

PhD Course

Lecture on

802.11 and Mesh Networking

Paal E. Engelstad

Outline

Basic 802.11 WLAN

(802.11a/b/g)

[Security in WLAN

(WEP, 802.11i/w)]

QoS in WLAN

(802.11e)

Markov Modeling

(Article)

Mesh networking

(802.11s)



This part now!

Agenda for Security in WLAN

- A framework for security in WLAN
- Some solutions at layer 3 and above
- Solutions at layer 2
- Security in Ad Hoc

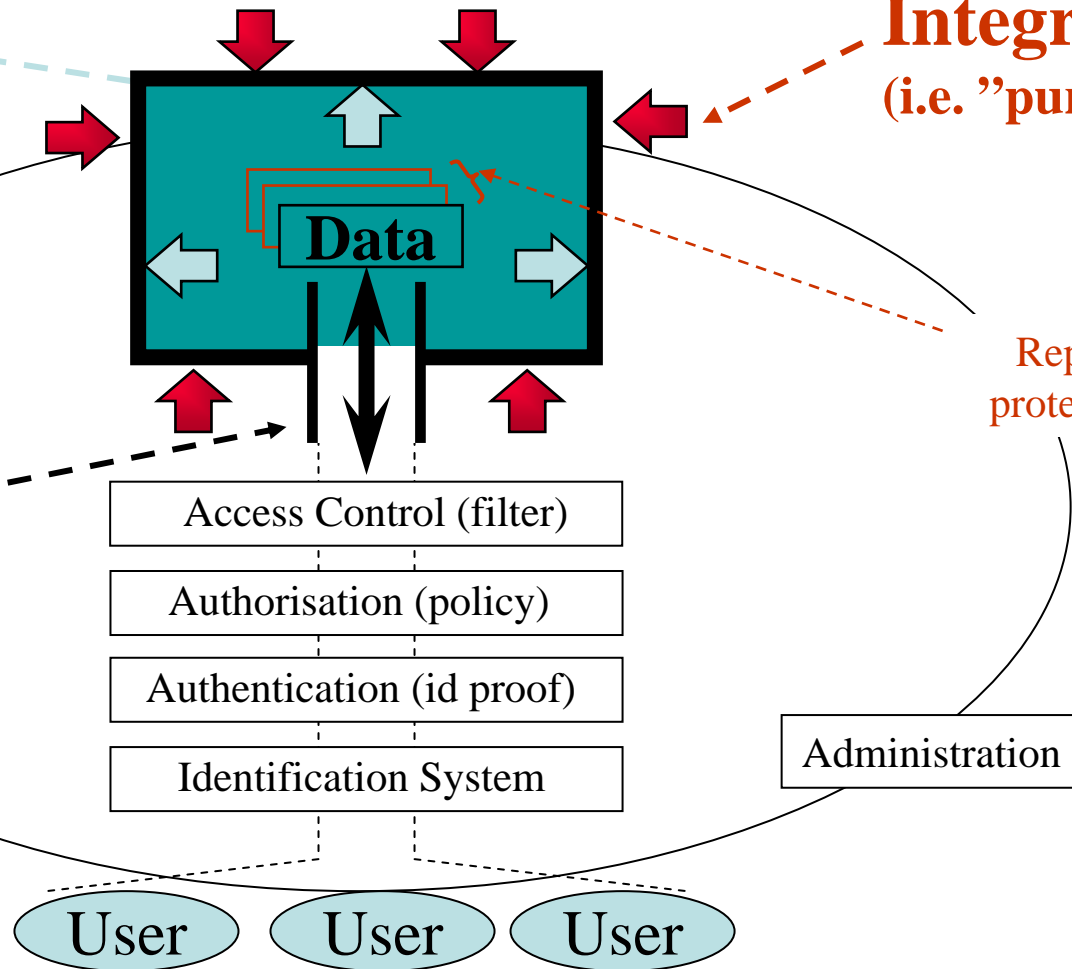
A framework for security

Privacy / Confidentiality
(i.e. "closedness")

Integrity
(i.e. "purity")

Availability
(only for authorized users)

Replay protection



Agenda for Security in WLAN

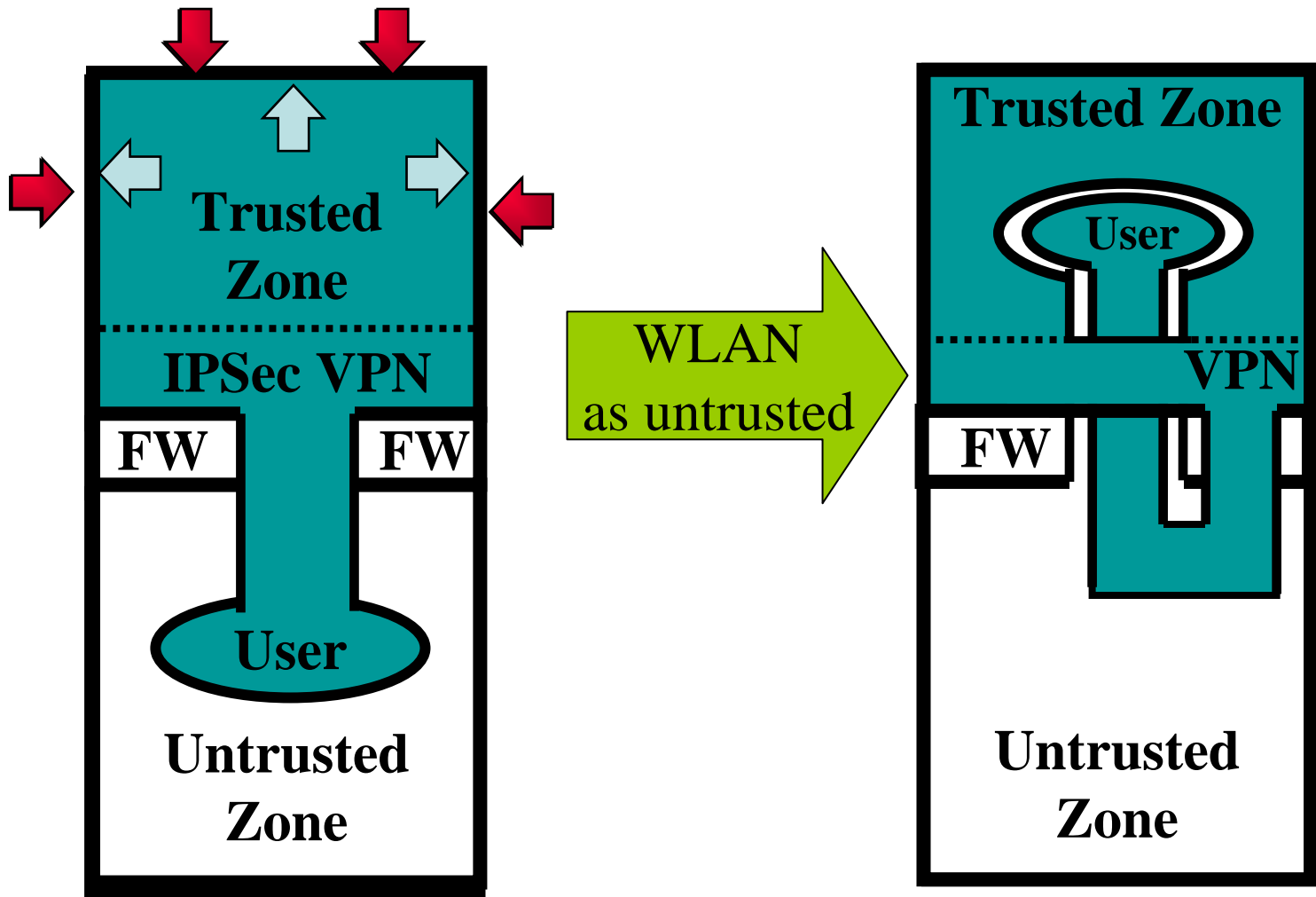
- A framework for security in WLAN
- Some solutions at layer 3 and above
- Solutions at layer 2
- Security in Ad Hoc

Security at L4 and above

1. "Sticky Page" authentication
 2. SSL proxy in the access network
- Drawbacks:
 - These solutions are restricted to http
 - Exposed to lower layer Denial-of-Service (DoS) attacks
 - A lower-layer solution is needed

SSL = "Secure Socket Layer"

Security at layer 3: VPN

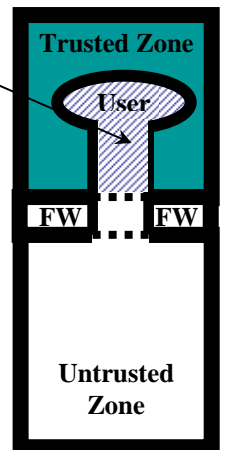


Traditional Security Architecture
Remote user in "trusted bubble"

WLAN user in untrusted zone
Treating WLAN user like remote user

Drawbacks of the VPN solution

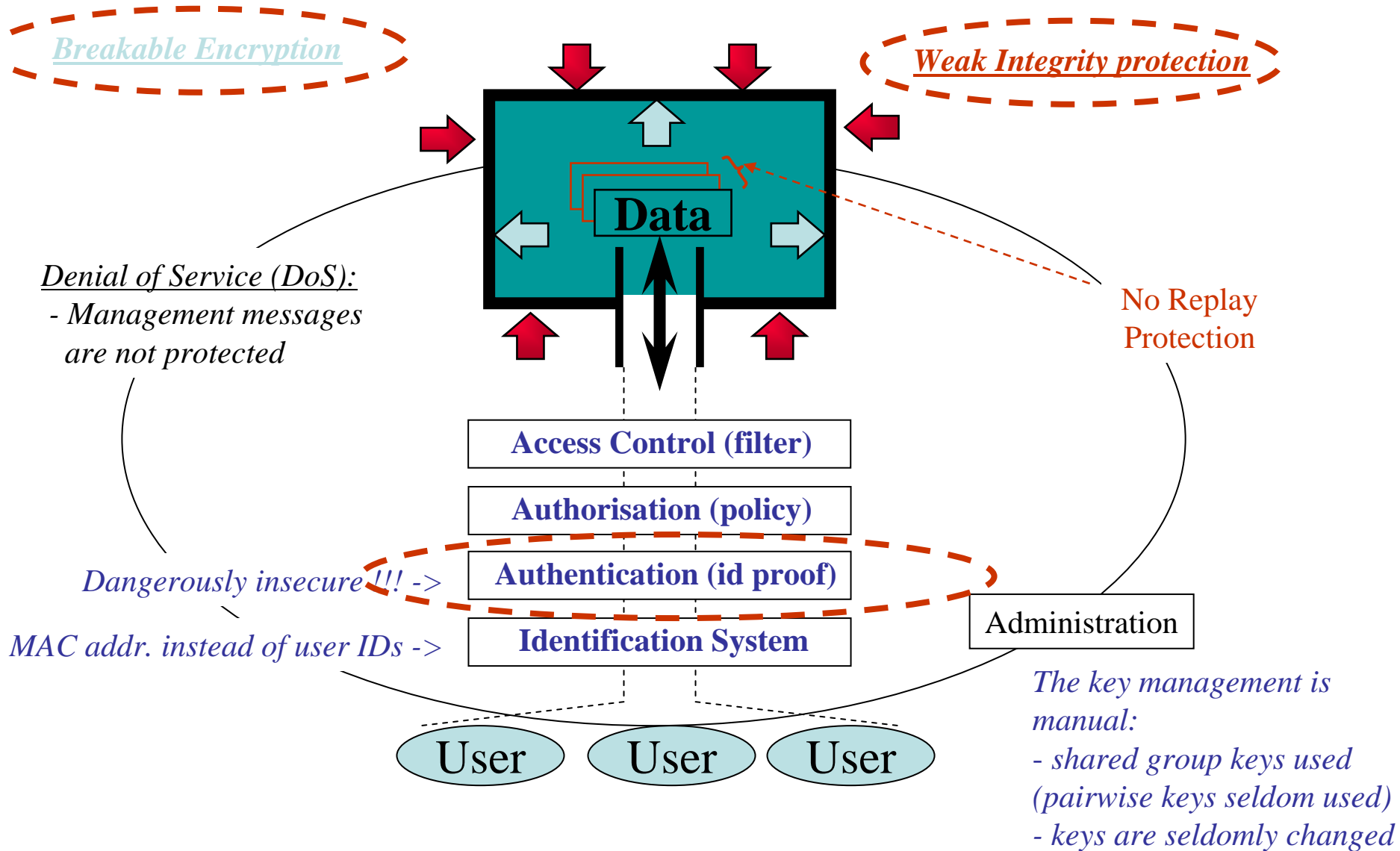
- Still exposed to lower layer DoS attacks, using for example:
 - 802.11 Management Messages (Layer 2)
 - Disassociation or Deauthentication message
 - ARP poisoning (Layer 2.5)
 - Use ARP to direct traffic to a non-existing MAC address
- “Better to secure the wireless network!”
 - Simpler: Need no VPN gateway
 - Better scalability
 - Not only IP frames are secured
 - e.g. ARP, Ethernet frames, etc.



