



Chapter 10

Security of Wireless LAN

- WEP – WPA – WPA2

WLAN Authentication and Encryption

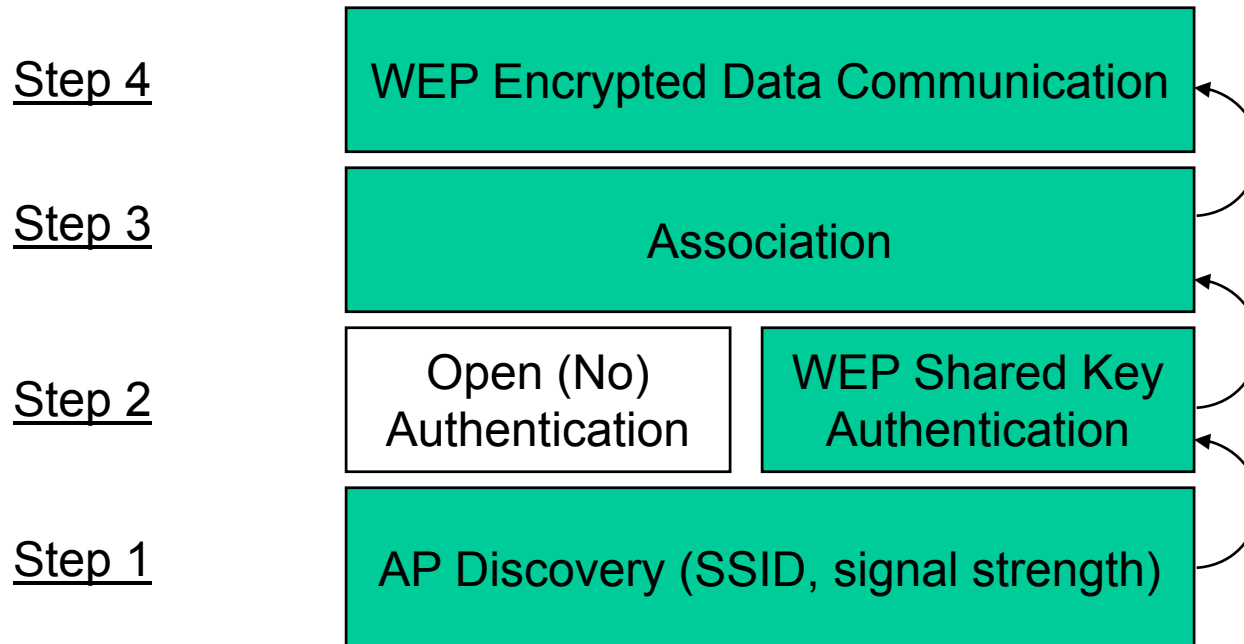


- ❑ WEP (Wired Equivalent Privacy) – First Generation
 - ❑ One way shared key authentication
 - ❑ RC4 encryption
 - ❑ This is not very strong, still popular in home market due to its simplicity

- ❑ WPA (WiFi Protected Access) – Second Generation
 - ❑ 802.1x authentication
 - ❑ TKIP encryption (variant of WEP, but stronger)

- ❑ 802.11i (WPA2/RSN) – Third Generation
 - ❑ 802.1x authentication
 - ❑ AES CCMP encryption

Connection Establishment using WEP

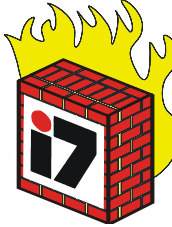


Security Services of IEEE 802.11



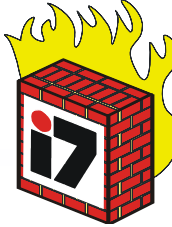
- ❑ Security services of IEEE 802.11 are realized by:
 - ❑ Entity authentication service
 - ❑ *Wired Equivalent Privacy (WEP)* mechanism
- ❑ WEP is supposed to provide the following security services:
 - ❑ Confidentiality
 - ❑ Data origin authentication / data integrity
 - ❑ Access control in conjunction with layer management
- ❑ WEP makes use of the following algorithms:
 - ❑ The RC4 stream cipher
 - ❑ The Cyclic Redundancy Code (CRC) checksum for detecting errors

