heig-vd
HAUTE ÉCOLE
D'INGÉNIERIE ET DE GESTION
DU CANTON DE VAUD
www.heig-vd.ch

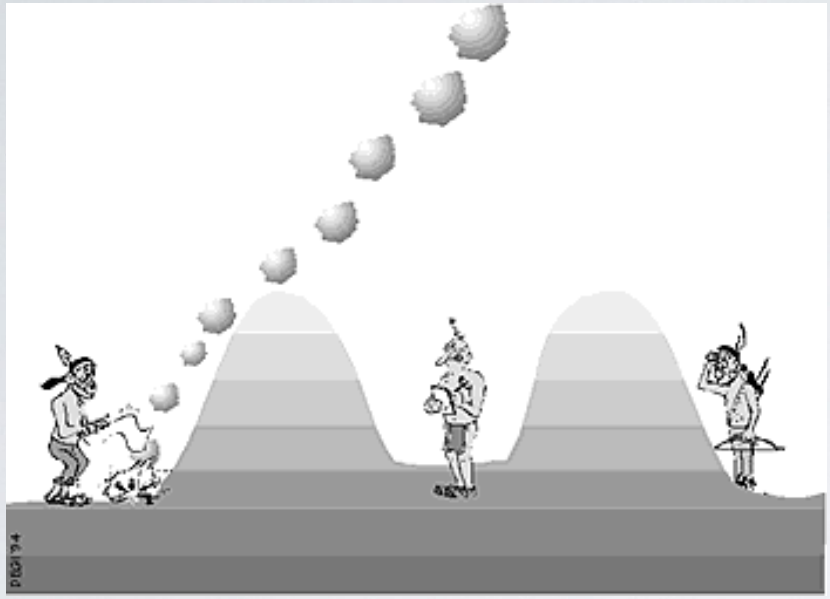
서울대학교 컴퓨터공학부
Seoul National University
Dept. of Computer Science and Engineering