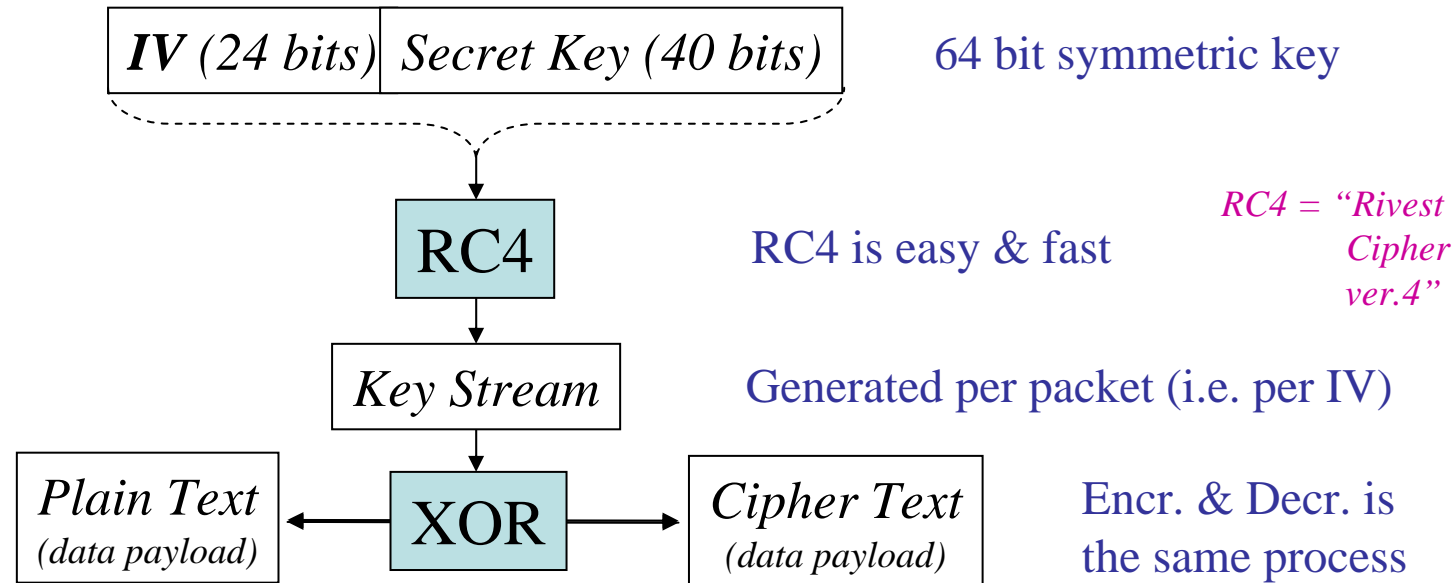
Agenda for Security in WLAN

- A framework for security in WLAN
- Some solutions at layer 3 and above
- Solutions at layer 2
 - WEP : Protection of Data Frames
 - The weaknesses of WEP
 - 802.11i : “Fixing WEP”
 - 802.11w: Protection of Management Frames
- Security in Ad Hoc

WEP weaknesses



WEP security is based on Encryption with the “RC4 Stream Cipher”



- **Initialization Vector (IV) – 24 bits**

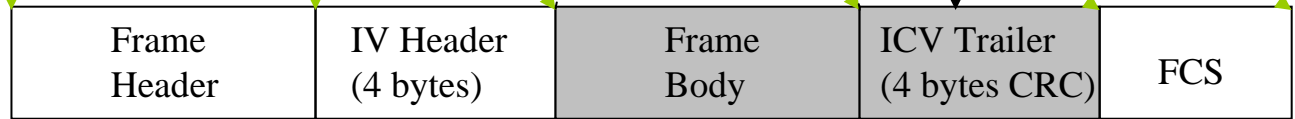
- IV sent openly in each packet
- Strength: Same packet with different IV \Rightarrow different key stream \Rightarrow different ciphertext

WEP Integrity Check Value (ICV)

Frame without WEP:



Using WEP:



①

32-bit CRC

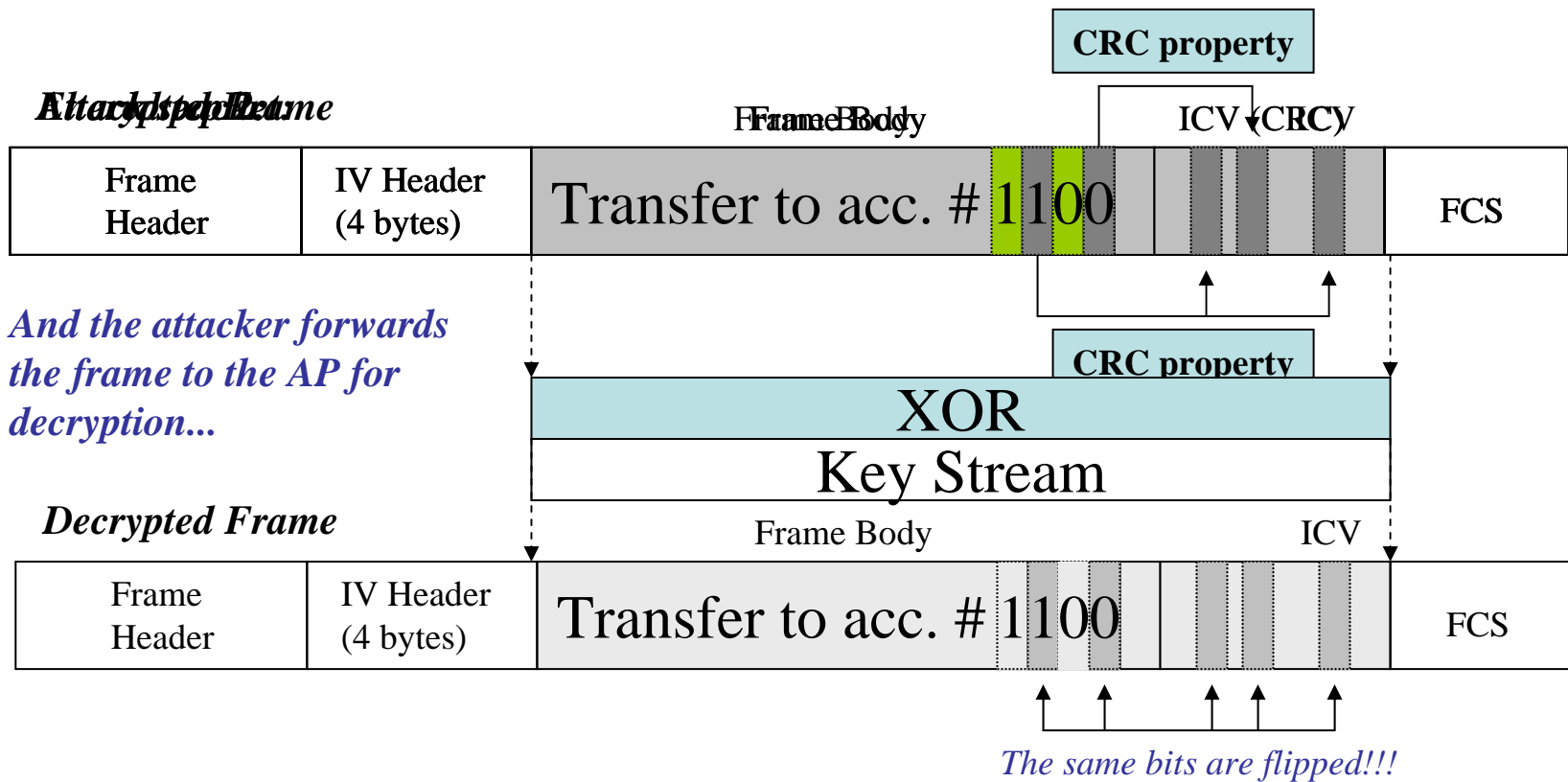
②

Protected by the RC4 encryption of WEP



WEP integrity protection does not work

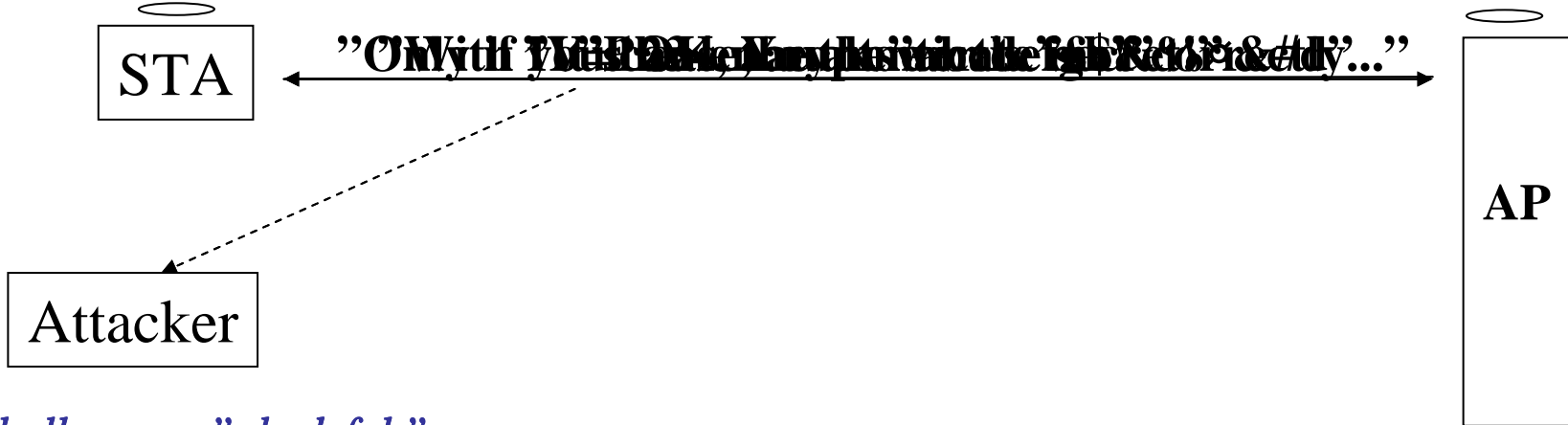
- Assume an attacker guesses the format and contents of an encrypted frame:



- Thus, the frame is OK'ed by the integrity check

WEP Authentication

- 1) KeyStream=RC4(1234,Secret)="XYZWQCHL"
- 2) Ciphertext = "abcdefgh" XOR "XYZWQCHL"
= "£\$&%α&#d"



Challenge = "abcdefgh"

Response = "£\$&%α&#d"

IV used = 1234

Note that STA never authenticated the AP,
i.e. the AP might really be an Attacker!

WEP *privacy* is breakable:

1) IV reuse

- IV reuse makes it possible to build a "decryption dictionary", using:
 - $C_1 \text{ XOR } C_2 = P_1 \text{ XOR } P_2$,
 - pattern recognition,
 - and comparison with the ICV
- ⇒ All 2^{24} different key streams are found in a few hours*)
- The IV is too short
 - 24 bits last only 7 hours without reuse at 500 pkts/sec
- IV selection rules are not properly specified
 - Some generates the IV randomly for each packet
 - 50% probability of collision after only 4823 packets (due to the "Birthday paradox")

**) Freeware "Airsnot" breaks WEP in terms of hours*

WEP **privacy** is breakable:

2) Weak IVs

- Together with well-known “Fixed Fields” in a packets, a “weak IV” reveals the secret key *)
 - Finding the first byte of the secret key requires only approx. 60 packets with “Weak IVs”
- Unfortunately, the number of weak IVs increases with key length
 - Double key length gives only doubled key entropy
 - I.e. A 104-bit WEP key is only 2,5 times better than a 40 bit key!

