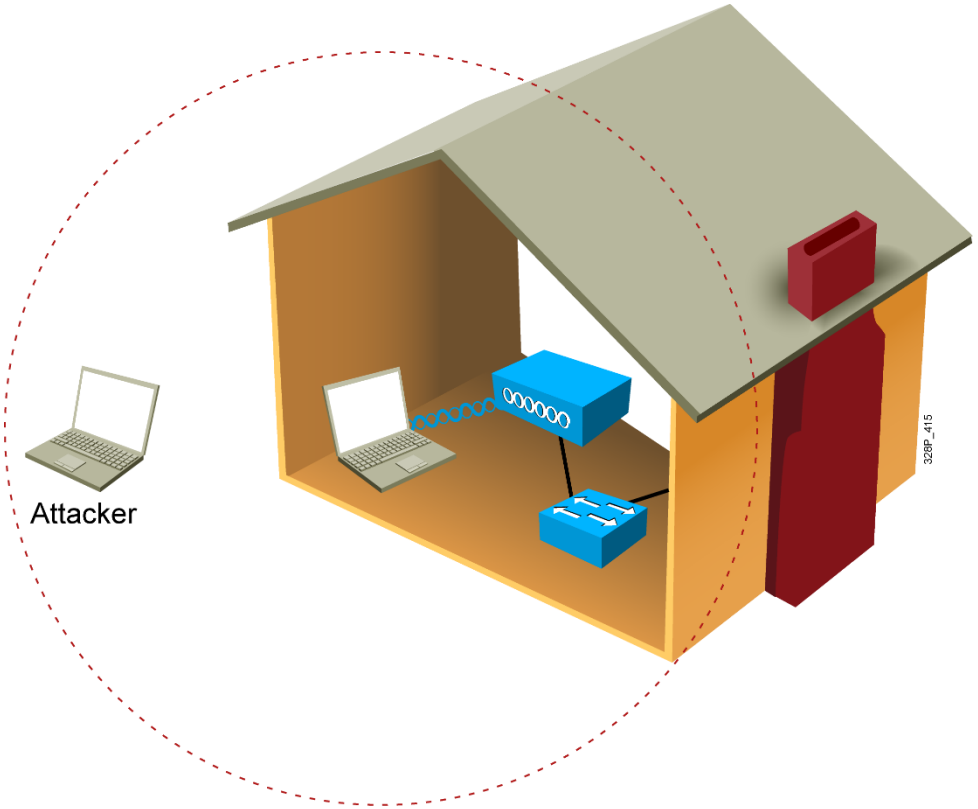
Agenda

1. Overview of WLAN Security
2. Wireless Vulnerabilities and Threats
3. Threat Mitigation Technologies
4. Strong Authentication and Encryption
5. Centralizing WLAN Authentication
6. Conclusion/Remarks/Resources

Overview of WLAN Security

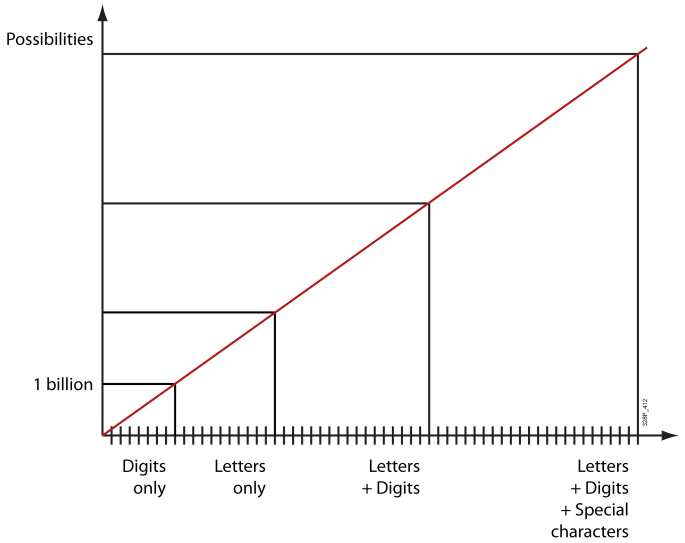
Wired vs. Wireless Privacy

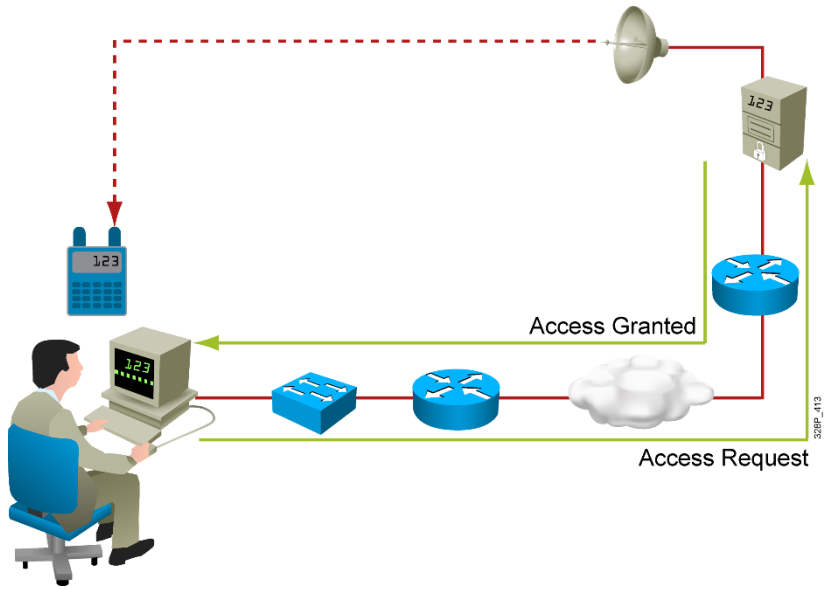




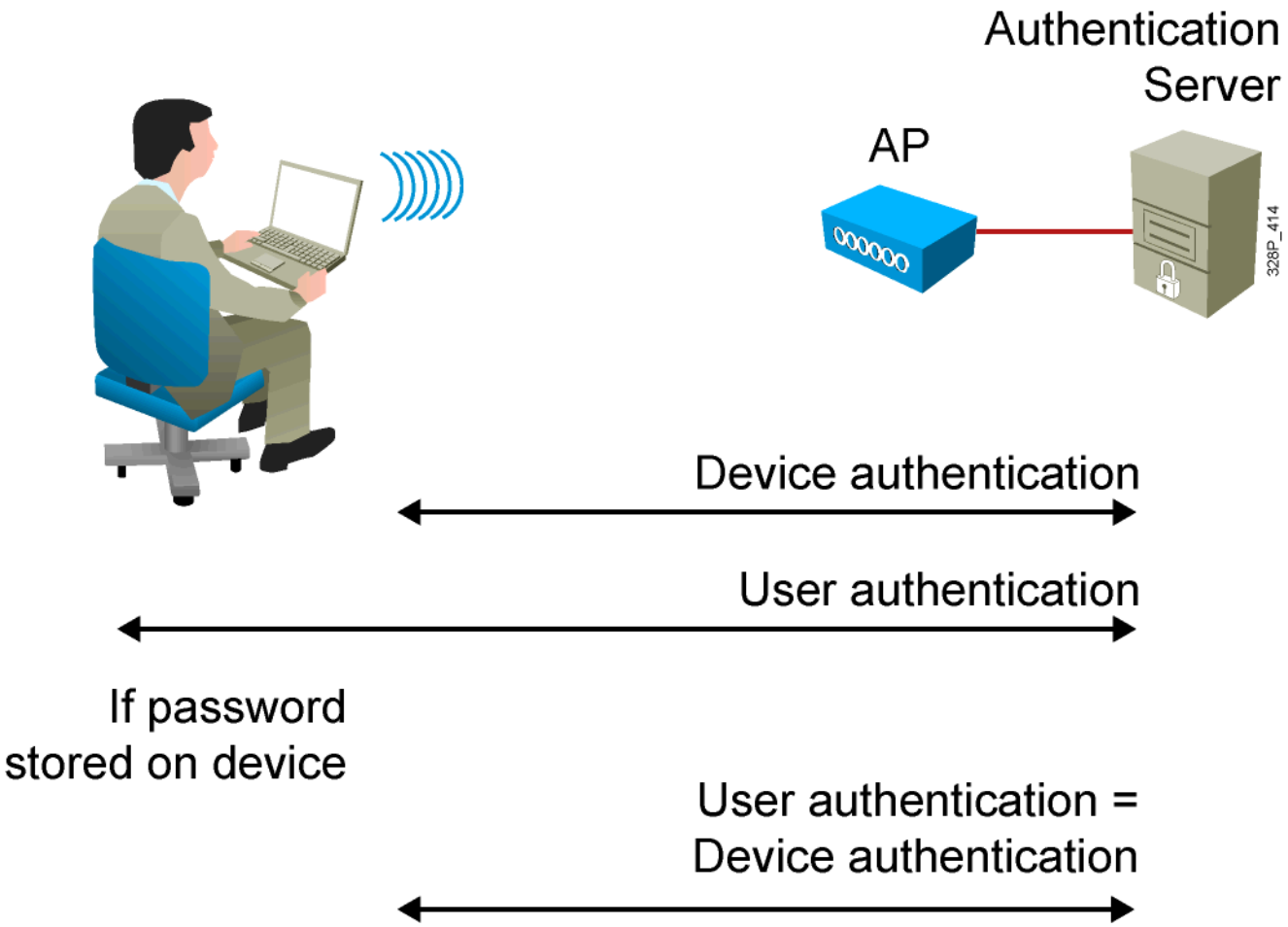
Authentication

- Proving identity can be done using:
  - Something you know
    - Password
    - Something you do
  - Something you have
    - Physical object
    - Value read from a device you have
  - Something you are
    - Biometric reading

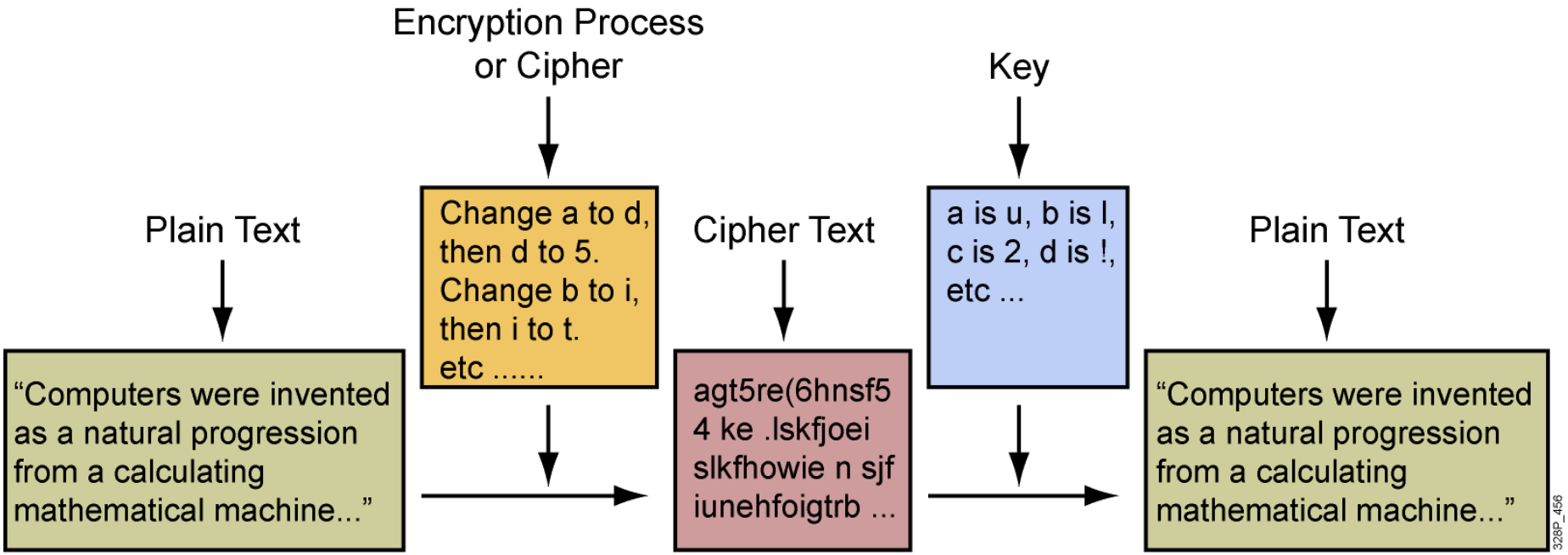




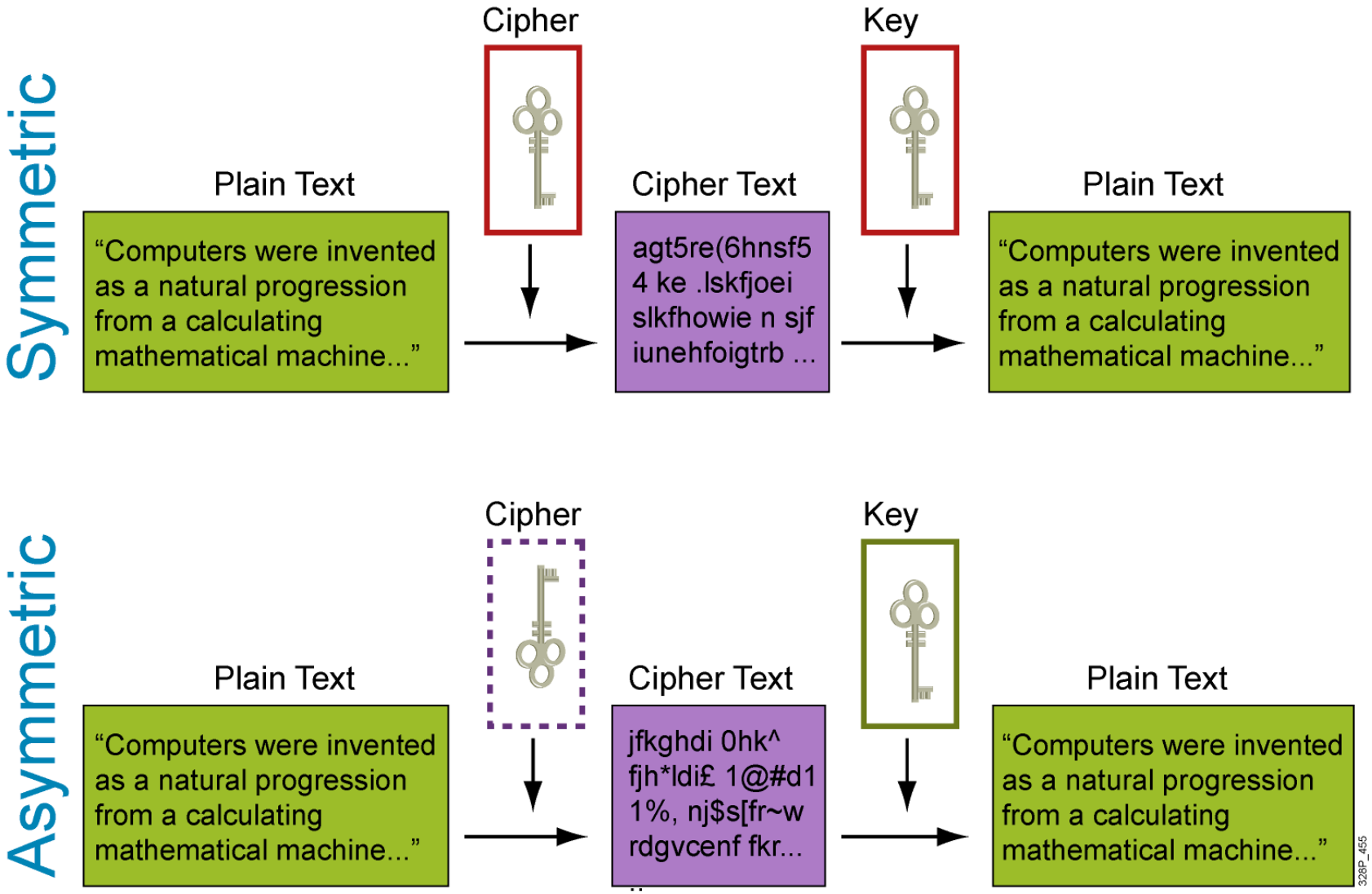
Authenticating Devices vs. Users



Encryption


Encryption Process
or Cipher
Key
Plain Text
Change a to d,
then d to 5.
Change b to i,
then i to t.
etc .....
Cipher Text
a is u, b is l,
c is 2, d is !,
etc ...
Plain Text
“Computers were invented as a natural progression from a calculating mathematical machine...”
agt5re(6hnsf5 4 ke .lskfjoei slkfhowie n sjf iunehfoigtrb ...
“Computers were invented as a natural progression from a calculating mathematical machine...”
328P_456

