

Wireless LAN Security

ผศ. ดร. อนันต์ พลเพิ่ม

Asst. Prof. Anan Phonphoem, Ph.D.

anan@cpe.ku.ac.th

<http://www.cpe.ku.ac.th/~anan>

Computer Engineering Department

Kasetsart University, Bangkok, Thailand

1



Agenda

- Security Characteristics
- WLAN Security
- Security Threats
- WLAN security management

2



TCP/IP Protocol Suite (Internet Model)

- 5 **Applications** User service and interface
- 4 **Transport** Process delivery + Error (TCP/UDP)
Reliable end-to-end (whole message)
- 3 **Network** Move packets from source to destination
Packet end-to-end (across network)
- 2 **Data Link** Provide frames
Node-to-node (same network segment)
- 1 **Physical** Transmission bit streams
(mechanical and electrical spec)

3



Security for TCP/IP

- 5 **Applications** Application layer security protocols
Secure Http (Https)
- 4 **Transport** VPN + Secure Socket Layer (SSL),
Transport Layer Security (TLS)
- 3 **Network** IPsec + Layer 2 Tunnel
(Changeable fields, e.g. TTL)
- 2 **Data Link** Encryption for set of MACs
(Not all the frame, e.g. header)
- 1 **Physical** Encryption all bit streams
(Point-to-point, banking)

4



Car Security Story

- Break/gear/Steering Wheel Lock
 - Avoid cars that have lock
 - Break windows + tools (hammer/screw driver)
 - Alarm system implemented
 - Scan the keychain frequency
 - Cut off the alarm signal
- Try to bypass/disable, not to break the encryption

5



Agenda

- Security Characteristics
- **WLAN Security**
- Security Threats
- WLAN security management

6



WLAN Security

- Non-Cryptographic Security Scheme
- Cryptographic Security Scheme

7



Non-Cryptographic Security Scheme

- Closed WLAN
 - Omit SSID in the Beacon MMPDU frame
 - Easy to eavesdrop and know
- MAC Filtering
 - Access list of MAC
 - Spoof MAC
- Screen out “baby” or “Casual” attacker

8



Cryptographic Security Scheme

- User Authentication
- Message Authentication/Verification
- Message Encryption

9



User Authentication

- Prove the user’s identity
- “Key” for authentication
 - Correct key → valid user ??
 - Spoof attacker has the key
- Need cryptographic

10



Message Authentication/Verification

- Encrypt the message before send
- A hash function (Integrity Check Value, ICV)
 - Arbitrary input → fixed-length output (hash)
 - Cyclic Redundancy Check (CRC)
 - Message Digest 5 (MD-5)
 - Secure Hash Algo. No.1 (SHA-1) [160 bits]
 - SHA-256, 384, 512 [bits]
- Header frame/data frame/key
- Verifying that message is not modified

11

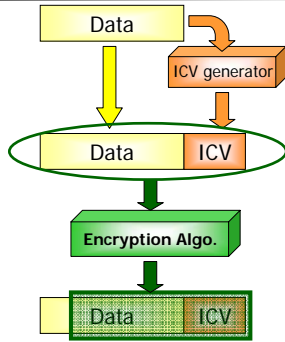


Message Encryption

- Encapsulation
- Cryptographic encryption algorithm
 - Block-oriented cipher
 - Data Encryption Standard (DES) / Triple DES
 - Advanced Encryption Standard (AES)
 - RC-2, RC-5, RC-6, etc.
 - Stream-oriented cipher
 - RC-4
- Key length

12

Message Encapsulation



13

Built-in WLAN Security

- Wired Equivalent Privacy (WEP)
 - Provides encryption based on RC-4 cipher
- 802.1x
 - Provides authentication using Extensible Authentication Protocol (EAP)
- Wi-Fi Protected Access (WPA)
 - Uses dynamic keys and advanced encryption
- 802.11i
 - Advanced encryption and authentication