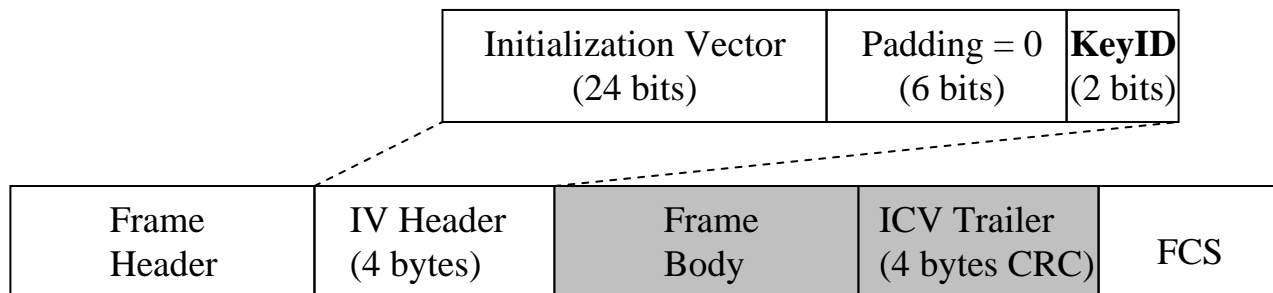
**) Flurer, Mantin and Shamir showed how to break RC4 for WEP i 2001*

WEP: No **key management** support makes the problem worse

- *Manual* means it's difficult to manage
 - Scales bad to large networks
- This means that in practice:
 - Keys are seldomly changed
 - This makes it easier to break the security
 - Keys normally shared by all users
 - This makes it easier to break the security (outsider's attack)
 - No protection between the users (insider's attack)

WEP: Pairwise keys are rarely used

- **Option 1: Default Keys (shared keys)**
 - Shared by all STAs in the WLAN
 - Max 4 different default keys, identified by the 2 bits key-ID in the IV-header



- **Option 2: Mapped Keys (pairwise keys)**
 - Each key pair is shared between the AP and a single STA

Summary of WEP weaknesses that need fixing

Breakable Encryption

- IV reuse
- "Weak" IVs

Weak Integrity protection

- CRC is a "linear" algorithm, that allows for bit-flipping

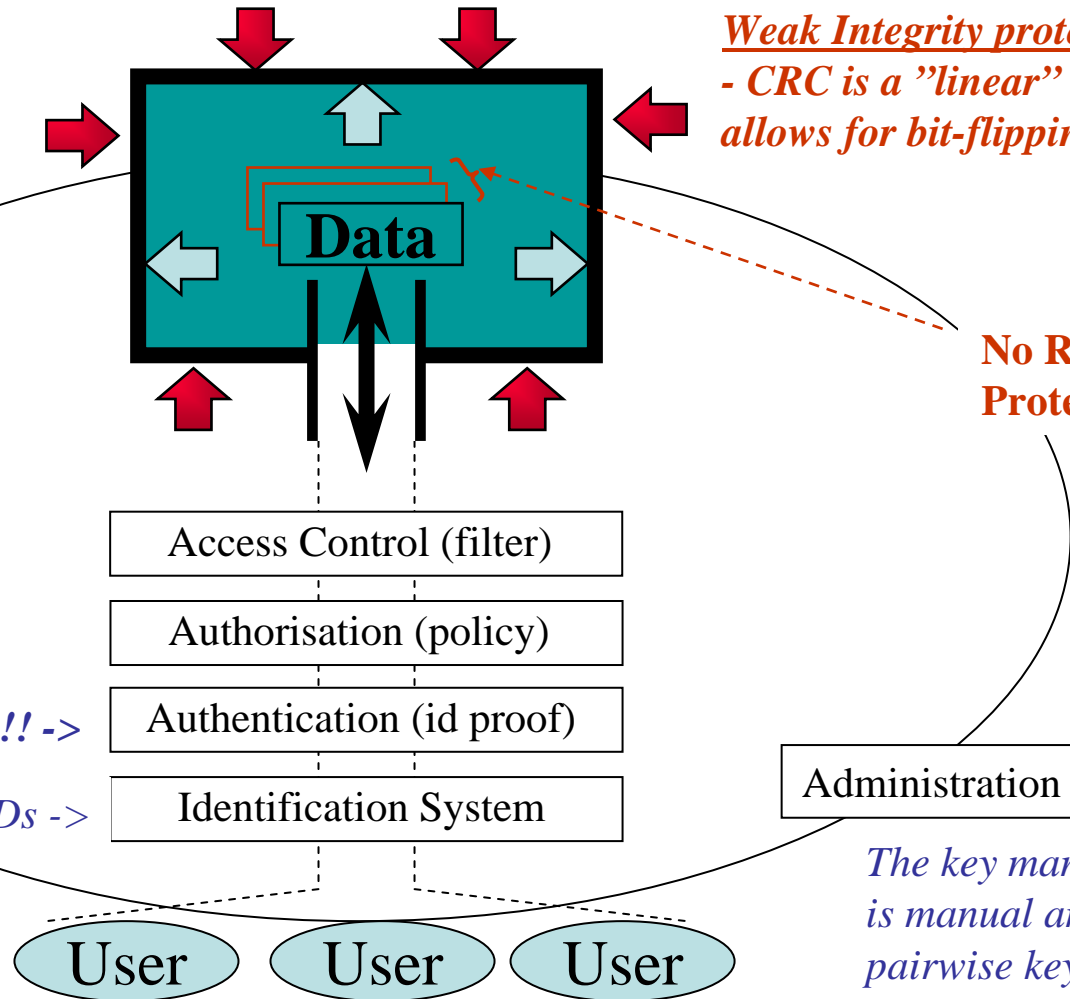
Denial of Service (DoS):

- Management messages are not protected

No Replay Protection

Dangerously insecure !!! ->

MAC addr. instead of user IDs ->



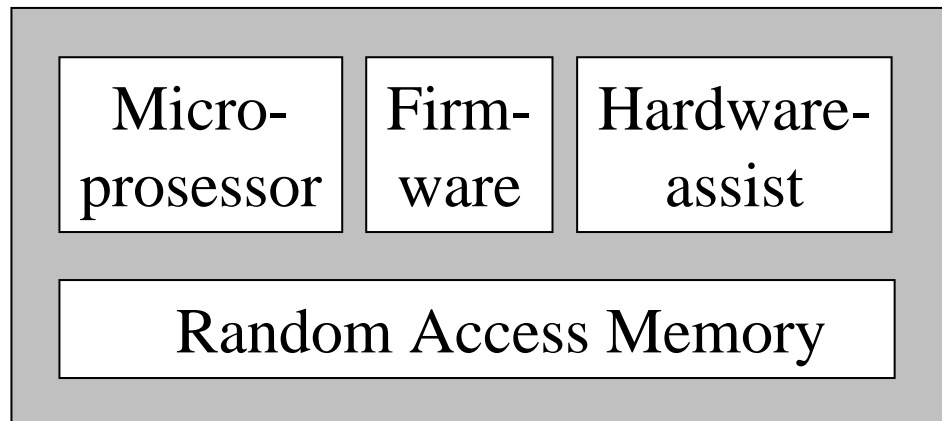
The key management is manual and pairwise keys are normally not used

Agenda for Security in WLAN

- A framework for security in WLAN
- Some solutions at layer 3 and above
- Solutions at layer 2
 - WEP
 - 802.11i: “Fixing WEP”
 - TKIP: Privacy & Integrity (Short-term fix)
 - 802.1x: Authentication
 - CCMP: Privacy & Integrity (Long-term solution)
 - 802.11w: Protection of Management Frames
- Security in Ad Hoc

What is TKIP?

- TKIP “fixes WEP” without requiring change in existing hardware
 - It reuses the RC4 encryption in hardware-assist
 - Simple pre-processing is done in the device driver



- TKIP is considered to have a high level of security

TKIP: "Fixing WEP"

Encryption:

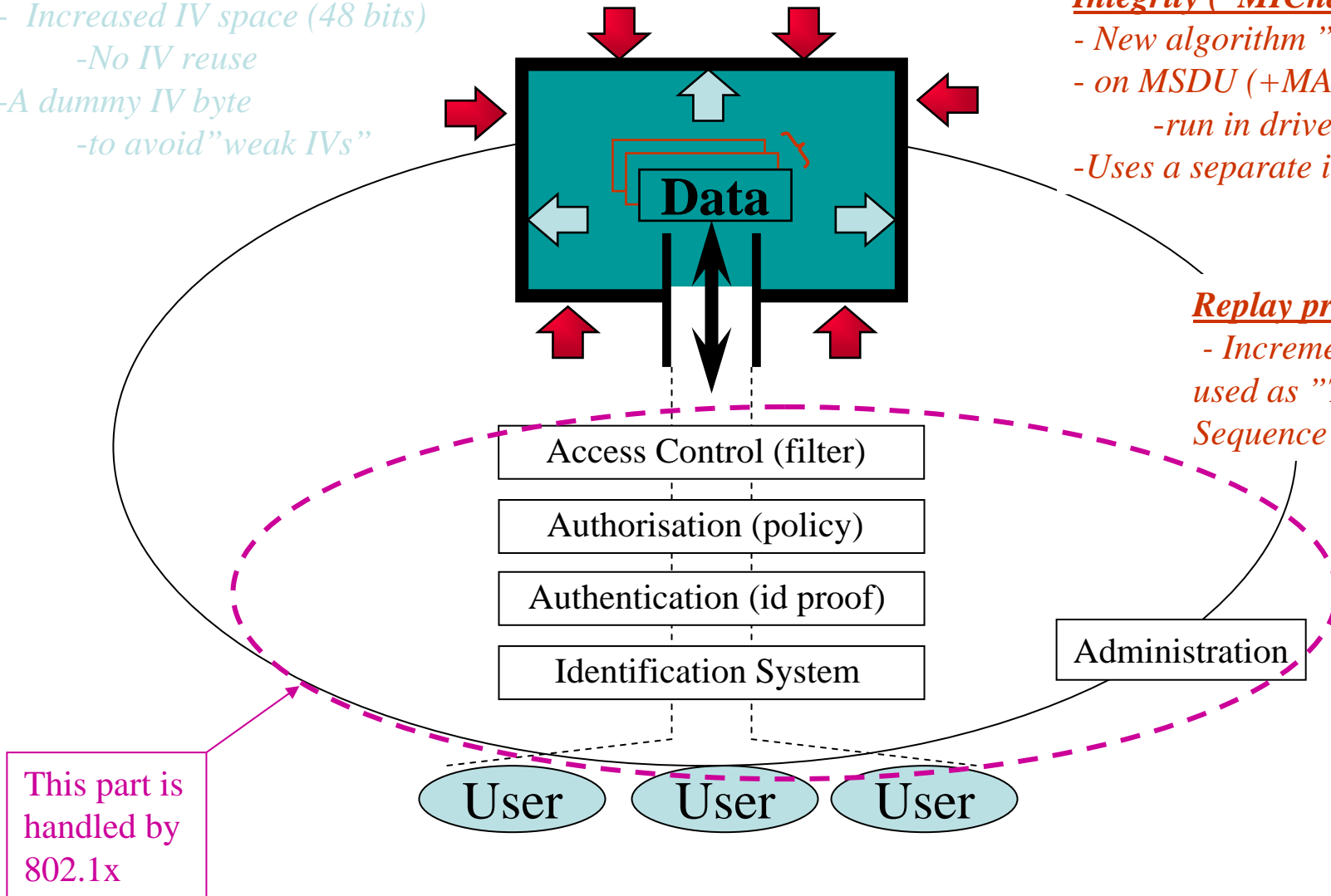
- Increased IV space (48 bits)
- No IV reuse
- A dummy IV byte
- to avoid "weak IVs"

Integrity ("MIChael"):