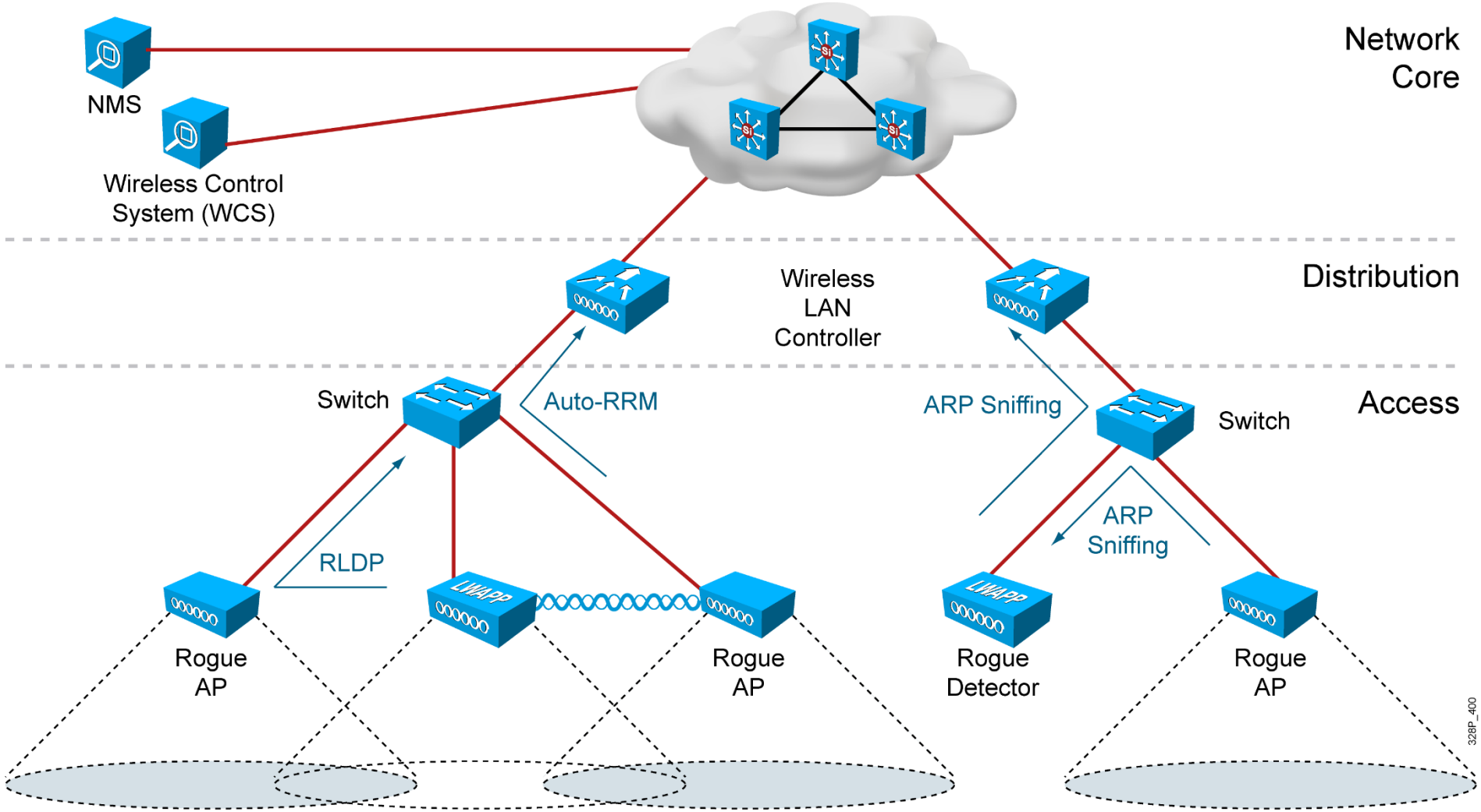
Symmetric and Asymmetric Encryption



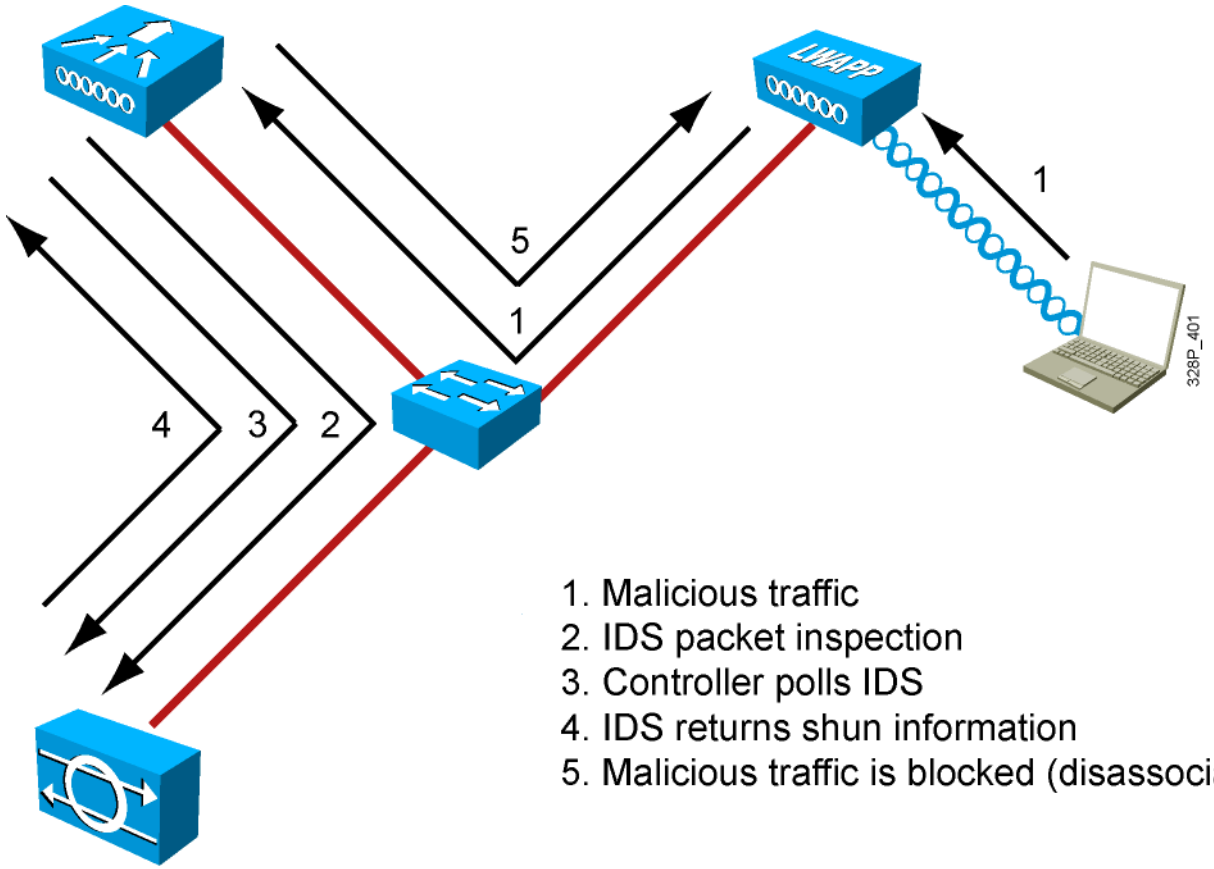
Wireless Threats

- Rogue access points:
  - Usually default configuration
  - Any client on a rogue access point is a rogue client
- Ad hoc networks:
  - Open potential weaknesses
  - Occupy one of your channels
- Client misassociation - accessing the right SSID on a rogue AP
- Wireless attacks:
  - Management frames spoofing
  - Active attacks
  - Passive attacks

Wireless IDS

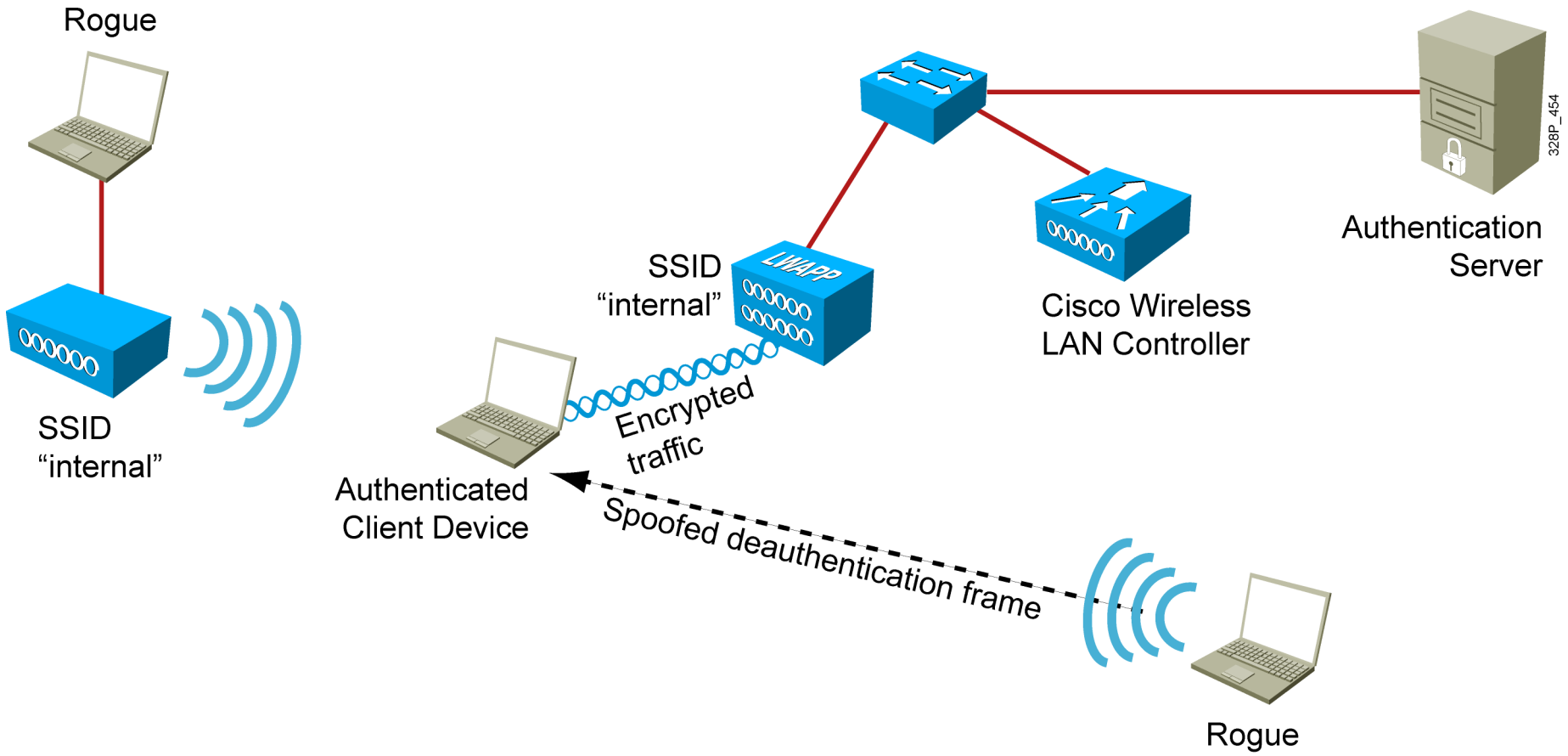


Wireless IPS



1. Malicious traffic
2. IDS packet inspection
3. Controller polls IDS
4. IDS returns shun information
5. Malicious traffic is blocked (disassociation)

Management Frame Protection



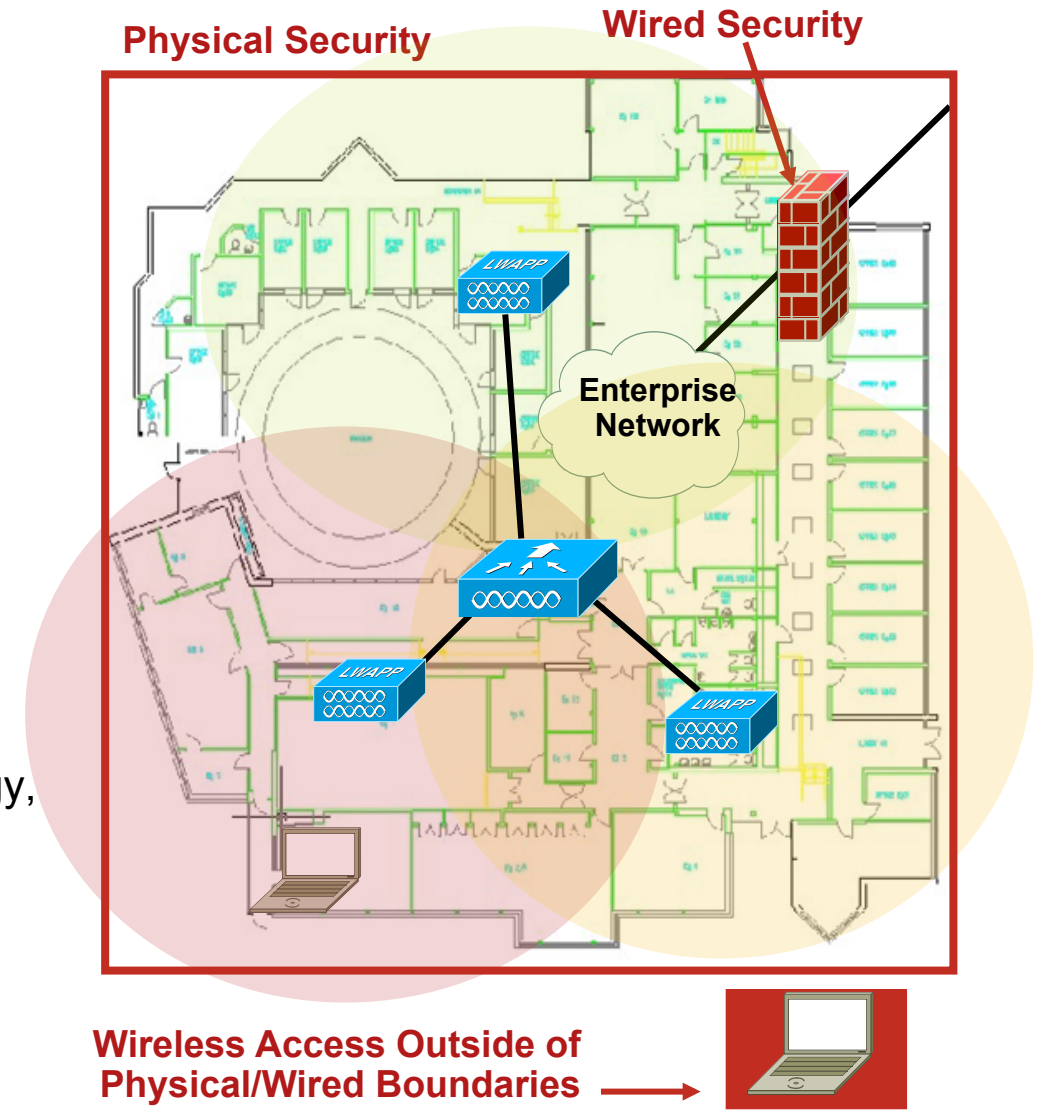
Summary

- In wireless networks, authentication determines who accesses the network, and encryption protects data privacy.
- User authentication can be done using something you know, something you have, or something you are. The devices used to access the network can also be authenticated.
- In wireless networks, encryption is used to add privacy.
- Authentication or encryption keys can be common to a cell or unique to each user.
- Controllers can be linked to Cisco IDS to cut Layer 3-to-Layer 7 attackers completely from the Layer 2 wireless connection.
- In Cisco networks, Management Frame Protection can limit the impact of attacks based on management frames.

