Security in 802.11 Data Link Protocols

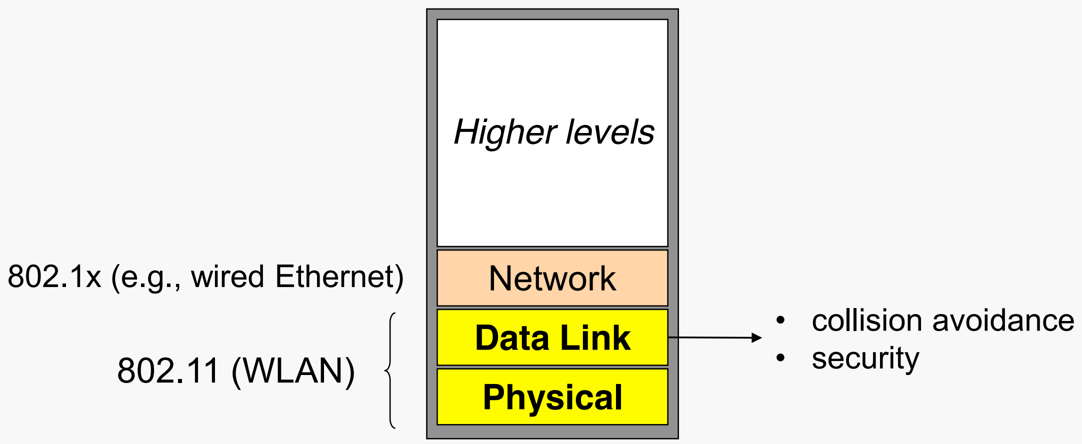
Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa, Italy
Via Diotisalvi 2, 56100 Pisa
gianluca.dini@ing.unipi.it

If you believe that any security problem can be solved by means of cryptography then you have not understood the problem (Roger Needham)

WIRELESS SECURITY IS DIFFERENT

- Wireless security is different from wired security
  - It gives potential attackers easy transport-medium access;
  - this access significantly increases the threat that any security architecture must address
- Wireless security requires a slightly different thinking

REFERENCE TO THE OSI MODEL



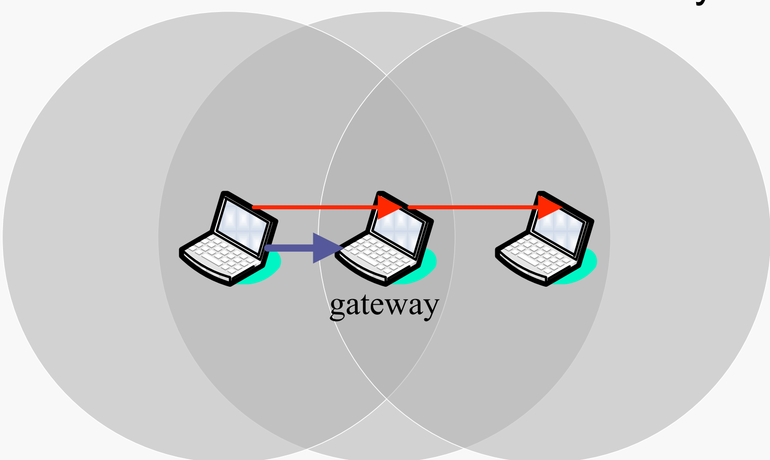
802.11 WIRELESS NETWORKS
modes

- Two networks topologies
  - ***Ad-hoc mode***
    Independent Basic Service Set, IBSS
  - ***Infrastructure mode***
    Basic Service Set, BSS

WLAN NETWORK TOPOLOGY
Ad-hoc mode

Clients can communicate directly

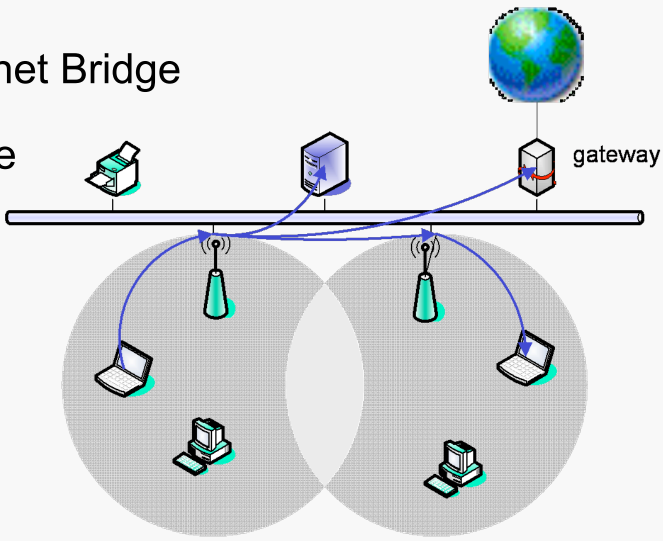
Each client communicates directly with clients in its cell



Each client operates as gateway and performs routing

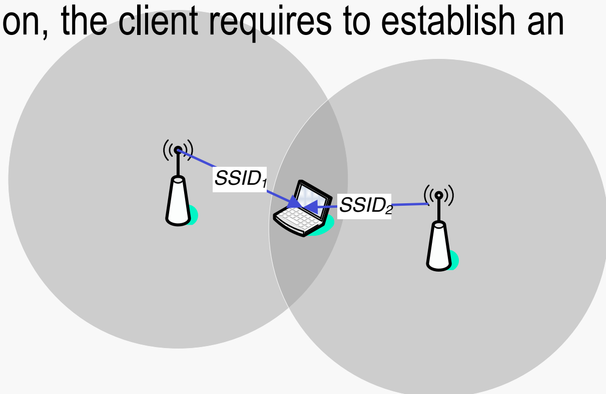
WLAN NETWORK TOPOLOGY
Infrastructure mode

- Each station sends all its communication to an Access Point (AP)
- AP acts as an Ethernet Bridge
- Prior to communicate a station and the AP must define an *association*



INFRASTRUCTURE MODE
Association / Beacon / Authentication

1. An AP sends a beacon (SSID) at fixed intervals
2. The client selects(*) the BSS to join
3. The client and the access point perform *mutual authentication*
4. After successful authentication, the client requires to establish an association



(*) A client may send a probe to find an AP affiliated with the desired SSID

ROADMAP
802.11 Security mechanisms and their weakness

- *Wired Equivalent Protection (WEP)*
  - Keystream reuse attack
  - Violation of message authentication (integrity)
  - Message decryption
- *Authentication and Access Control*
  - Open Systems Authentication
  - Closed Network Access Control
  - Shared Key Authentication

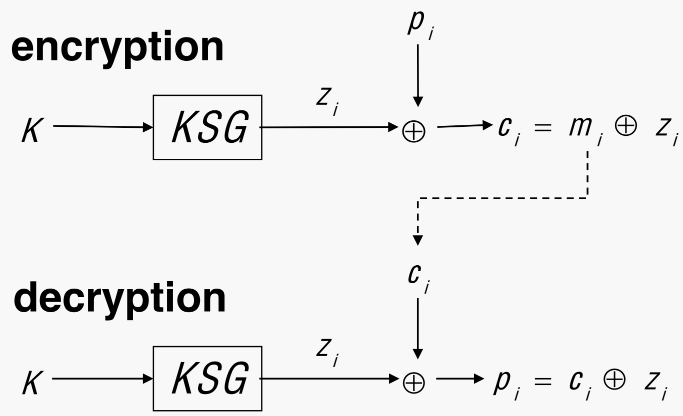
WIRED EQUIVALENT PRIVACY (WEP)