- New algorithm "MIChael"
- on MSDU (+MAC addresses)
- run in driver, compatible
- Uses a separate integrity key

Replay protection

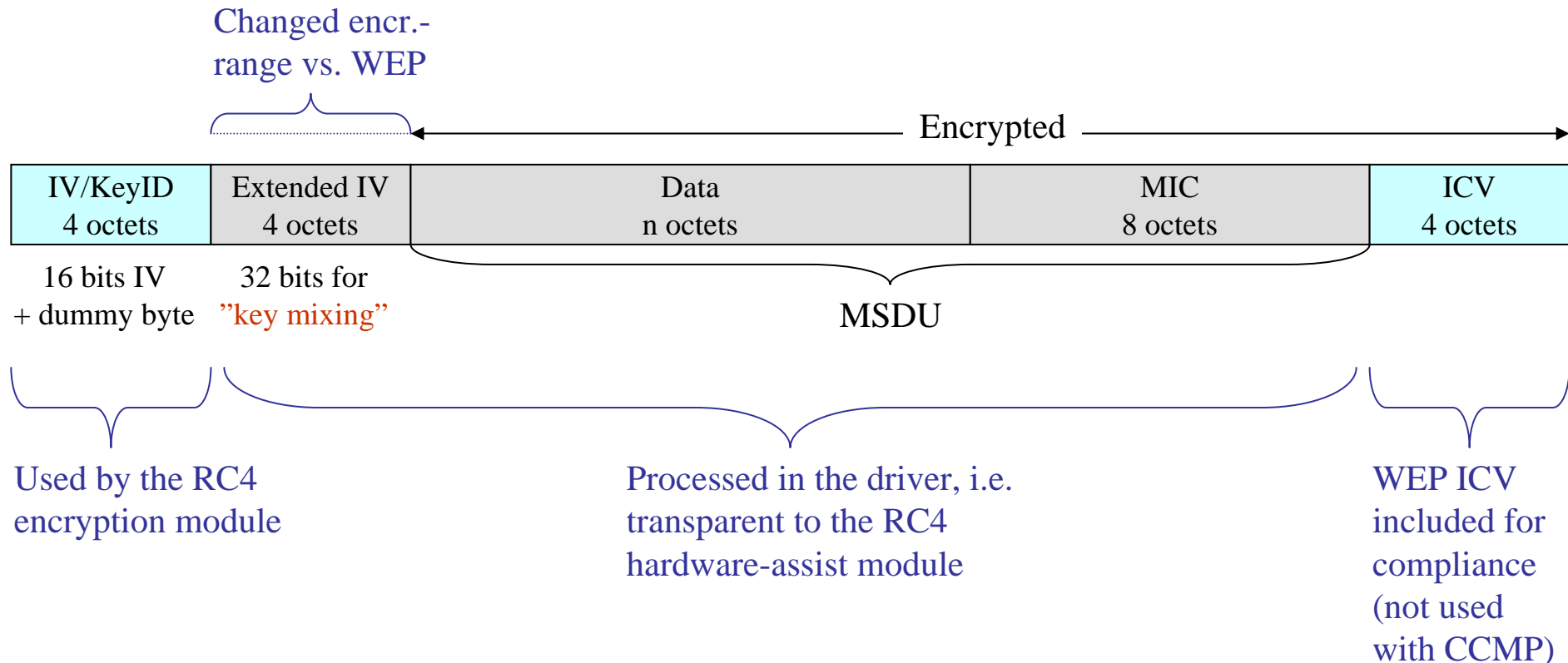
- Incrementing IV -
- used as "TKIP
- Sequence Counter"



This part is handled by 802.1x

TKIP runs “on top of” WEP

- A MAC frame is sent to the RC4 hardware assist...



- ...together with a the 40 bit secret key (from “key mixing”)
 - The 32 bits ICV comes into play by “mixing” the ICV and MAC-addresses, with 128 bits Data Encryption Key (from 802.1x EAP Authentication)
 - A 40 bit secret is produced. The secret changes with changing IV!
 - MAC address in key mixing -> IV-reuse only possible per source address

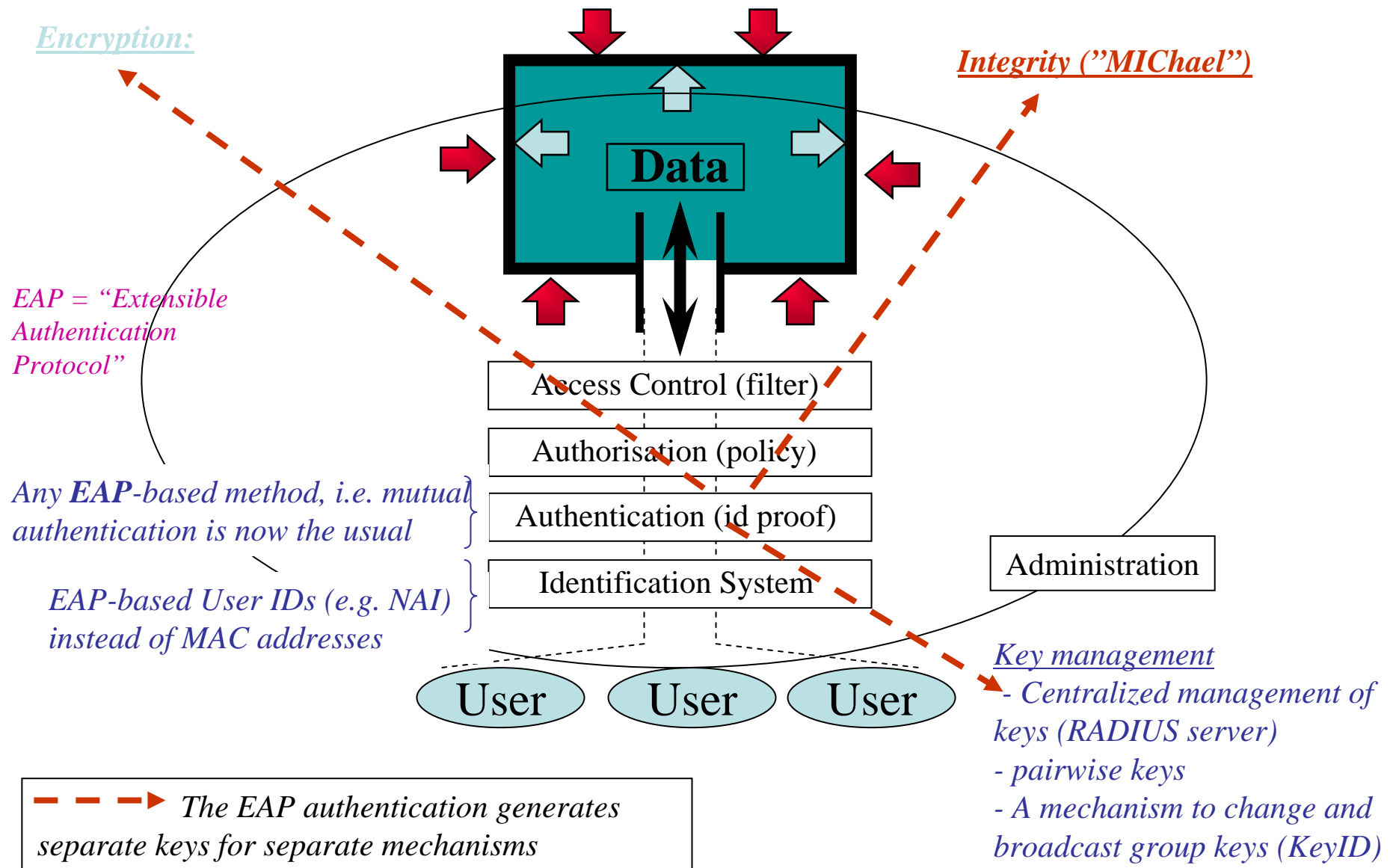
Michael DoS Weakness

- Michael is designed to be computed efficiently (xor, add, shift etc, and no multiplications) for weak processors
 - The 8 byte Message Integrity Code (MIC) corresponds only to 20 bits effective protection
 - Since Michael is weak, it needs additional “Countermeasures”:
 - If a MIC-error is detected, the link is shut down for 60 seconds.
- This makes DoS-attack possible, however, although hard:
 - The attacker must 1) stop the packet transmission, 2) use the same TKIP sequence number, to avoid that the packet is dropped as “Out-of-Sequence”, 3) change the MIC-field, and 4) re-calculate the ICV
- Thus, there are easier ways to launch a DoS attack
 - e.g. by sending Disassociate-messages on behalf of other STAs

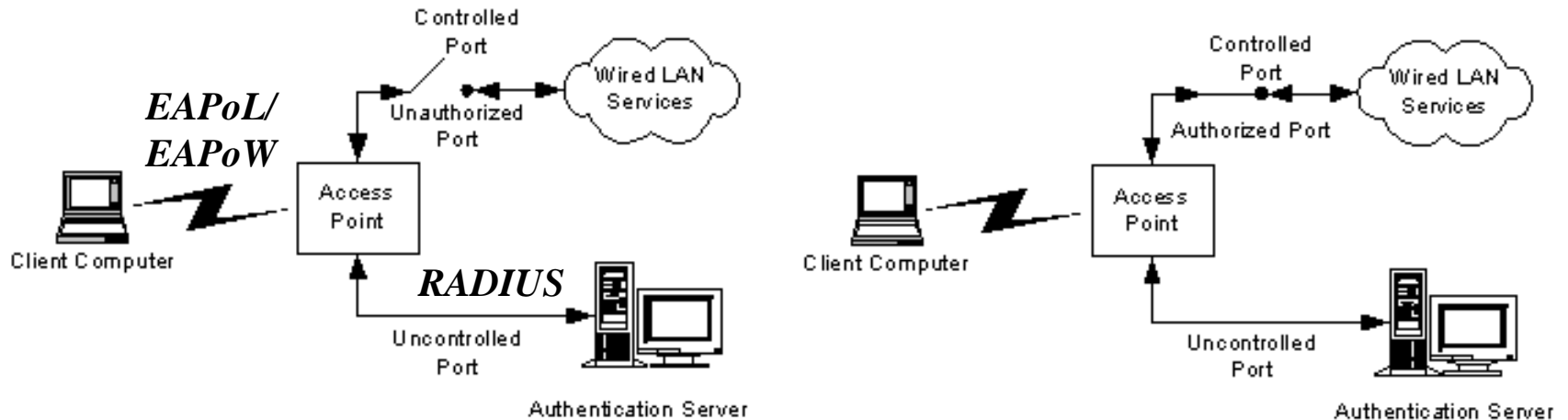
Agenda for Security in WLAN

- A framework for security in WLAN
- Some solutions at layer 3 and above
- Solutions at layer 2
 - WEP
 - 802.11i: “Fixing WEP”
 - TKIP: Privacy & Integrity (Short-term fix)
 - 802.1x: Authentication
 - CCMP: Privacy & Integrity (Long-term solution)
 - 802.11w: Protection of Management Frames
- Security in Ad Hoc

