WiFi Security:
Deploying WPA/WPA2/802.1X and EAP in the Enterprise

Michael Disabato
Service Director
Network & Telecom Strategies
mdisabato@burtongroup.com

Diana Kelley
Senior Analyst
Security & Risk Management Strategies
dkelley@burtongroup.com
www.burtongroup.com

August 16/17, 2005

WiFi Security

Agenda

- Enterprise needs for WiFi Security
- Why WEP is not appropriate for Enterprise
- WPA/WPA2 – PSK/Enterprise
- 802.1X
- EAP-Types – pros/cons why to use and why
- Steps for deployment

Enterprise Needs for WiFi Security

Is WiFi Different from LAN?

- It’s still a (IEEE 802) network
- Layers 1 and 2 have changed
  - Now we’re *broadcasting* network traffic on a radio
  - On ISM (Industrial Scientific Medical) unlicensed bands
  - Jamming
- Layer 2 Attack Vectors
  - Management/control frames
  - Data payload
- Enterprise security needs are the same
  - Confidentiality, Integrity, Availability
  - How can these be met in the wireless world?

The Moving Target

New Vulnerabilities

- Connection sharing and Stolen Bandwidth
  - Wireless technologies built into laptops
  - Connection sharing enabled by default can allow access to enterprise network or contents of mobile device
- Data loss
  - No encryption means no protection
  - Sniffing via RFMON
  - The Pringles Effect (no special hardware needed for snooping)
- Public hotspots are not secure
  - Not even Wired Equivalent Privacy (WEP) is enabled
  - Systems are open to ad hoc connections

In order to ensure a positive “out of the box experience”, all connectivity is enabled, and all security is disabled

Why WEP is Not Appropriate for Enterprise

Because it’s “broken”

- Poor implementation for Enterprise requirements
  - Manual key management leads to static keys and reuse
  - All STAtions share the same key for encryption *and* authentication
  - Lose one key and compromise the whole network
- Misuse of RC4 encryption on a “lossy” network
  - Uses the Initialization Vector (IV) as part of they key, and when the IV wraps around, data can be easily recovered
- Other concerns
  - No forgery protection
  - No integrity check to detect packet tampering
  - No replay protection

Wired Equivalent Privacy (WEP)

Key Recovery Attacks

- Fluhrer-Mantin-Shamir (FMS) Attack: Paper published in August 2001, described weaknesses in key scheduling algorithm of RC4
- Stubblefield: Shortly after - proved this in practice
- Utilities (AirSnort, WEPCrack) have been developed that are able to recover static WEP keys
- Common features of these utilities:
  - Collection of data for attack can be done passively
  - Once the secret key is recovered all traffic can be read until the key is changed
  - Less than 20,000 packets encrypted with the same key are required for this to work for weak IVs
  - TCP ACK packets add to the traffic count and allow a known plain text attack

WPA – Better than WEP

WPA (Wi-Fi Protected Access)

- Certification managed by the Wi-Fi Alliance since October 2002
- “Stop-gap” solution based on emerging 802.11i IEEE Standards
  - Added TKIP (Temporal Key Integrity Protocol) to prevent key reuse and provide per-packet key mixing
    - Longer 48-bit Initialization Vector (IV)
    - Stronger derived encryption keys
    - Message Integrity Check (MIC)
    - Support for re-keying
  - *Optionally*: Can use 802.1X for dynamic key delivery to obviate WEP’s key management issues
    - And PSK cracking concerns
- Built for backward compatibility
  - In most cases required only a firmware upgrade or patch

WPA2 – Better than WEP ***and*** WPA

WPA2 WLAN components are certified by the WiFi Alliance

- Based on IEEE 802.11i
- Replaces RC4 with the Advanced Encryption Standard (AES)
  - Symmetric-key block cipher using 128-bit keys
  - Generates CCM Protocol (CCMP)
    - CCM = Counter mode with CBC-MAC
    - CBC = Cipher Block Chaining
    - MAC = Message Authentication Code
- Pre-Authentication and Key Caching Options
  - To reduce data latency and increase ease of AP to AP handoff without need for 802.1X reauthentication
- Hardware accelerated
  - Will require replacement of most access points and some NICs
- All access points and client radios must have firmware and drivers that support WPA2 in order to interoperate