Wireless Security - SU'19

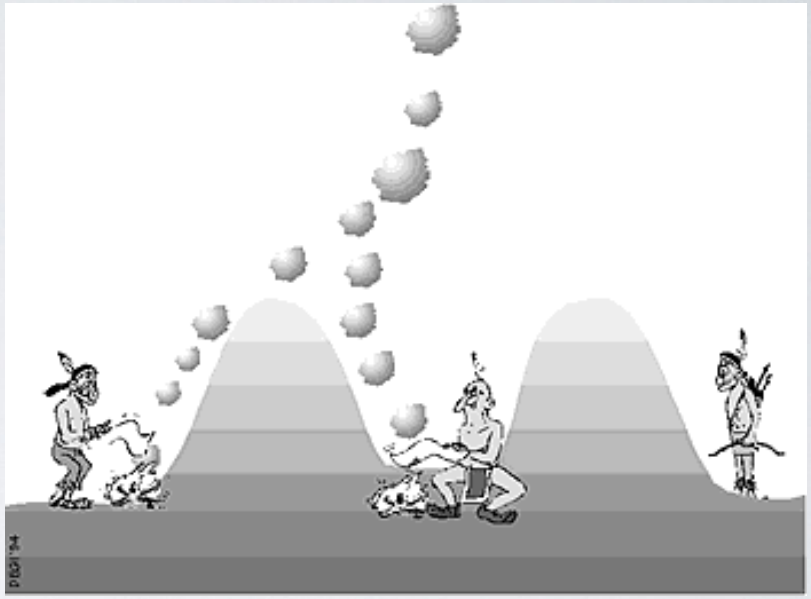
abraham.rubinstein@heig-vd.ch

Chapter II

Wireless Security - WEP

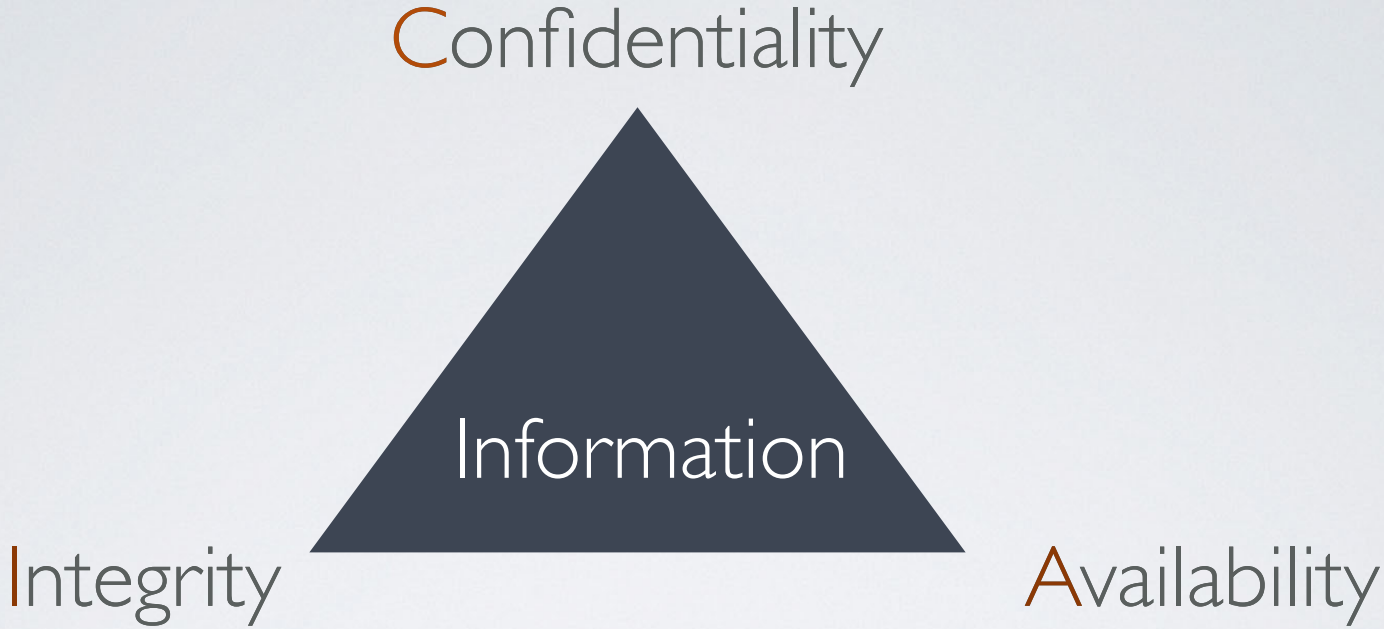


Confidentiality



Integrity

Authentication



CIA

Information Security

CIA Triad

Information Security

One of these three **cannot** be taken for granted in Wireless Networks

A. Confidentiality

B. Integrity

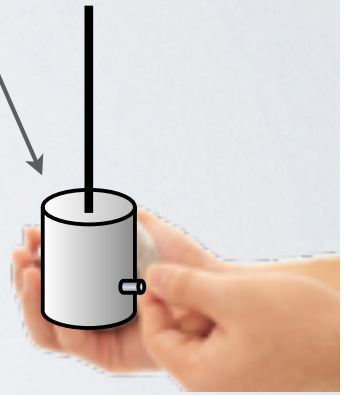
C. Availability

Attacking Availability

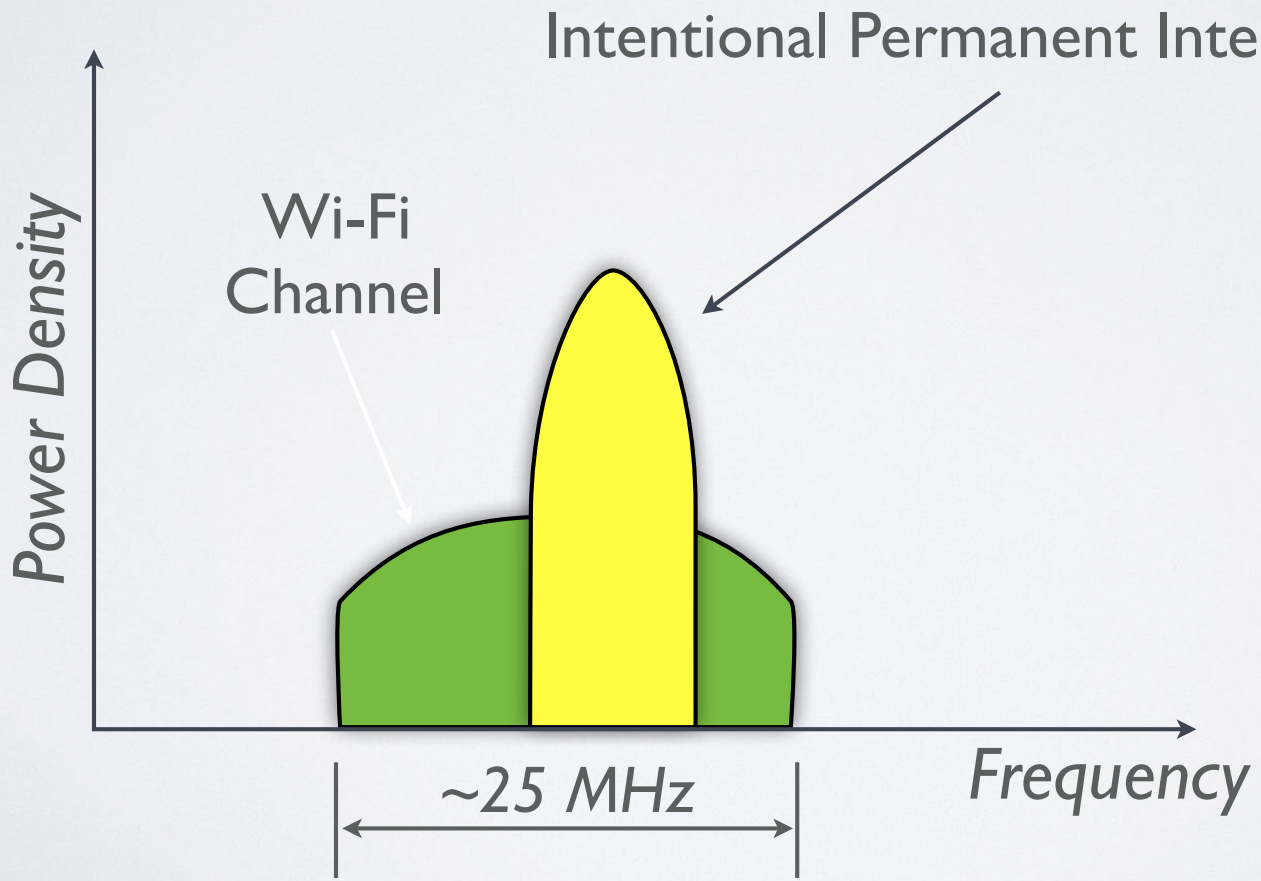
Denial of Service (DoS)