- WEP is a standard link-level protocol
- WEP is intended to enforce
  - *confidentiality* (main objective)
  - *authentication* (secondary objective)
  - *integrity* (secondary objective)
- WEP uses RC4 (stream cipher)

STREAM CIPHER

- m_i: *i*-th byte of the plaintext
- c_i: *i*-th byte of the ciphertext
- z_i: *i*-th byte of the key sequence

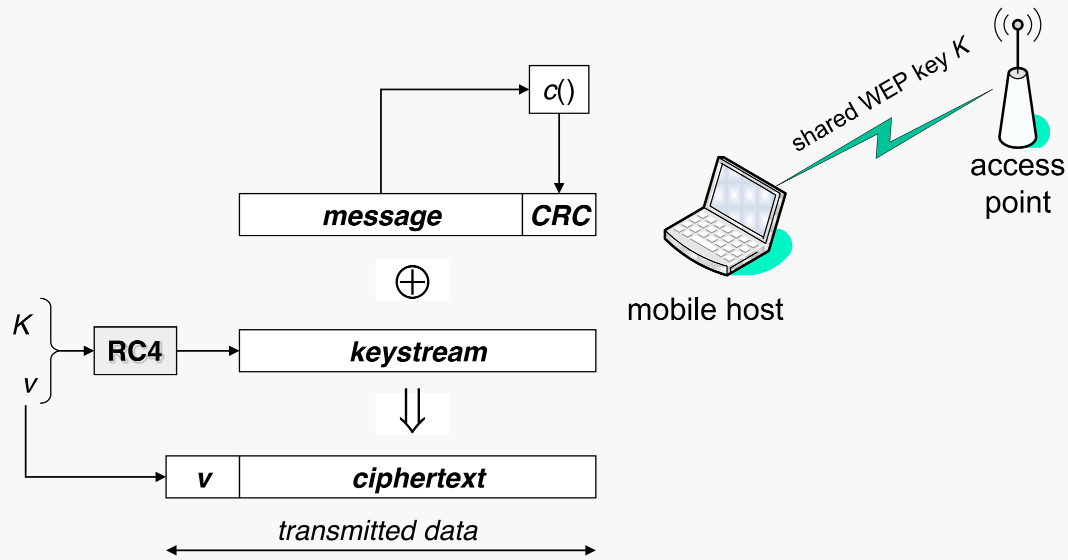
KSG: **Key Sequence Generator**



$$\begin{cases} C = P \oplus KSG(K) \\ P = C \oplus KSG(K) \end{cases}$$

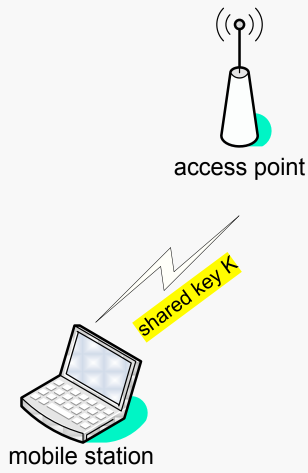
WEP
The protocol

- ***K***: **secret WEP key**
- **v: public initialization vector**

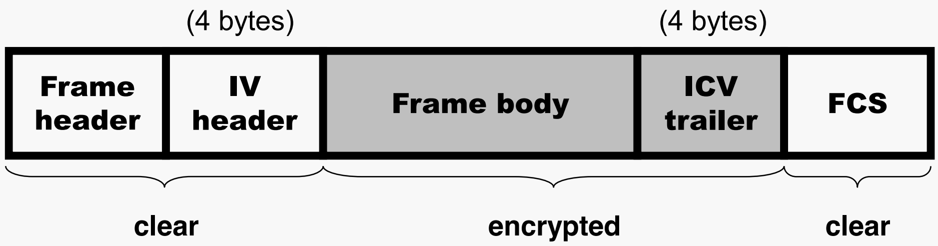


WEP
The protocol

- In order to send a message *M* to *B*, the station performs the following actions:
  - compute the integrity checksum $c = c(M)$ of message *M* and concatenate the two to obtain the plaintext $P = \langle M, c \rangle$;
  - choose a public initialization vector v and computes $C = P \oplus \text{RC4}(K, v)$;
  - build the frame $F = \langle v, C \rangle$ and send it to the access point;
- Upon receiving the frame *F*, the access point performs the following actions
  - compute $P' = C \oplus \text{RC4}(K, F.v)$;
  - split P' into $\langle M', c' \rangle$;
  - check whether $c' = c(M')$ (if not, *F* is rejected)



Frame



IV header
- **Initialization vector (24 bit)**
- **Pad (6 bit)**
- **Key identifier (2 bit)**

WEP
A few technical details

- The size of the initialization vector is fixed at 24-bit in the standard
- Two classes of WEP implementation
  - *standard implementation* (64-bit)
  - *extended implementation* (128-bit)
- 802.11 does not specify any key distribution
  - WEP relies on external mechanisms

KEY MANAGEMENT

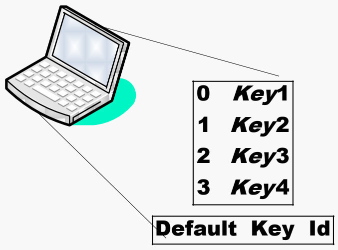
802.11 does not specify any key management

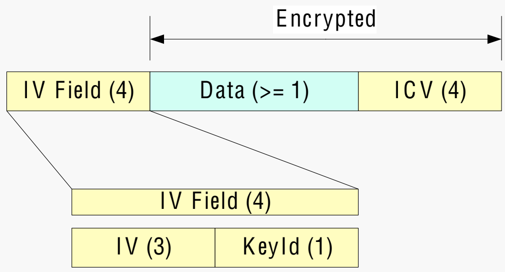
- Key management is left as an exercise for vendors
- The standard allows for a unique key for each mobile station however
- In practice, most installations use a single key for an entire network
  - Manual configuration by system administrator
  - most non-scalable management protocol

KEY MANAGEMENT
Default Keys

Four keys in each station

- ➢ One key is (manually) designed as a transmit key
- ➢ The four keys can be used to decrypt messages

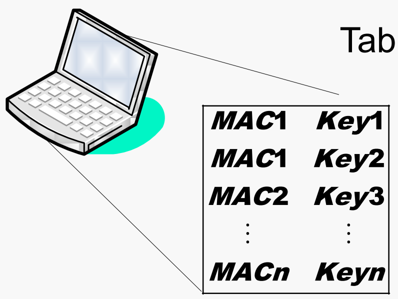




- ➢ **Stations and AP can share the same key**
- ➢ **Stations can use individual keys**

KEY MANAGEMENT
Mapped Keys

Each station maintains a *WEP Key Mappings Table*



WEP Key Mappings Table

Tables in two stations that need to communicate must
- contain each other's MAC address
- map these MAC addresses to the same key value

- AP can support both mapped keys and default keys simultaneously
  - Mapped keys MUST be used if at least one mapping is present
  - Default keys MUST be used when no mapping is present