Encryption Method Comparison

	WEP	WPA	WPA 2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-based	EAP-based

WPA and WPA both Come in Two Flavors

WPA/WPA2 – SOHO (a/k/a Personal)

- STAs and APs use the same pre-shared key (PSK)
  - Authenticates users
  - Generated from an ASCII passphrase
  - Becomes Pairwise Master Key (PMK) for TKIP key mixing function
  - A weak PSK is still easy to crack – make them 20 characters and higher
- Intended for Small Office and Home use

WPA/WPA2 – Enterprise

- Uses an authentication server to authenticate users
  - Supports dynamic (rather than pre-shared) delivery of master keys
- Intended for Enterprise use
- Must implement a full 802.1X infrastructure to support

WPA 2/802.11i

Should you upgrade to WPA2 with AES after WPA?

- An investment in new hardware (access points, NICs) may be needed
- Does your risk analysis indicate the extra protection is warranted
- WPA has not been broken (yet)
- Is there a compelling business reason to do so

However…

- WPA has not met the challenge of live traffic
- Network equipment will change over the next few years
- Eventually, RC4 will succumb to Moore’s Law

What is 802.1X?

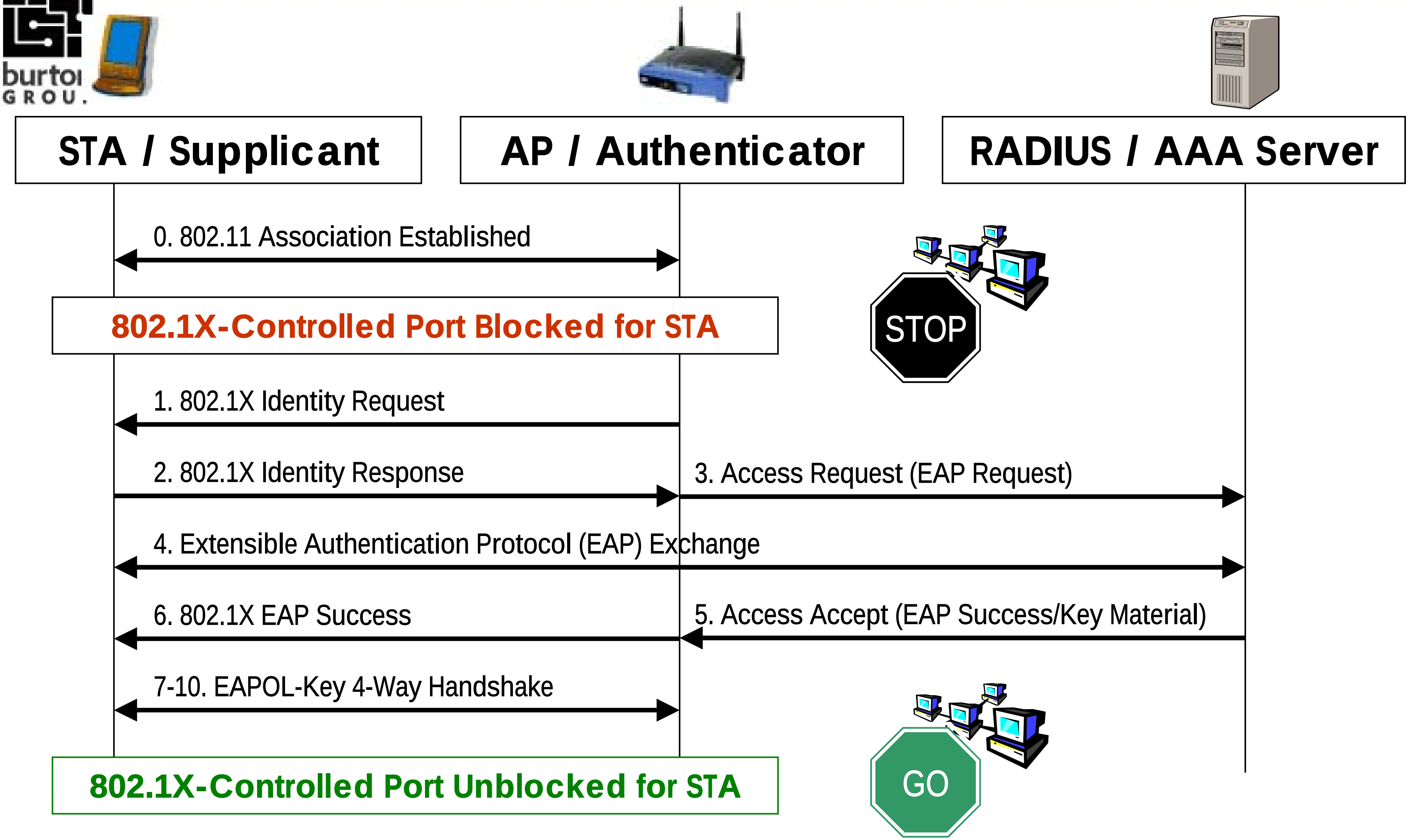
802.1X Port-based Access Control Framework