Physical Jamming

Blocking device

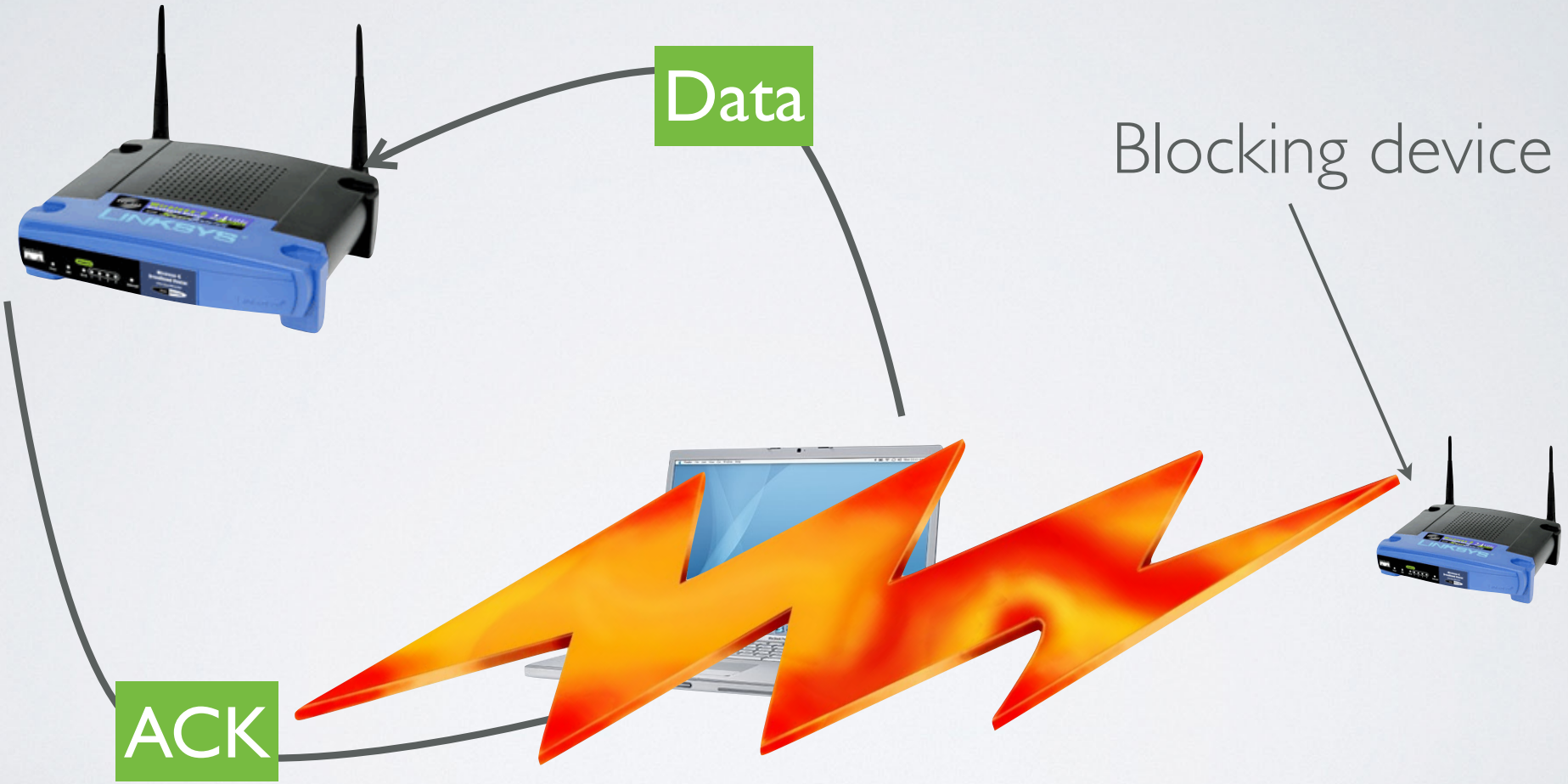


“Dumb” Physical Jamming

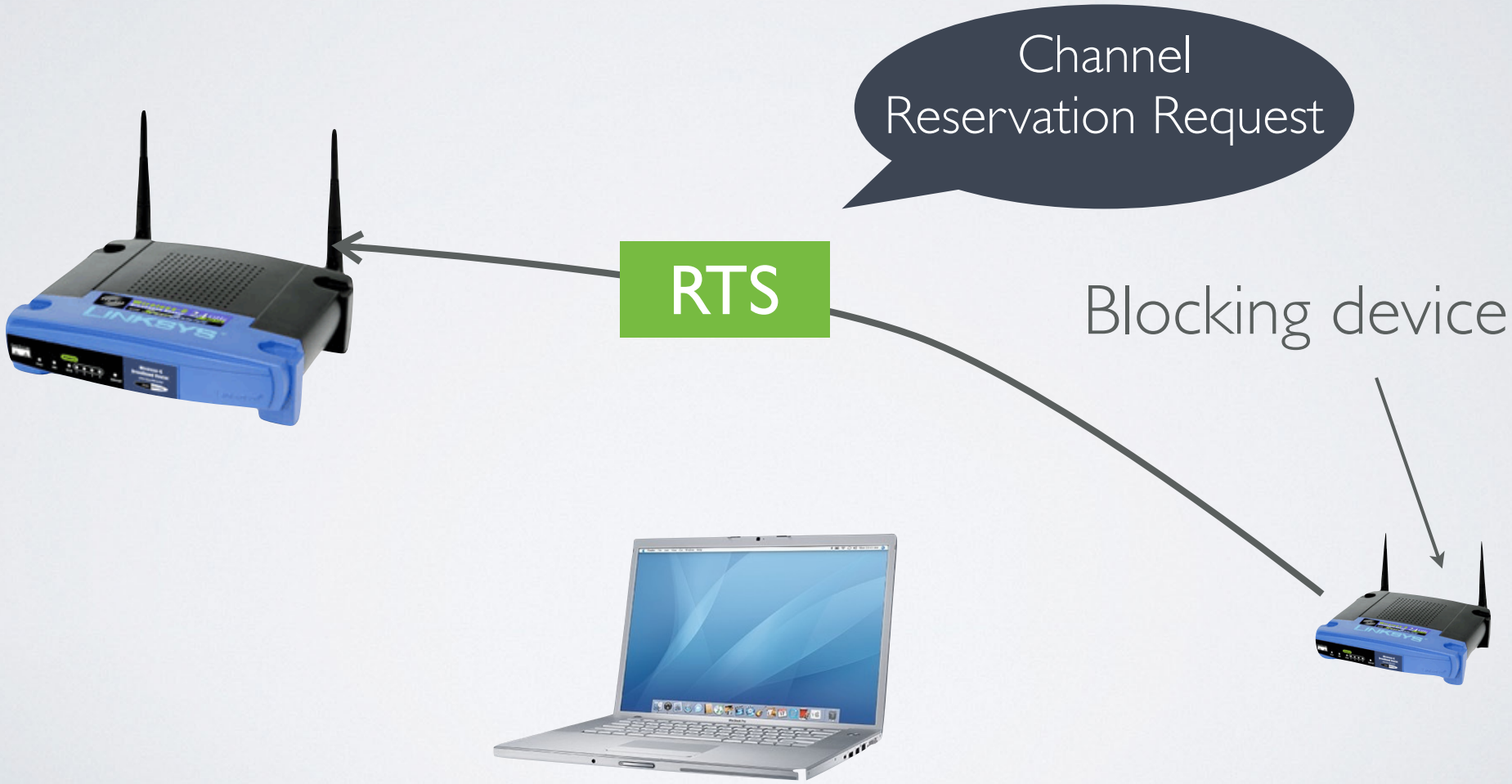


"Dumb" Physical Jamming

“Smart” Jamming



"Virtual" Jamming



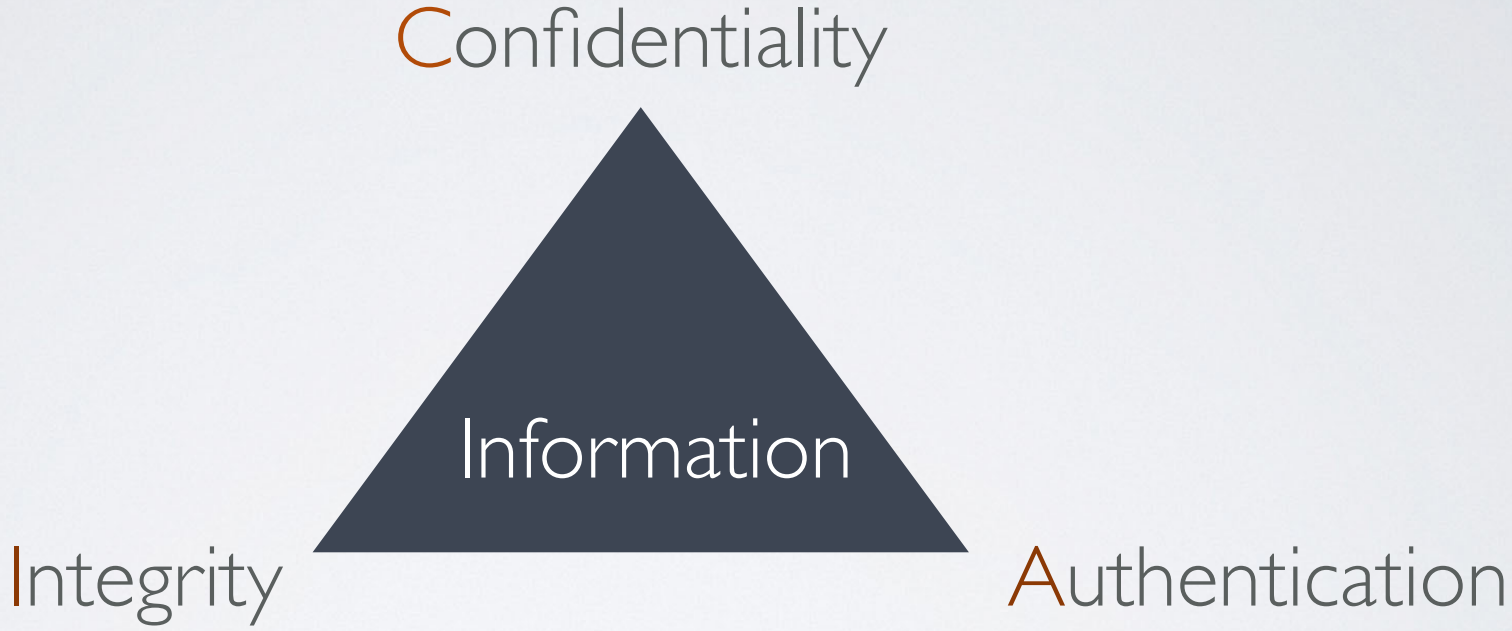
Fake Channel Beacon

Information Security

CIA

Cannot be taken for granted for 802.11 networks

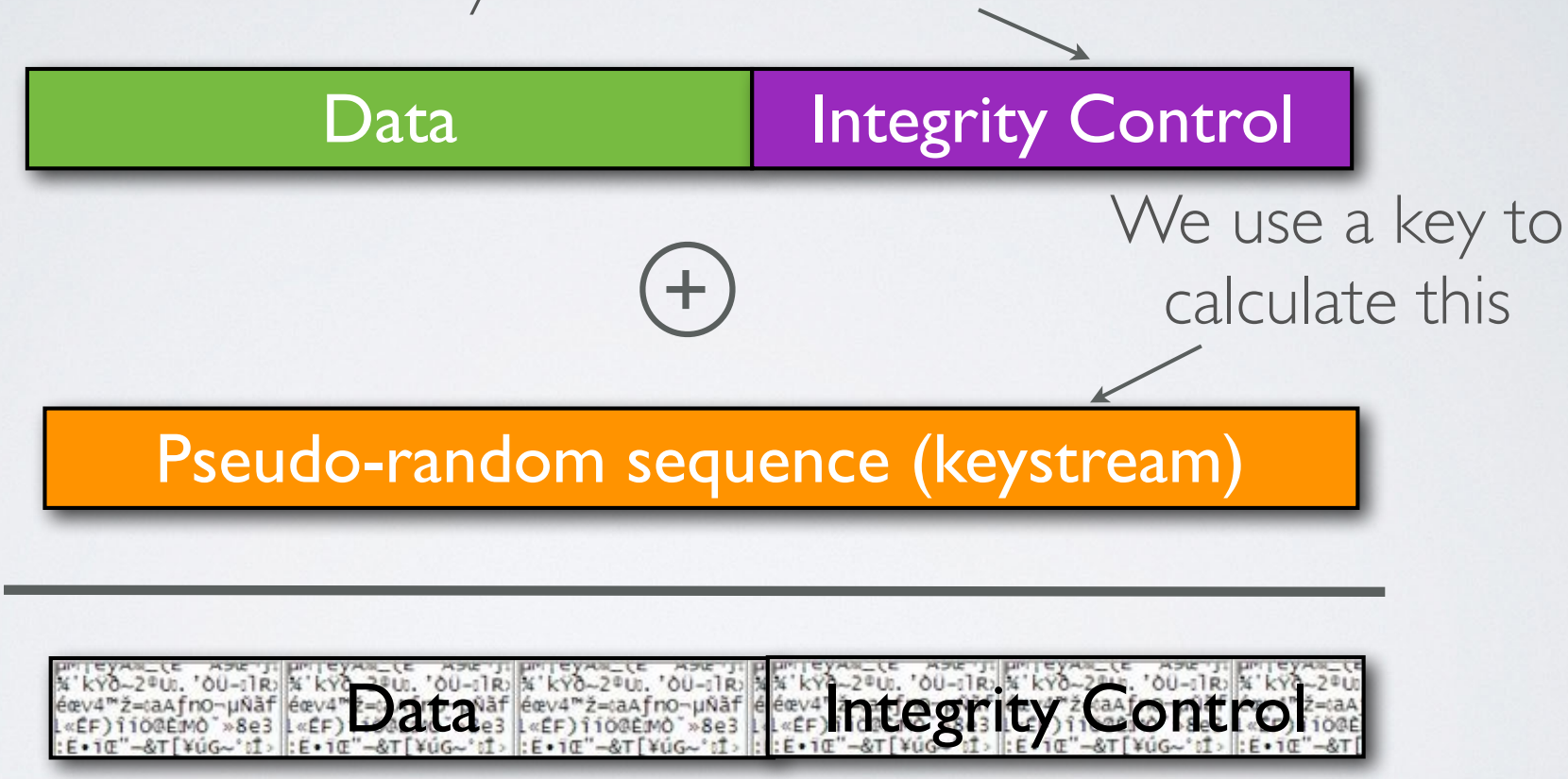
Information Security



C I A

Easy but Powerful Encryption

Ideally, we would use
a key to calculate this



Old, but Not So Old Security

WEP - Wired Equivalent Privacy