IEEE 802.11 Entity Authentication



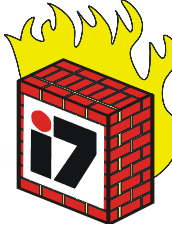
- ❑ IEEE 802.11 provides a very basic authentication service:
 - ❑ Authentication should be performed between stations and access points and could also be performed between arbitrary stations
 - ❑ When performing authentication, one station is acting as the *requestor (A)* and the other one as the *responder (B)*
 - ❑ The authentication dialogue:
 - 1.) $A \rightarrow B: (\text{Authentication}, 1, ID_A)$
 - 2.) $B \rightarrow A: (\text{Authentication}, 2, r_B)$
 - 3.) $A \rightarrow B: \{\text{Authentication}, 3, r_B\}_{K_{A,B}}$
 - 4.) $B \rightarrow A: (\text{Authentication}, 4, \text{Successful})$
 - ❑ As can be easily deduced from the above protocol, mutual authentication requires two independent protocol runs, one in each direction

IEEE 802.11 Entity Authentication

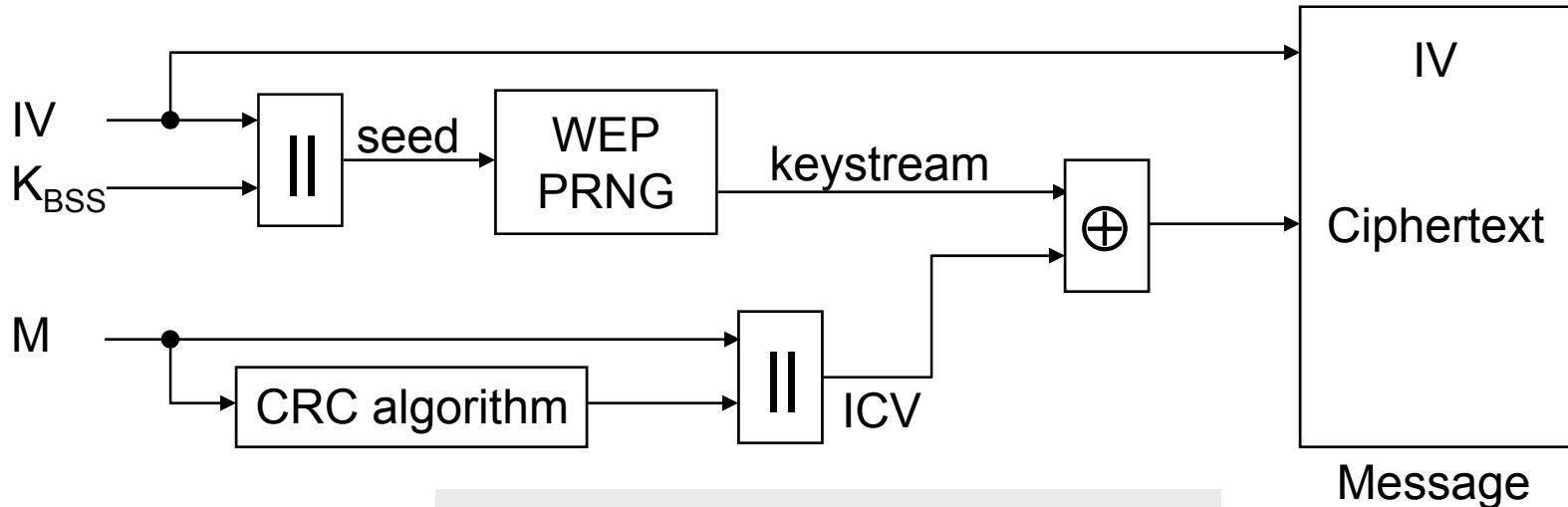


- ❑ IEEE 802.11 authentication comes in two “flavors”:
 - ❑ *Open System Authentication*:
 - “Essentially it is a null authentication algorithm.” (IEEE 802.11, section 8.1.1)
 - ❑ *Shared Key Authentication*:
 - “Shared key authentication supports authentication of nodes as either a member of those who know a shared secret key or a member of those who do not.” (IEEE 802.11, section 8.1.2)
 - “The required secret, shared key is presumed to have been delivered to participating nodes via a secure channel that is independent of IEEE 802.11”
- ❑ Concluding, IEEE 802.11 does not provide sufficient means for authentication in truly mobile environments:
 - ❑ As a result of the missing key management very often “open system authentication” is used

IEEE 802.11 Wired Equivalence Privacy

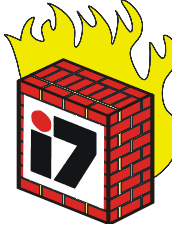


- ❑ IEEE 802.11's WEP uses RC4 as a pseudo-random-bit-generator:
 - ❑ For every message M to be protected a 24 bit *initialization vector* (IV) is concatenated with the shared key K_{BSS} to form the seed of the PRNG
 - ❑ The *integrity check value* (ICV) of M is computed with CRC and appended (" $||$ ") to the message
 - ❑ The resulting message ($M || ICV$) is XORed (" \oplus ") with the keystream generated by $RC4(IV || K_{BSS})$

