Wireless LAN Security

Indira Mohandoss

Monica González
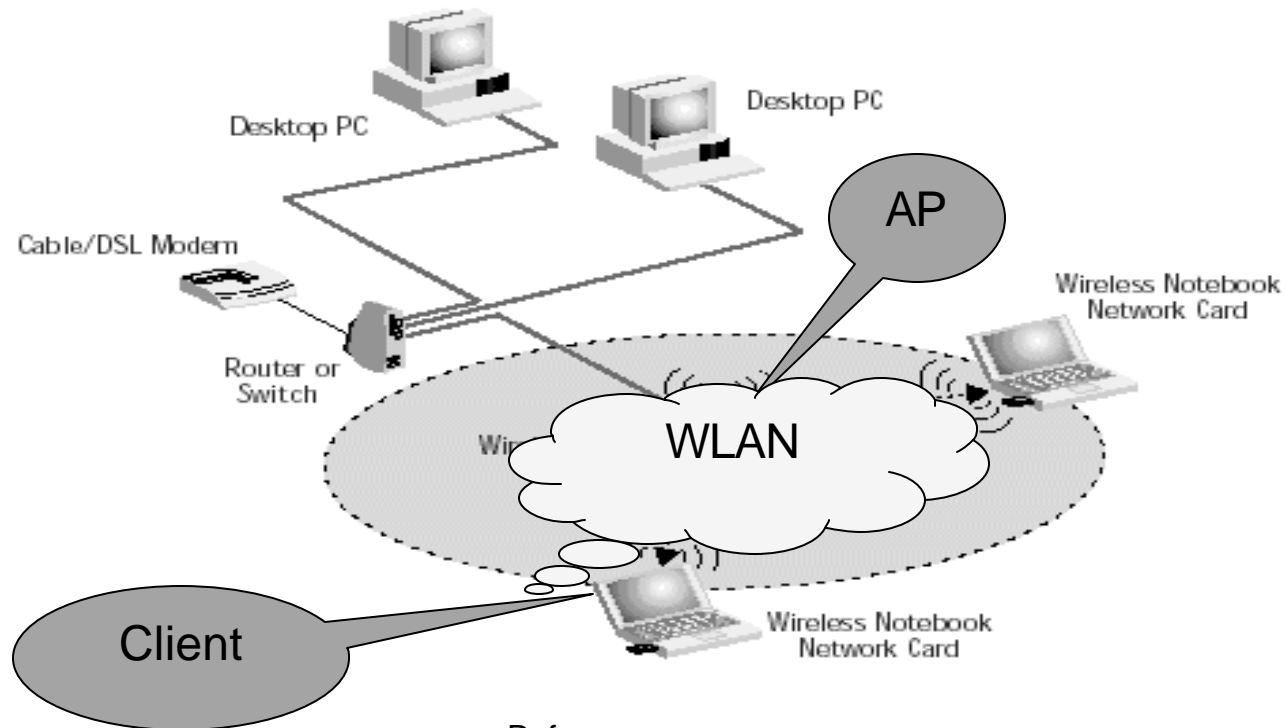
Outline

- Introduction
- Benefits of WLAN
- Common threats
- Methods to secure WLANs
- Comparison of methods
- Conclusion

What is a WLAN?

- Also, referred to as LAWN is a closely grouped system of devices
- Communicate through radio waves instead of wires

Reference :
http://www.windowsnetworking.com/arti
cles_tutorials/wlan.html

Wireless Networks - Types

☐ Three types of wireless network:

    ☐ Adhoc network (IBSS)

- Station within communication range via wireless medium
- Spontaneous, Limited time, small area

    ☐ Basic Infrastructure Network (BSS)

- Controlled by a single coordinator called Access Point(AP)

Wireless Networks - Types

☐ Infrastructure Network (ESS)

- Number of BSS connected together through other networking technology

- Stations roam transparently within the ESS

- No standard yet for roaming stations

Benefits of Wireless LANs

- Core business benefits
  - Increased flexibility and mobility of workforce
    - Study showed that WLANs increased availability of corporate network by 70 minutes a day, enhancing productivity by as much as 22%
  - Online information is always available
    - Improves productivity & quality of meetings
  - Integration of new devices – PDAs, tablets

Benefits of Wireless LANs

- Operational benefits
  - Lower capital and operational costs
  - Network can be easily scaled
  - Capital does not need to be tied into building infrastructure
  - Networks can be provisioned at locations that are not cabled for networks, or where wired networks would be impractical

WLAN Security – An oxymoron?