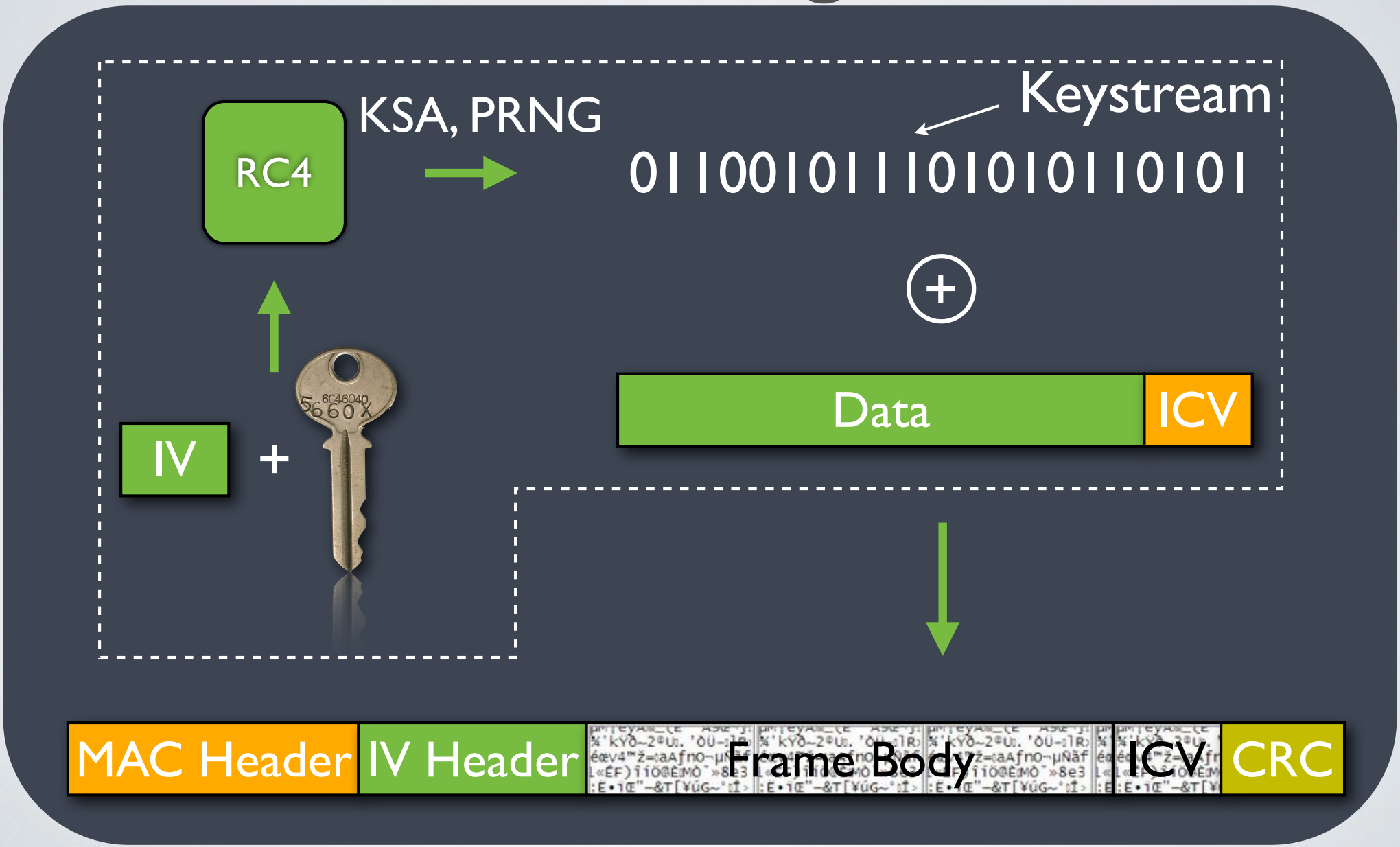
Security Before WPA

WEP (Wired Equivalent Privacy)

- Confidentiality
    - Data encryption using RC4
- Integrity
    - Integrity Check Value (ICV)
- Authentication
    - Optional: Shared Key Authentication
- Protection against re-injection
    - None

WEP and Confidentiality

THE WEP Algorithm



Shared Key

- Shared secret -- 40 bits or 104 bits
- Known by the AP and the authorised STAs
- Can be derived from a passphrase
- The conversion algorithm to go from passphrase ⟶ key is proprietary