Wireless Vulnerabilities and Threats

Why Are Wireless LANs Prone to Attack?

- Open air nature of RF
- Propagation Control is difficult
  - No physical barriers to intrusion
- Standard 802.11 protocol
  - Well-documented and understood
  - The most common attacks against WLAN networks are targeted at management frames
- Unlicensed
  - Easy access to inexpensive technology, for deployments and attack



Need for WLAN Security

- **Open, Pervasive nature of RF**

  Can't control RF Propagation, don't need physical access to launch attacks anymore

- **Business impact of stolen data**

  Potential legal and financial implications (specially in retail, healthcare and government verticals)

- **Innate design, per IEEE 802.11, was designed with basic security needs in mind – times have changed**

  Known vulnerabilities over time

  WLANs are easy DoS targets: jamming, floods, man-in-the-middle attacks, and dictionary attacks…

  No protection of 802.11 Management and Control frames, most solutions address 802.11 Data frames only

- **Need to protect and authorize access to network services and resources**

Security Risk Assessment

- **Sensitive data**

  What is classified as Sensitive varies by organization

  Determined at all levels of an organization what data must be protected from both a legal and business viewpoint

  Appropriate data is protected with proper protection.

  Intellectual property, trade secrets, identity information, financial information, health information, and employee and customer databases

  Possibility that some data is too high a security risk

- **Network services**

  Availability of a company's network, and such actions would cause damage to the company's productivity and affect sales.

  Services : E-mail services, file servers, database services, directory services, Internet connectivity, Web-based applications, virus and intrusion detection services, and custom application services.

Security Policy and what it means

- **Security Policy**

  An organization needs a security policy to define how to protect sensitive data and network services.

  What to do if systems or policies fail..

- **Network services**

  IT organization needs to work with the Security organization to help define the Security Policy and deploy network services inline with the Security Policy

- **Client Capabilities**

  Understanding the capabilities of the network and more importantly the capabilities of the client endpoints will ensure a secure WLAN deployment able to meet the requirements of the business.

Why Is WLAN Security Important?

Vulnerabilities:

Hackers/Criminal

THE WALL STREET JOURNAL.

MONDAY, FEBRUARY 5, 2001 WSJ.com

Hackers Can Penetrate Wireless Network

By Jared Sandberg
Staff Reporter of The Wall Street Journal

A group of respected security research- ple, brought to light by network-security specialists around the globe. Mr. Goldberg himself found a significant flaw in the rel." He adds that the IEEE is working on future versions that won't be vulnerable. But Mr. Ennis says this type of attack

connect to networks using simple radio antennas in their laptop or desktop PCs. The technology, also called Wi-Fi, is sold by many vendors but was popularized by Apple Computer Inc. under the name AirPort and is quickly being deployed in networks at a growing number of businesses, college campuses, hotels and airports. By the end of 2001, an estimated 10 million Wi-Fi radios will be developed, according to research firm Cahners In-Stat. Starbucks Corp., for instance, plans to use the technology to allow latte quaffers to noodle

The weakness is another reminder of the difficulty in implementing effective network security.

chief scientist at Zero Knowledge Systems

Employees

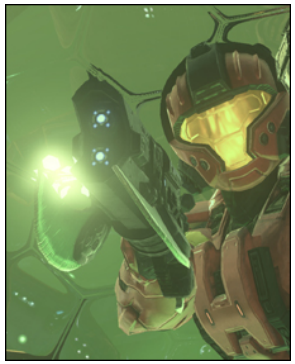
"War Driving"

Lessons:

- Do not rely on basic WEP encryption; requirement for enterprise class security (WPA, EAP/802.1x protocols, Wireless IDS, VLANs/SSIDs, etc.)
- Employees often install WLAN equipment on their own (compromises security of your entire network)
- Business impact due to stolen data: Potential financial and legal consequences (laws to protect data confidentiality; example: healthcare, retail, financial, government)

WLAN Security “Visibility”

- Prevalence of technology
  - PWLAN (Public Wireless LAN) and other public 802.11 networks
- Other security fears—identity theft, phishing, etc.
  - “Hackers target Xbox Live players”, Feb 20, 2009
  - http://news.bbc.co.uk/2/hi/technology/7888369.stm
  - “Crime to boom as downturn blooms” Dec 30, 2008
  - http://news.bbc.co.uk/2/hi/technology/7797946.stm
  - Public availability of tools
  - Aircrack—WEP key exploit
  - coWPAtty—WPA-PSK exploit
  - Kismac—MAC-based implementation of Kismet
  - http://www.darknet.org.uk/2006/04/top-15-securityhacking-tools-utilities

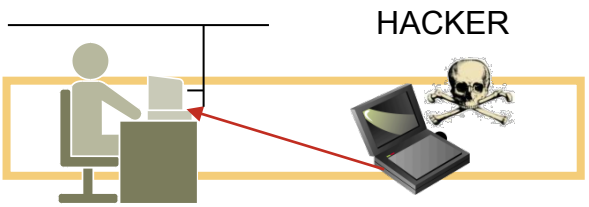


Wireless Security Threats

Classifying the attack types

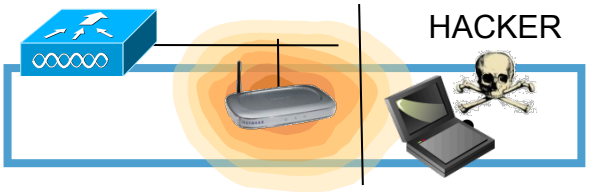
On-Wire Attacks

Ad-hoc Wireless Bridge



Client-to-client backdoor access

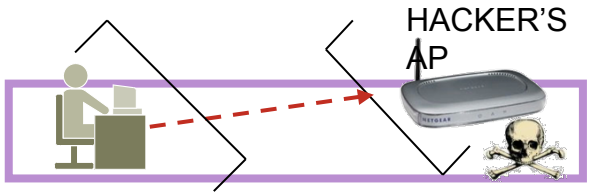
Rogue Access Points



Backdoor network access

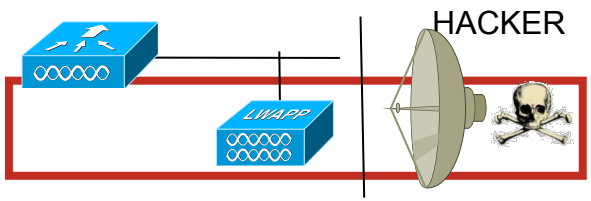
Over-the-Air Attacks

Evil Twin/Honeypot AP



Connection to malicious AP

Reconnaissance

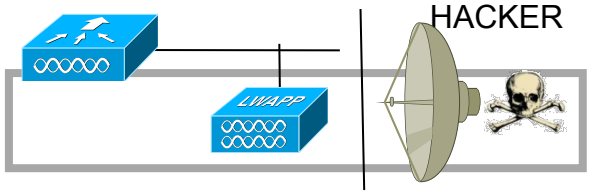


Seeking network vulnerabilities

Denial of Service

Service disruption

Cracking Tools



Sniffing and eavesdropping

Non-802.11 Attacks

BLUETOOTH AP

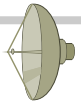
Backdoor access

Service disruption

MICROWAVE

BLUETOOTH

RF-JAMMERS



RADAR

WLAN Security Vulnerabilities and Threats

Examples of Existing Vulnerabilities and Threats

- WLAN sniffing/war driving
- Encryption vulnerabilities: WEP
- Denial of Service (DoS) attacks: using 802.11 de-authentication/disassociation frames, RF jamming, etc.
- Authentication vulnerabilities: dictionary attacks, MITM attacks
- Address spoofing: MAC-address spoofing and IP address spoofing (both hostile/outsider attacks as well as insider attacks)

An Example:
How Does a Wireless Exploit Take Place?

- Probe response “listening” (to get SSID)
- Passive WEP key sniffing
- Initial phases of WLAN security exploit

  Discovery of WLAN networks by monitoring for probe/probe responses

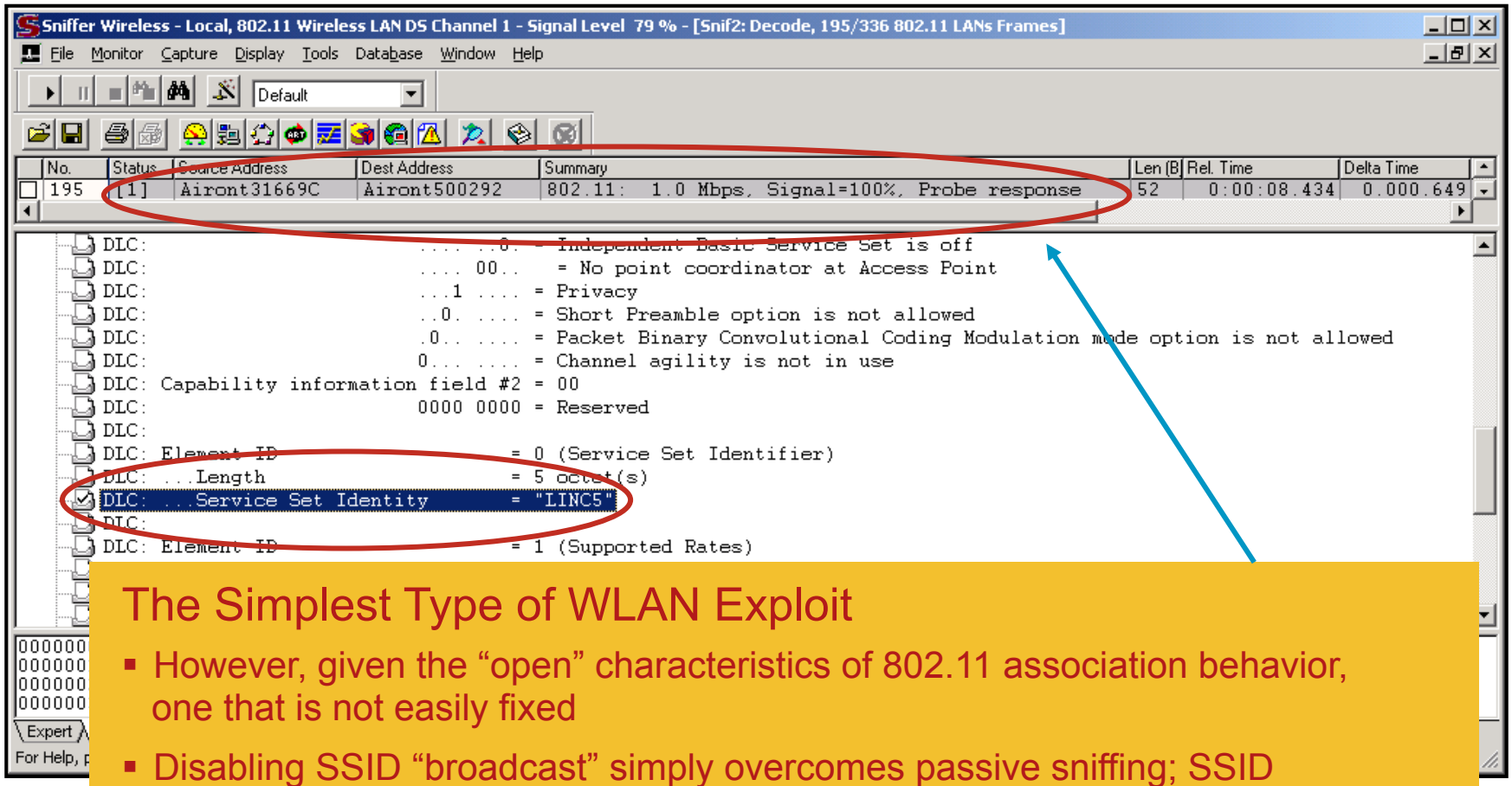
  Collection of sufficient encrypted packets, offline processing and attempt to calculate WEP key

An Example:
How Does a Wireless Exploit Take Place?

Active De-Auth to Induce Clients to Probe
(Reduces Time to Overcome SSID “Cloaking”

- For example, “Kismac” tool: offers a “suite” of exploit tools with a easy-to-use GUI
- http://www.ethicalhack.org/videos.php
- Authentication exploits can then be undertaken, once a client has been provoked to re-authenticate
- Or, if client may be induced to negotiate unauthenticated/unencrypted connection, a direct exploit on client may be undertaken

WLAN Sniffing and SSID Broadcasting



The Simplest Type of WLAN Exploit

- However, given the “open” characteristics of 802.11 association behavior, one that is not easily fixed
- Disabling SSID “broadcast” simply overcomes passive sniffing; SSID is easily discovered by observing probe responses from clients
- Thus, SSID “cloaking” shouldn’t be considered a security mechanism

802.11 WEP Vulnerabilities

- **802.11 Static-WEP is flawed: encryption passive attacks**

  RC4 Key Scheduling algorithm uses 24-bit Initialization Vector (IV) and does not rotate encryption keys

  Practical tools that have implemented FMS attack (example: AirSnort) can uncover the WEP key after capturing 1,000,000 packets

  This is about ~ 17 minutes to compromise the WEP key in a busy network; this attack is passive and all the attack tool needs to do is “listen” to the WLAN network (i.e., sniff WLAN packets)

- **802.11 Static-WEP is flawed: encryption active attacks**

  Does not protect the WLAN user data integrity

  Several forms of attacks possible: Replay attacks, bit-flipping attacks, etc.

