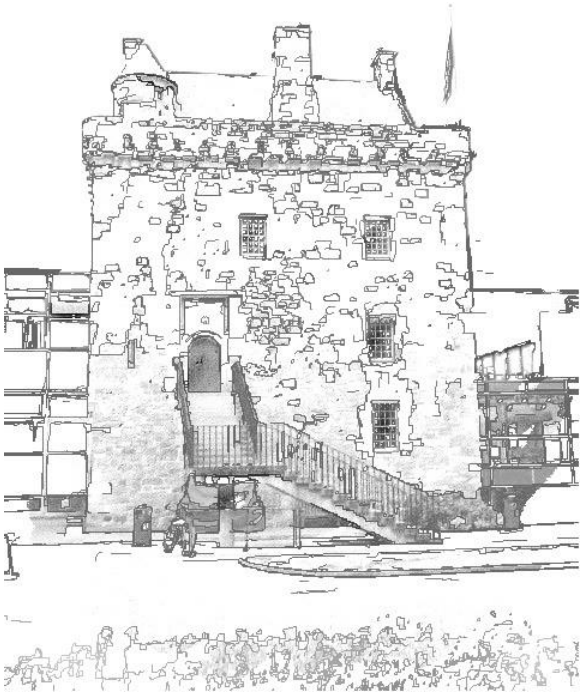
Wireless LAN
CO72047

Unit 4: Wireless Encryption



Wireless LAN
Centre for Dist. Computing and Security
Prof W Buchanan

NAPIER UNIVERSITY
EDINBURGH

Author: Bill Buchanan

Wireless connections … which technology?

Areas covered:

Basic Principles

Untrusted, trusted and DMZ

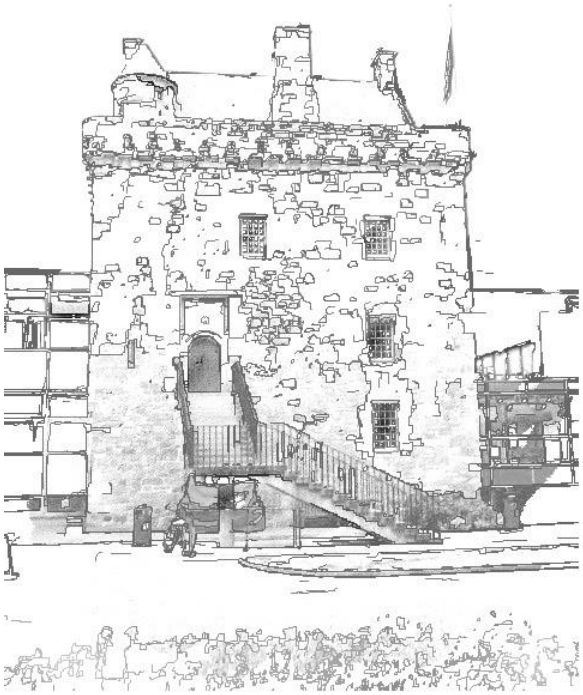
WEP – The weakest security ever!

The weaknesses of WEP

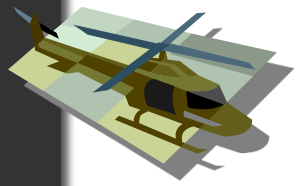
TKIP – An improvement...

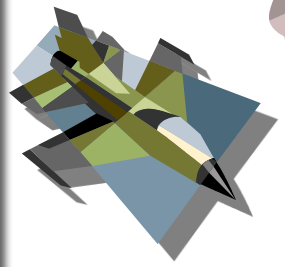
The basic model.

A few principles...

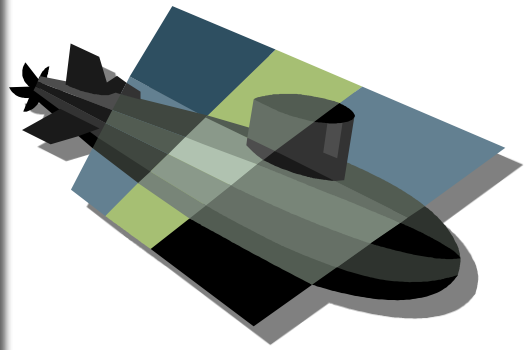


Trusted, untrusted and de-militarized zones





Our side (trusted)



DMZ - an area where military actions are prohibited.