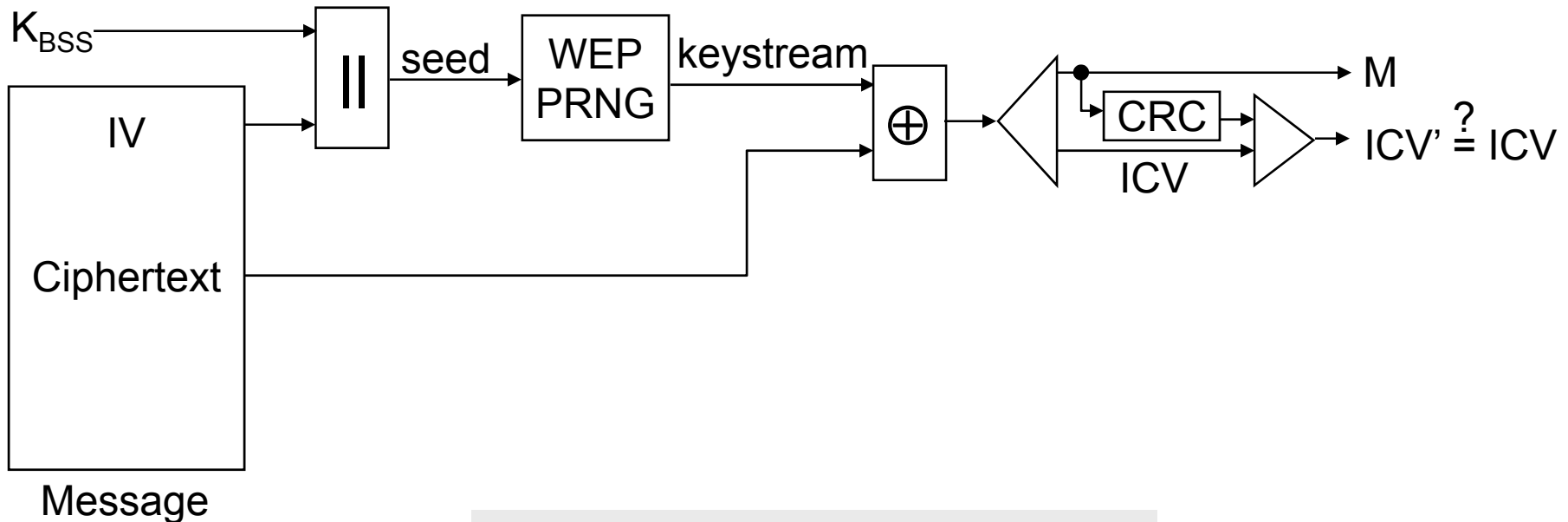


WEP Encryption Block Diagram

IEEE 802.11 Wired Equivalence Privacy



- ❑ As IV is send in clear with every message, every receiver who knows K_{BSS} can produce the appropriate keystream to decrypt a message
 - ❑ This assures the important *self-synchronization property* of WEP
- ❑ The decryption process is basically the inverse of encryption:



WEP Decryption Block Diagram

IEEE 802.11 Security Claims



- ❑ The WEP has been designed to ensure the following security properties:
 - ❑ Confidentiality:
 - Only stations that possess K_{BSS} can read messages protected with WEP
 - ❑ Data origin authentication / data integrity:
 - Malicious modifications of WEP protected messages can be detected
 - ❑ Access control in conjunction with layer management:
 - If set so in the layer management, only WEP protected messages will be accepted by receivers
 - Thus stations that do not know K_{BSS} can not send to such receivers

- ❑ Unfortunately, none of the above claims holds...

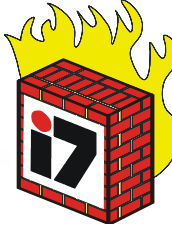
Weakness #1: The Keys



- ❑ IEEE 802.11 does not specify any key management:
 - ❑ Manual management is error prone and insecure
 - ❑ Shared use of one key for all stations of a BSS introduces additional security problems
 - ❑ As a consequence of manual key management, keys are rarely changed