KEY MANAGEMENT
A single key for the entire network

This practice seriously impacts the security of the system

- A secret shared among many users cannot remain secret for long
- Reuse of a single key makes key-stream reuse attacks simpler
- The fact that many users share the same key means that it is difficult to replace compromised key material

WEP
An embarrassing history (1)

- **January 2001: Borisov, Goldberg and Wagner [Borisov01, Walker00]**
  - Encrypted messages can be modified without fear of detection
  - Authentication protocol can be trivially defeated
- **Later, Arbaugh implemented BGW attack [Arbaugh01]**
  - It is possible to decrypt any *chosen* packet in a few hours
- **August 2001: Fluhrer, Mantin and Shamir attack [Fluhrer01]**
  - An eavesdropper who can obtain several million encrypted packets whose *first byte of plaintext is known* can deduce the base RC4 key by exploiting properties of the RC4 key schedule
  - An attacker can decrypt intercepted traffic, defeating confidentiality
  - An attacker can forge new encrypted packets, defeating integrity and authentication
  - A devastating attack!
  - FMS attack is in **AirSnort** and **aircrack**

WEP
An embarrassing history (2)

- **A week later Stubblefield, Ioannidis and Rubin implemented the FMS attack [Stubblefield02]**
  - The first byte encrypted under WEP is fixed and known
  - Ciphertext-only attack
  - Few hours
  - Attack is purely passive and can be done from a distance of a mile or more ➔undetectable
- **Since then, others implemented FMS**
  - Off-the-shelf hardware and software
  - Publicly available

WEP
Security problems

- *24-bit IV's are too short and this puts confidentiality at risk*
- *CRC is insecure and does not prevent adversarial modification of intercepted packets*
- *WEP combines IV with the key in a way that enables cryptanalytic attacks*
- *Integrity protection for source and destination addresses is not provided*

KEYSTREAM REUSE ATTACK
General concepts

Encrypting two messages under the same keystream can reveal information about both messages

- Let $C_1 = P_1 \oplus \text{RC4}(K, v)$ and $C_2 = P_2 \oplus \text{RC4}(K, v)$ then
  - $C_1 \oplus C_2 = P_1 \oplus P_2$
  - if P_1 is known, then $P_2 = P_1 \oplus C_1 \oplus C_2$ and $\text{RC4}(K, v) = C_1 \oplus P_1$
- General keystream reuse attacks [Dawson96]
  - ✓ Real-world plaintext have enough redundancy that it is possible to recover both P_1 and P_2 given only $P_1 \oplus P_2$
  - ✓ The attack is even more effective if the attacker has *n* ciphertexts deriving from the *same* keystream

KEYSTREAM REUSE ATTACK
Per-packet Initialization Vector

- *The use of a per-packet IV was intended to prevent keystream reuse but WEP fails this goal*
- *Potential causes are improper key and IV management*
- *IV reuse leads to keystream reuse*

KEYSTREAM REUSE ATTACK
Per-packet Initialization Vector

Improper management of IV's

- The WEP standard *recommends* but *does not require* that IV is changed after every packet
- The WEP standard *does not say anything* about how to select IV's
- The WEP standard specifies that IV is only 24 bits wide
  - this nearly guarantees that the same IV is reused for different messages;
  - this vulnerability is fundamental

KEYSTREAM REUSE ATTACK
Birthday attack to randomly selected IV's

Let

- $p(t)$ = probability that there is at least one collision after t packets;
- $q(t)$ = probability that there is no collision after t packets = 1 – $p(t)$
- $V = 2^{24}$, $\alpha = 1/V$ and $t \gg 1$

Then

$$q(t) = \frac{V-1}{V} \times \frac{V-2}{V} \times \cdots \times \frac{V-(t-1)}{V} = (1-\alpha) \times (1-2\alpha) \times \cdots \times [1-(t-1)\alpha] \cong$$

$$q(t) = 1 - [1 + 2 + \cdots + (t-1)]\alpha = 1 - \frac{(t-1)t}{2}\alpha \cong 1 - \frac{1}{2}t^2\alpha.$$

$$p(t) = \frac{1}{2}t^2\alpha$$

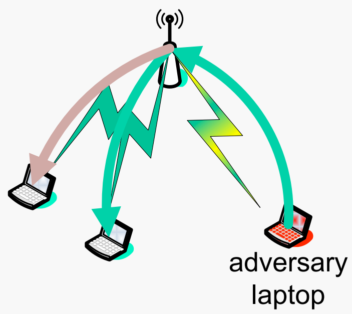
If we want $p(t) > \frac{1}{2}$ then $t > \sqrt{V} = 2^{12} = 4096$

EXPLOITING KEYSTREAM REUSE

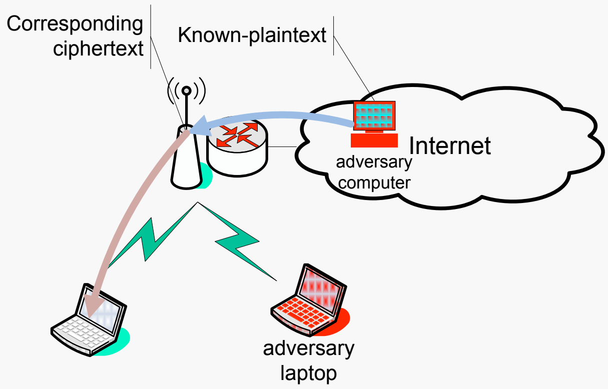
How to obtain plaintext

Many fields of IP traffic are predictable

Known-plaintext attacks



AP sends broadcast packets in both encrypted and unencrypted form



EXPLOITING KEYSTREAM REUSE

Dictionary attack

Over time, the attacker can build a dictionary

⟨IV, keystream⟩

- With 40 bits keys, exhaustive key search is more convenient but vendors have begun to support larger keys
- Poorly chosen IV's make it possible to reduce the size of the dictionary

SUMMARY

If you believe that any security problem can be solved by means of cryptography then you have not understood the problem
(R. Needham)

- *Any protocol that uses a stream cipher must take special care to ensure that keystreams never get reused*
- *A protocol designer should pay attention to the complications that use of stream ciphers adds to a protocol when choosing an encryption algorithm*

MESSAGE AUTHENTICATION ATTACK
CRC-32

WEP uses CRC-32 checksum to ensure that packets do not get modified in transit

- Unfortunately, CRC-32 checksum is not sufficient to guarantee integrity against a malicious attacker
- Vulnerability of CRC-32 is exacerbated by the use of RC4

MESSAGE MODIFICATION ATTACK
CRC is a linear function

Property I. *The WEP checksum is a linear function of the message with respect to* ⊕, i.e.,

$$\forall \text{ couple of messages } x, y,\ c(x \oplus y) = c(x) \oplus c(y)$$

- ***Corollary***. *This property can be exploited to make arbitrary modifications to an encrypted message without being detected*

MESSAGE MODIFICATION ATTACK
Corollary: arbitrary modification to a message

Let $C = RC4(K,v) \oplus \langle M, c(M) \rangle$ where M is the original message