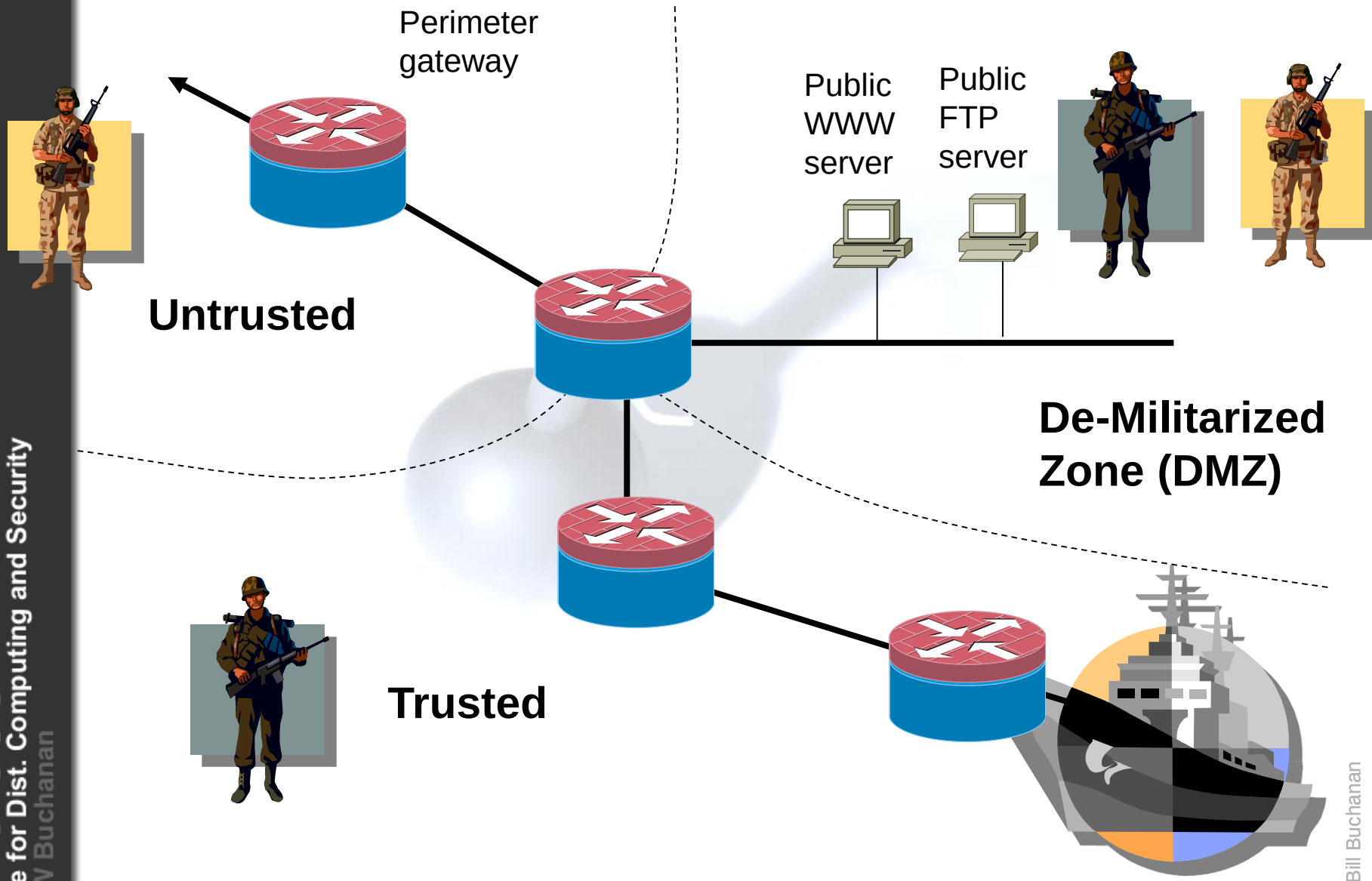
Their side (untrusted)

Wireless LAN
Centre for Dist. Computing and Security
Prof W Buchanan

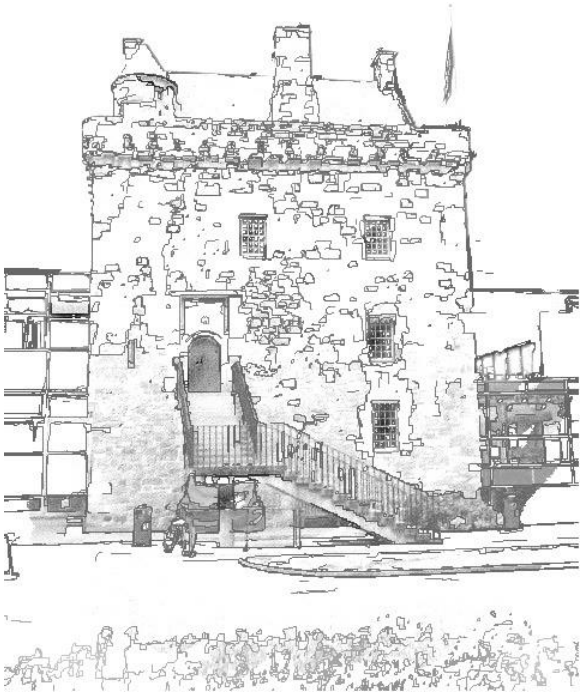
Edinburgh Napier UNIVERSITY

Author: Bill Buchanan

Trusted, untrusted and de-militarized zones



Types of attacks ...