 - ❑ As a another consequence, “security” is often even switched off!

- ❑ Key Length:
 - ❑ The key length of 40 bit specified in the original standard provides only poor security
 - ❑ The reason for this was exportability
 - ❑ However, today’s wireless LAN cards often also allow keys of 128 bit

Weakness #2: WEP Confidentiality is Insecure



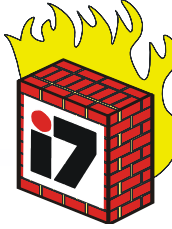
- ❑ Even with well distributed and long keys WEP is insecure
- ❑ The reason for this is reuse of keystream:
 - ❑ Recall that encryption is **re-synchronized with every message** by prepending an IV of length 24 bit to K_{BSS} and re-initializing the PRNG
 - ❑ Consider two plaintexts M_1 and M_2 encrypted using the same IV_1 :
 - $C_1 = P_1 \oplus RC4(IV_1, K_{BSS})$
 - $C_2 = P_2 \oplus RC4(IV_1, K_{BSS})$
- then:
 - $C_1 \oplus C_2 = (P_1 \oplus RC4(IV_1, K_{BSS})) \oplus (P_2 \oplus RC4(IV_1, K_{BSS})) = P_1 \oplus P_2$
- ❑ Thus, if an attacker knows, for example, P_1 and C_1 he can recover P_2 from C_2 without knowledge of the key K_{BSS}
- ❑ How often does reuse of keystream occur?
 - ❑ In practice quite often, as many implementations choose IV poorly
 - ❑ Even with optimum choice, as IV 's length is 24 bit, a busy base station of a 11 Mbit/s WLAN will exhaust the available space in half a day