- **802.11 Static-WEP shared key authentication is flawed**

  AP challenges (plaintext challenge) the WLAN user to ensure possession of valid encryption key

  Attacker can obtain key stream ➔ plaintext challenge XOR ciphertext = Key Stream

Wireless: Man in the Middle Attacks

- A MiTM is when an attacker poses as the network to the clients and as a client to the actual network

  Attacker must first force client off of intended network in order to lure wireless station to associate to “rogue network”

  The attacker gains security credentials by intercepting user traffic

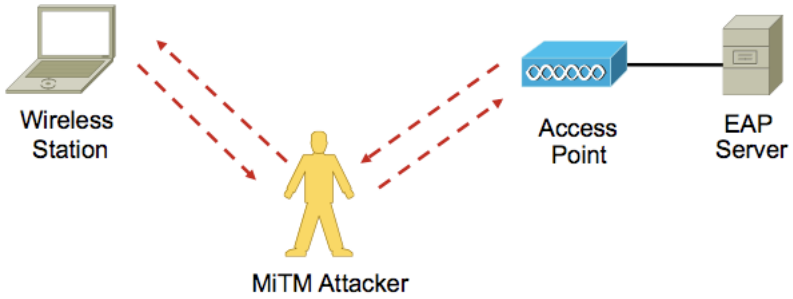
- Very easy to do with:

  MAC Address Spoofing

  Rogue Device Setup

  DoS Attacks

  Easier Sniffing, and war-driving



Wireless: Rogue Devices

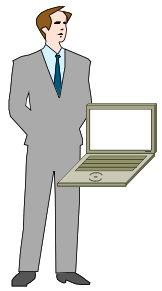
- **What is a Rogue?**
  - Any device that's sharing your spectrum, but not managed by you
  - Majority of rogues are setup by insiders (low cost, convenience, ignorance)
- **When is a Rogue dangerous?**
  - When setup to use the same ESSID as your network (honeypot)
  - When it's detected to be on the wired network too
  - Ad-hoc rogues are arguably a big threat, too!
  - Setup by an outsider, most times, with malicious intent
- **What needs to be done?**
  - Classify
  - Detect
  - Reporting, if needed
  - Track (over-the-air, and on-the-wire) and Mitigate (Shutdown, Contain, etc)

Rogue AP Vulnerability: Both Internal and External Sources

Frustrated insider

- User that installs wireless AP in order to benefit from increased efficiency and convenience it offers
- Common because of wide availability of low cost APs
- Usually ignorant of AP security configuration, default configuration most common

Most Rogue APs

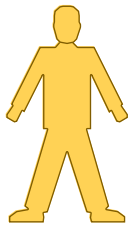


James from Accounting

Malicious hacker

- Penetrates physical security specifically to install a rogue AP
- Can customize AP to hide it from detection tools
- Hard to detect—more effective to prevent via 802.1x and physical security
- More likely to install LINUX box than an AP

Less likely



What Is a Dictionary Attack Tool?

- **What is a dictionary?**

  Contains variations of passwords

  Weak passwords can be cracked using standard dictionaries (found easily in various Internet discussion forums and web sites)

- **Success factors for this tool depend on:**

  Variation of the user's password must be found in the dictionary used by the attacker

  Attacker's experience and knowledge in generating dictionaries

  Password strength

    A weak six character password will be easily compromised compared to a strong ten letter password

    Attacker's dictionary strength determines whether the password can be compromised

MAC Address Spoofing

- As with wired networks, **MAC address and IP address spoofing** are possible, if not easy, in Wireless Networks
- **Outsider (hostile) attack scenario**

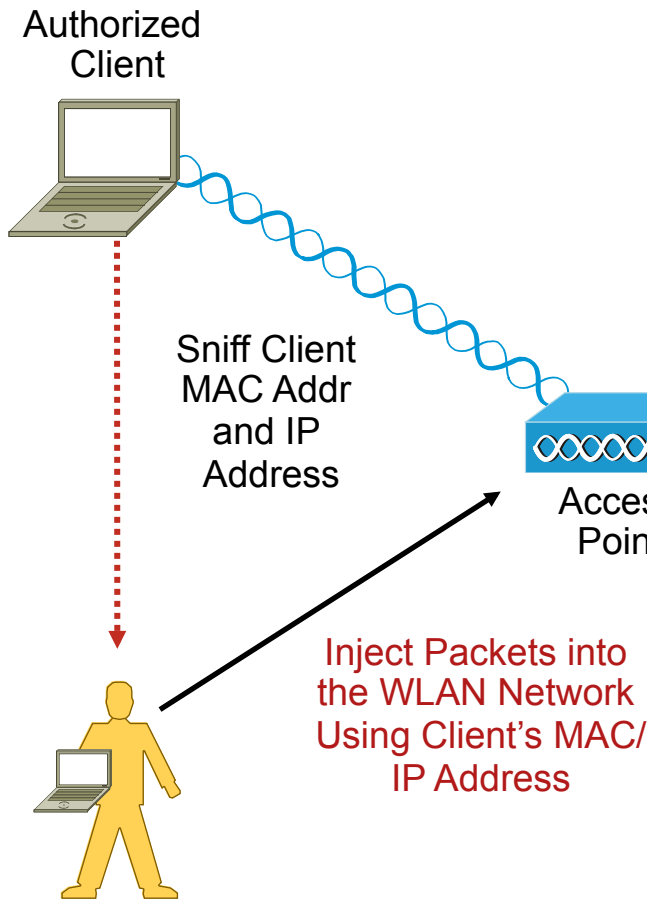
  Does not know key/encryption policy

  IP Address spoofing is not possible if Encryption is turned on (DHCP messages are encrypted between the client and the AP)

  MAC Address spoofing alone (i.e., without IP Address spoofing) may not buy much if encryption is turned on
- **Insider attack scenario**

  Seeking to obtain users' secure info

  MAC address and IP Address spoofing will not succeed if EAP/ 802.1x authentication is used (unique encryption key is derived per user (i.e., per MAC address))



Wireless Sniffing: Good and Bad

- First – Sniffing, or capturing packets over the air, is an extremely useful troubleshooting methodology
- Sniffing, in the old days was reliant on very specific cards and drivers
- Very easy to find support for most cards and drivers today
- Cost (if you like to pay for it) of such software is negligible (or, just use free/ opensource software)
- Provides an insight (with physical proximity) into the network, services, and devices which comes in handy when performing network reconnaissance

WLAN Security

Denial of Service Attacks

- RF Jamming
  - –Any intentional or un-intentional RF transmitter in the same frequency can adversely affect the WLAN
- DoS using 802.11 Management frames (MPF can help mitigate)
  - –Management frames are not authenticated today
  - –Trivial to fake the source of a management frame
  - –De-Authentication floods are probably the most worrisome
- Misuse of Spectrum (CSMA/CA – Egalitarian Access!)
  - –“Silencing” the network with RTS/CTS floods, Big-NAV Attacks
- 802.1X Authentication floods and Dictionary attacks
  - –Overloading the system with unnecessary processing
  - –Legacy implementations are prone to dictionary attacks, in addition to other algorithm-based attacks

Authentication Vulnerabilities

- **Management frames are not authenticated** !
- **Dictionary attacks**

  On-line (active) attacks: active attack to compromise passwords or pass-phrases

  Off-line attacks: passive attack to compromise passwords or pass-phrases

- **MITM attacks**

  Active attacks: an attacker attempts to insert himself in the middle of authentication sequence

- Can be employed in 802.1X as well as PSK environments

  Multiple known WEP weaknesses, and many exploits out there

Exploits Using 802.11 as a Launchpad

- Standard Layer 2 exploits, e.g., Dsniff, Nmap
- Penetration test—server and service vulnerabilities:

  Metasploit project—open source RPC injector http://metasploit.com

  Immunity CANVAS

  Core security technology impact
- Application security—exploit/malware
- Specific examples that have been launched:

  Installation of various viruses, worms, and other malware, thereby complicating detection—Security Conference, Canfield University, UK

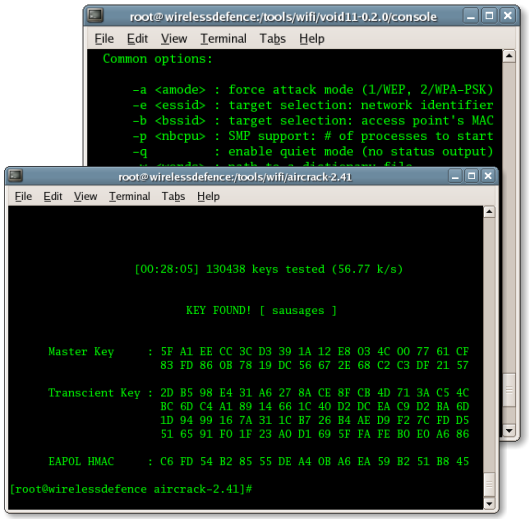
  Simple sniffing of unencrypted user ID, passwords, account nos., etc.—Wi-Fi hotspots

WLAN Security Vulnerabilities and Threats Summary

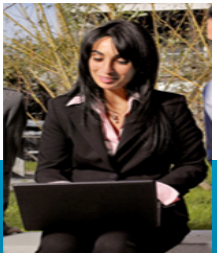
- Wireless LANs have become easy targets for both “traditional” network exploits, as well as criminal element
- Passive SSID probe sniffing and WEP key attacks are just the first stage in WLAN exploits
- More sophisticated WLAN exploits are likely to employ management frames, as there is currently no encryption capable for these 802.11 media management packets
- If an attacker can gain access to a WLAN, it is possible to launch a variety of higher-layer exploits over this media

Quick Look: Common WLAN Exploits/Tools

- Remote-Exploit/Backtrack/Auditor
- Aircrack, WEPcrack, etc
- coWPAtty
- Kismet
- NetStumbler, Hotspotter, etc
- AirSnort
- Sniffing tools: OmniPeek, Wireshark
- dsniff, nmap
- wellenreiter
- asleap



Over-the-Air Attack Techniques and Tools



Network Profiling and Reconnaissance

- Honeypot AP
- Netstumbler
- Kismet
- Wellenreiter
- Excessive device error
- Excessive multicast/broadcast

Authentication and Encryption Cracking

- Dictionary attacks
- AirSnarf
- Hotspotter
- WEPCrack
- ASLEAP
- EAP-based attacks
- CoWPAtty
- Chop-Chop
- Aircrack
- Airsnort
- PSPF violation
- WEP Attack
- Illegal frame types
- Excessive association retries
- Excessive auth retries
- LEAPCracker

Man-in-the-Middle

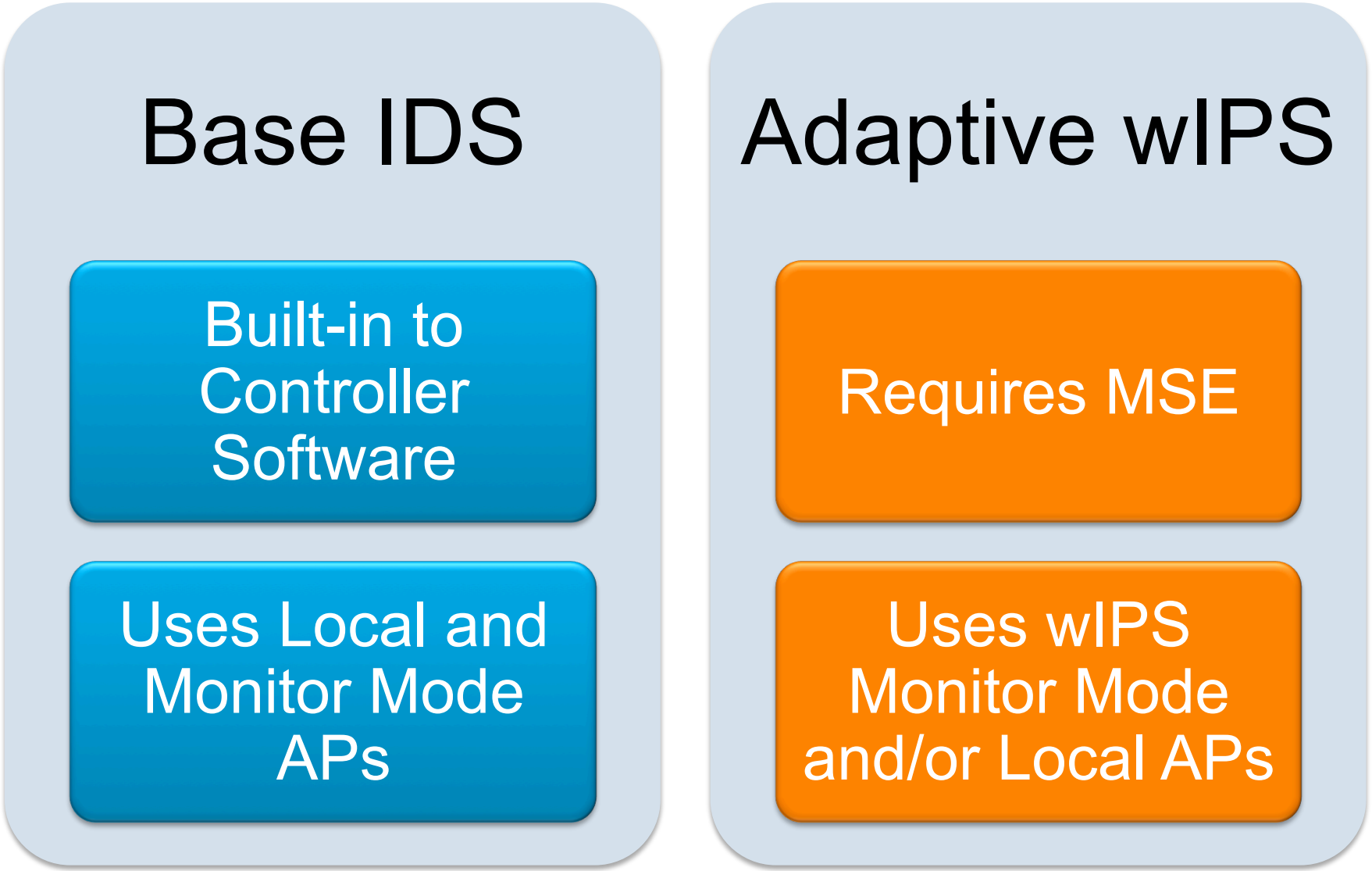
- MAC/IP Spoofing
- Fake AP
- Evil Twin AP
- ARP Request Replay Attack
- Fake DHCP server
- Pre-standard APs (a,b,g,n)

Denial of Service

- Malformed 802.11 frames
- FATA-Jack, AirJack
- Fragmentation attacks
- Excessive authentication
- De-auth attacks
- Association attacks
- CTS attacks
- RTS attacks
- Excessive device bandwidth
- EAPOL attacks
- Probe-response
- Resource management
- RF Jamming
- Michael
- Queensland
- Virtual carrier
- Big NAV
- Power-save attacks
- Microwave interference
- Bluetooth interference
- Radar interference
- Other non-802.11 interference
- Device error-rate exceeded
- Interfering APs
- Co-channel interference
- VoWLAN-based attacks
- Excessive roaming