- IEEE Standard – data is blocked prior to successful authentication
  - http://www.ieee802.org/1/pages/802.1x.html
- Works on WLANs as well as LANs
- Provides STA and User Level Authentication
  - Type of authentication governed by EAP (Extensible Authentication Protocol) selected

Port Access Entities (PAEs)

- Supplicant = 802.1X Client software on STA
- Authenticator = ex: Access Point or Switch
- Authentication Server = AAA Server (e.g., RADIUS)

How 802.1X Works



STA / Supplicant

AP / Authenticator

RADIUS / AAA Server

0. 802.11 Association Established

802.1X-Controlled Port Blocked for STA

1. 802.1X Identity Request

2. 802.1X Identity Response

3. Access Request (EAP Request)

4. Extensible Authentication Protocol (EAP) Exchange

5. Access Accept (EAP Success/Key Material)

6. 802.1X EAP Success

7-10. EAPOL-Key 4-Way Handshake

802.1X-Controlled Port Unblocked for STA

Source: © Lisa Phifer and Diana Kelley, 2005

What EAP does for 802.1x

EAP (Extensible Authentication Protocol), RFC 2284

- EAP is pass-through carrier for authentication protocols
- Closes some of the known vulnerabilities in 802.1x
  - Some EAP types mitigate lack of mutual authentication between user and authentication server, for example
- Authentication security is dependent on EAP type selected

When used in WLAN, authentication information is typically passed from AP to back-end RADIUS server

- RADIUS server must support EAP or be chained/proxied to one that does

Don’t Panic!

The EAP Alphabet Soup – Navigating a solution

- There are many EAP types to chose from
- Selection of an EAP for 802.1X can seem overwhelming
- We’ll review the most commonly adopted EAPs
- There’s a “cheat sheet” at the end

Important questions that will help with navigation

- What are your company’s requirements for WLAN access?
- What current authentications methods are in use?

EAP Choices: EAP-TLS

EAP-TLS (Transport Layer Security)

- Windows XP has native supplicant
- Requires a certificate server (PKI) or purchased certificates
- Certificates required for all stations (IDs machine or user)

Considerations

- Considered to provide the strongest authentication of all EAPs
- Less vulnerable to MitM
- Certificates add administrative overhead
- May be difficult to support in heterogeneous environments such as those that support small-footprint/CPU stations or handhelds

EAP Choices: LEAP

Lightweight EAP, aka Cisco-EAP

- Cisco Proprietary
- Authentication is UID/Password
- Works with Cisco Aironet, Apple Airport, and other Wi-Fi cards that implement Cisco-Compatible Extensions (CCX)

Considerations

- May violate strong authentication policies for access
- LEAP is vulnerable to dictionary attack (e.g., ASLEAP)
  - Cisco is encouraging customers to move off of LEAP

EAP Choices: EAP-TTLS

EAP-TTLS (Tunneled Transport Layer Security)

- Provides mutual authentication - Server provides server certificate
- Supports multiple client authentication methods (PAP, CHAP, MS-CHAPv2, Generic Token Card)
- Authentication info protect via an encrypted tunnel

Considerations

- Protects the client ID information through the encrypted tunnel
- Can reuse existing user credentials

EAP Choices: PEAP

PEAP (Protected EAP)

- Originally backed as a single standard by Cisco and Microsoft
  - Phase 1: Server authenticated with certificate via TLS
  - Phase 2: Client authenticated with any EAP over TLS tunnel

Not a single standard any longer!