Weakness #3: WEP Data Integrity is Insecure



- ❑ Recall that CRC is a linear function and RC4 is linear as well
- ❑ Consider A sending an encrypted message to B which is intercepted by an attacker E:
 - ❑ $A \rightarrow B: (IV, C)$ with $C = RC4(IV, K_{BSS}) \oplus (M, CRC(M))$
- ❑ The attacker E can construct a new ciphertext C' that will decrypt to a message M' with a valid checksum $CRC(M')$:
 - ❑ E chooses an arbitrary message Δ of the same length
 - ❑
$$\begin{aligned} C' &= C \oplus (\Delta, CRC(\Delta)) = RC4(IV, K_{BSS}) \oplus (M, CRC(M)) \oplus (\Delta, CRC(\Delta)) \\ &= RC4(IV, K_{BSS}) \oplus (M \oplus \Delta, CRC(M) \oplus CRC(\Delta)) \\ &= RC4(IV, K_{BSS}) \oplus (M \oplus \Delta, CRC(M \oplus \Delta)) \\ &= RC4(IV, K_{BSS}) \oplus (M', CRC(M')) \end{aligned}$$
 - ❑ Note, that E does not know M' as it does not know M
 - ❑ Nevertheless, a “1” at position n in Δ results in a flipped bit at position n in M' , so E can make controlled changes to M
 - \Rightarrow Data origin authentication / data integrity of WEP is insecure!

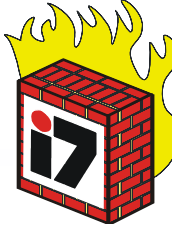
Weakness #4: WEP Access Control is Insecure



- ❑ Recall that the integrity function is computed without any key
- ❑ Consider an attacker who learns a plaintext-ciphertext pair:
 - ❑ As the attacker knows M and $C = \text{RC4}(\text{IV}, K_{\text{BSS}}) \oplus (M, \text{CRC}(M))$, he can compute the keystream used to produce C
 - ❑ If E later on wants to send a message M' he can compute $C' = \text{RC4}(\text{IV}, K_{\text{BSS}}) \oplus (M', \text{CRC}(M'))$ and send the message (IV, C')
 - ❑ As the reuse of old IV values is possible without triggering any alarms at the receiver, this constitutes a valid message
 - ❑ An “application” for this attack is unauthorized use of network resources:
 - The attacker sends IP packets destined for the Internet to the access point which routes them accordingly, giving free Internet access to the attacker