802.1x: Fixes the authentication problem of WEP



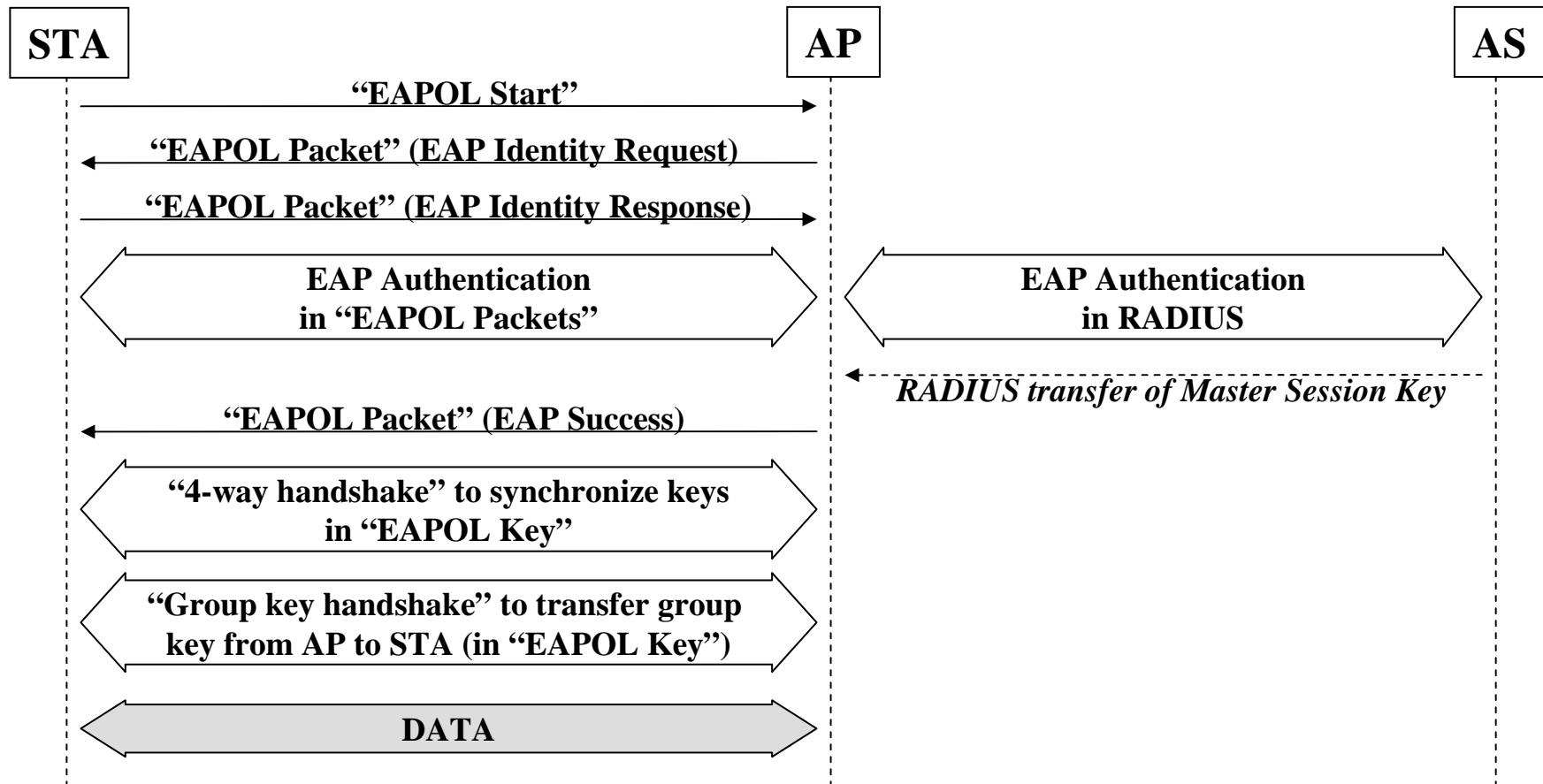
802.1x with 802.11i



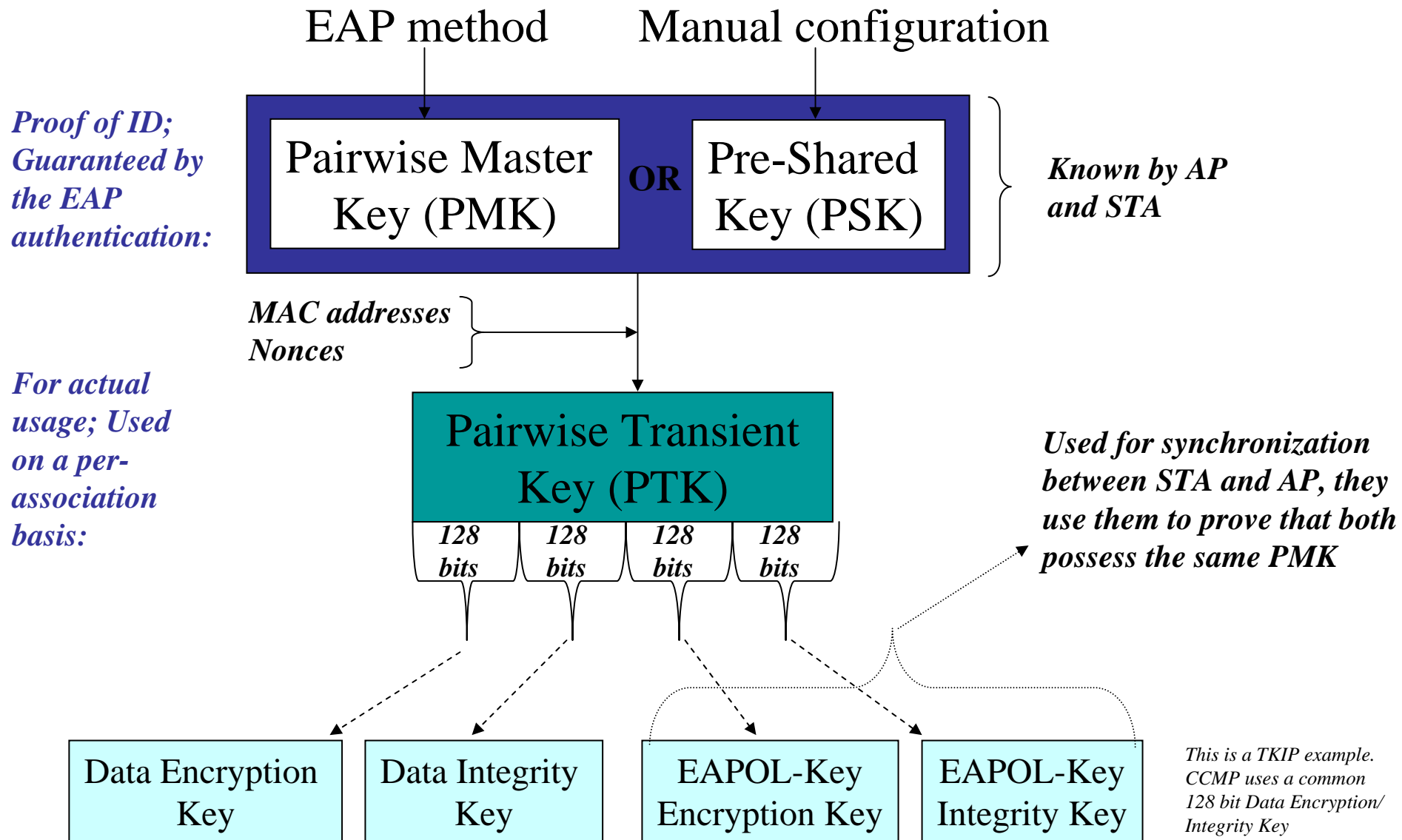
- EAPoL is extended to allow group keys (generated by AP) be transferred to the STAs
- RADIUS is extended to allow the AP to transfer the Master Session Key to the AP
 - Because the EAP authentication happens directly between STA and AS

802.11i handshake with 802.1x

- Security is negotiated using information elements in Beacon/Probe response and association messages.
 - Open Systems Authentication is used
- 802.1x follows the association response:



Pairwise key hierarchy of 802.1X



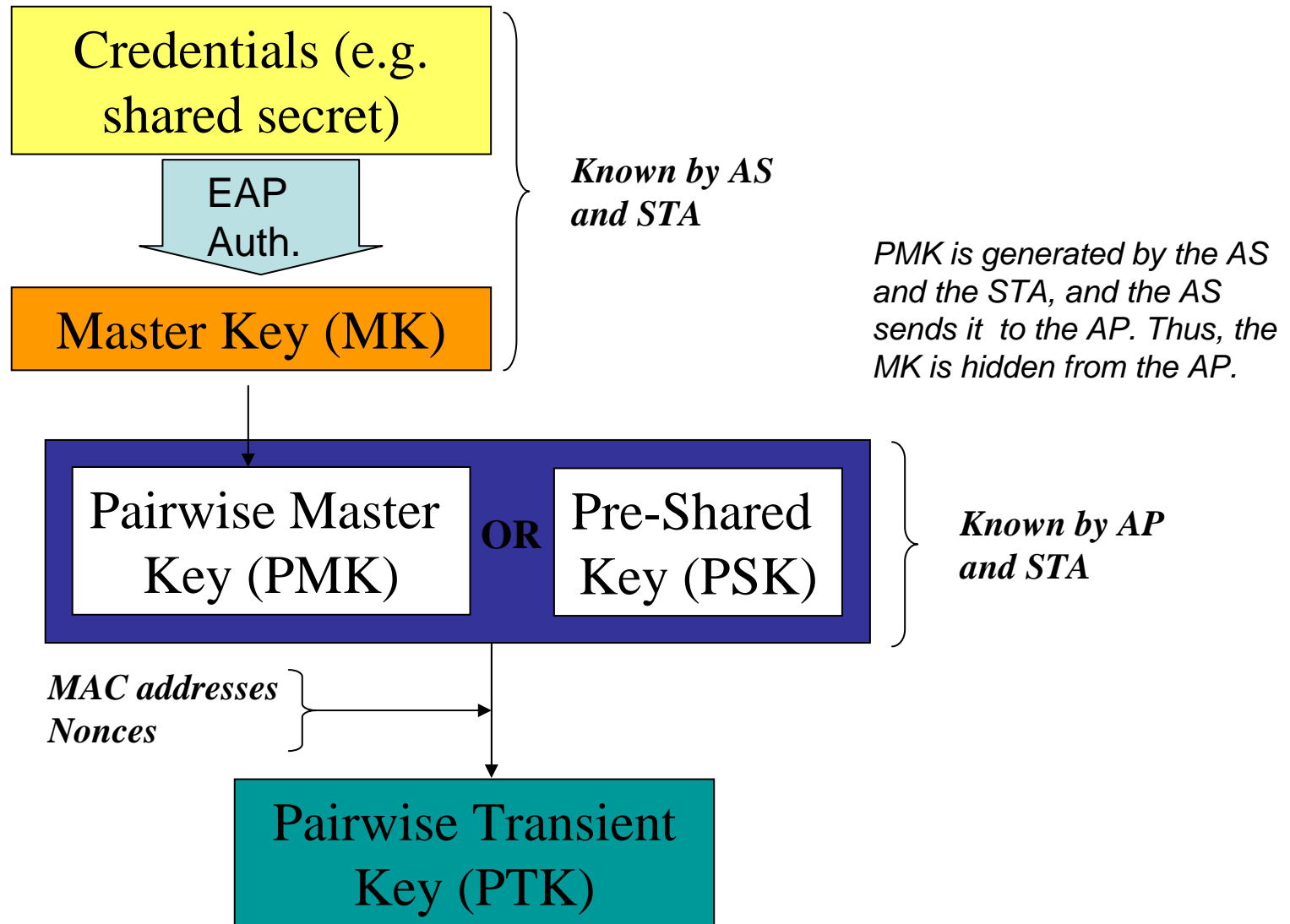
EAP is used to derive the PMK

Proof that ID corresponds to user

Key valid per-authentication session. E.g. for access control.