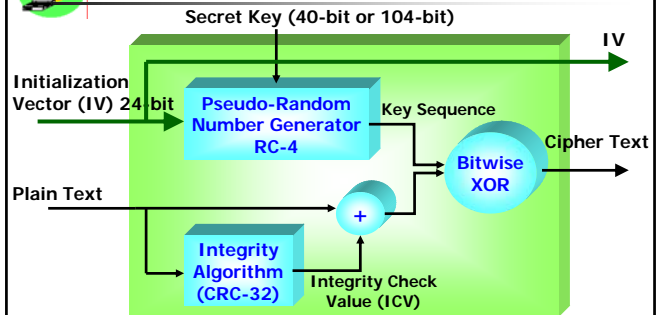
14

WEP

- Wired Equivalent Privacy (WEP)
 - Goal: protecting air traffic as wired traffic
 - Strong enough for casual eavesdropping
 - WEP deploys RC4 (RSA Security)
- Provides 64-128 bit encryption
- Privacy
 - Controlling personal info. not too widely spread out
- Confidentiality
 - Preventing others to understand our communications

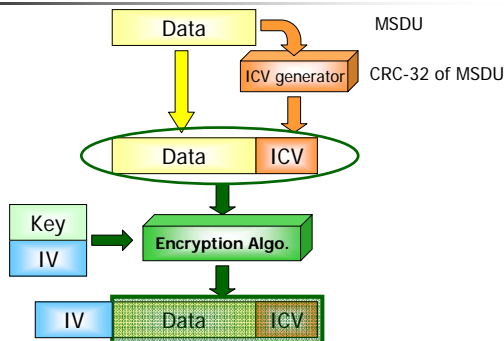
15

WEP Block Diagram



16

WEP Encapsulation



17

WEP

- Based on Exclusive-OR Operation
- Encryption $C = P \oplus K$
- Decryption $P = C \oplus K$
- Interesting Properties

$$P = C \oplus K$$

$$= (P \oplus K) \oplus K$$

$$= P \oplus (K \oplus K)$$

$$= P$$
- Can re-create keystream \rightarrow can decrypt a frame

18

WEP Issues

- Weak Point is IV not RC-4
- Static encryption keys — must be changed manually
- Attacker's tools: Aircnort, Yellowjacket, Airtart
- Encryption keys can be cracked in 3 seconds
- Default setting is "OFF"

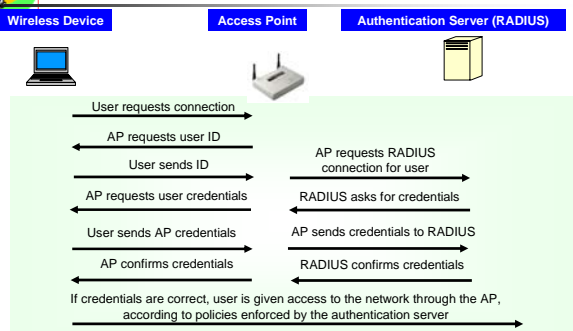
19

802.1x — A New Hope

- Provides secure access using port control
- Uses EAP (Extensible Authentication Protocol)
- Supports Kerberos, smart cards, one-time passwords, and so on
- Components required:
 - Wireless device
 - AP
 - Authentication server, typically Remote Authentication Dial-in User Service (RADIUS)

20

How 802.1x Works



21

802.1x — The Downside

- Only does authentication
- Encryption is still required
- If used with WEP, the encryption keys are still static even though the authentication keys change
- Authenticator and device must use the same authentication method
- Only supports client-level authentication

22

Wi-Fi Protected Access (WPA)



23

Wi-Fi Protected Access (WPA)

- WPA = 802.1X + TKIP
 - WPA requires authentication and encryption
 - 802.1X authentication choices include LEAP, PEAP, TLS
- WPA has strong industry supporters
 - Adds to 802.1X and TKIP
 - Widespread adoption of WPA will add robust security and remove the "security issue" from the WLAN industry
 - WPA will become accepted as the standard

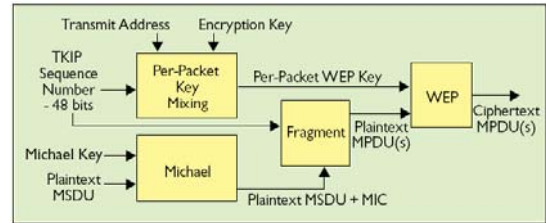
24

Temporal Key Integrity Protocol (TKIP)