⇒ WEP Access Control can be circumvented with known plaintext

Weakness #5: Weakness in RC4 Key Scheduling



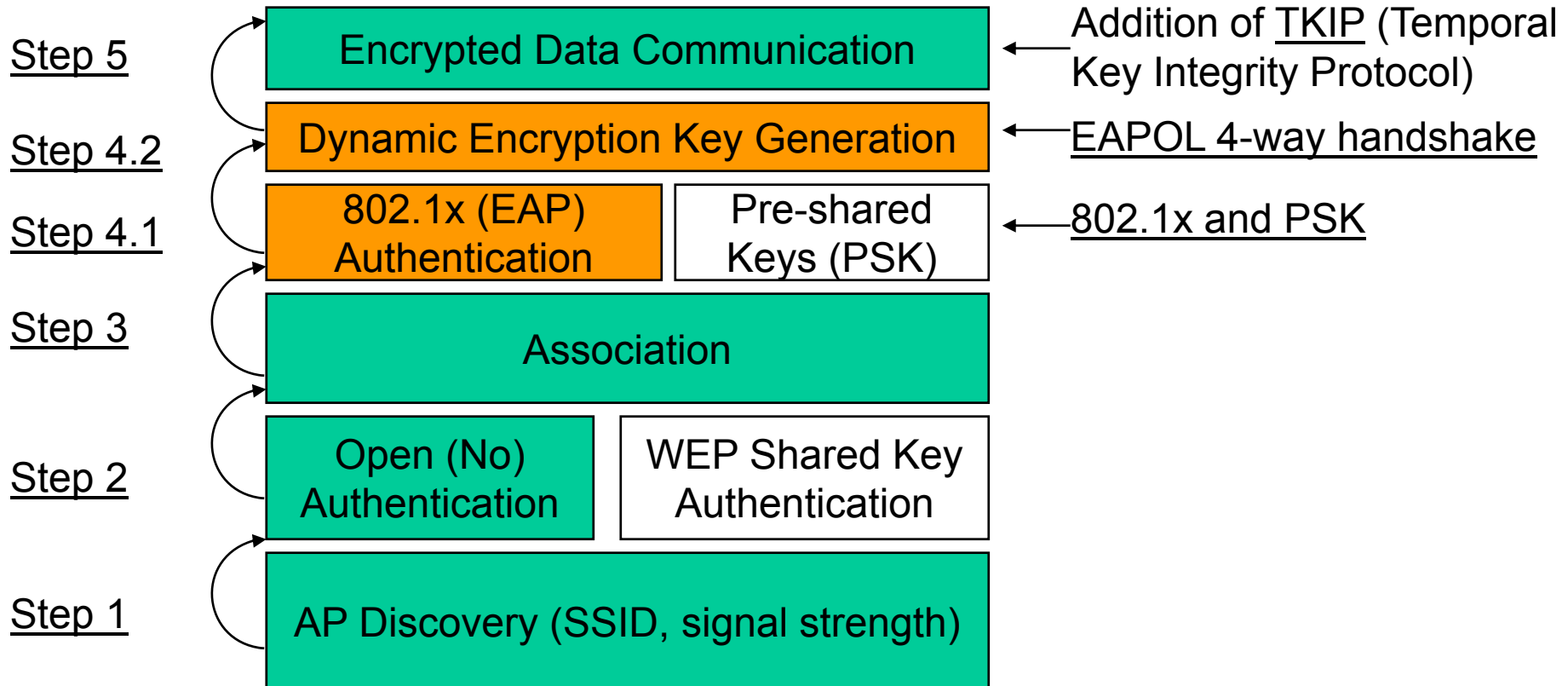
- ❑ In 2001, a new attack was discovered (see [SMF01a] and [SIR01a]):
 - ❑ The shared key can be retrieved in less than 15 minutes provided that about 4 to 6 million packets have been recovered
 - ❑ The attack is basically a known-plaintext attack, that makes use of the following properties of RC4 and WEP's usage of RC4:
 - RC4 is vulnerable to deducing bits of a key if:
 - many messages are encrypted with keystream generated from a variable initialization vector and a fixed key, and
 - the initialization vectors and the plaintext of the first two octets are known for the encrypted messages
 - The IV for the keystream is transmitted in clear with every packet
 - The first two octets of an encrypted data packet can be guessed
 - ❑ R. Rivest comments on this [Riv01a]:

“Those who are using the RC4-based WEP or WEP2 protocols to provide confidentiality of their 802.11 communications should consider these protocols to be broken [...]”