Initialisation Vector

Initialisation Vector (IV) - 24 bits

2^{24} = 16'777'216 different combinations

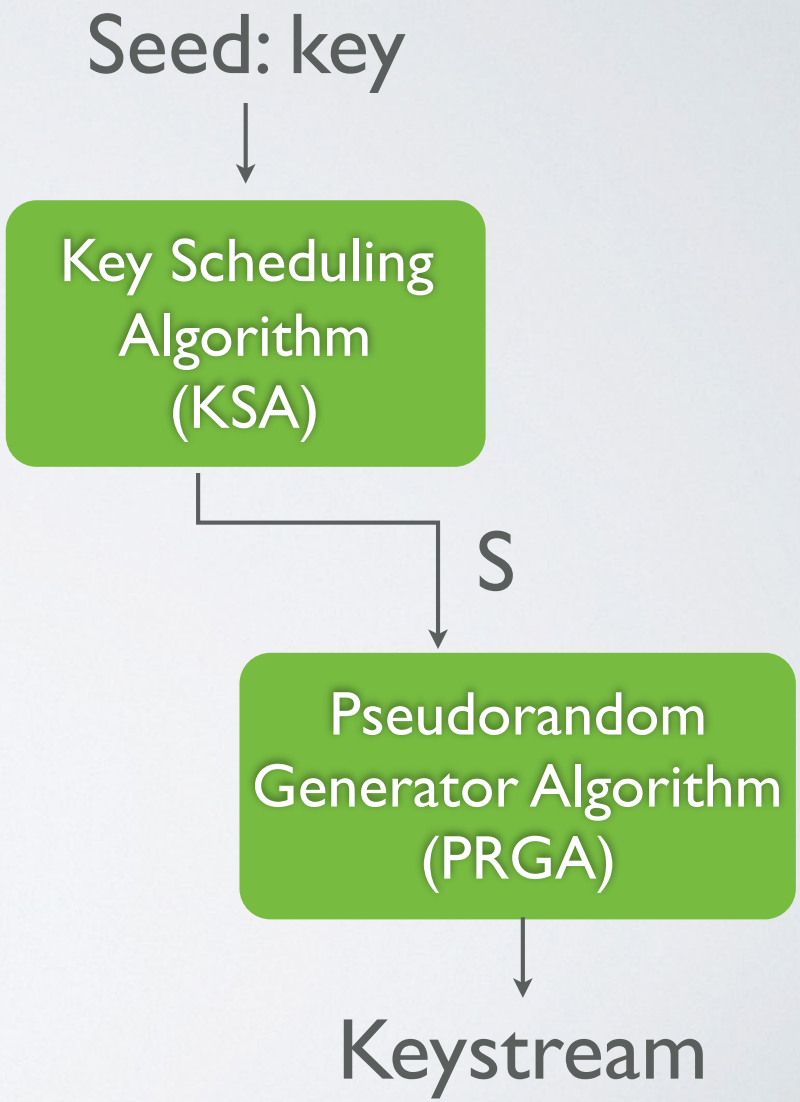
Supposed to make each encryption key "**unique**"

IV: Robustness

- The standard does not specify how to change/ treat the IVs
  - In principle, an IV that does not change, is compliant with the standard
  - In practice, many implementations increment monotonously from "0"
  - Collisions appear from the first messages

RC4

- Stream cipher
- Ron Rivest Cipher 4
- Created in 1987
- Leaked in 1994
- Extremely simple and fast
- Vulnerable to Keystream reuse



KEY = IV || WEP_KEY

KSA

Vector S :

0	1	2	3	4	5	6	...	...	254	255

Vector T :

K	E	Y	K	E	Y	K	Y	K

Pseudocode

```
j = 0
for i from 0 to 255
    j = (j+S[i]+T[i]) mod 256
    swap (S[i], S[j])
endfor
```

(0+0+67

(67+1+76

(144+2+69

(67))

(144))

(215))

Vector S :

67	144	215	...	...	...	...	...	...	...	...

PRGA

Scrambled Vector S :

67	144	215	…	…	…	…	…	…	…	…

Keystream (K):

…	…	…	…	…	…	…	…	…	…	…

Iterations

i = (0 + 1) mod 256 = 1
j = (0 + 144) mod 256 = 144
swap(S[1], S[144])
K = S[(S[1]+S[144]) mod 256] = …
…
…

Pseudocode

```
i = 0; j = 0
do while (required)
   i = (i + 1) mod 256
   j = (j + S[i]) mod 256
   swap(S[i], S[j])
   K = S[(S[i] + S[j]) mod 256]
endwhile
```

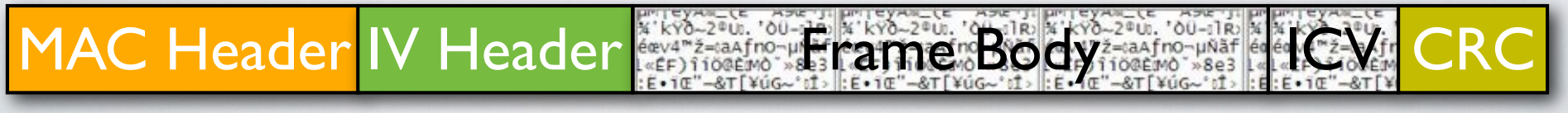
WEP

- Calculate the CRC over the data payload
- Concatenate the ICV to the end of the data
- Concatenate the 24 bit IV with the shared key (40 bit or 104 bit) to create the RC4 seed
- Generate a pseudo-random sequence with the same length as (payload + ICV). We call this the keystream
- Calculate the XOR of the keystream with the (payload + ICV)
- Add the IV to the beginning of the frame
- Send frame as a normal data frame

WEP Decryption

The receiving station just runs the algorithm again

- Concatenate IV + KEY
- Use RC4 to generate Keystream
- XOR encrypted message with Keystream
- Verify ICV

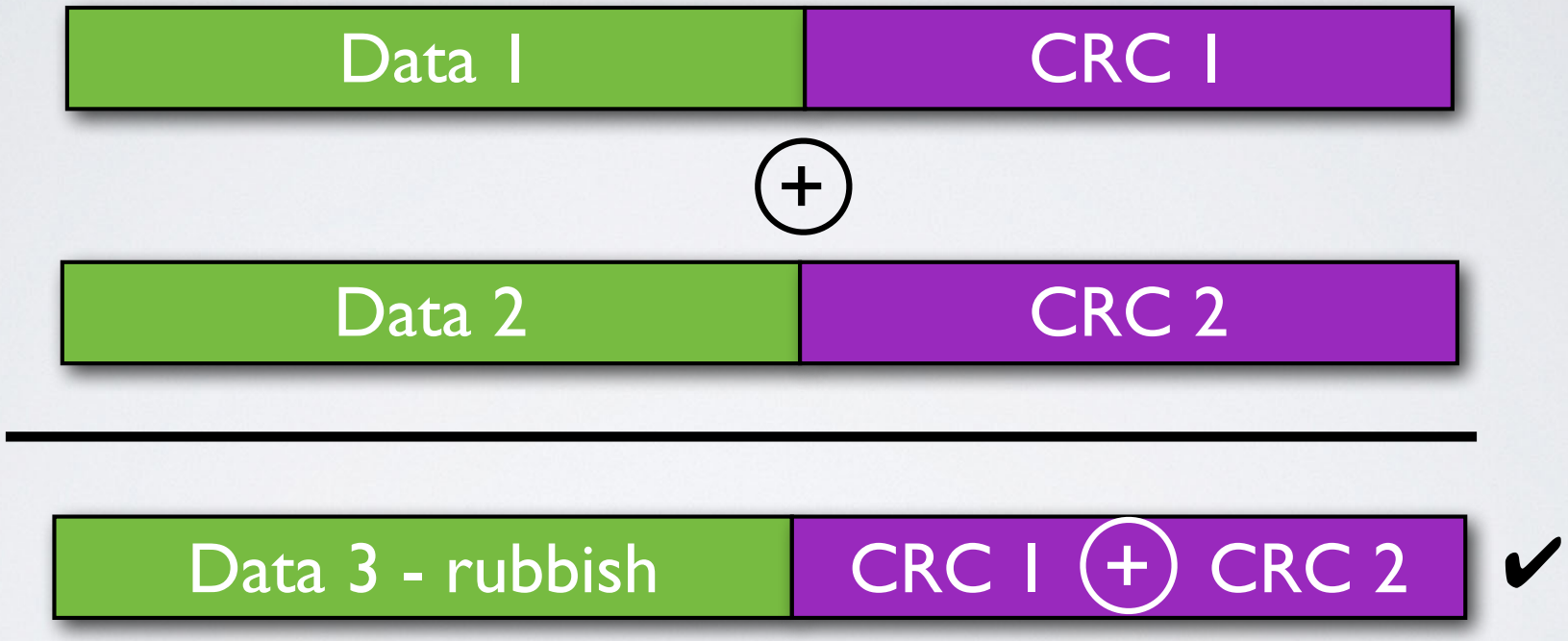


WEP AND Integrity

Integrity Check Value (ICV)