Threat Mitigation Technologies

Cisco's Attack Detection Mechanisms



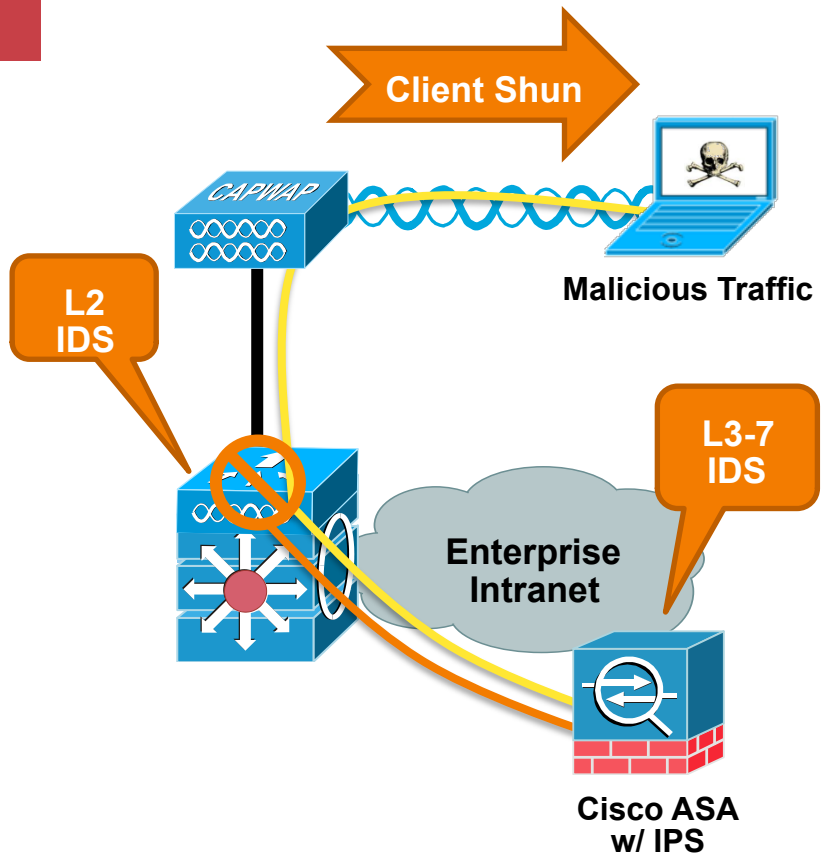
Cisco Wired IPS Integration

Unified Intrusion Prevention

Business Challenge

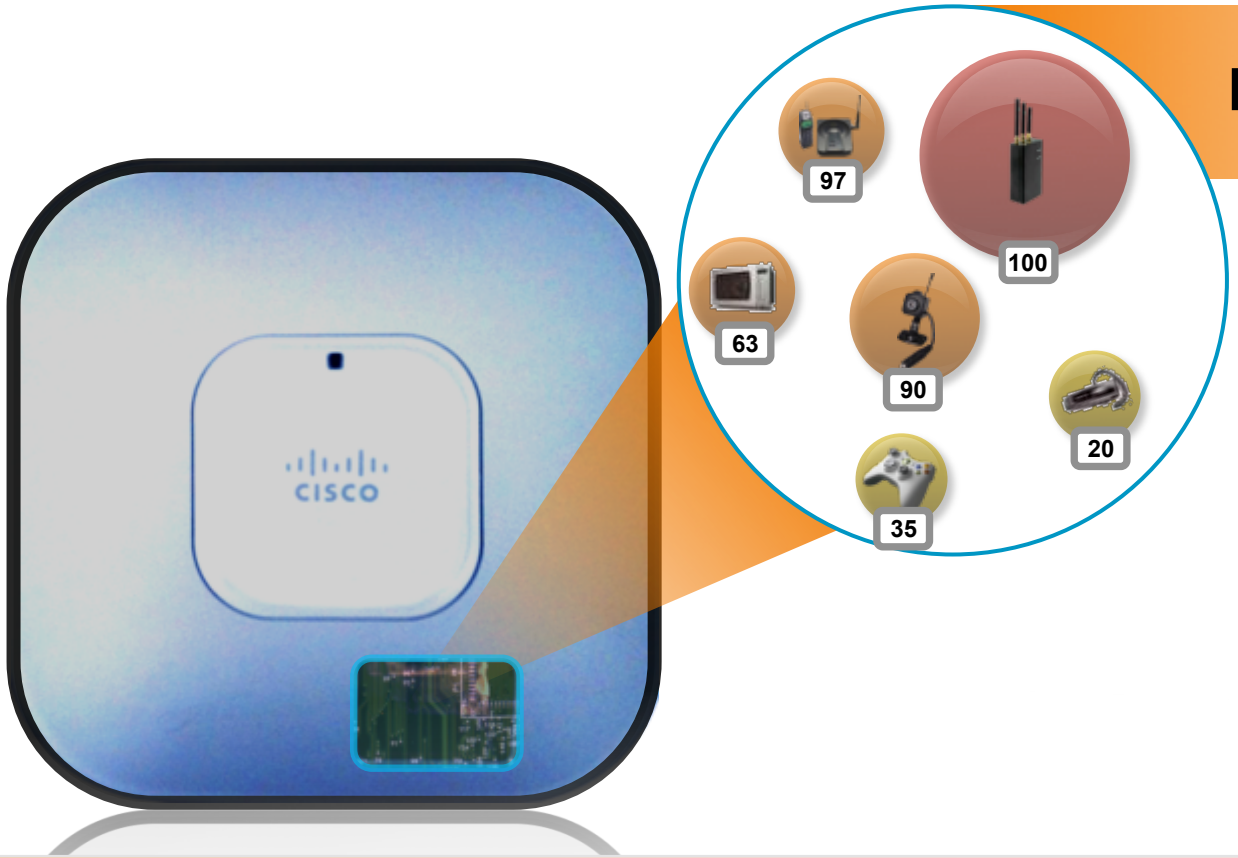
Mitigate Network Misuse, Hacking and Malware from WLAN Clients

- Inspects traffic flow for harmful applications and blocks wireless client connections
- Layer 3-7 Deep Packet Inspection
- Eliminates risk of contamination from wireless clients
- Zero-day response to viruses, malware and suspect signatures



http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a008080dc8c.shtml

What is CleanAir?



Detect and Classify

- Uniquely identify and track multiple interferers
- **Detects security-risk interferers** like RF Jammers and Video Camera.
- Assess unique impact to Wi-Fi performance
- Monitor AirQuality

Cisco CleanAir

High-resolution interference detection and classification logic built-in to Cisco's 802.11n Wi-Fi chip design. Inline operation with no CPU or performance impact.

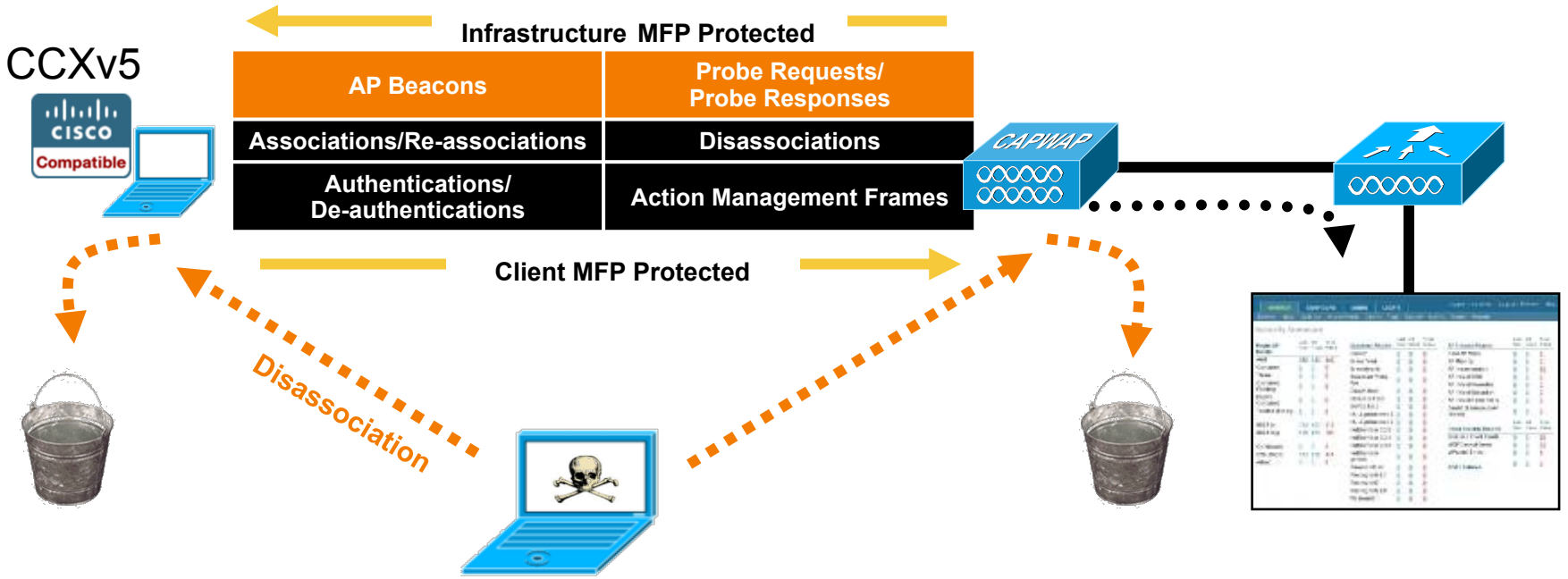
Management Frame Protection
Concept

Problem

- Wireless management frames are not authenticated, encrypted, or signed
- A common vector for exploits

Solution

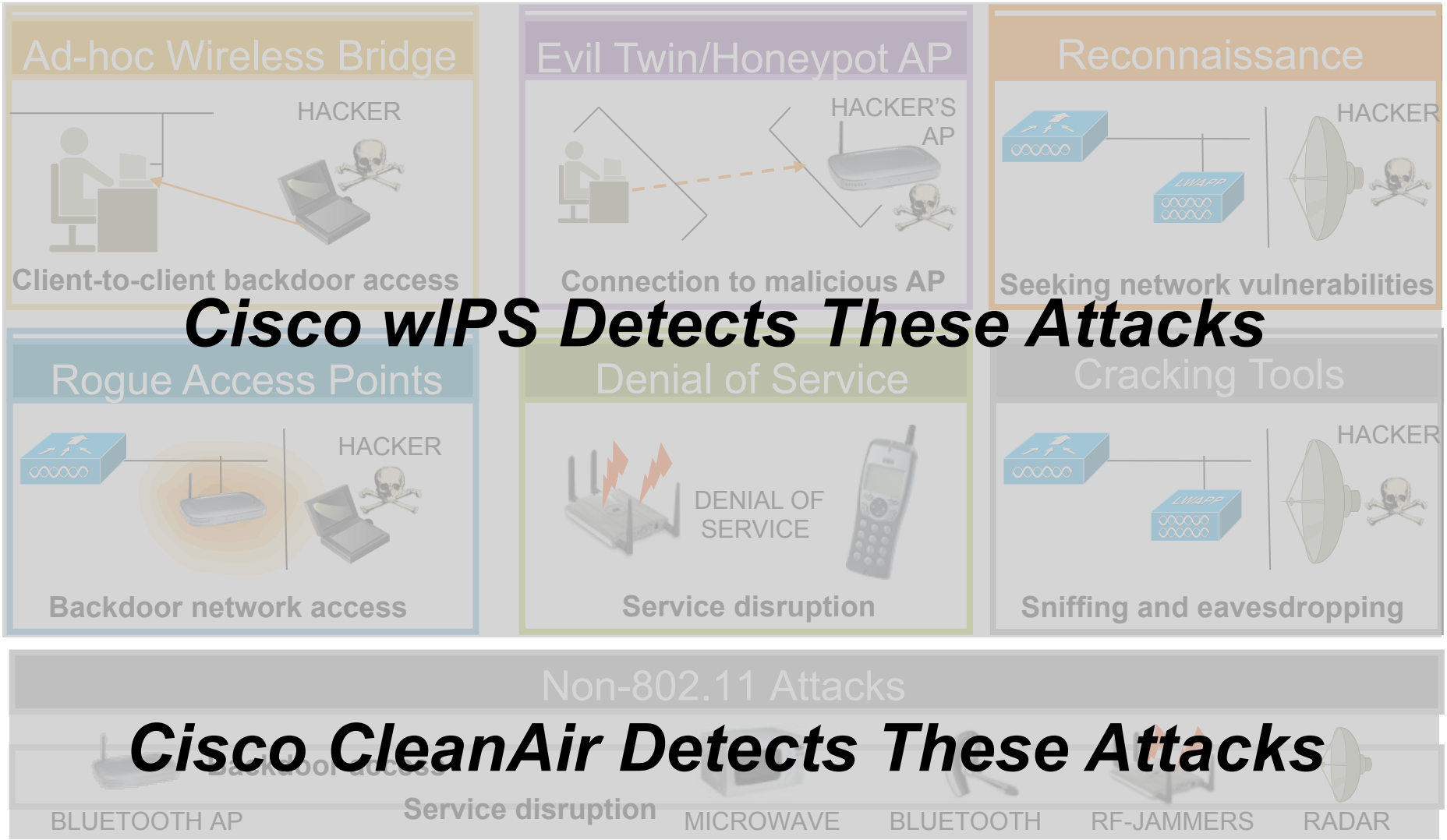
- Insert a signature (Message Integrity Code/MIC) into the management frames
- Clients and APs use MIC to validate authenticity of management frame
- APs can instantly identify rogue/ exploited management frames