Proof of ID; Guaranteed by the EAP authentication:

For actual usage; Used on a per-association basis:



Group key hierarchy of 802.1X

*AP uses crypto-quality
Random Number
Generation*

*256
bits*

**Group Master
Key (GMK)**

*Known by AP
and STAs*

*AP's MAC address
Nonce from the AP*

**Group Transient
Key (GTK)**

*128
bits*

*128
bits*

**Group Encryption
Key**

**Group Integrity
Key**

*This is a TKIP example.
CCMP uses a common
128 bit Group Encryption/
Integrity Key*

*Used to transfer securely to the STAs a new
Group Key + KeyID generated by the AP*

Integration of 802.1x with 802.11

- AP advertises security options in probe response
 - Only placed in probe response if STA explicitly asks for it in the probe request
- STA chooses between the security options
 - Association request
- AP accepts or rejects in association response
- If accepted, the 802.1x / EAP message exchange follows subsequently

Upgrade with animation

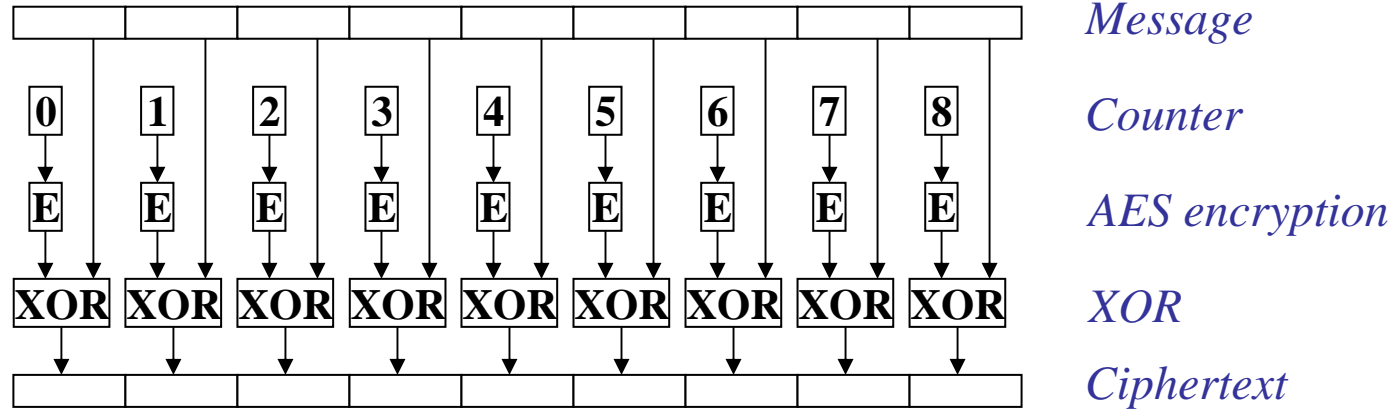
Agenda for Security in WLAN

- A framework for security in WLAN
- Some solutions at layer 3 and above
- Solutions at layer 2
 - WEP
 - 802.11i: “Fixing WEP”
 - TKIP: Privacy & Integrity (Short-term fix)
 - 802.1x: Authentication (Permanent fix)
 - CCMP: Privacy & Integrity (Permanent fix)
 - CCMP:
 - » Encryption: “Counter Mode”
 - » Integrity: “CBC-MAC”
 - 802.11i-specific use of CCMP
 - 802.11w: Protection of Management Frames
 - Security in Ad Hoc

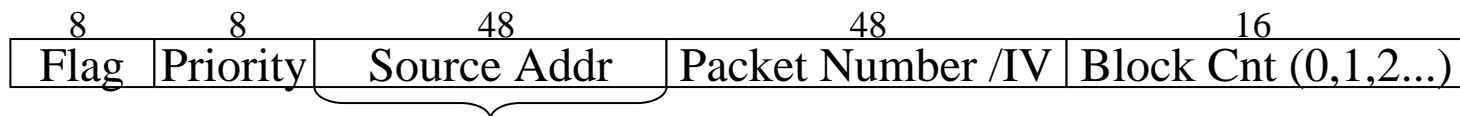
AES - Counter Mode Encryption

AES = "Advanced Encryption Standard"

- Cipher Block Chaining



The counter used:



Since 2 parties are using the same key

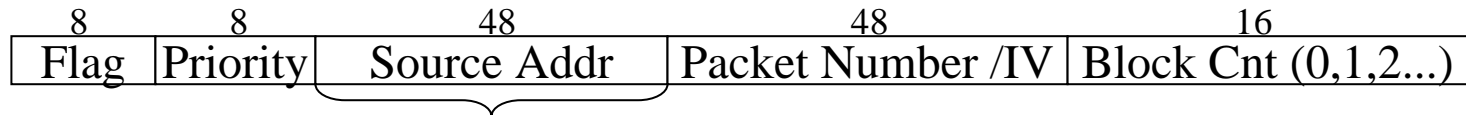
- Compelling characteristics of "Counter Mode"
 - Encryption and decryption is the same process (double XORing)
 - Counter values are known in advance
 - Parallel processing / pre-processing is possible

CBC – MAC for integrity

1. Initialization: Encrypt a unique counter-block with AES
 1. Uniqueness: The counter is set as [1 + the counter used to encrypt the last block of the packet]
 - Integrity is thus cryptographically separated from the encryption
 - Thus, same key can be used for both Integrity and Encryption
 2. XOR the result with the first message block, and then encrypt the result with with AES
 3. XOR the result with the second message block, and then encrypt the result with AES
 4. XOR the result with the next block, and then encrypt that... and so on.
- The integrity protection covers parts of the packet not covered by the encryption
 - Compatible with Counter Mode Encryption... but cannot run in parallel

802.11i-specific use of CCMP

- Subsequent blocks (and packets) are cryptographically separated by the encrypted counter:



*Since 2 parties are
using the same key*

- The first encrypted block of CBC-MAC is:



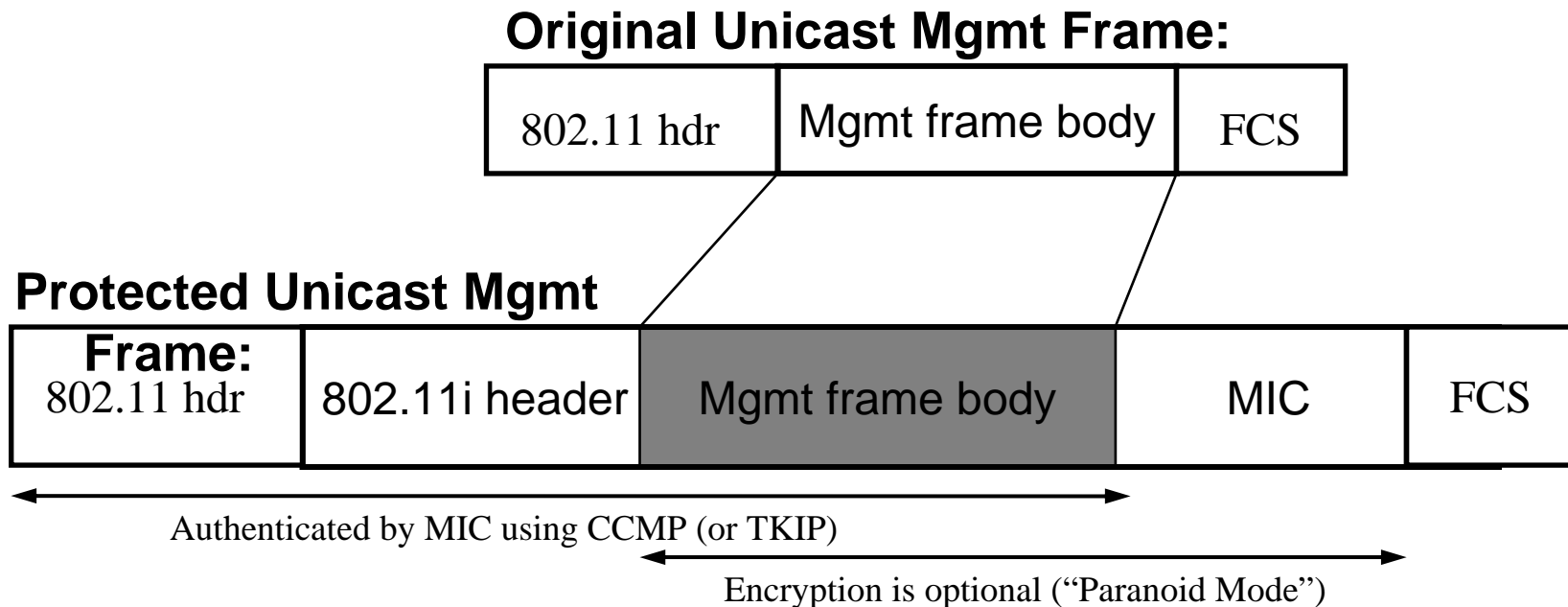
- I.e. Counter Mode and CBC-MAC are crypto independent
 - Thus, a common key for both encryption and integrity can be used
- The integrity protection covers parts of the packet not covered by the encryption
 - It includes the MAC-header, except the “mutable fields” that are changed right before transmission

Agenda for Security in WLAN

- A framework for security in WLAN
- Some solutions at layer 3 and above
- Solutions at layer 2
 - WEP
 - 802.11i: “Fixing WEP”
 - 802.11w: Protection of Management Frames
- Security in Ad Hoc

802.11w: Reuse 802.11i to protect Mgmt Frames after key establishment

- Messages: *Deauthentication, Disassociation, Action* Frames (of .11e and .11h). *Re-association* delegated .11r / TGr



- Need also to solve "lockout problem" if key state is lost
- Similar scheme for the protection of broadcast also proposed

Agenda for Security in WLAN

- A framework for security in WLAN
- Some solutions at layer 3 and above
- Solutions at layer 2
- Security in Ad Hoc

Security in an IBSS

- IBSS: Ad Hoc mode, but here only one hop!
- 802.11i (i.e. TKIP/CCMP and 802.1x) is also used in IBSS
- However, the authentication process differs slightly
 - Roles:
 - A STA takes the role of both a supplicant and an authenticator
 - A STA might also take the role of an AS.
 - Keys:
 - Each pair of STAs in the IBSS needs to form a pairwise key for the unicast traffic they are exchanging.
 - Each STA also need to form a group key for all multicast/broadcast traffic it is transmitting, and to convey this key to all each neighbours.
- The same Authenticator Key State-Machine is used,
 - 4-way handshake for the initial key establishment
 - The 4-way handshake is done in each direction between a pair of STAs
 - This means that a group key (for broadcast) is conveyed in each direction
 - However, it gives two pairwise keys between each node for unicast traffic – only one is needed!
 - The 4-way handshake initiated by the STA (of the two STAs) with the highest MAC address, gives the pairwise key to be used for the unicast traffic

Backup Slides

Security - at which layer?

- At a high layer:
 - High granularity
 - per-application, per-port, per-address etc.
 - Typically end-to-end
 - For the highest sublayers of L3, and above
 - Proxy/gateway can restrict the security to only the first hop(s)
- At a lower layer:
 - A general solution
 - providing security to all higher layers
 - Typically hop-by-hop
 - For the lowest sublayers of L3, and below

Some security attacks in WLAN

Snooping & Encr. attacks:

- Eavesdropping, tr.analysis
- Brute-force attacks
- Dictionary attacks
- Algorithmic attacks

Denial of Service (DoS):

- AP spoofing.
- Rogue managm. messages
- Jamming

Session hi-jacking, ARP redirects ->

Exploiting group keys ->

Brute Force, Dictionary, Encr.,
Man-in-the-middle (MITM)