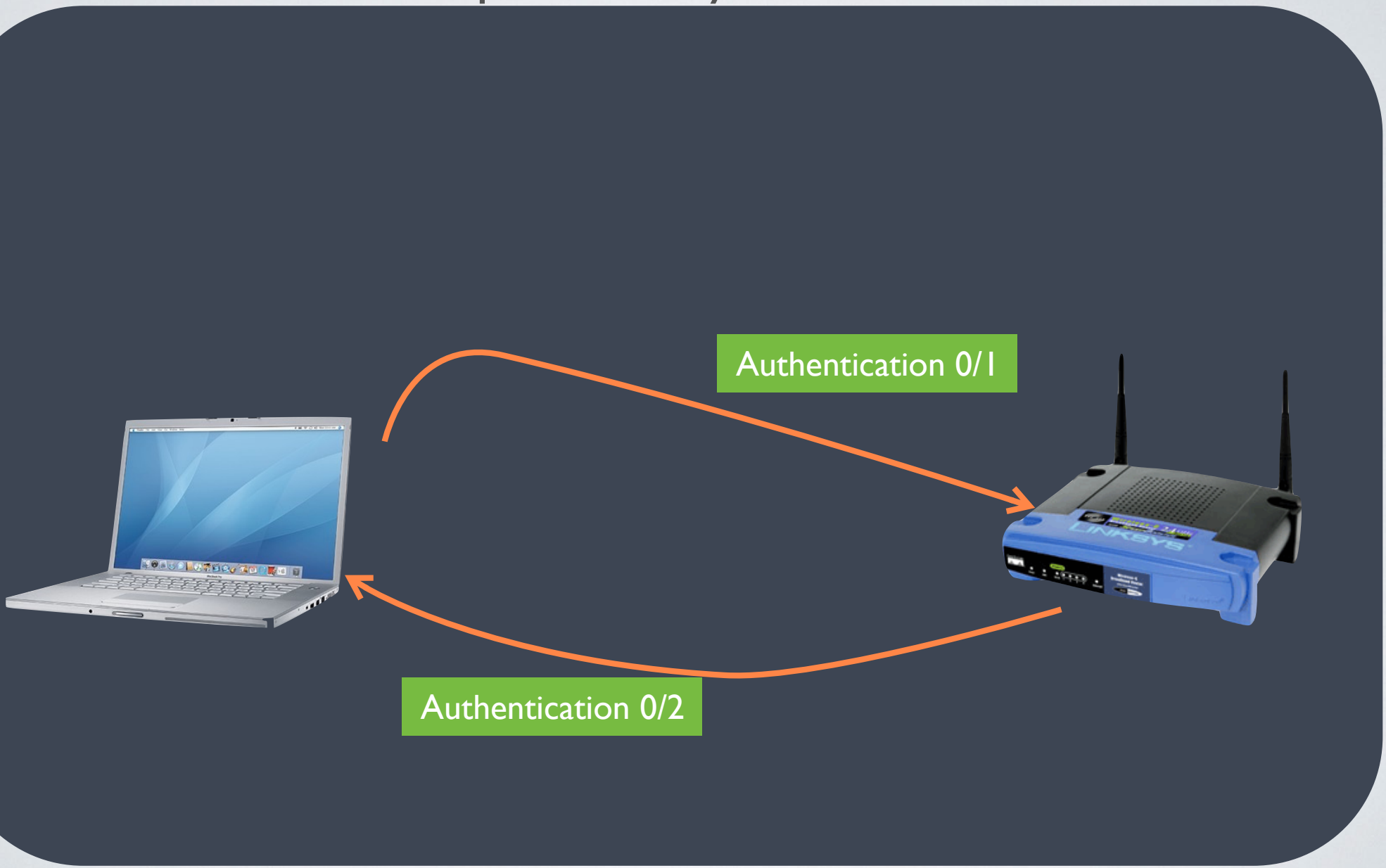
- Data Integrity is ensured by the ICV
- “Normal” 32-bit CRC
- Not really an integrity check

Integrity Check Value (ICV)