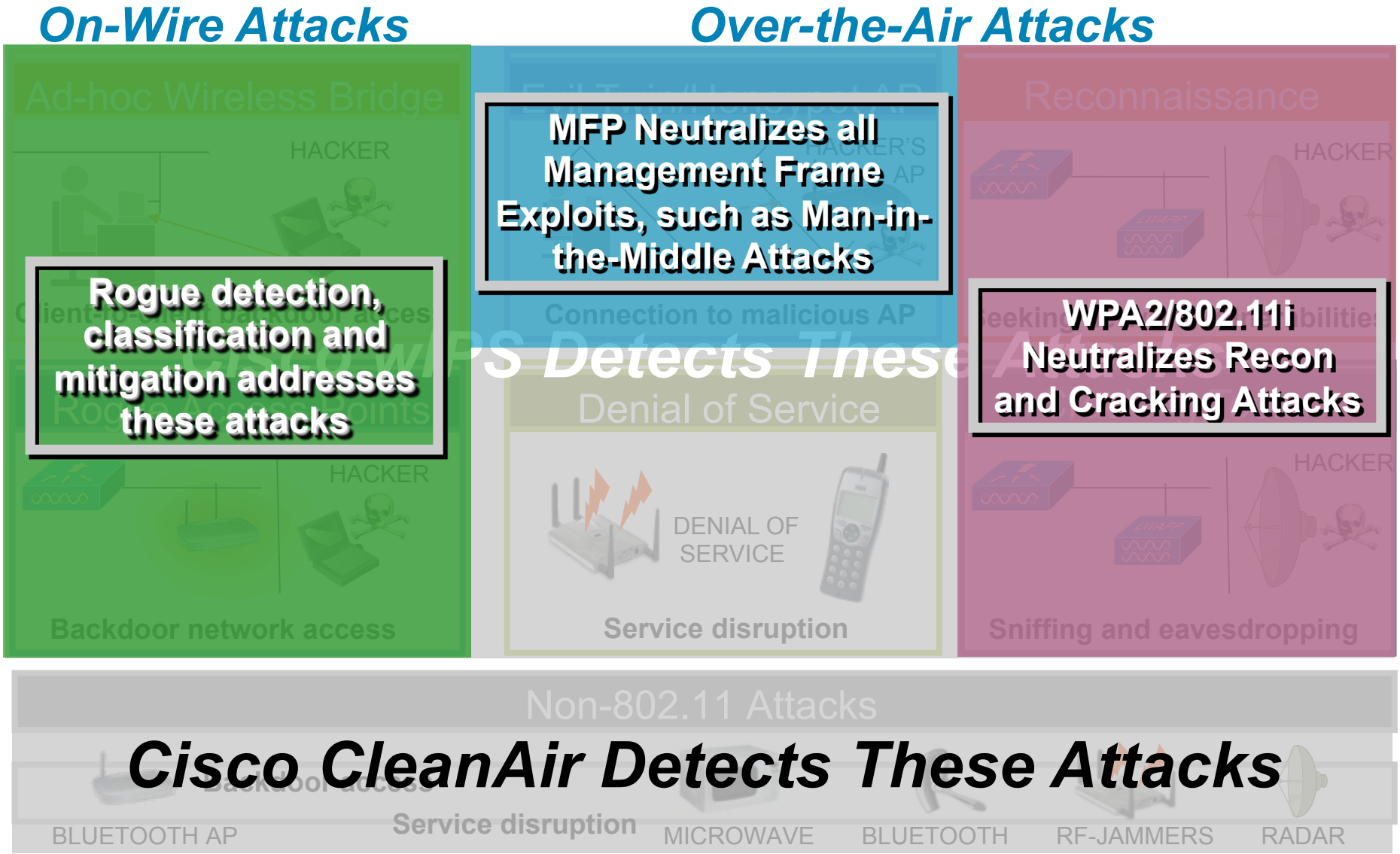
WLAN Security

Vulnerabilities and Threats

On-Wire Attacks ***Over-the-Air Attacks***

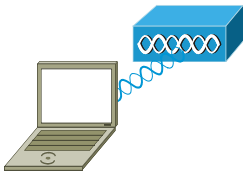


WLAN Security
Vulnerabilities and Threats



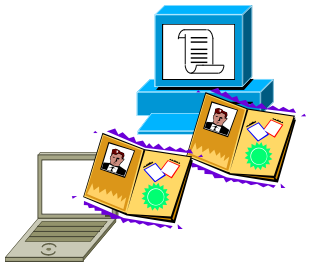
Strong Authentication and Encryption

802.11 Security Fundamentals: Setting up a secure 802.11 link



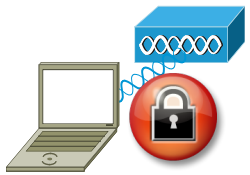
Authentication

- Enforce strong, mutual authentication of client & server
- Recommendation is 802.1X/EAP
- 802.1X blocks user access until authentication successful



Association

- Establish a virtual port for the link



Encryption

- Enforce strong encryption to provide data privacy over the 802.11 link
  - Recommendation is AES (WPA2) or TKIP (WPA)

Secure or open SSID?

Secure SSID

Open SSID

A secure SSID cannot fall back to open.

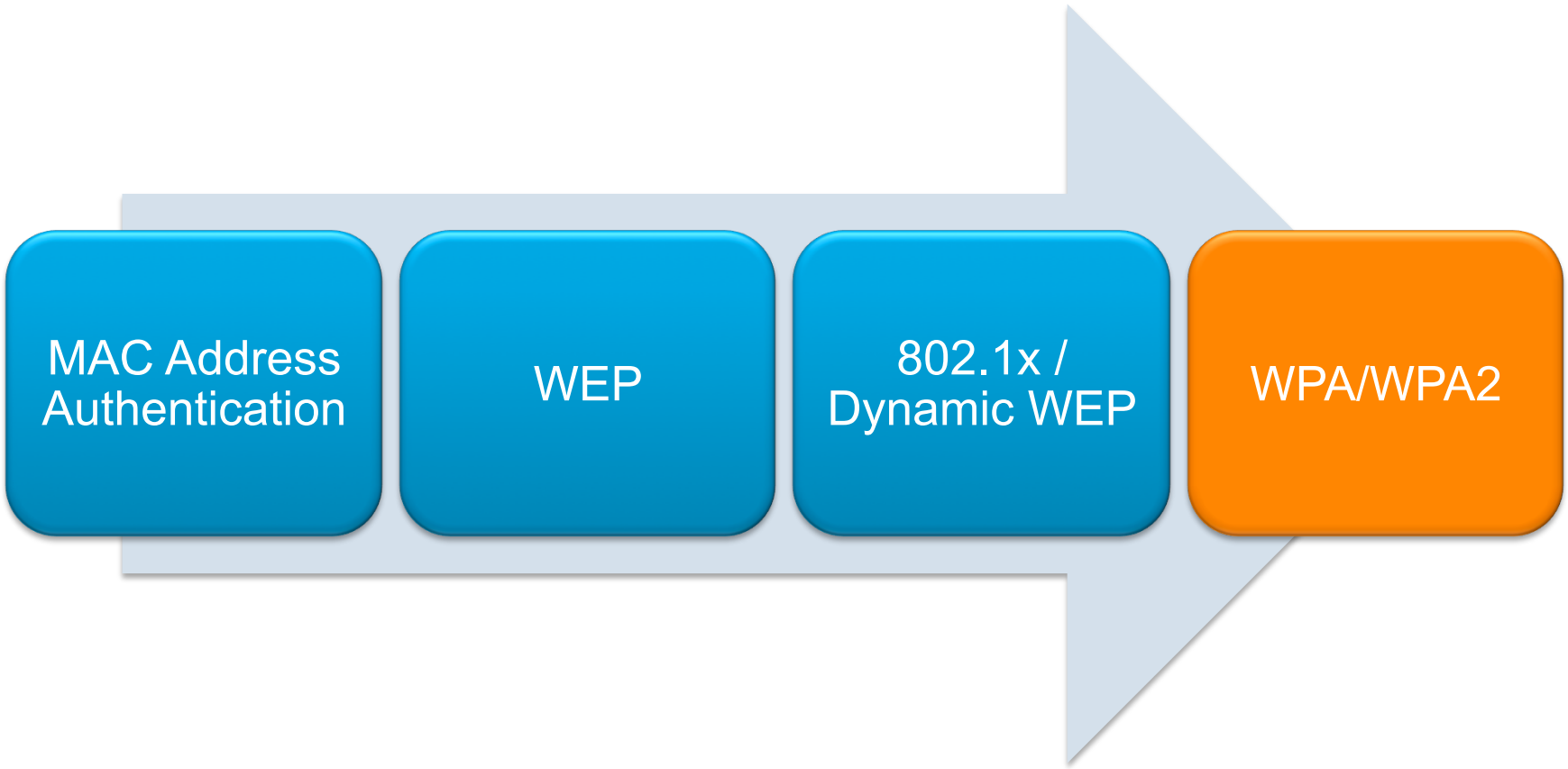
- Example: users not supporting 802.1X cannot fall back to web portal authentication on the same SSID as corporate users.

Pre-shared keys (PSK) and keys derived from 802.1X cannot co-exist on a secure SSID.

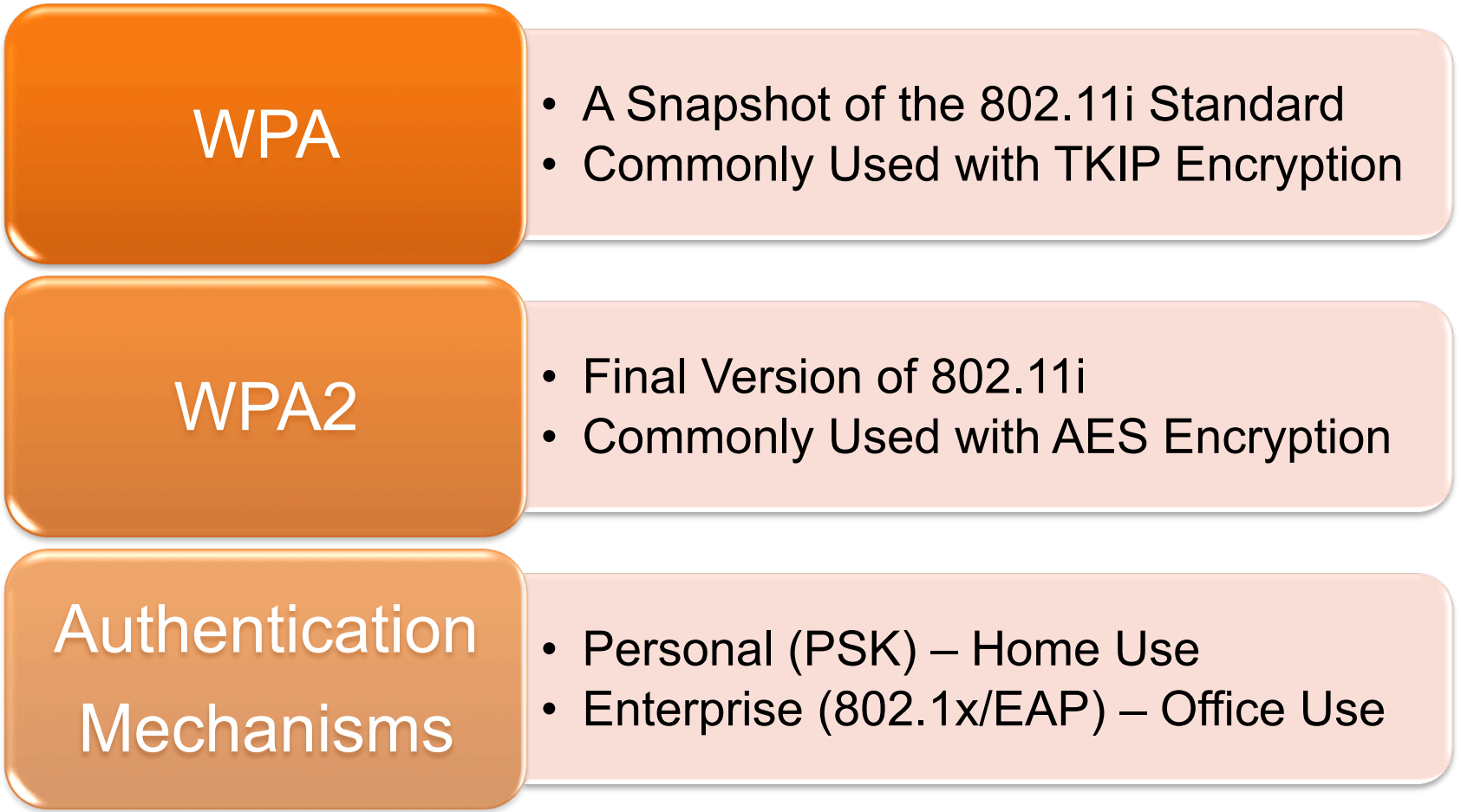
On both types of SSIDs you can combine multiple identity services if needed.

- Examples: guest users going through posture assessment, employees going through MDM, employees going through web portal after device authentication, etc.

Authentication Evolution



WPA/WPA2 Breakdown



Authentication: Open

1- Client sends probe request. [RF-Packet]

2- Access points (A/B) send probe response. Client evaluates access point response, selects best access point. [RF-Packet]

3- Client sends authentication request to selected access point (A). [RF-Packet]

4- Access point (A) confirms authentication and registers client. [RF-Packet]

5- Client sends association request to selected access point (A). [RF-Packet]

6- Access point (A) confirms association and registers client. [RF-Packet]

Authentication: PSK (WEP)

Step 1-3 are the same as with open authentication

4- Access point (A) sends authentication response containing the unencrypted challenge text. [RF-Packet]

5- Client encrypts the challenge text using one of its WEP keys and sends it to access point (A). [RF-Packet]

6- Access point (A) compares the encrypted challenge text with its copy of the encrypted challenge text. If the text is the same, access point (A) will allow the client onto the WLAN. [RF-Packet]

Authentication: PSK (WEP) (Cont.)

- WLAN security protocol defined in the 802.11 specification:
  - Operates at Layer 2 and does not offer end-to-end security
- Uses key plus initialization vector:
  - Initialization vector is a random number generated through the WEP algorithm
  - Key and initialization vector are used in encryption of the data
- Three user-specified key lengths:
  - 40-bit key, combined with initialization vector to yield 64 bits
  - 104-bit key, combined with initialization vector to yield 128 bits
  - 128-bit key, combined with initialization vector to yield 152 bits
- Cisco wireless supports pre-shared key authentication:
  - Disabled by default

WEP Limitations

- No per-packet authentication or message integrity check
- Hackers can easily obtain challenge phrase and encrypted response:
  - Crack the WEP key
  - Correctly decrypt captured data traffic
- Weak encryption of data
- Repeating initialization vector can provide insight into cracking WEP key
- Each client and AP must be configured with matching WEP key
- Managing keys can be difficult in enterprise WLAN
- Less secure than using open Layer 2 association and then applying user authentication with dynamic encryption method

Wi-Fi Protected Access (WPA)

- WPA introduced in late 2003
- Pre-standard implementation of IEEE 802.11i WLAN security
- Addresses currently known security problems with WEP
- Allows software upgrade on already deployed 802.11 equipment to improve security
- Components of WPA
  - Authenticated key management using 802.1X: EAP authentication, and PSK authentication
  - Unicast and broadcast key management
  - Standardized TKIP per-packet keying and MIC protocol
  - Initialization vector space expansion: 48-bit initialization vectors
  - Migration mode—coexistence of WPA and non-WPA devices (optional implementation that is not required for WPA certification)

WPA Authentication Modes

Enterprise (802.1X Authentication)	Personal (PSK Authentication)
Authentication server required	Authentication server not required
RADIUS used for authentication and key distribution	Shared secret used for authentication
Centralized access control	Local access control
Encryption uses TKIP, AES optional	Encryption uses TKIP, AES optional

WPA2 and IEEE 802.11i

- 802.11i
  - Ratified in June 2004
  - Standardizes
    - 802.1X for authentication
    - AES to be used for encryption
    - Key management
- WPA2
  - Supplement to WPA ”version 1”, which uses TKIP encryption
  - Provides for AES encryption to be used
  - Third-party testing and certification for WLAN device compatibility

IEEE 802.11i and AES Encryption

Uses AES encryption in lieu of RC4 encryption

- Specific AES implementation used in 802.11i is called "AES Counter Mode with CBC-MAC authentication" (a.k.a. AES-CCMP)
- 128-bit, symmetric block cipher (versus RC4 stream cipher)
- AES cryptographically more robust than RC4 (and requires more computational power)
- AES is implemented in hardware