- Corporations hesitant to implement WLAN
- Efforts to improve security have historically had problems:
  - Introduce new vulnerabilities
  - Require expensive proprietary hardware
  - Layer on complex technology, such as VPN, rather than solve the root problem

Threats to WLAN Security

- Eavesdropping
- Interception and modification of transmitted data
- Spoofing
- Denial of service (DOS)
- Free-loading (Resource Theft)
  - NetStumbler, Wardriving
- Accidental threats
- Rogue WLANs

WLAN standards

- ## 802.11 – first WLAN standard
  - Creates a standardized approach for wireless communication
    - 802.11b – 11Mbps, 2.4 GHz ISM
    - 802.11a – 54 Mbps, 5 GHz UNII
    - 802.11g – 54 Mbps , 2.4 GHz ISM
    - 802.1x – port-based network control
    - 802.11i – 802.1x with EAP

Methods for Securing WLAN

- Do not deploy WLAN technology
- Use 802.11 static WEP security
- Use VPN
- Use IPSec
- Use 802.1X authentication and data encryption

No WLAN

- Excludes benefits of WLANs
- Unauthorized WLANs expose organization to security threats
- Must take active rather than passive approach
  - Clear policy against use of wireless equipment and consequences for violations
  - Scanning equipment to detected unauthorized wireless equipment on your network

Static WEP(Basic 802.11 security)

- Same key is used to control access to the network and encrypt wireless traffic
- Key is static, easy to discover
- MAC filtering may improve security, but has poor scalability
  - Enterprise wireless gateways – centralized security
  - MAC spoofing – still a threat

VPN

- Ideally suited to secure traffic passing over hostile networks
- Not designed to secure traffic on internal networks
- Advantages
    - ☐ Uses software encryption, so algorithms can be easily updated or changed
    - ☐ Independent of WLAN hardware
    - ☐ Protects against traffic analysis

VPN

- **Disadvantages**
  - ☐ Data is protected, but WLAN itself is not
  - ☐ Lacks transparency, requires manual connection
  - ☐ Prone to disconnections when clients roam between access points
  - ☐ VPN servers can become a bottleneck
  - ☐ Idle, logged-off computer cannot be remotely managed
  - ☐ Roaming profiles, logon scripts may not work

IPsec – Tunnel Mode

- A form of VPN, works by encrypting a whole IP packet and encapsulating it within a protected IPsec packet

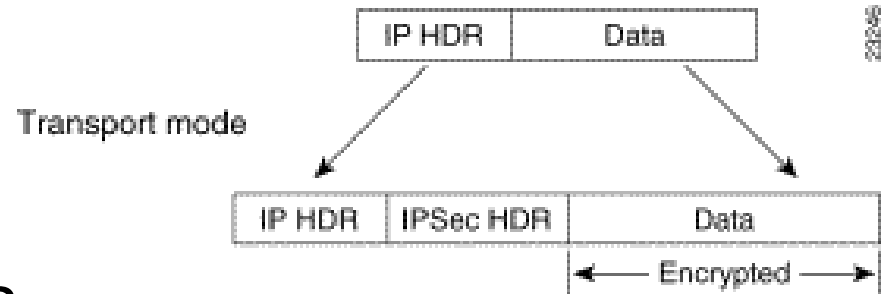- Advantages and disadvantages similar to VPN

IP HDR	Data

Tunnel mode

← — Encrypted — →

New IP HDR	IPSec HDR	IP HDR	Data

Image reference:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/ipsec/conipsec.htm#60564

IPsec – Transport Mode

- Only payload is encrypted, original headers left intact

- Advantages
  - Transparent to users
  - Independent of WLAN hardware
  - Use of cryptographic algorithms not constrained by WLAN hardware

Image reference:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/ipsec/conipsec.htm#60564