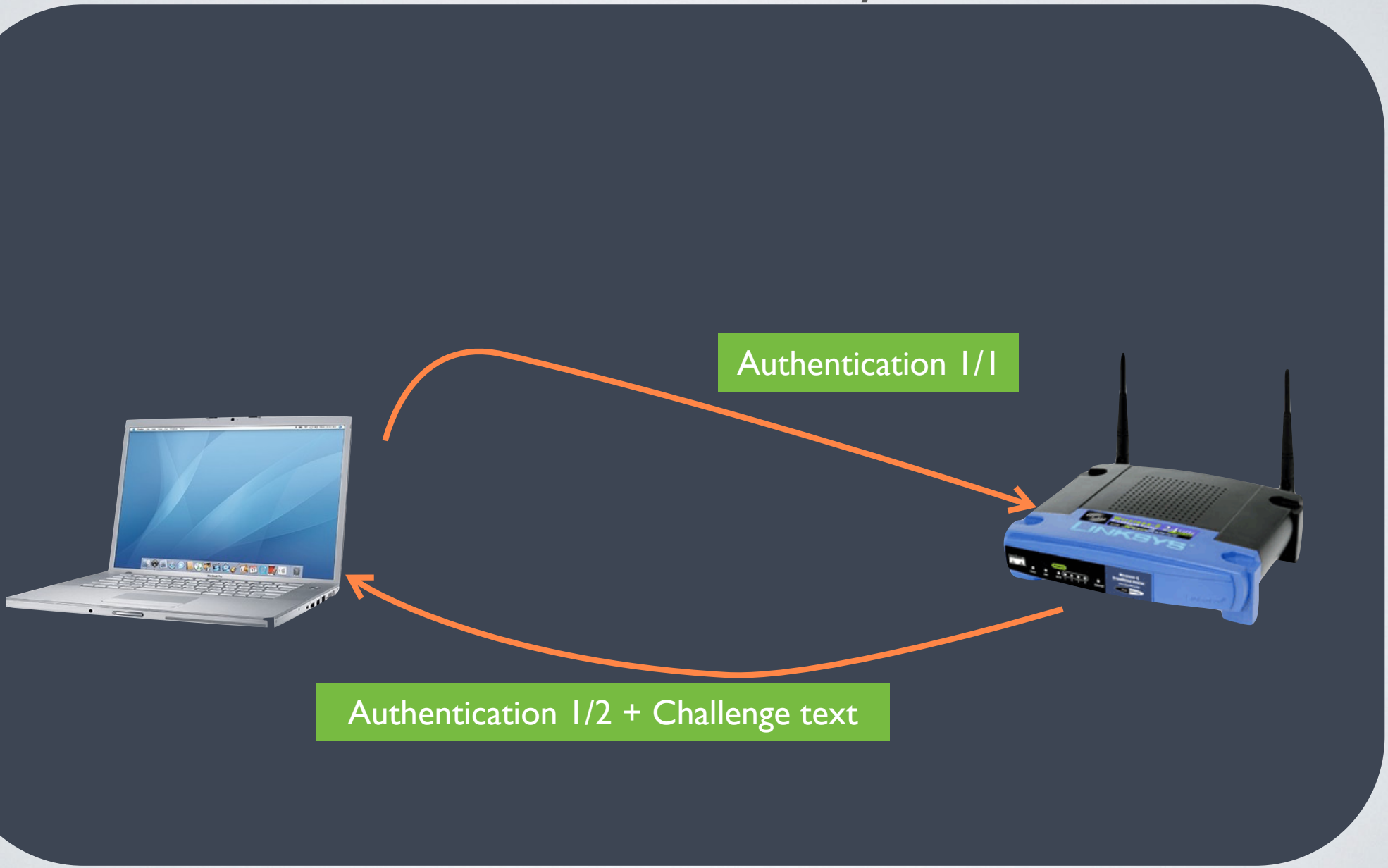


WEP and Authentication

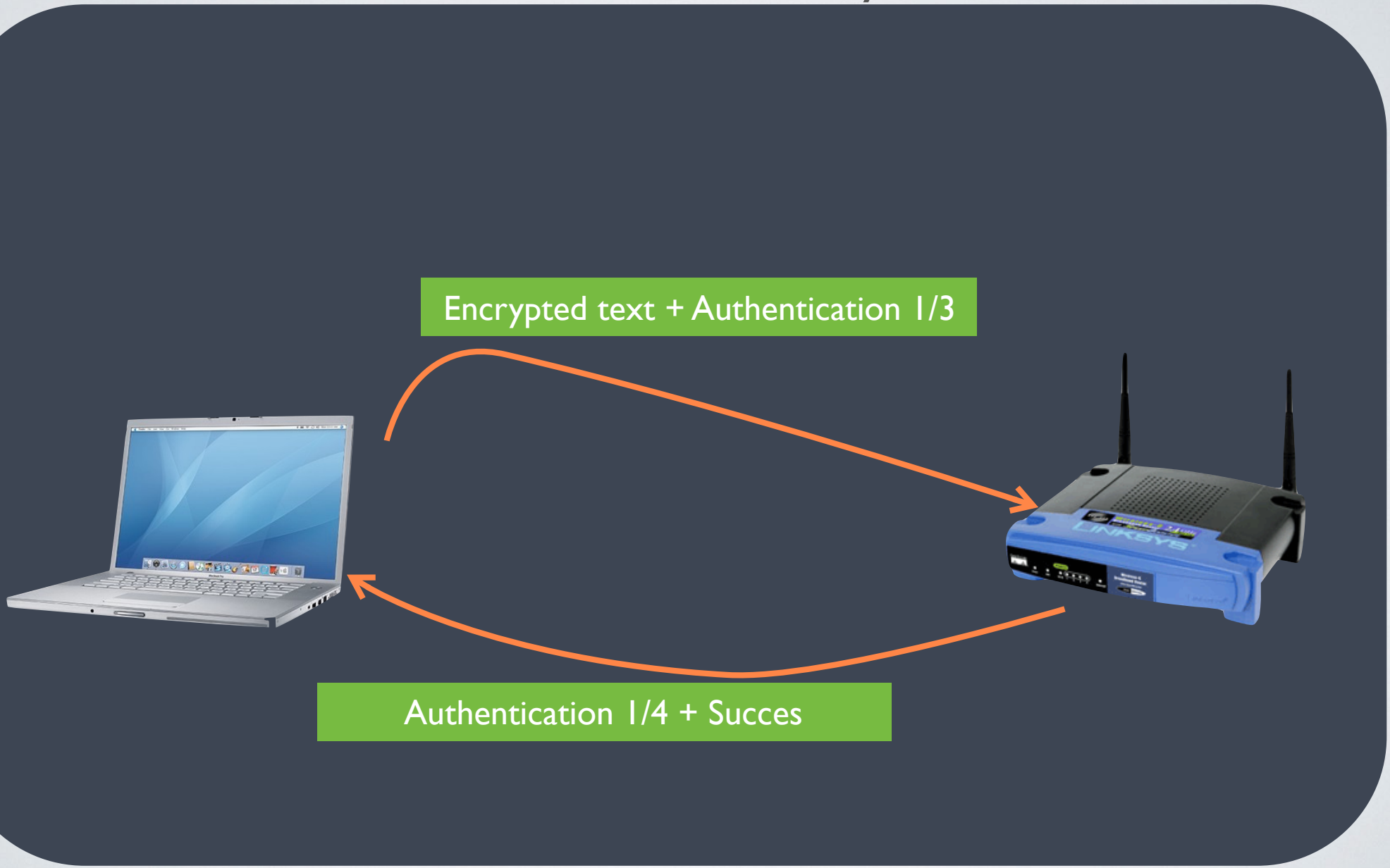
Open System



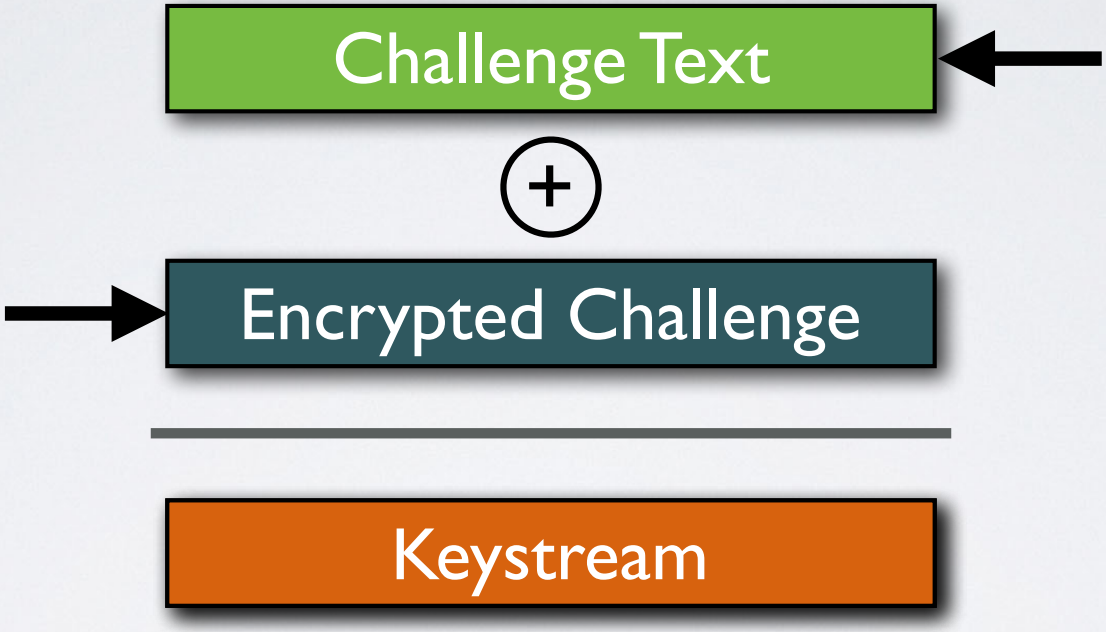
Shared Key



Shared Key


Encrypted text + Authentication 1/3
Authentication 1/4 + Succes

Problem ?