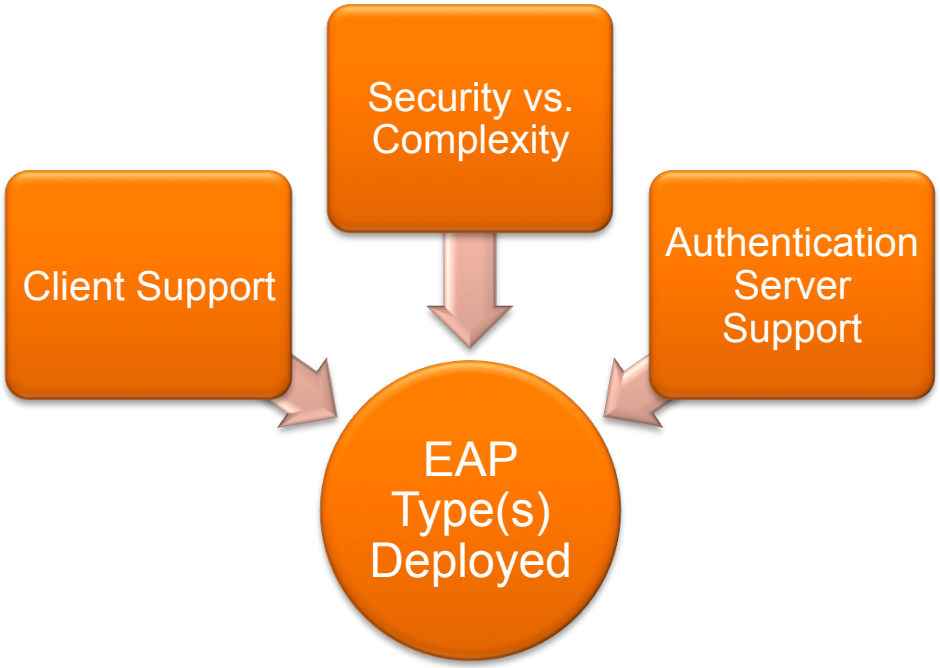
WPA/WPA2/802.11i Comparison

WPA	WPA2	802.11i
SOHO	Enterprise	Enterprise
802.1X authentication/PSK	802.1X authentication/PSK	802.1X authentication
128-bit RC4 w/ TKIP encryption cipher	128-bit AES encryption cipher	128-bit AES encryption cipher
Ad hoc not supported	Ad hoc not supported	Allows ad hoc
Test devices for compliance	Test devices for compliance	No test, specification

MAC Filtering

- Allows clients based on their MAC addresses
- The option is enabled on a per WLAN basis
- Controller checks for the presence of the client MAC address:
  - In a local database
  - If the address is not present, relays to a RADIUS server
- Local list contains 500 addresses, can be extended to 2000
  - The database is shared by local management users (including lobby ambassadors), net users (including guest users), MAC filter entries, and disabled clients.

Choosing an EAP Method



- Most clients such as Windows, Mac OSX, Apple iOS devices support EAP-TLS, PEAP (MS-CHAPv2).

  Additional supplicants can add more EAP types (Cisco AnyConnect).

- Certain EAP types (TLS) can be more difficult to deploy than others depending on device type.

Authentication Best Practices:

WPA2-Enterprise

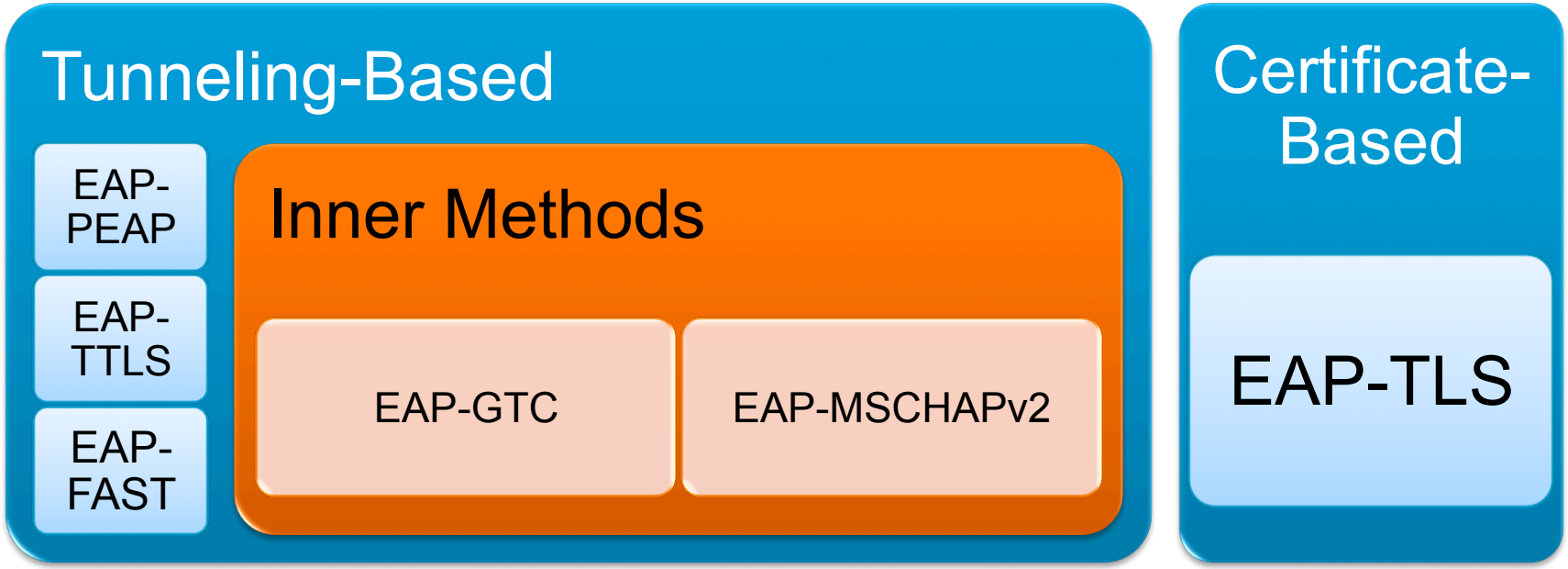
Strong Authentication

- Extensible Authentication Protocol (EAP)
- Outside Methods (Protective Tunnel):
  - PEAP
  - EAP-FAST
- Inside Methods (Authentication Credentials):
  - EAP-MSCHAPv2
  - EAP-GTC
  - EAP-TLS (Certificate Based)

Strong Encryption

- AES

EAP Authentication Types



- Tunnel-based - Common deployments use a tunneling protocol (EAP-PEAP) combined with an inner EAP type such as EAP-MSCHAPv2.

  This provides security for the inner EAP type which may be vulnerable by itself.

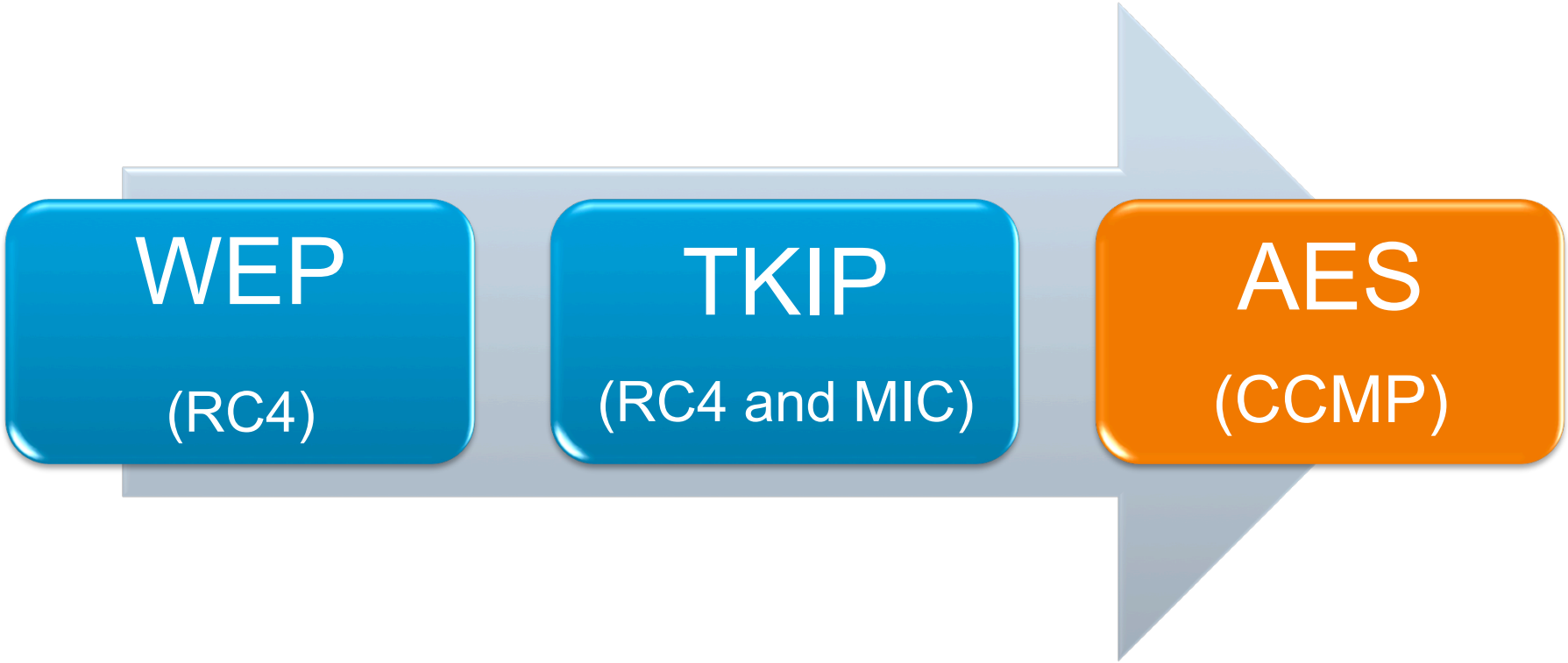
- Certificate-based – For more security EAP-TLS provides mutual authentication of both the server and client.

EAP Methods Comparison

	EAP-TLS	PEAP	EAP-FAST
Fast Secure Roaming (CCKM)	Yes	Yes	Yes
Local WLC Authentication	Yes	Yes	Yes
OTP (One Time Password) Support	No	Yes	Yes
Server Certificates	Yes	Yes	No
Client Certificates	Yes	No	No
PAC (Protected Access Credentials)*	No	No	Yes
Deployment Complexity	High	Medium	Low

* PACs can be provisioned anonymously for minimal complexity.

Encryption Evolution



Encryption Best Practices:
TKIP and AES

TKIP (Temporal Key Integrity Protocol)

- Use only for legacy clients without AES support
- Often a software update for WEP clients
- Can be run in conjunction with AES (mixed-mode)
- Is being discontinued by the WiFi Alliance for certification.

AES (Advanced Encryption Standard)

- Requires hardware support (~2005 chipsets or later)
- Achieves line-rate speeds
- Only encryption standard supported for 802.11n data rates

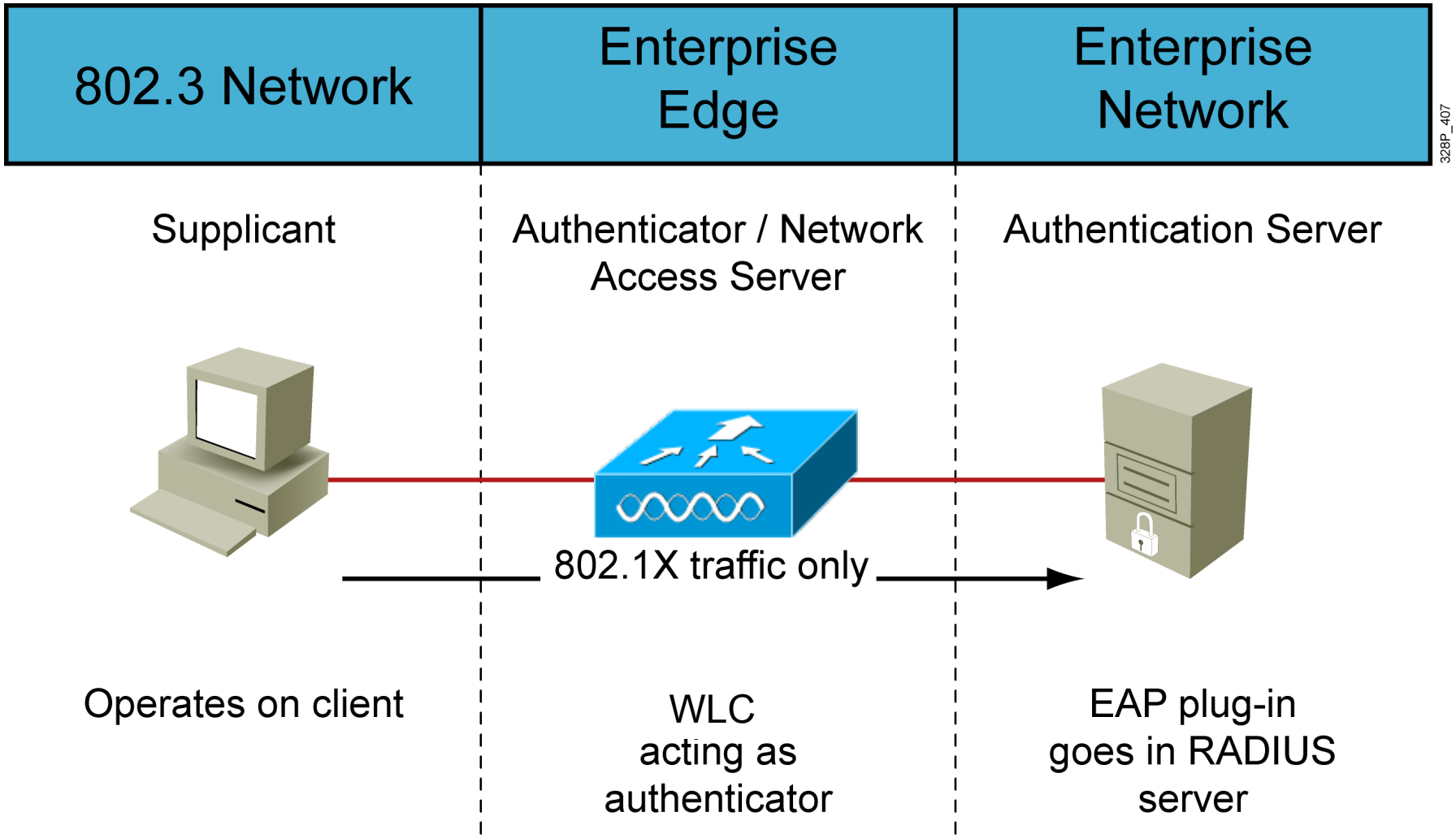
The TKIP Vulnerability

- Once thought safe, TKIP encryption is cracked: http://www.pcworld.com/businesscenter/article/153396/once_thought_safe_wpa_wifi_encryption_is_cracked.html
- Security researchers claim that they can crack the message integrity (MIC) key used in TKIP
- Recovery of MIC key facilitates packet forgeries, but only between AP and client
- Encryption key is *not* recovered, therefore data traffic cannot be read via this attack – this is not like the WEP crack of years back
- What is the Risk?