We define $C' = C \oplus \langle \Delta, c(\Delta) \rangle$ where Δ is an arbitrary modification

$$C' = RC4(K,v) \oplus \langle M, c(M) \rangle \oplus \langle \Delta, c(\Delta) \rangle =$$

$$= RC4(K,v) \oplus \langle M \oplus \Delta, c(M) \oplus c(\Delta) \rangle = \text{(apply Property I)}$$

$$= RC4(K,v) \oplus \langle M \oplus \Delta, c(M \oplus \Delta) \rangle =$$

$$= RC4(K,v) \oplus \langle M', c(M') \rangle$$

- It follows that
  - C' is the ciphertext of $M' = M \oplus \Delta$
  - It is possible to modify a packet (even) with only partial knowledge of its contents

MESSAGE INJECTION ATTACK
The basis for spoofing network access control

Property II. *The WEP checksum is an unkeyed function of the message*

- The checksum field can be computed by the adversary who knows the message

Property III. *It is possible to reuse old IV values without triggering any alarms at the receiver*

- Reuse of old IV does not require the adversary to block the reception of the original message

MESSAGE INJECTION ATTACK
An attack sketch

- If an attacker gets hold of a ciphertext/plaintext of a packet then
  - he can recover both the keystream and IV, and
  - he create a *new packet* with the same IV (Property II), and
  - he can repeat this process *indefinitely* (Property III) (*The attack does not rely on Property I*)
- The attack can be avoided by disallowing IV reuse
- The attack can be avoided by using a MAC (e.g., SHA1-HMAC)

802.11 NETWORK ACCESS CONTROL
Open System Authentication

A station is allowed to join a network without any identity verification, i.e., no authentication

- Default
- Required
- Authentication management frames are sent in the clear even when WEP is enabled

802.11 NETWORK ACCESS CONTROL
Closed Network Authentication

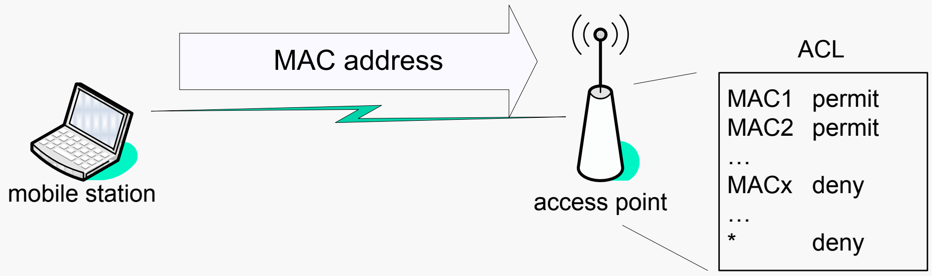
Only the clients with the knowledge of the network name, or SSID, can join

- AP is configured to not send the beacon
- SSID acts as a shared secret
- proprietary

Weakness

- Several management frames contain SSID
- These frames are broadcast in the clear even when WEP is enabled
- An attacker can easily sniff the secret (SSID)

802.11 NETWORK ACCESS CONTROL
Ethernet MAC Address ACL



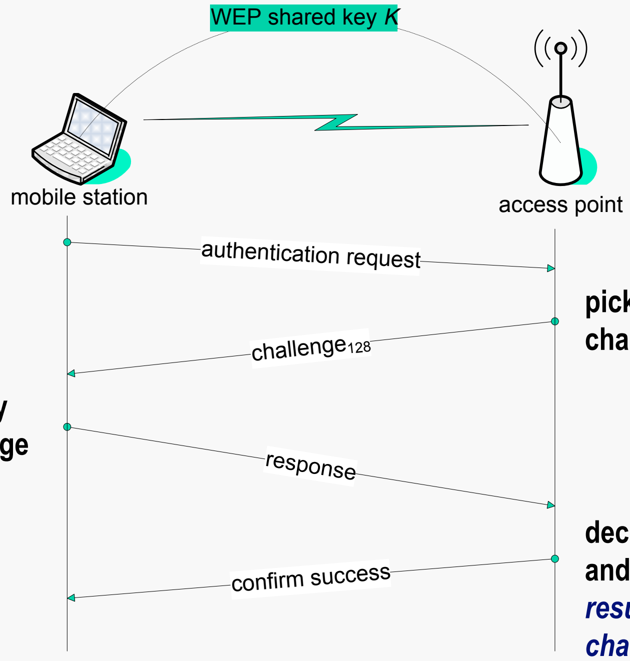
- ACL's are not part of 802.11 but are a security technique commonly used by vendors
- Flaws
  - MAC addresses can be easily sniffed
  - MAC address of a card can be changed via software

802.11 AUTHENTICATION
Shared Key Authentication

A station is allowed to join a network if it proves possesion of a WEP key shared

- Challenge-response protocol
- Not required

802.11 SHARED KEY AUTHENTICATION
Shared Key Authentication

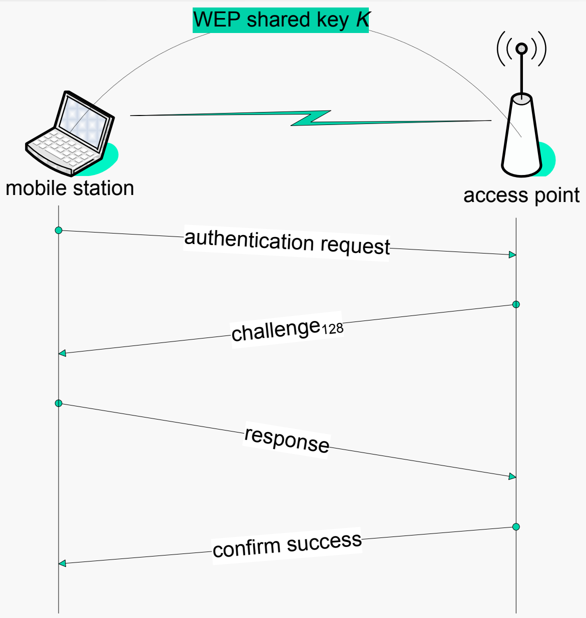


pick a random challenge

produce a response by encrypting the challenge with WEP

decrypt the *response* and check whether the *result* is equal to the *challenge*

802.11 AUTHENTICATION
Authentication Spoofing



Security protocols are three-line programs that people still manage to get wrong (R. Needham)

AUTHENTICATION SPOOFING [Arbaugh01]

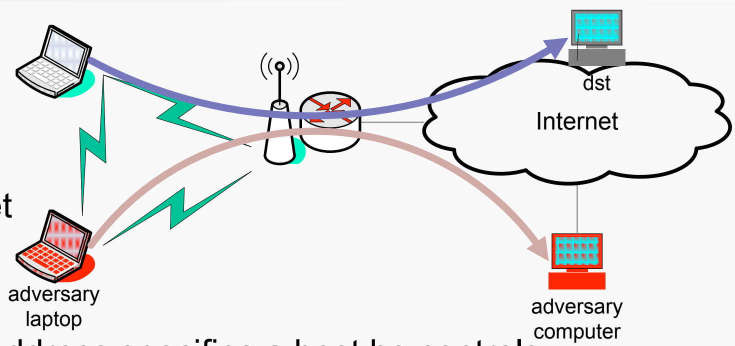
- An attacker eavesdrops a pair (***challenge, response***);
- The attacker recovers the keystream
  keystream = challenge ⊕ response
  (*keystream* is just of the right bit size)
- The attacker *reuses keystream* to authenticate himself indefinitely