- An adversary can capture an authentication exchange, extract the keystream and use it to authenticate

Authentication

- There is no mutual authentication
  - The user cannot verify the identity of the AP
- Easy to produce a fake WEP AP

Traffic (Re-)Injection

- There are two conditions the AP to accept a frame
  - It comes from an authenticated source
  - It passes integrity control
- An attacker and capture a frame and re-inject it forever
- If a keystream is obtained, a new frame can be forged and injected

So… WEP Problems…

Confidentiality

- Not designed or supervised by cryptographers
- Bad choice of the encryption algorithm
  - RC4 encryption has known weaknesses
- The WEP key is the same for everybody

Confidentiality

- Part of the RC4 key (IV) is in clear text! - 24 bits
- The IV is 24 bits long (the RC4 seed is reused soon) —> **collisions are a know weakness of RC4**
- STAs typically use the same IV when they start transmitting
- Random IVs —> statistically: collisions after 5000 frames
- **The first 8 bytes of almost every data frame are the same**

Integrity

- The integrity check is not cryptographically secure
  - Using CRC is "ok" for random errors but not for deliberated/intentional errors
- It is possible to modify messages without being detected and without even knowing the key
  - Change data and ICV

Authentication

- Optional
  - Open system - default
- No mutual authentication
  - Only the STA gets authenticated
- The challenge exchange in shared-key authentication takes place in "clear text" and keystream can be easily extracted
  - An adversary can capture challenge and response

Duplicated Frames

- No protection against duplication
- It gets really serious in WPA

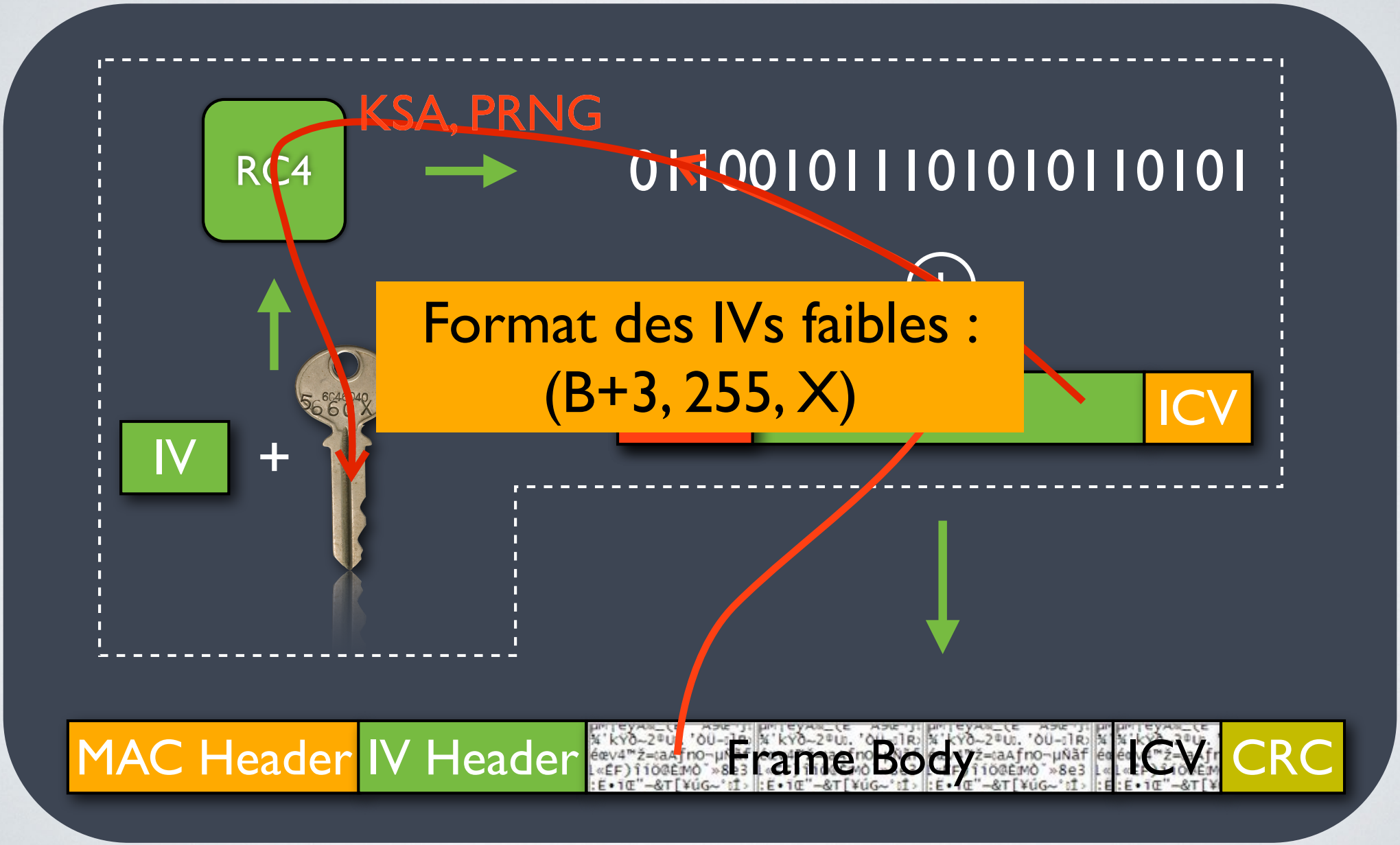
Not "Wired Equivalent Privacy" At All!

- Some people still believe that WEP vulnerabilities are "theoretical" or too hard to exploit
  - The first WEP cracking methods needed enormous amounts of collected data
- Last generation WEP attacks are a lot more aggressive, faster and much easier...

Passive Attack to Crack the WEP Key

- A passive observer can intercept all wireless traffic
- A known imperfection in the RC4 algorithm makes that certain IVs reveal information about the WEP key (weak IVs)
- There are about 9000 weak IVs among the total 16'700'000
- The WEP key can be obtained (cracked) using a few thousands of these weak IVs
- Just a couple of minutes on a busy network
- FMS (Fluhrer, Mantin, Shamir)

FMS Method


KSA, PRNG
RC4
01100101110101011010101
Format des IVs faibles :
(B+3, 255, X)
ICV
IV
+
MAC Header
IV Header
Frame Body
ICV
CRC

WEAK IVs

Format of IV:

RC4 Key:

B = Target Byte

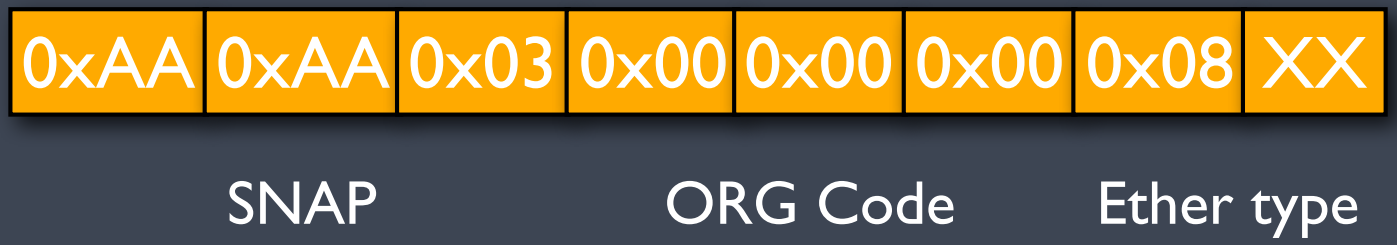
Accelerated FMS

- The FMS attack needs many frames with keak IVs
- Why wait ? We may force them!
- An encrypted frame can be captured and re-injected
  - Remember: no protection against duplicates!
  - One of the critical failures of WEP
- Capture a frame that generates a response (ARP request). Can be identified by length, for example
- Re-inject the frame several times recording the responses... at 54 Mbps!
- It's possible to crack a 128 bit (104) WEP key while having a coffee

The Pyshkin Tews Weinmann (PTW) Attack

- All paquets can be used
  - No restrictions on IVs
- Only 35000 to 40000 packets are needed in order to get a 50% success probability on a 104 bit key

Fragmentation Attack



- LLC/SNAP header contained in practically all 802.11 data frames
- Type is almost always IP or ARP
- Can be identified by type
- 8 bytes of clear text known
  - —> 8 bytes of keystream known

Fragmentation Attack

- Forge an ARP request (28 bytes)
- Fragment the request - 16 fragments can be used
- It is possible to send data in chunks of 4 bytes (4 bytes needed for CRC)
- We may send 16x4=64 bytes of data
  - Enough for the ARP request