IPsec – Transport Mode

- **Disadvantages**
  - ☐ Computer-level authentication only, no user-level authentication
  - ☐ Some devices may not be IPsec-capable
  - ☐ Not fully transparent to network devices such as firewalls
  - ☐ Cannot support broadcast or multicast traffic
  - ☐ Data is protected, but WLAN itself is not
  - ☐ Encryption and decryption load the CPU
    - Processing can be offloaded to specialized network cards, but not usually installed by default

802.1X Authentication and Data Encryption

- Elements of WLAN security
  - Authenticate the person or device attempting to connect to the WLAN
  - Authorize the person or device to use the WLAN
  - Protect the data transmitted on the network

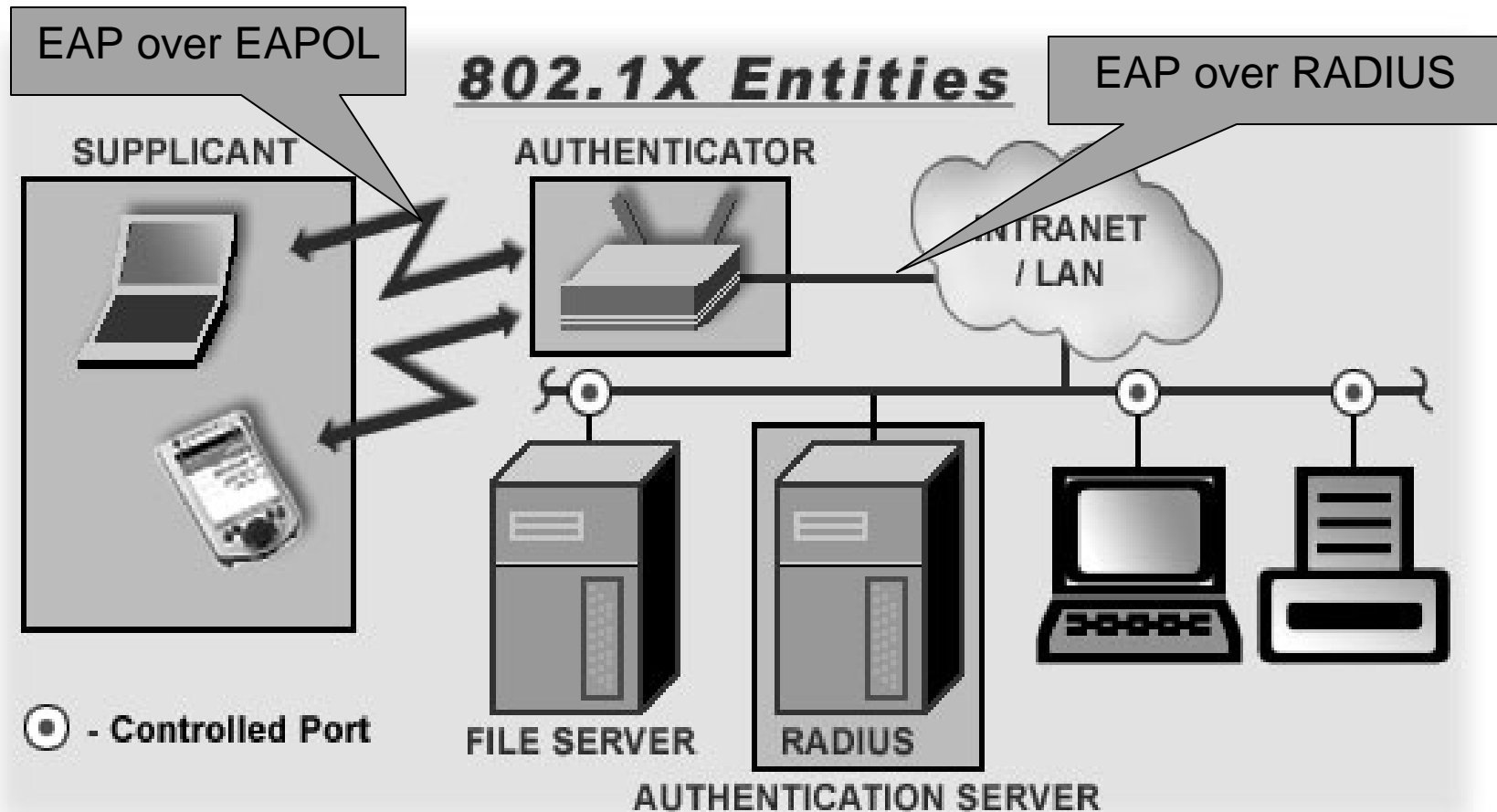# 802.1X Authentication and Data Encryption