- Based on RC4
- Effective patch for WEP
- Dynamic key management (based on 802.1x)
- Initialization vector sequencing
- Rapid re-keying
- Per-packet key hashing

25

TKIP



<http://www.cs.berkeley.edu/~daw/papers/wireless-cacm.pdf>

26

Feature Comparison

	WEP	TKIP	CCMP
Cipher Key Size(s)	RC4 40- or 104-bit encryption	RC4 128-bit encryption, 64-bit authentication	AES 128-bit
Key Lifetime Per-packet key	24-bit wrapping IV Concatenate IV to base key	48-bit IV TKIP mixing function	48-bit IV Not needed
Integrity Packet Header	None	Source and destination addresses protected by Michael	CCM
Packet Data Replay detection	CRC-32 None	Michael Enforce IV sequencing	CCM Enforce IV sequencing
Key Management	None	IEEE 802.1X	IEEE 802.1X

<http://www.cs.berkeley.edu/~daw/papers/wireless-cacm.pdf>

27

802.11i

- Mutual authentication
- Dynamic session key
- Message Integrity Check (MIC)
- Temporal Key Integrity Protocol (TKIP)
- Future
 - Stronger encryption schemes, such as AES

28

802.11i and WPA

- Uses 802.1x authentication
- Uses Temporal Key Integrity Protocol (TKIP) to dynamically change encryption keys after 10,000 packets are transferred
- Uses Advanced Encryption Standard (AES) encryption, which is much better than WEP
- A subset of 802.11i, Wi-Fi Protected Access (WPA) is available as a firmware upgrade today

29

802.11i and WPA Pitfalls

- Keys can be cracked using much less than 10,000 packets
- Michael feature — shuts down AP if it receives two login attempts within one second. Hackers can use this to perpetrate a DoS attack.
- 802.11i is yet to be released

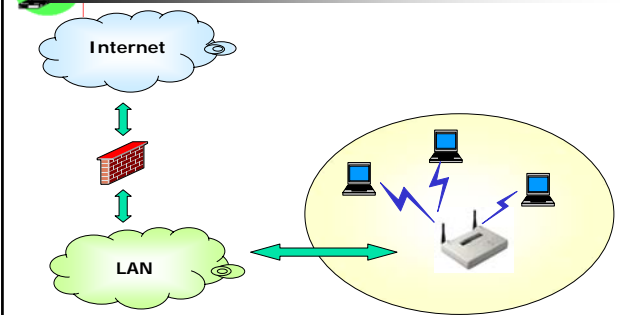
30

Agenda

- Security Characteristics
- WLAN Security
- **Security Threats**
- WLAN security management