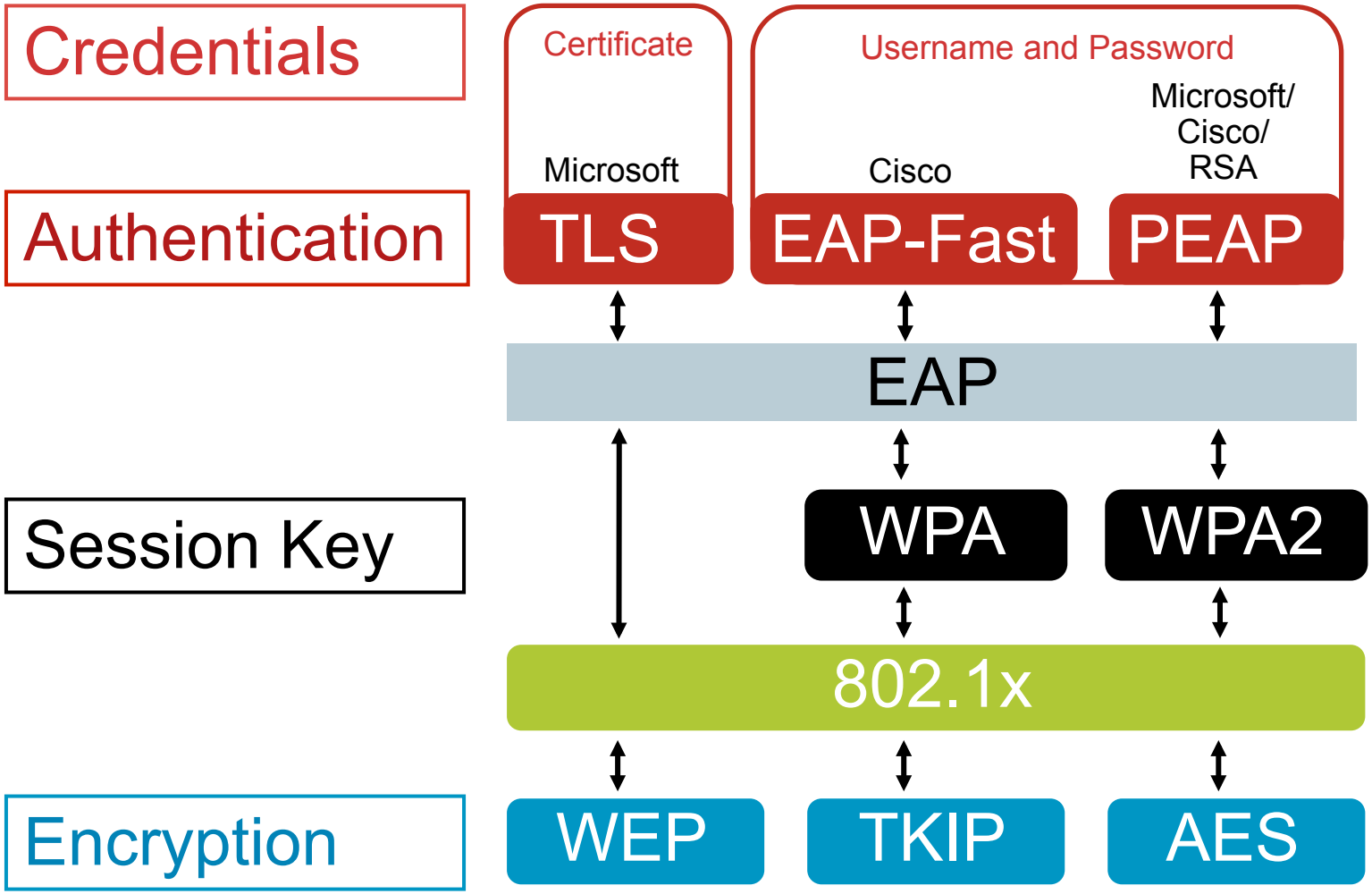
  Common traffic types, such as ARP and DNS, can be replayed to client for very limited duration… at most 7 times

Centralizing WLAN Authentication

802.1x


802.3 Network
Enterprise Edge
Enterprise Network
328P_407
Supplicant
Authenticator / Network Access Server
Authentication Server
802.1X traffic only
Operates on client
WLC acting as authenticator
EAP plug-in goes in RADIUS server

802.1x Architecture



802.1x Identity Information Types

fferent types for different mobility use cases:

Username/Password Combination
- User authentication (also Machine Auth for Windows)
- Active Directory/LDAP/RADIUS ID Stores
- EAP types: PEAP-MSCHAPv2, PEAP-GTC, EAP-FAST

Two-Factor Authentication
- Something you know, you have, you are
- Mostly for user authentication
- RSA SecurID and other token-based ID Systems
- EAP types: PEAP-GTC, EAP-FAST/EAP-GTC

Digital Certificates
- Signed/emitted by a public or private Certificate Authority
- Can be used for user and/or device authentication
- Microsoft AD Certificate Services, Entrust, Verisign, etc.
- EAP types: EAP-TLS, EAP-FAST

EAP

Extensible Authentication Protocol

PEAP

Protected EAP

GTC

Generic Token Card

FAST

Flexible Authentication via Secure Tunneling

TLS

Transport Layer Security

Local EAP

- The following EAP methods are supported with local EAP:
  - LEAP
  - EAP-FAST (both username and password with PAC and certificates)
  - EAP-TLS
  - PEAP
- MAC authentication is also supported in addition to the above methods
- Local EAP authentication can be used if the Cisco WLC fails to reach the configured RADIUS servers
- Supports local users or LDAP users
- Requires WLAN configuration

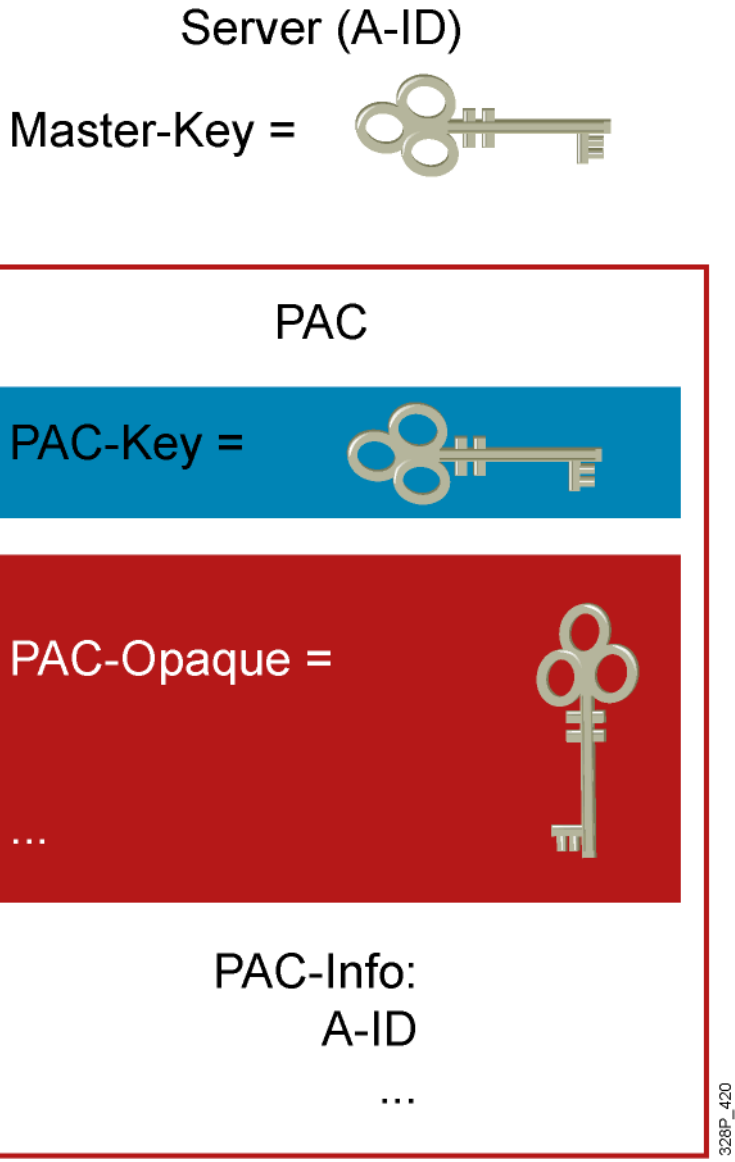
LEAP

- Cisco WLAN security solution
- User authentication via user ID and password
- Single login using Windows NT/2000 Active Directory
- Dynamic WEP keys and mutual authentication
  - Key integrity protocol/message integrity recommended
- Simplified deployment and administration
- Supports multiple operating systems
  - Windows, Mac OS, Windows CE, DOS, and Linux
- Strong password policy recommended

EAP-FAST

Considered in three phases:

- Protected Access Credentials (PAC) is generated in phase zero (Dynamic PAC provisioning)
  - Unique shared credential used to mutually authenticate client and server
  - Associated with a specific user-ID and an Authority ID
  - Removes the need for PKI
- A secure tunnel is established in phase one
- Client is authenticated via the secure tunnel in phase two



EAP-TLS

Client support

- Windows 2000, XP, Vista and Windows CE (natively supported)
- Linux, Mac AirPort Extreme
- Each client requires a user certificate

Infrastructure requirements

- EAP-TLS-supported RADIUS server
- RADIUS server requires a server certificate
- Certificate Authority server (PKI Infrastructure)

Certificate management

- Both client and RADIUS server certificates to be managed

PEAP

- Hybrid authentication method
  - Server side authentication with TLS
  - Client side authentication with EAP authentication types
    - EAP-GTC
    - EAP-MSCHAPv2
- Clients do not require certificates
- RADIUS server requires a server certificate
  - RADIUS server self-issuing certificate capability
  - Purchase a server certificate per-server from public PKI entity
  - Setup a simple PKI server to issue server certificates
- Allows for one-way authentication types to be used
  - One-time passwords
  - Proxy to LDAP, Unix, Microsoft NT and Active Directory, Kerberos

CCX—Providing Security Alternatives/ Tools/Cross-Platform Compatibility

More Than Just Standards

CCX v1

802.1x authentication

EAP-TLS and LEAP

Cisco pre-standard TKIP

Client rogue reporting

CCX v3

- **WPA2 compliance**
- **EAP-FAST**
- **CCKM with EAP-FAST**
- **AES encryption**

CCX v5

- **MFP**
- **Client policies/ reporting**

CCX v2

- **WPA compliance**
- **Fast roaming with CCKM**
- **PEAP**

CCX v4

- **CCKM with EAP-TLS, PEAP**
- **WIDS**
- **MBSSID**

EAP Protocols: Feature Support

	EAP-TLS	PEAP	LEAP	EAP-FAST
Single Sign-on	Yes	Yes	Yes	Yes
Login Scripts (MS DB)	Yes[1]	Yes[1]	Yes	Yes
Password Expiration (MS DB)	N/A	Yes	No	Yes
Client and OS Availability	Vista, XP, CE, and Others[2]	Vista, XP, CE, CCXv2 Clients[3], and Others[2]	Cisco/CCXv1 or Above Clients and Others[2]	Cisco/CCXv3 Clients[4] and Others[2]
MS DB Support	Yes	Yes	Yes	Yes
LDAP DB Support	Yes	Yes[5]	No	Yes
OTP Support	No	Yes[5]	No	Yes[6]

1 Windows OS supplicant requires machine authentication (machine accounts on Microsoft AD)
2 Greater operating system coverage is available from via CSSC and third party supplicants
3 PEAP/GTC is supported on CCXv2 clients and above
4 Cisco 350/CB20A clients support EAP-FAST on MSFT XP, 2000, and CE operating systems
EAP-FAST supported on CB21AG/PI21AG clients with ADU v2.0 and CCXv3 clients
5 Supported by PEAP/GTC only
6 Supported with 3rd party supplicant

EAP Protocols: Feature Support

	EAP-TLS	PEAP	LEAP	EAP-FAST
Off-Line Dictionary Attacks?	No	No	Yes[1]	No
Local Authentication	No	No	Yes	Yes
WPA Support	Yes	Yes	Yes	Yes
Application Specific Device (ASD) Support	No	No	Yes	Yes
Server Certificates?	Yes	Yes	No	No
Client Certificates?	Yes	No	No	No
Deployment Complexity	High	Medium	Low	Low
RADIUS Server Scalability Impact	High	High	Low	Low/Medium

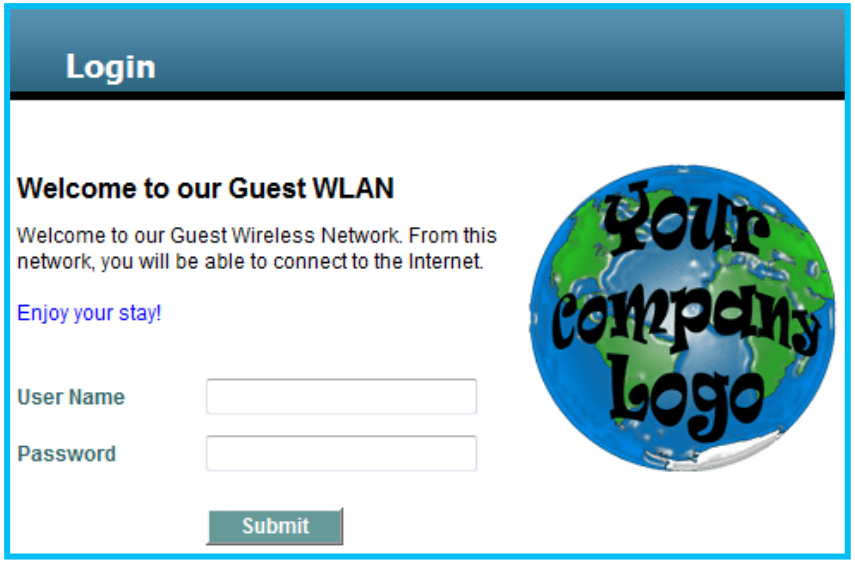
1 Strong password policy mitigates dictionary attacks; please refer to:
http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00801cc901.html

Web Authentication

- This allows users to authenticate through a web interface
- Clients who attempt to access the WLAN using HTTP are automatically directed to a login page:
  - Login page is customizable for logos and text
  - Maximum simultaneous authentication requests using web authentication is 21
  - Maximum number of local web authentication users is 2048 (default 512)
- This is generally used for guest access
- The Login page on the controller is now fully customizable

Web Authentication Page Configuration

Default Login Page



Customized Login Page (based on the previous slide's configurations and a custom logo uploaded to the controller)

Conclusion/Remarks/Resources

onclusion / Remarks

When Deploying Wireless Networks… Security should always be the primary concern.

Deploy WLAN Security with a MINIMUM security configuration of WPA2/PSK and AES Encryption.

Guest Wireless Access should adhere to the MINIMUM security configuration, but in the event that is not feasible, use WebAuth with a Splash Page and disclaimers and a Logir

Enterprise WLAN Deployments should ALWAYS separate Guest Access and Corporate Access with WVLANs and separate SSIDs.

WLANs are always being scanned… Be aware and monitor your RF environment.

esources

The Cisco Learning Network

https://learningnetwork.cisco.com/welcome

CCNA Wireless Study Materials

https://learningnetwork.cisco.com/community/certifications/wireless_ccna/wifund/study-material

CCNA Wireless Certification Exam Topics

https://learningnetwork.cisco.com/community/certifications/wireless_ccna/wifund/exam-topics

Thank you.

Cisco Networking Academy

Mind Wide Open