- Authentication and authorization
  - 802.1X involves:
    - Network user
    - Network access device (or gateway)
    - RADIUS server (Remote Authentication Dial-In User Service)
  - EAP (Extensive Authentication Protocol) used to converse between client and RADIUS server via access point

Authentication using RADIUS

EAP over EAPOL

EAP over RADIUS

802.1X Entities

SUPPLICANT

AUTHENTICATOR

INTRANET / LAN

⊙ - Controlled Port

FILE SERVER

RADIUS

AUTHENTICATION SERVER

RADIUS conversation

- **RADIUS Protocol**

  The RADIUS protocol standard is described in RFC 2058. A RADIUS conversation goes like this:
  - Laptop: Hello, access point? Let me in!
  - Access point: Hello, Radius? This guy wants to get in.
  - Radius: Ask him his name.
  - Access point: Laptop, what's your name?
  - Laptop: Mary.
  - Access point: Radius, it's a girl. She says she's Mary.
  - Radius: Ask her for her password.
  - Access point: Mary, what's your password?
  - Laptop: abc123.
  - Access point: Radius, Mary says abc123.
  - Radius: Hmm, let me check... Ok, let her in.
  - Access point: Ok Mary, you're cool.
  - Laptop: Thanks, access point. Now let's see, gimme my e-mail, a buncha websites, a telnet session, some instant messaging...

802.1X Authentication and Data Encryption

□ EAP methods in use for WLANs are:

- EAP-TLS

- Protected EAP (PEAP)

- Tunneled TLS (TTLS)

- Lightweight EAP (LEAP)

EAP-TLS

- Uses public key certificates for mutual authentication between the client and the RADIUS server

- Establishes encrypted TLS session between the two

PEAP

- Two-stage authentication method

- First, TLS session is established and server authenticates itself to client with its certificate

- Second, client authenticates itself to server using any other EAP method within protection of TLS session

- Less cost and complexity because only one certificate is required

- Microsoft Windows has built-in support for PEAP

TTLS

- Two-stage authentication, similar to PEAP
- Can tunnel traditional 'weak' PPP authentication methods, such as CHAP, MS-CHAP, or any EAP methods
- Not supported by Microsoft or Cisco

LEAP

- Proprietary EAP method developed by Cisco

- Uses passwords to authenticate clients

- Only works with hardware and software from Cisco

- Can only authenticate the user, not the computer

802.1X Authentication and Data Encryption

- **Data protection**
  - EAP generates an encryption key that is unique to each client
  - RADIUS sever regularly forces generation of new encryption keys
  - These measures allow WEP encryption algorithms to be used more safely (dynamic WEP)

Dynamic WEP

- WEP with 802.1X dynamic re-keying - Problems
  - Uses separate static key for broadcasts which is not regularly renewed
  - Network frames have poor integrity protection
  - Increased transmission speeds and improvements in computational power and cryptanalysis will require keys to be renewed more often

802.11i (Robust Security Network)

- **Adds several features to 802.1x**
  - ☐ Key distribution framework
  - ☐ Use of AES encryption allowed
    - Stronger encryption algorithm than DES because of longer length keys
  - ☐ Backwards compatible with RC4

WPA

- WPA (Wi-Fi Protected Access) contains a subset of features of 802.11i (RSN)
- Two modes:
  - WPA – uses 802.1X and RADIUS for authentication
  - WPA-PSK – uses pre-shared key for authentication
- Can be implemented with simple firmware upgrade

WPA

- WPA eliminates known vulnerabilities of WEP
  - Uses unique encryption key for each packet
  - Uses much longer initialization vector
  - Adds a signed message integrity check value that cannot be spoofed or tampered with
  - Incorporates an encrypted frame counter to prevent replay attacks