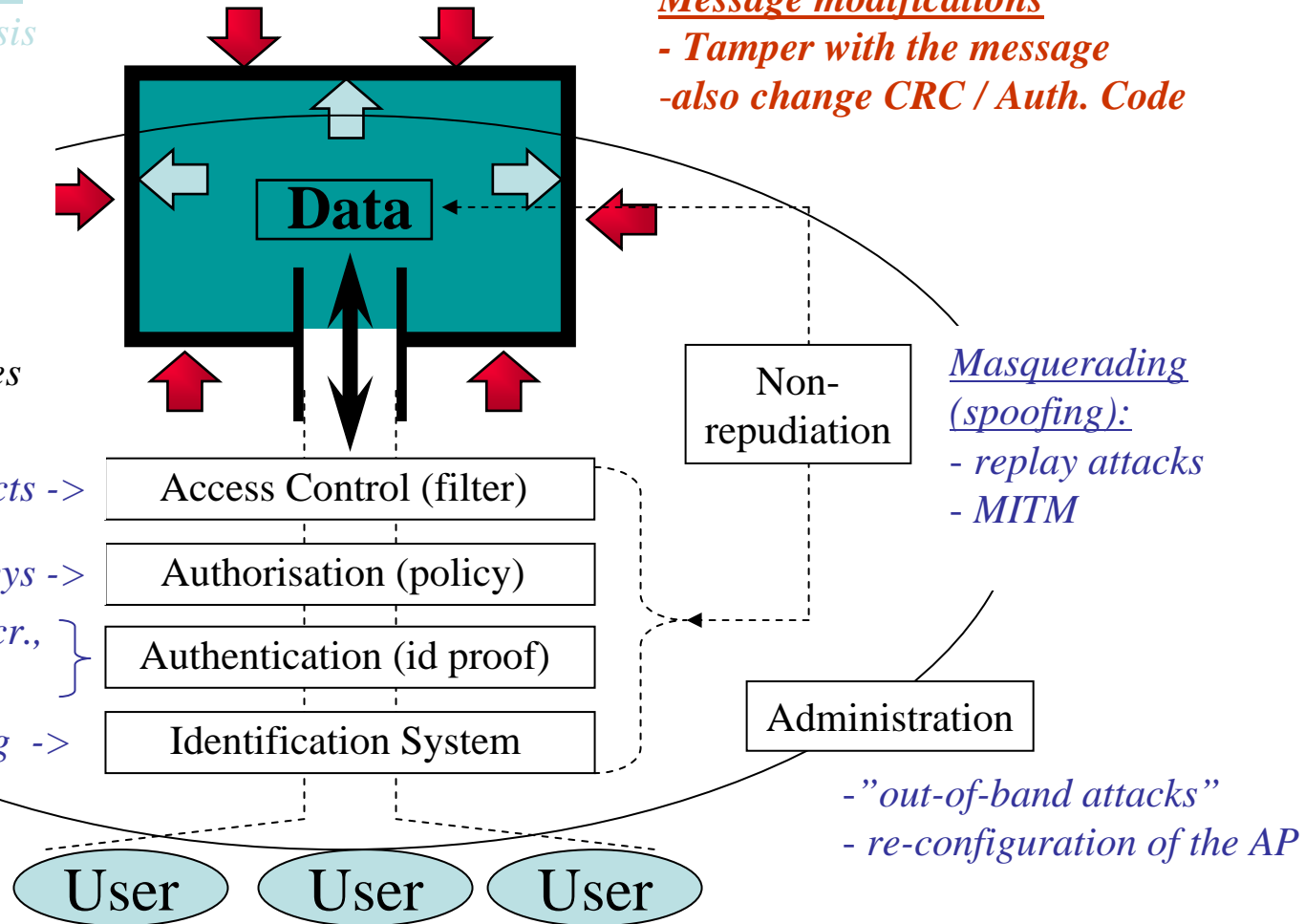
Masquerading ->

Message modifications

- Tamper with the message
- also change CRC / Auth. Code

Masquerading (spoofing):

- replay attacks
- MITM



- "out-of-band attacks"
- re-configuration of the AP

Enforcement of security

Encrypting data:

- symmetric key
- Block cipher
- Stream cipher
- public key

Attaching a proof to the data:

- Message Integrity Code (MIC)
- Signed hash, CRC, etc

DoS prevention:

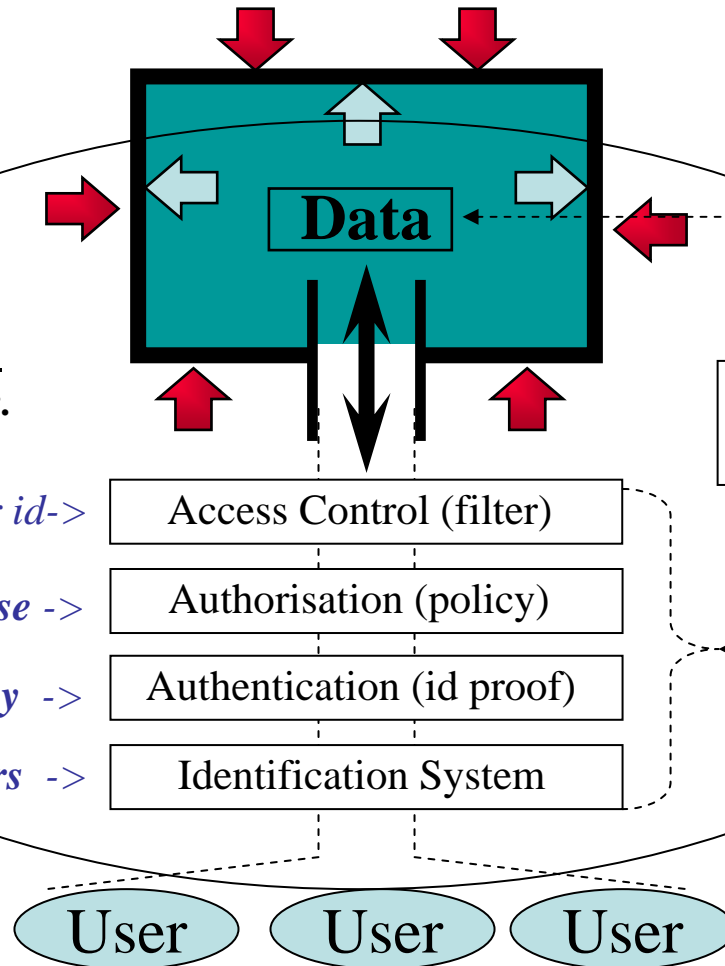
- e.g. cookies etc.

Filtering e.g. on address, SA or id ->

Checking with a policy database ->

E.g. proof by knowledge of key ->

A system of unique identifiers ->



Non-repudiation

- sequence no.
- timestamps
- public key sign.
- ...etc...

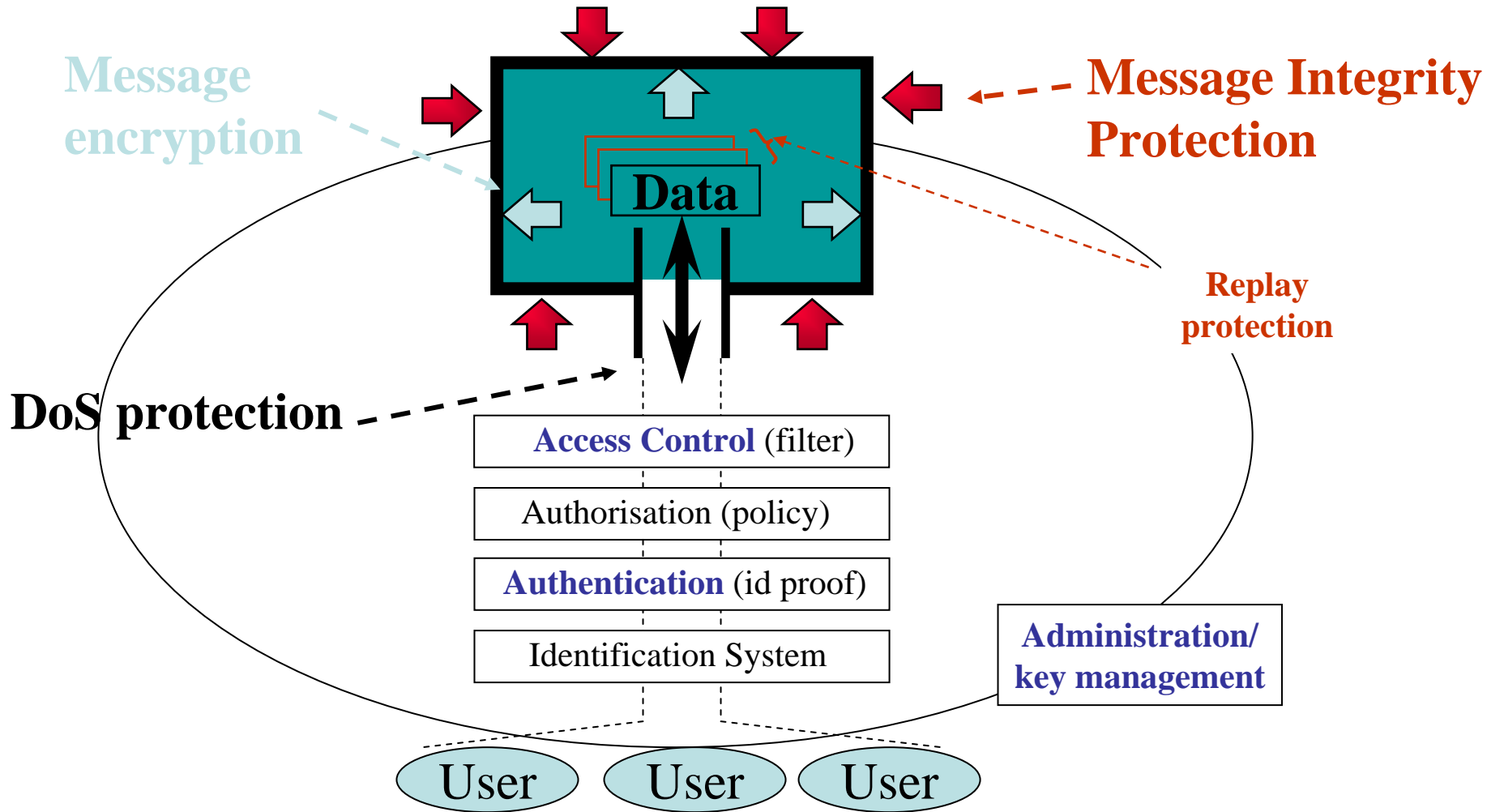
Administration

- id management.
- **key management !!!**
- logging of events
- organizational measures
- physical enforcement
- system configuration
- ... etc...

Simple methods

- No security is certainly the simplest
 - 802.11 with WEP turned off
- Additional "hurdles"
 - "Authentication"
 - Hidden SSID
 - Access control
 - MAC address filtering

How WEP works: The issues



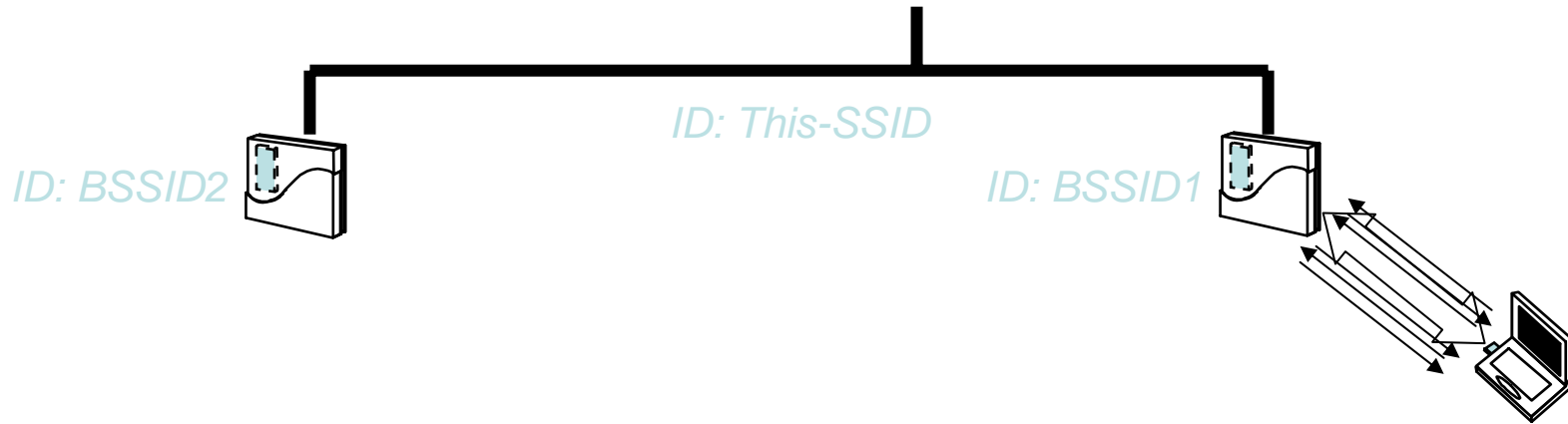
Secure access control not supported by WEP







- The authentication generates no secret token (e.g. integrity key) for subsequent access control
 - MAC address filtering is assumed
-

WEP provides no replay protection

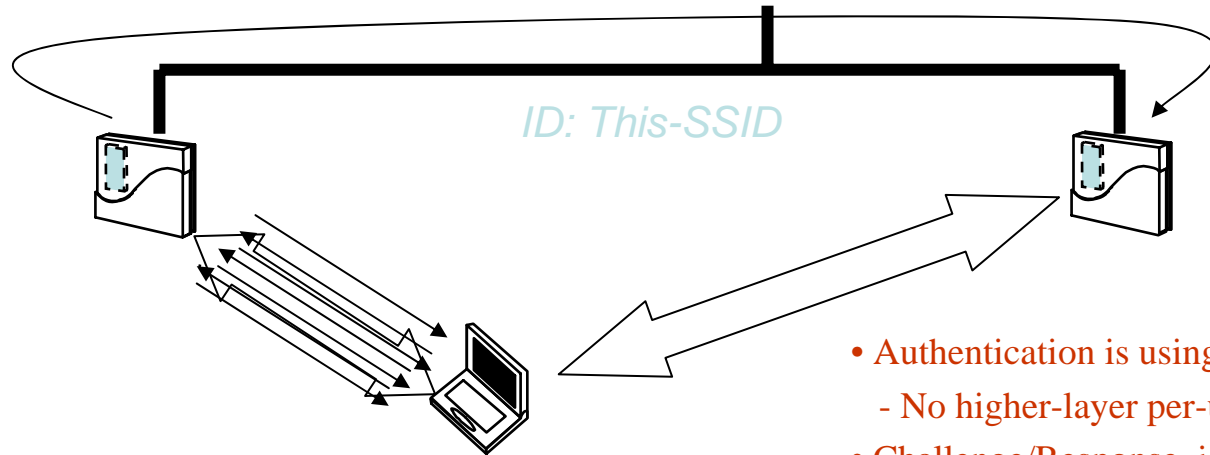
- The sequence number in the MAC header is not protected by the ICV
- Thus, an attacker can snoop a packet and re-send it
 - E.g. the packet may perform a server operation !