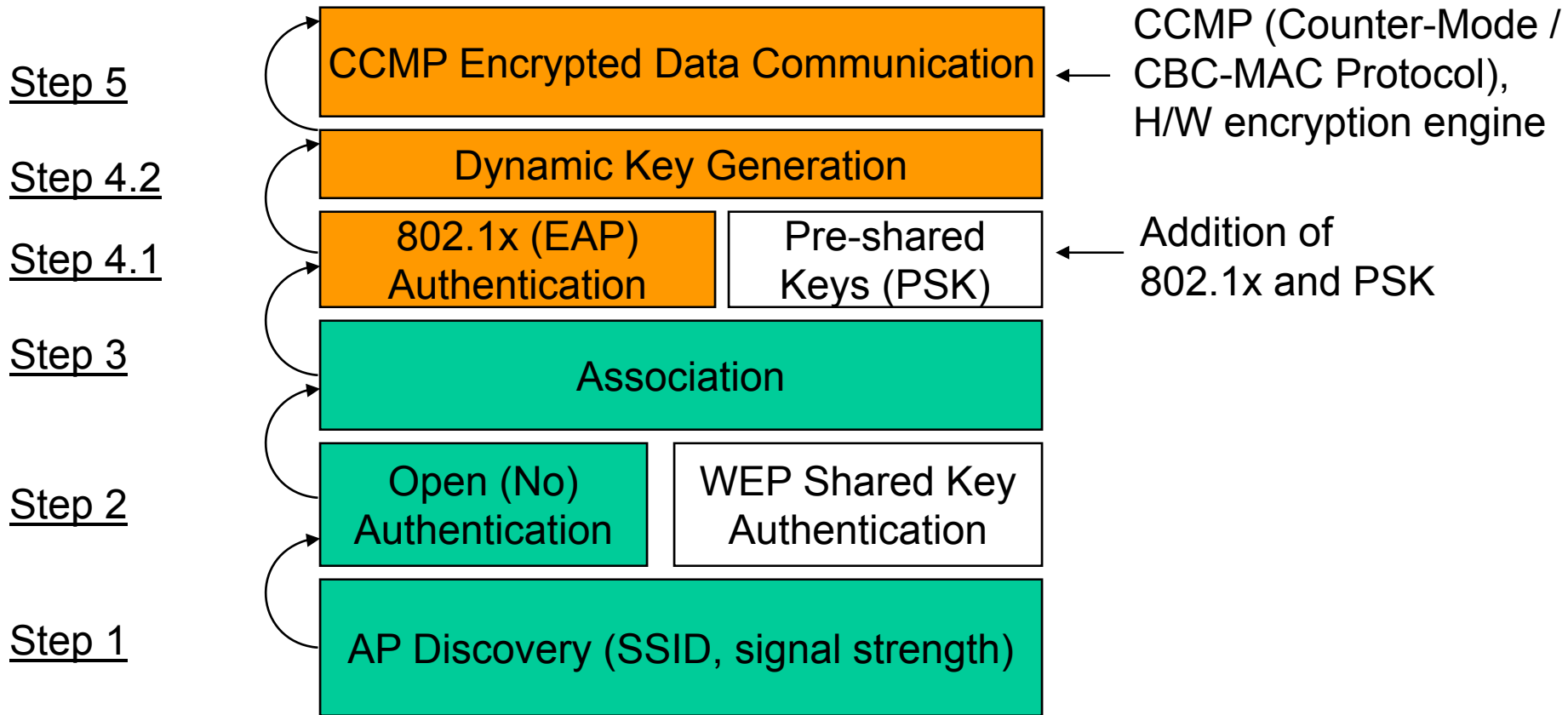
Connection Establishment using WPA



□ WPA – Wi-Fi Protected Access



Connection Establishment using 802.11i (WPA2)



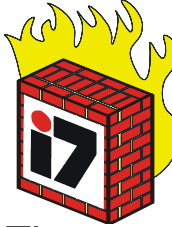
Note: CCMP is using AES in CBC mode

Summary (what do I need to know)



- ❑ Security objectives for WLAN security
- ❑ Principles of WEP

Additional References



- [BGW01a] N. Borisov, I. Goldberg, D. Wagner. *Intercepting Mobile Communications: The Insecurity of 802.11*. 7th ACM SIGMOBILE Annual International Conference on Mobile Computing and Networking (MOBICOM), Rome, Italy, July 2001.
- [IEEE97a] IEEE. *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE Std 802.11-1997, The Institute of Electrical and Electronics Engineers (IEEE), 1997.
- [Riv01a] R. Rivest. *RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4*. <http://www.rsa.com/rsalabs/technotes/wep.html>, 2001.
- [SIR01a] A. Stubblefield, J. Ioannidis, A. D. Rubin. *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*. AT&T Labs Technical Report TD-4ZCPZZ, August 2001.
- [SMF01a] Adi Shamir, Itsik Mantin and Scott Fluhrer. *Weaknesses in the Key Scheduling Algorithm for RC4*. http://eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf, August 2001.