MESSAGE DECRYPTION ATTACK
Tricking the AP

The ability to modify encrypted packets without detection can be leveraged to decrypt packets (Corollary of Property I)

- Attacking RC4 is practically impossible
- However, it is possible to trick the AP into decrypting some ciphertext for us

MESSAGE DECRYPTION
IP redirection



- The adversary
  - sniffs an encrypted packet off the air,
  - modifies the packet so that the new destination address specifies a host he controls
- The access point
  - decrypts the packet and
  - forwards it to such a destination
- The most of firewalls let the packet to pass (*from* the wireless network *to* the Internet)

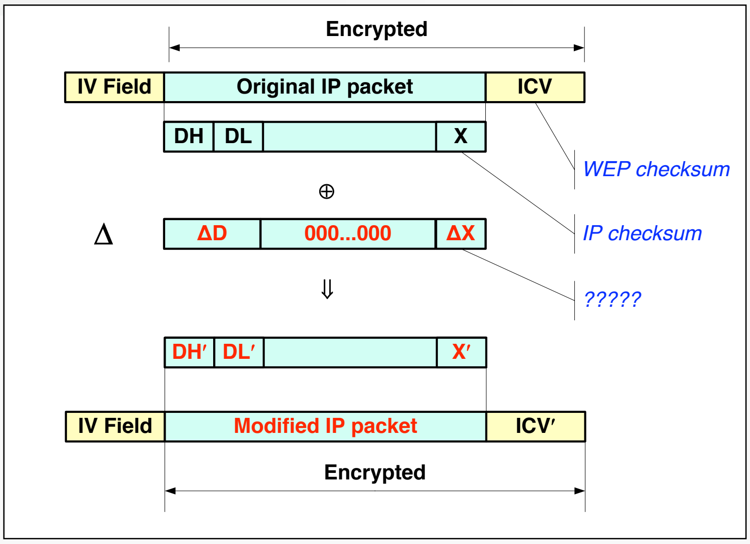
MESSAGE DECRYPTION
IP redirection

The adversary has to solve a few problems

- The adversary has to guess the dst IP addres
  (*not difficult*)
- The adversary modifies the *dst* IP address using the technique described in *Message Modification Attack*
  (*not difficult*)
- The adversary has ensure that *the checksum on the modified IP packet* is still correct
  (*difficult*)

MESSAGE DECRYPTION
IP redirection — how to make a correct IP checksum

- ***Definitions***
  - D = original destination
  - D′ = new destination
  - X = checksum of the original IP
  - X′ = checksum of the new IP packet
  - D_H, D_L = highest, lowest 16-bit word of D



- ***Property.*** *It can be proven that* $X' = X + D'_H + D'_L - DH - DL$ (1's complement)
- ***The problem:*** *The adversary knows what to add to X but not what to* ***xor*** *to X*

MESSAGE DECRYPTION
IP redirection — how to make a correct IP checksum

- *The adversary knows X*

  the problem is trivial

  ✓ the adversary calculates X′ then

  ✓ the adversary modifies the packet by xoring (X′ ⊕ X) which changes X into X′

- *The adversary arranges that X = X′*
  - compensate the change in D with a change in another field that does not affect the packet delivery and so that X = X′ (e.g., the source address S)

    ✓ $S'_L = S_L + (X - X')$

MESSAGE DECRYPTION
IP redirection — how to make a correct IP checksum

- *The adversary does not know X*

  Difficult task: given $\xi = (X' - X)$, calculate $\Delta = (X' \oplus X)$

  - A possible approach is the following

    ✓ given ξ, determine (X_i, X_i', Δ_i), $\Delta_i = X_i' \oplus X_i$, s.t. $(X_i' - X_i) = \xi$

    (*not all triples are possible and some of them are more frequent than others*)

    ✓ the adversary is free to make multiple attempts

    (*AP drops silently drops unsuccessful attempts*)

MESSAGE DECRYPTION ATTACK

Reaction attack(*)–the idea

This attack does not require connectivity to the Internet, but it is effective only against TCP traffic

The idea is:

we monitor the reaction of a TCP packet and

we use what we observe to infer information about the unknown text

(*) Reaction Attacks were initially discovered by Bellovin in the context of the IP Security Protocol [Bellovin 96]

MESSAGE DECRYPTION

Reaction attack–acceptance of a TCP packet

In more details

- A TCP packet is accepted only if the TCP checksum is correct
- In this case, a TCP ACK packet is sent in response (*even if the packet is a duplicate*)
- ACK packets are easily identified, even in their encrypted form, by their size, without requiring decryption
- The recipient's reaction discloses whether the TCP checksum was valid when the packet was decrypted

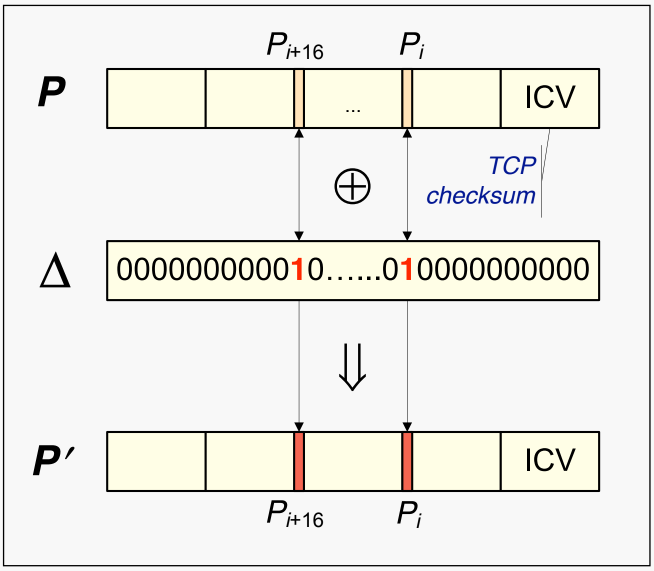
MESSAGE DECRYPTION ATTACK

Reaction attack–a property of TCP checksum

The attack exploits a property of TCP checksum

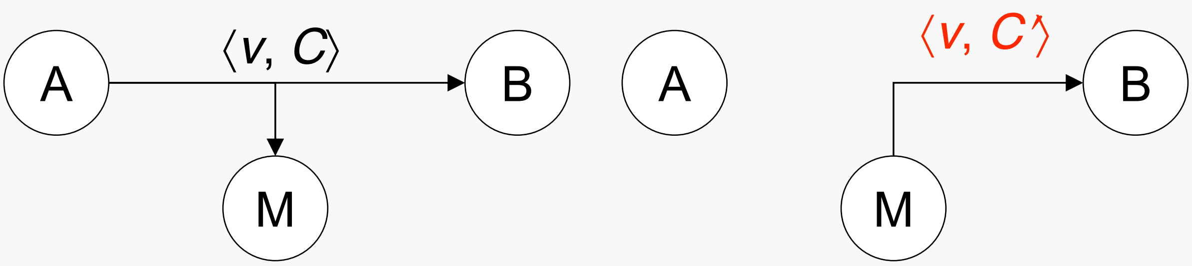
- We can flip pair of bits, e.g. P_i and P_{i+16}