- Microsoft PEAPv0
  - EAP-TLS (certs/smartcards) or EAP-MS-CHAPv2 (hashed passwords) stored in NT Domains or ADS
- Cisco PEAPv1
  - EAP-GTC (generic token card) or OTPs with RSA and Secure Computing Tokens
  - Static passwords used with LDAP, NDS, other non-MS user databases

EAP Choices: EAP-FAST

EAP-FAST (Flexible Authentication via Secure Tunneling)

- Internet Draft in v.2 w/IETF 4/2005
  - http://www.ietf.org/internet-drafts/draft-cam-winget-eap-fast-02.txt
- Uses TLS to support tunneled user authentication
- Shared secrets speed subsequent re-authentication

Considerations

- Now available only from Cisco; industry support TBD
- Supports fast handoff for VoIP handsets using Cisco APs
- Supports Single Sign-On when used with Windows ADS

Which EAP is Right for Your Enterprise?

Some considerations:

- What type of authentication is required?
  - LEAP would violate a two-factor authentication policy
- What user databases are in the company?
  - Corporations with deployed PKI may prefer EAP-TLS
  - For MS-centric company consider TTLS or PEAP/EAP-MS-CHAPv2
- A proprietary EAP may lock enterprise into particular AP hardware
- If your company does not have a PKI already,
  is EAP-TLS a good enough reason to install one?
- You can use more than one EAP type if you want to – does it make sense?
- What about the migration path, what’s the best approach?

EAP Summary

EAP-Type	EAP-TLS	LEAP	EAP-TTLS	PEAP(S)	EAP-SIM	EAP-FAST
Mutual Auth	Yes	Yes	Yes	Yes	Yes	Yes
Certs Required	Server and Client	None	Server Only	Server Only	Server Derived	Server Optional
Key Delivery	Yes	Yes	Yes	Yes	Yes	Yes
Security	Highest	Low	High	High	Medium	Medium-High
Pros	Strongest security	Availability (CCX), DB reuse	Encrypted credentials, DB reuse	Encrypted credentials, Availability (MS, Cisco), DB reuse	Supported by phones	Encrypted credentials, DB reuse, fast roaming
Cons	Requires PKI for client certs	Cisco Proprietary, Dictionary Attack	Proprietary Clients	Multiple Versions	Authenticates the server with derived leys, currently best supported by phones and SIM devices	Draft status, Cisco-only today

Table Source: derived from © Lisa Phifer and Diana Kelley, 2005

Steps for Deployment - Recap

The cookbook

- Site survey/coverage plan
- Install WPA2 capable equipment
- Install RADIUS server
- Select EAP type
- Select and install supplicant
- Upgrade client firmware and enable WPA2

Whence 802.1X?

Business Benefits of 802.1X

- Blocking users at the port
- Dynamic master key distribution for WLAN protection

Assessing corporate readiness

- Is 802.1X being deployed on the LAN?
  - Can the investment be leveraged?
- What devices require 802.1X access?
  - PDAs?
  - Printers?
  - Surveillance Cameras?
  - VoIP phones?
- Is there a VPN solution already in place?
  - Simply treating wireless access as remote access from an untrusted network may be a viable solution

Recommendations

General

- Conduct a risk assessment for all information that travels over mobile connections or resides on mobile devices
- Evaluate the cost of implementing security against the cost to the enterprise of a security or privacy breach, loss of confidence, bad press, etc.
- Determine if WPA2 is viable or if other ways of implementing WLAN security should be used

References

Network and Telecom Strategies

- Securing WLANs: Good, Better, AES
- Managing and Securing the Mobile Device

Security and Risk Management Strategies

- Handheld Device Security
- Impact of the Disappearing Perimeter: Strategies for Securing Internal Networks and Endpoints
- Technical Position: Perimeters and Zones