WPA - PSK

- Used in SOHO environments
- Allows the use of a Pre-Shared key
  - □ Used as Authentication credential
  - □ Strong enough to thwart simple password-guessing attacks
- Individual encryption keys for each wireless client
  - □ Access using PSK; receive unique encryption key to protect data

Comparison of Security Methods

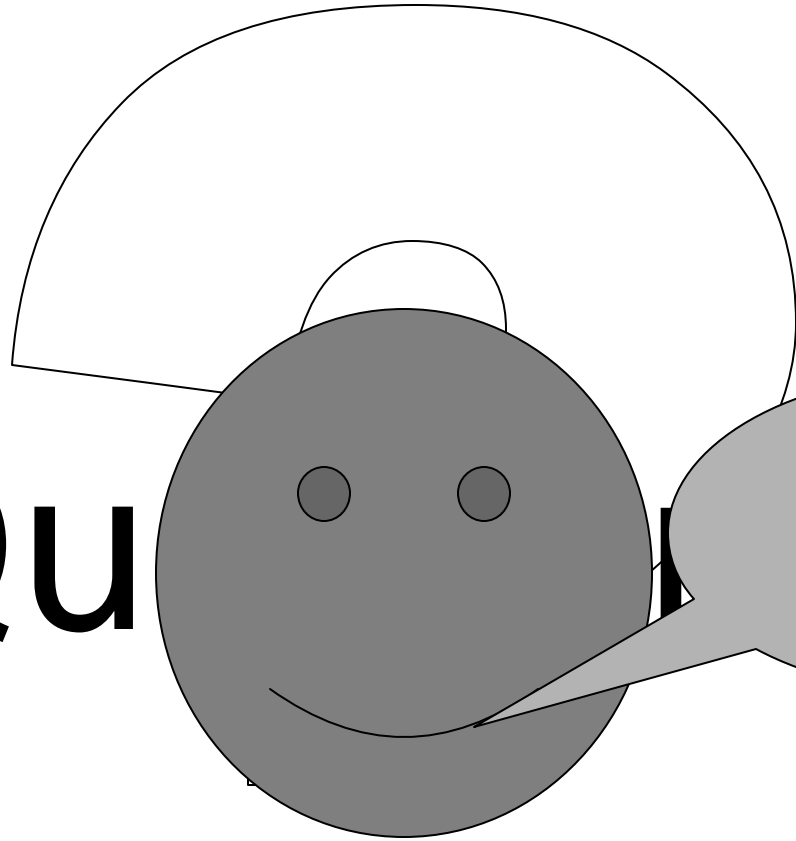| Feature	802.1X	Static WEP	VPN	IPsec
Strong authentication	Yes	No	Yes, but not VPNs using shared key authentication	Yes, if using certificate or Kerberos authentication
Strong data encryption	Yes	No	Yes	Yes
Transparent connection and reconnection to WLAN	Yes	Yes	No	Yes
User authentication	Yes	No	Yes	Yes
Computer authentication	Yes	Yes	No	Yes
Broadcast and multicast traffic protected	Yes	Yes	Yes	No
Additional network devices required	RADIUS servers	No	VPN servers, RADIUS servers	No
Secures access to the WLAN itself	Yes	Yes	No	No

Future of WLAN Security

- 802.11i recently ratified, not yet widely deployed
  - ☐ Possible vulnerabilities have not been identified
- Alternate authentication methods for WLAN
  - ☐ Smart/Challenge cards
  - ☐ Kerberos
  - ☐ SIM
- Proper integration of standard, Several layers of defense

References

- Microsoft Solutions for Security: Choosing a Strategy for Wireless LAN Security, 2004

- Joon S. Park and Derrick Dicoi, WLAN Security: Current and Future, IEEE Internet Computing, 2003

- http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_60/ipsec/conipsec.htm#60564

- Matthew Gast, Wireless LAN Security: A Short History, 2002

- John Vollbrecht, Wireless LAN Access Control and Authentication, 2002

- Sandra Kay Miller, Facing the Challenge of Wireless Security, Computer, July 2001

- Frank Bulk, Learn the Basics of WPA2 Wi-Fi Security, Information Week, January 2006

- RFC for EAP http://www.ietf.org/rfc/rfc3748.txt

Questions?

Thank you!