  TCP checksum remains undisturbed if $P_i \oplus P_{i+16} = 1$
- The presence or not of the ACK packet reveals one bit of information about P
- The attack can be repeated for many choices of i



MESSAGE DECRYPTION ATTACK

Reaction attack–the attack



- The adversary intercepts ⟨v, C⟩ and flips bit P_i and P_{i+16} by means of the *Message modification attack*
- The adversary injects the modified packet ⟨*v*, *C*′⟩ in the network and watch to see whether B sends back a TCP ACK.
- The adversary repeats the attack for many choices of *i*

MESSAGE DECRYPTION ATTACK
Reaction attack–a few comments

*The attack exploits the willingness of the recipient to decrypt **arbitrary** messages*

*The recipient's **reaction** can be viewed as a **side channel***

*We have used the recipient as an **oracle** to unknowingly decrypt the intercepted ciphertext for us*

The use of a secure MAC (instead of CRC) would have prevented reaction attacks

COUNTERMEASURES
VPN and key management

Use a VPN to access the internal network

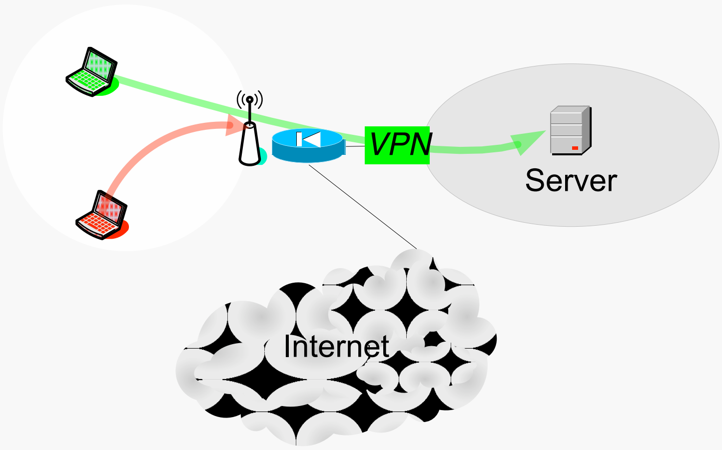
- obviate the need for link-layer security
- reuse a well-studied mechanism

Improve the key management

- every host has its own encryption key
- key are changed with high frequency
  (attacks to message authentication remain applicable)

COUNTERMEASURES
VPN approach

Place the wireless network outside of the organization firewall



- the wireless network is a threat
- legitimate clients employ a VPN solution to access the internal network
- illegitimate clients can neither access the internal network nor the Internet

VPN obviates the need for link-level security and reuses a well-studied mechanism

LESSONS

Design secure protocols is difficult and requires expertise beyond that acquired in engineering network protocols

- *Well-established principles in network engineering but dangerous from a security standpoint*
  - privilege performance
  - be liberal in what a protocol accepts
  - be stateless

Rely on expertise of others

- *Reuse past designs*
- *Offer new designs for public reviews*

COUNTERMEASURES
short-/long-term

WiFi Protected Access (WPA) is the TGi's short-term solution

- WPA requires only changes to firmware and drivers
- Temporal Key Integrity Protocol (TKIP)

CCMP: IEEE 802.11i long-term solution

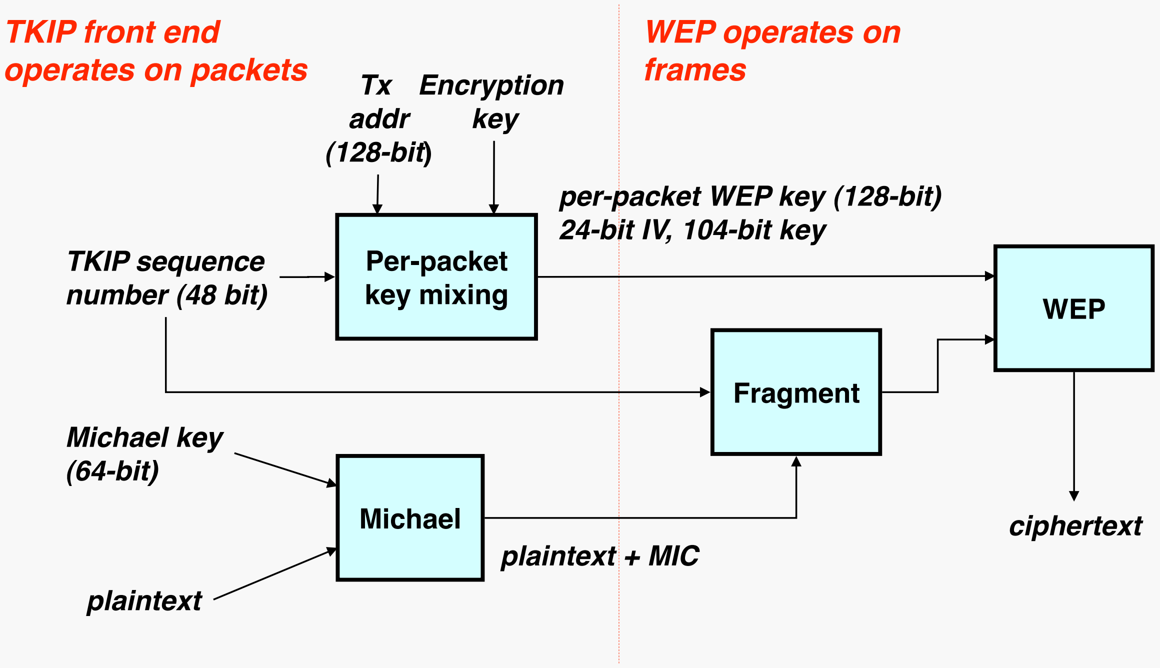
- Significant modification to existing IEEE 802.11 standard
- Highly robust solution, addresse all known WEP deficiences, but requires new hardware and protocol changes

IEEE 802.1x, a new standard for port-based authentication and key distribution

IEEE 802.11I SHORT-TERM SOLUTION
TKIP–constraints and new elements

- *constraints*
  - allow deployed system to be software or firmware upgradeable
  - allow the current WEP implementation to remain unchanged
  - minimize performance degradation imposed by fixes
- *three new elements*
  - a message integrity code (MIC) to defeat forgeries
  - a packet sequencing discipline to defeat replay attacks
  - a per-packet key mixing function to defeat FMS attack

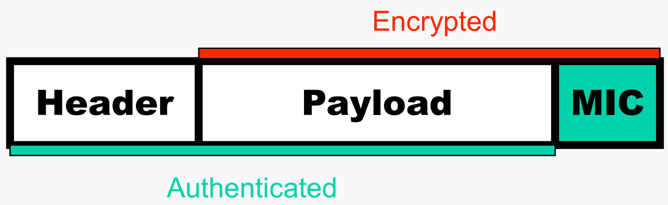
IEEE 802.11I SHORT-TERM SOLUTION
TKIP–conceptual scheme



IEEE 802.11 LONG-TERM SOLUTION
Counter Mode CBC MAC Protocol (CCMP)