Scenario 1: No WEP authentication



1.  Probe_Request(SSID='/0', STA_rates)
 2.  Probe_Response(Timestamp, beacon_interval, AP_capabilities, SSID="This-SSID", AP_rates, PHY-parameters)
 3.  Authentication(Algorithm_no=0, sequence_no=0)
- "Open System Authentication": Authentication is required before association is possible*
4.  Authentication(Algorithm_no=0, sequence_no=3, Status_code=Success)
 5.  Association_Request(STA_capabilities, listen_interval, SSID="This-SSID", STA_rates)
 6.  Association_Response(AP_capabilities, Status_code = "Success", Association_ID, AP_rates)

Scenario 2: WEP authentication



- Authentication is using the MAC address as identifier
- No higher-layer per-user authentication
- Challenge/Response, i.e. AP not authenticated

1. 🖱️ DATA TRANSMISSIONS

2. 🖱️ Beacon(Timestamp, beacon_interval, AP_capabilities, SSID="This-SSID", AP_rates, PHY-parameters, etc...)

3. 🖱️ Authentication(Algorithm_no=1, sequence_no=0)

4. 🖱️ Authentication(Algorithm_no=1, sequence_no=1, Challenge="abcdefgh")

5. 🖱️ Authentication(Algorithm_no=1, sequence_no=2, Challenge=RC4(key, "abcdefgh"))

6. 🖱️ Authentication(Algorithm_no=1, sequence_no=3, Status_code=Success)

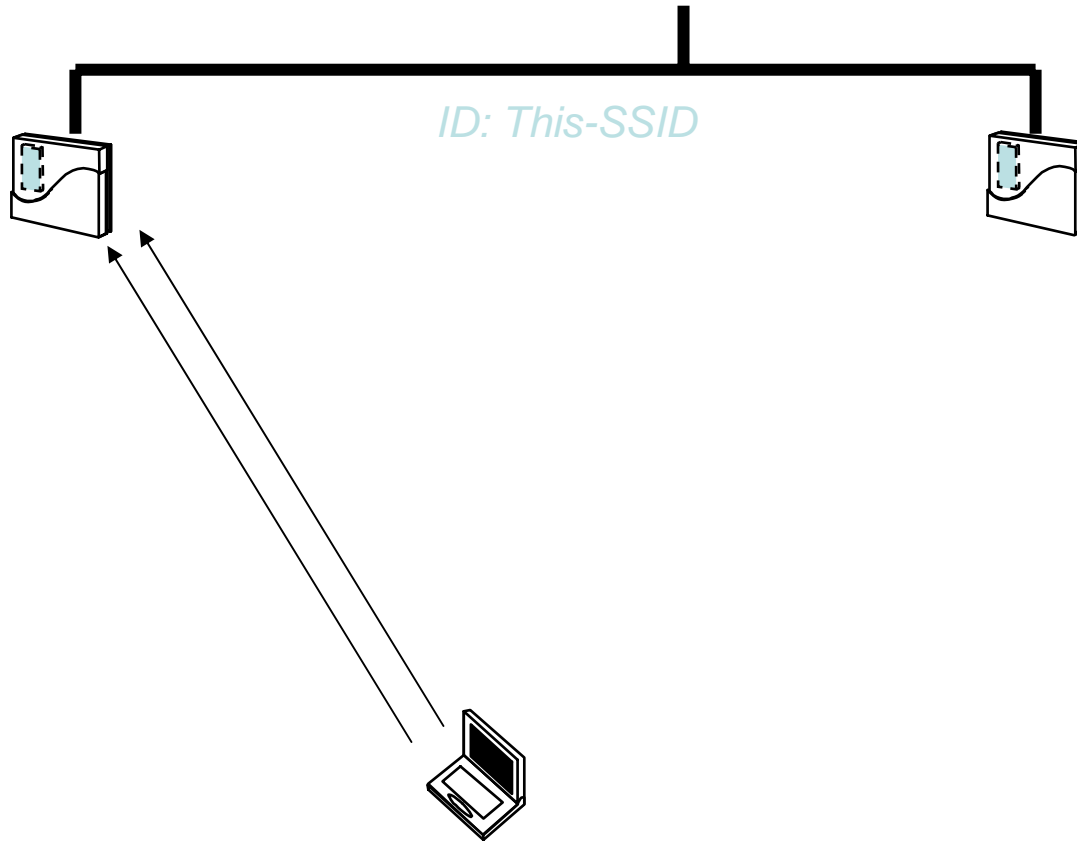
7. 🖱️ Re-Association_Request(STA_capabilities, listen_interval, SSID="This-SSID", STA_rates, Current_AP_Address)



8. 🖱️ Reassociation message sent to Current_AP_Address using IAPP or proprietary protocol

9. 🖱️ Re-Association_Response(AP_capabilities, Status_code = "Success", Association_ID, AP_rates)

10. 🖱️ DATA TRANSMISSIONS

Scenario 3: De-authentication



1.  Disassociation (Reason_code = 4 (i.e. "Disassociated due to inactivity"))
2.  Deauthentication (Reason_code = 3 (i.e. "Deauthenticated because STA is leaving"))

WEP integrity protection does not work

- An attacker can modify every bit he wants in the frame body and find an ICV that is consistent !!!
 - Property of CRC: A flipped bit in the frame body, results in a set of flipped bits in the ICV
 - The bit-flipping "survives" the RC4 encryption
 - Because bit-flipping "survives" the XOR operation!
 - The attacker can deliberately flip any bit in the frame body and ensure that the ICV is kept consistent with the change


Secure Neighbor Discovery (SeND) -I


- Neighbor Discovery (ND), IPv6 protocol to replace
 - Address Resolution (corresponds to IPv4's ARP)
 - Address Resolution is lifted up to a pure L3 protocol
 - Router Discovery (corresponds to ICMPv4's RA/RS)
 - IPv6 Address Autoconfiguration and Duplicate Address Detection (DAD)
 - Neighbor Unreachability Detection (NUD)
 - Redirect (to a better router, or directly to a node that is on-link)
- SeND mitigates the IPv6 counterpart to an ARP-spoofing attack

Secure Neighbor Discovery (SeND) -II

- It uses Cryptographically Generated Addresses (CGA)
 - A node constructs a public/private key-pair
 - A station encodes a hash of its public key into the interface identifier of the IPv6 address
 - Each ND message is signed (RSA) with the private key, and contains the public key
- Timestamp and Nonce options
- CGA chosed instead of Address Based Keys (ABK)
- SeND is a complex topic, that would require a full presentation by itself.

Important future challenges

-  Seamless mobility and roaming
 - Voice traffic requires fast handovers
 - The 802.11i authentication becomes a bottleneck
 - TGr (802.11r) will start studying this (Status: Sept. 2005)
 - Single Sign-On
 - Improving RADIUS for back-end signaling

-  Denial-of-Service (DoS) prevention
 - Improve various protocol weaknesses (e.g. EAP)
 - Protection of the management frames of 802.11
 - TGw (802.11w) has started working on this issue

Conclusion

- 802.11i will play an important role for securing WLANs in the coming future
 - Securing data frames
 - A basis for the protection of management frames (.11w)
 - I.e. 802.11i features will be compelling even for VPN and SSL solutions
- VPN and SSL solutions will probably also persist
 - To a larger extent for securing multi-hop access, and more seldomly for only securing the first hop

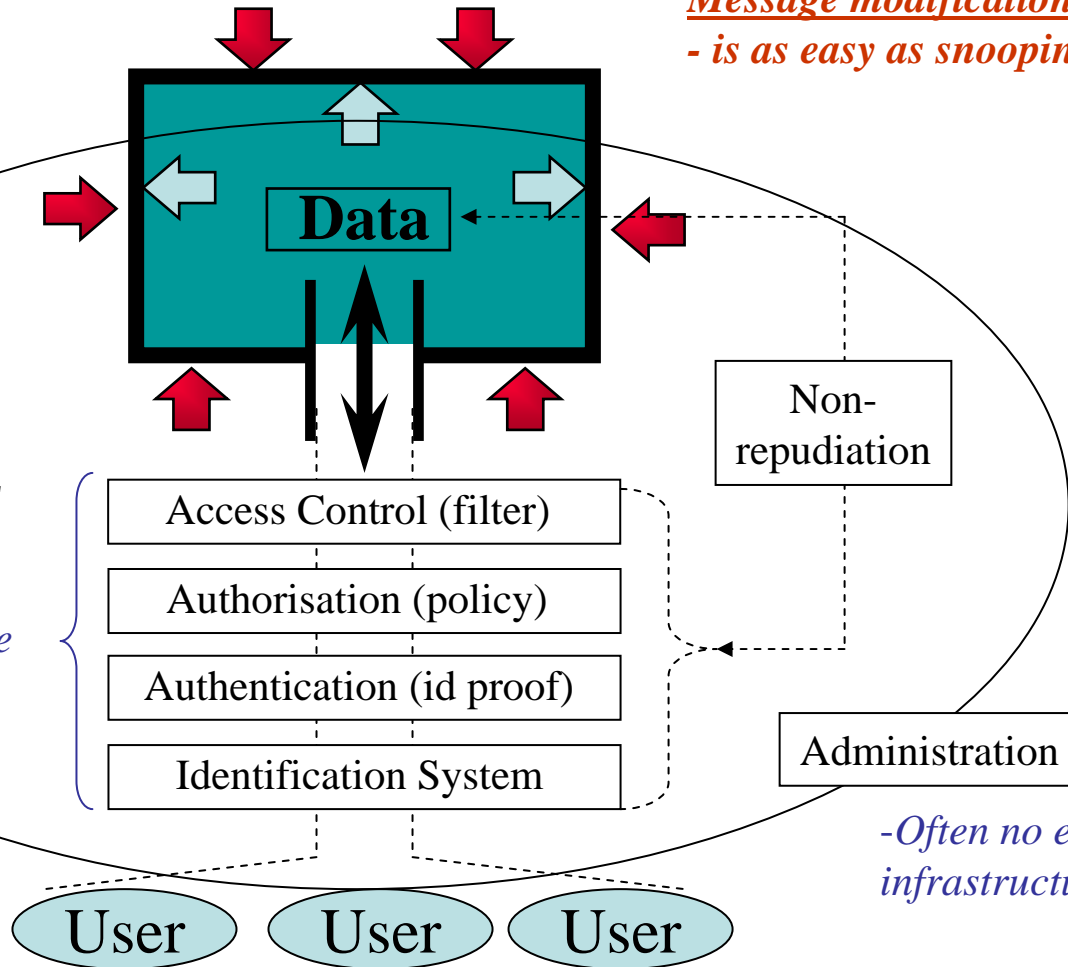
Security in Ad Hoc

Snooping is easy
-and efficient if the
the authentication
part is weak

Message modifications
- is as easy as snooping

Denial of Service (DoS):
Disrupt Routing - Nodes
depend on each other for
relaying
Battery Exhaustion Attacks
Jamming

Often no infrastructure



*-Often no existing
infrastructure*