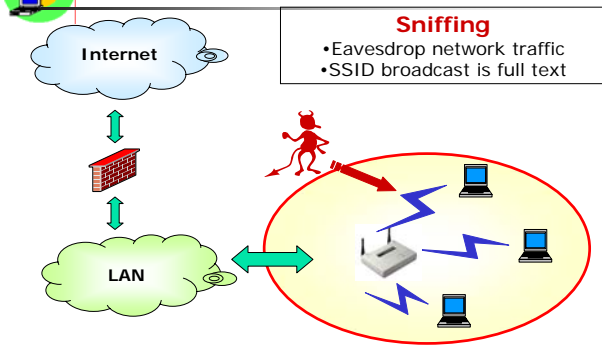
31

Typical WLAN Topology



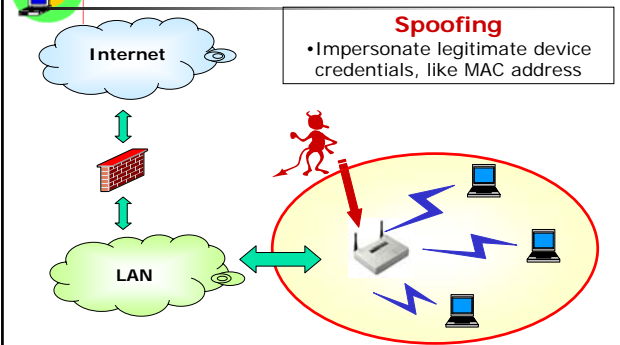
32

Types of Attacks



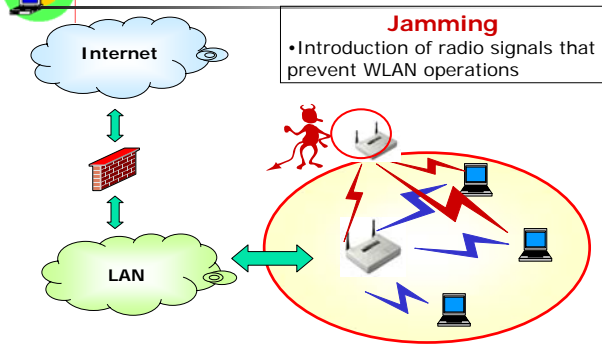
33

Types of Attacks



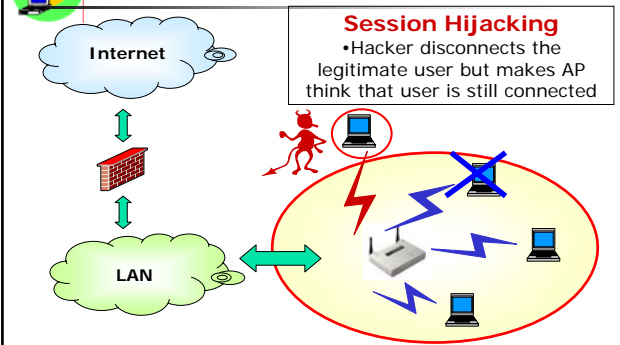
34

Types of Attacks



35

Types of Attacks



36

Types of Attacks

DoS

- Flood the network with useless traffic (e.g. repeated login requests) and eventually shut it down

37

Types of Attacks

Man in the Middle

- All WLAN traffic from devices is passed through the rogue device
- Lack of strong AP level authentication

38

Types of Attacks

WarDriving

Driving around town looking for unprotected WLAN connections to get Internet access

39

War Driving in Southern Cal.

<http://pasadena.net/apmap/losangeleslarge.gif>

40

Agenda

- Security Characteristics
- WLAN Security
- Security Threats
- WLAN security management**

41

Wireless Security Concerns

- Management of device security
- Corruption of data sent to wireless devices
- Malicious code (viruses, Trojans, worms)
- Unauthorized users
- Confidentiality of data sent wirelessly
- Security of data stored on a handheld device

42

WLAN security management

- Open Access
 - No WEP
 - Broadcast Mode
- Basic Security
 - 40-bit, 128-bit, 256-bit Static Encryption Key
- Enhanced Security
 - Dynamic Encryption Key / Scalable Key Management
 - Mutual 802.1x/EAP Authentication
 - TKIP/WPA
- Traveling Security
 - Virtual Private Network (VPN)

43

Wireless Policy Issues

- Policy needs to dictate permitted services and usage
- Needs a means of identifying and enforcing wireless policies
- Existing organization security policies need to be updated to cater to wireless security issues
- Policy needs to indicate how access will be controlled, for instance, time of day

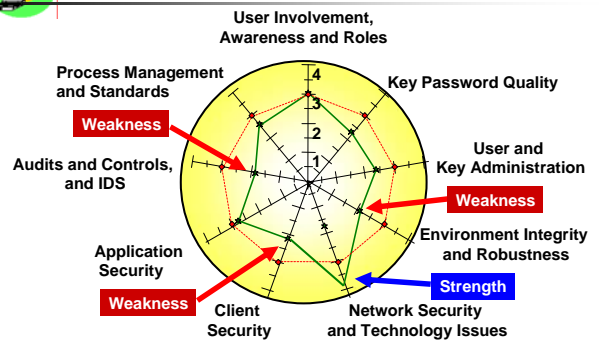
44

Wireless Policy Issues

- All access needs to be logged
- User compliance and standards enforcement
- Centralized control of security policies
- Wireless intrusion alert issues
- Process to update client software levels
- Intrusion detection policies