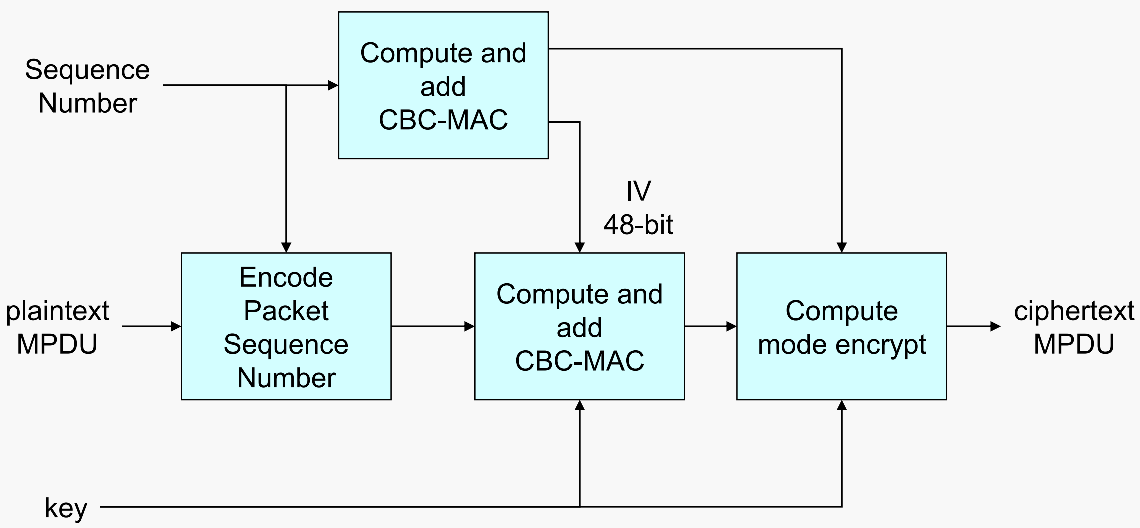
- New mode CCMP
  - merge counter mode for encryption and CBC-MAC for integrity
  - same key for encryption and integrity
  - all new protocol with a few concessions to WEP
  - packet oriented, no streams
- AES was selected for the encryption algorithm
  - AES overhead requires new hw for AP
  - AES overhead may require new STA hw for hend-held, but not PCs
- CCMP has been submitted to NIST for consideration as a FIPS

CCM Mode Overview

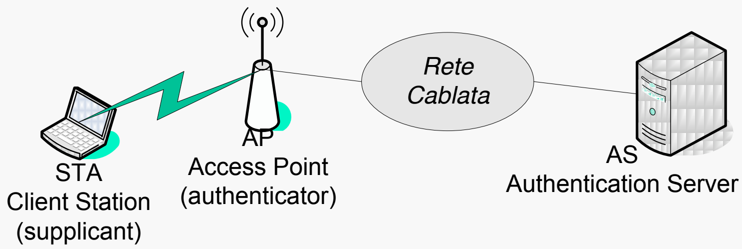


- CBC-MAC to compute MIC on plaintext header, length of plaintext header, and the payload
- Use CTR to encrypt the payload
  - Counter values 1, 2, 3, …
- Use CTR to encrypt the MIC
  - Counter value = 0

IEEE 802.11 LONG-TERM SOLUTION
Counter Mode CBC MAC Protocol (CCMP)



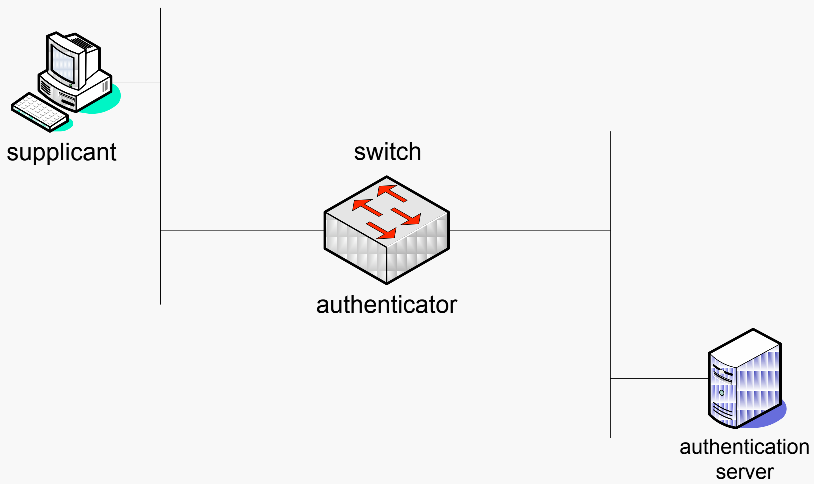
IEEE 802.1x
Port-based authentication: architecture



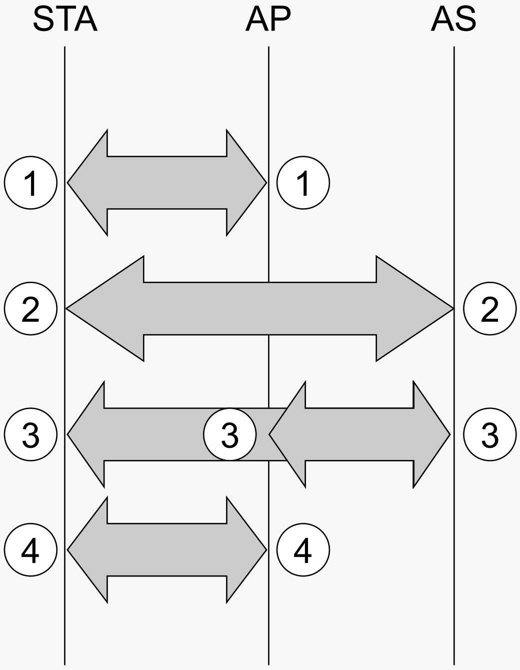
The authentication architecture is enriched with an *Authentication Server* AS

An Authentication Server may serve multiple Access Points

IEEE 802.1x
Entities



IEEE 802.1x
Phases

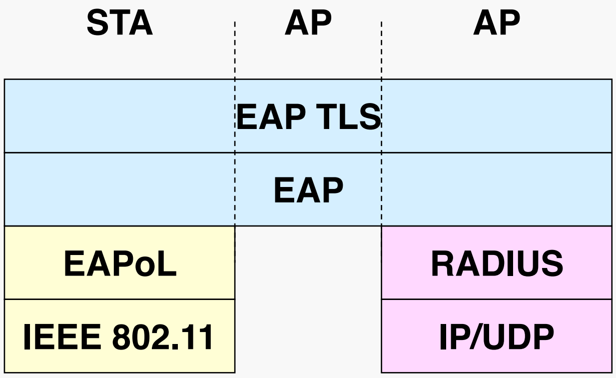


1. Discovery
2. Mutual Authentication and Master Key Generation (MK)
3. Pair wise Master Key Generation (PMK)
4. Temporary Key Generation (TK)

IEEE 802.1x
Phases

1. Discovery
   - STA and AP negotiate the encryption and authentication suite
2. Mutual Authentication and Master Key Generation (MK)
   - STA and AS mutually authenticate and generate a shared MK
   - AP acts as a repeater
   - Extensible Authentication Protocol, EAP [RFC 2284]
3. Pair wise Master Key Generation (PMK)
   - STA and AS use MK to generate PMK
   - AS sends PMK to AP
4. Temporary Key Generation (TK)
   - AP and STA use PMK to generate TK for wireless data transmission