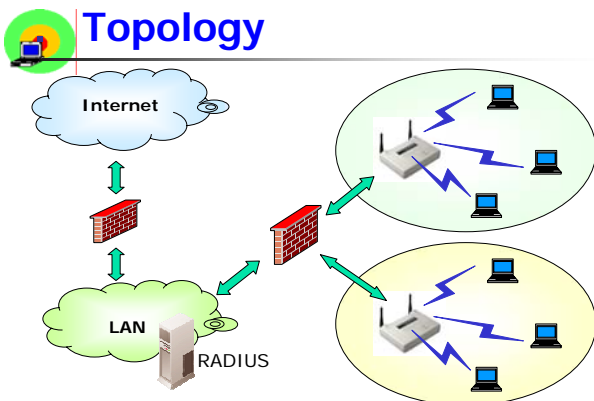
45

Knows Your Organization



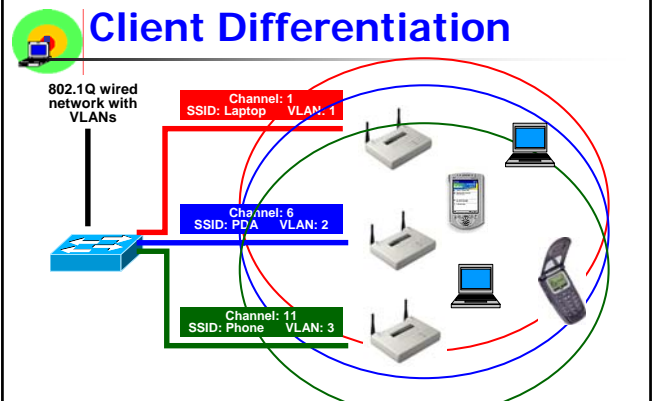
46

More Secure WLAN Topology



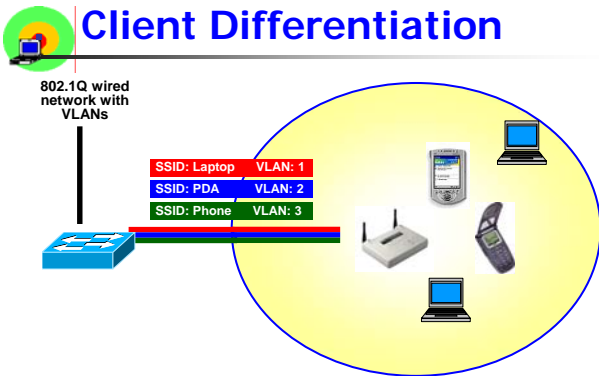
47

Client Differentiation



48

Client Differentiation



49

Conclusions

- Wireless technology is becoming embedded
 - Notebooks, PDAs, cell phones, etc.
- WLAN is currently unsecure
 - 802.11 WEP security is insufficient for the enterprise
 - 802.11i and WPA offer great improvements
- People, processes, policies and architecture are required to deploy WLAN securely

50

References

- “Who’s Watching Your Wireless Network?” by **Ian Hameroff**, Computer Associates, eTrust™ Security solutions, CA World 2003
- “Wireless Configuration and Security Issues” by **Greg Gabet**, IBMGS, CA world 2003
- “Addressing the Challenges of Adopting Secured Mobility in the Enterprise” by **Hans-Georg Büttner**, Ernst & Young IT-Security GmbH, Germany, CA World 2003
- “Wireless Local Area Network Security” by **Robert Simkins**, University of Derby, UK

51

References

- “A Field Guide to Wireless LANs for Administrators and Power Users” by **Thomas Maufer**, Prentice Hall, 2003
- “Security Flaws in IEEE 802.11 Data Link Protocols”, By **Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker**, COMMUNICATIONS OF THE ACM May 2003/Vol. 46, No. 5, pp 35-39 (<http://www.cs.berkeley.edu/~daw/papers/wireless-cacm.pdf>)

52