IEEE 802.1x
Protocol stack



- EAPoL EAP over LAN [IEEE 802.1X
- RADIUS [RFC 2138]]

- EAP is a point-to-point protocol between STA and AP
  - EAP TLS is the TLS authentication mode supported by EAP
- EAP messages are encapsulated in EAPoL over 802.11 wireless link
- EAP messages are encapsulated in RADIUS over wired link

IEEE 802.1x
Extensible Authentication Protocol (EAP)[RFC 2284]

EAP can carry authentication data between two entities that want to set up authenticated communications between themselves

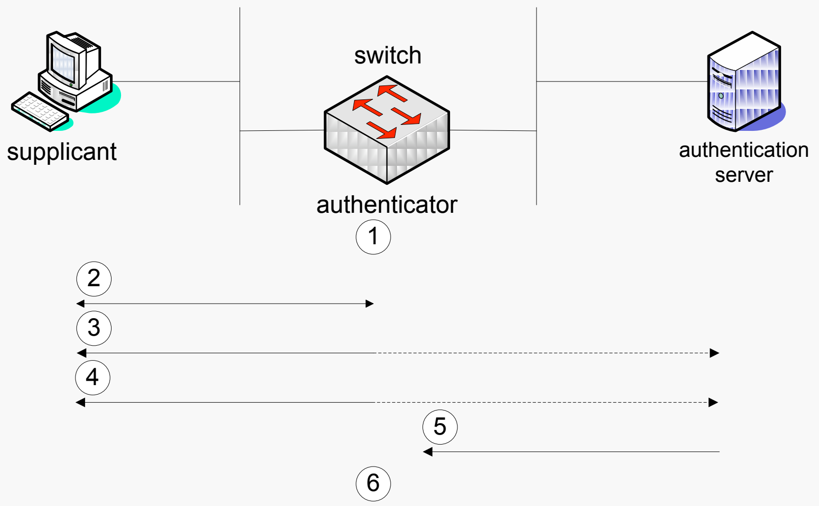
It supports a variety of authentication mechanisms

- MD-5 challenge response
- One-time passwords [RFC 1938]
- TLS messages [RFC 2716]
  - ✓mutual authentication

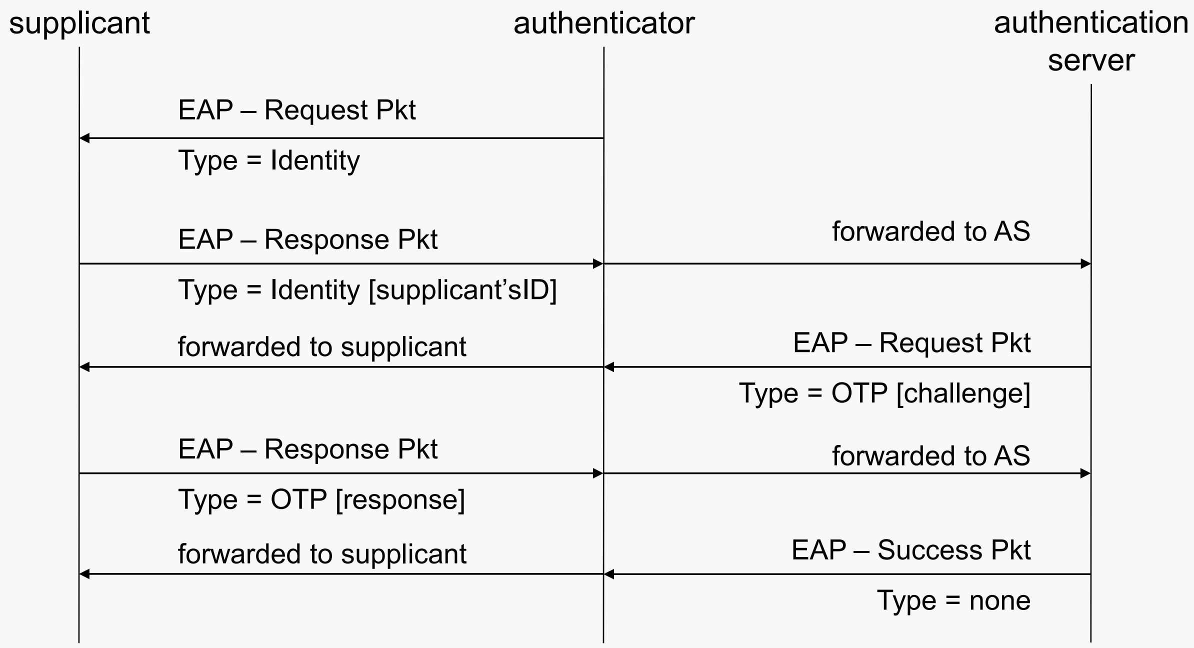
IEEE 802.1x
Encapsulating/decapsulating EAP packets

- 802.1x defines *EAP Over LAN* (EAPOL)
  an encapsulating/framing standard to allow communication between the supplicant and the authenticator
  - EAPOL encapsulation is defined separately for both Token Ring and Ethernet
- The EAP packets encapsulated in EAPOL are decapsulated and put into RADIUS/TACACS+ packets
  - RADIUS is generally preferred because it has EAP extensions built-in

IEEE 802.1x
Overall architecture and Flow



IEEE 802.1x
EAP exchange involving successful OTP auth



References

[Arbaugh01] W.A. Arbaugh, N. Shankar, and W.J. Wan, *Your* 802.11 *wireless network has no clothes*. http://www.cs.umd.edu/~waa/wireless.pdf, March 2001.

[Arbaugh01] W. Arbaugh, An Inductive Chosen Plaintext Attack Against WEP/WEP2. *IEEE Document 802.11-02/230*. May 2001. grouper.ieee.org/groups/802/11.

[Arbaugh03] W.A. Arbaugh, Wireless Security is Different, *IEEE Computer*, pp. 99–101, August 2003.

[Bellovin96] S. M. Bellovin, Problem areas for the IP security protocols, 6*th USENIX Security Symposium*, San Jose, California, July 1996.

[Borisov01] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: The insecurity of 802.11. *Proceedings of the International Conference on Mobile Computing and Networking*, pp. 180–189, July 2001.

[Dawson96] E. Dawson and L. Nielsen. Automated cryptanalysis of XOR plaintext strings. *Cryptologia*, (2):165–181, April 1996.

[Fluhrer01] S. Fluhrer, I. Mantin, and A. Shamir. A weakness in the key schedule algorithm of RC4. *Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography*, 2001.

[Potter03] B. Potter, Wireless Security's Future, *IEEE Security & Privacy*, pp. 68–72, July/August, 2003.

[Stubblefield02] A. Stubblefield, J. Ioannidis, and A. Rubin. Using Fluhre, Mantin, and Shamir attack to breal WEP. *Proceedings of the 2002 Network and Distributed System Security Symposium*, pp. 17–22, 2002.

[Walker00] J. Walker. Unsafe at any key size: An analyisis of the WEP encapsulation. *IEEE Document 802.11-00/362*. October 2000. grouper.ieee.org/groups/802/11.

Thanks for your attention!