Known plaintext attack

Known plaintext attack. Where the hacker knows part of the ciphertext and the corresponding plaintext. The known ciphertext and plaintext can then be used to decrypt the rest of the ciphertext.

Hello How are you?

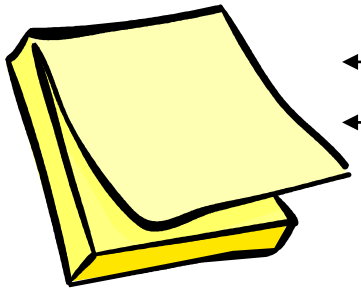
kG&$s &FDsaf *fd$

kG&$s

The mapping is used to crack the code

Exhaustive search

Exhaustive search. Where the hacker uses brute force to decrypt the ciphertext and tries every possible key.



Key: 00000.....00000000?

Key: 00000.....00000001?

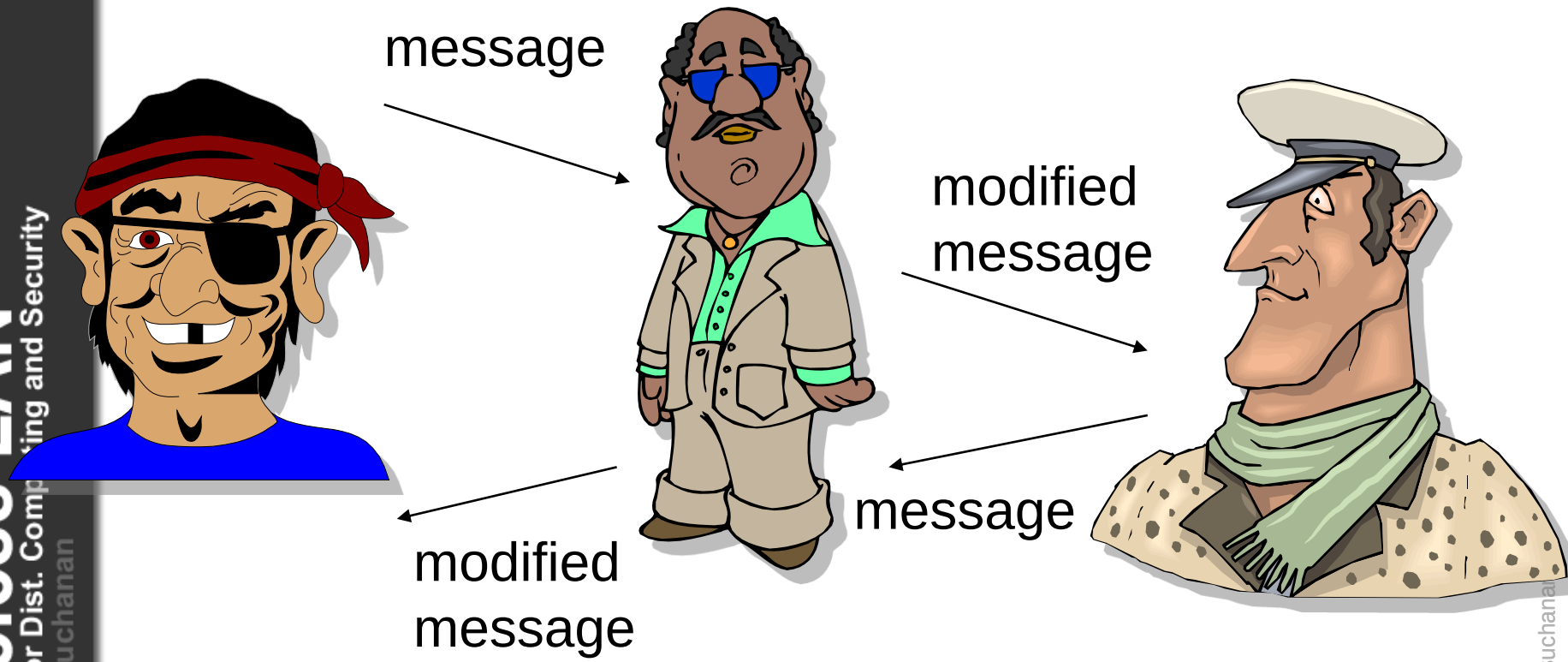
Key: 11111.....11111111?

Result

Is this a valid output?

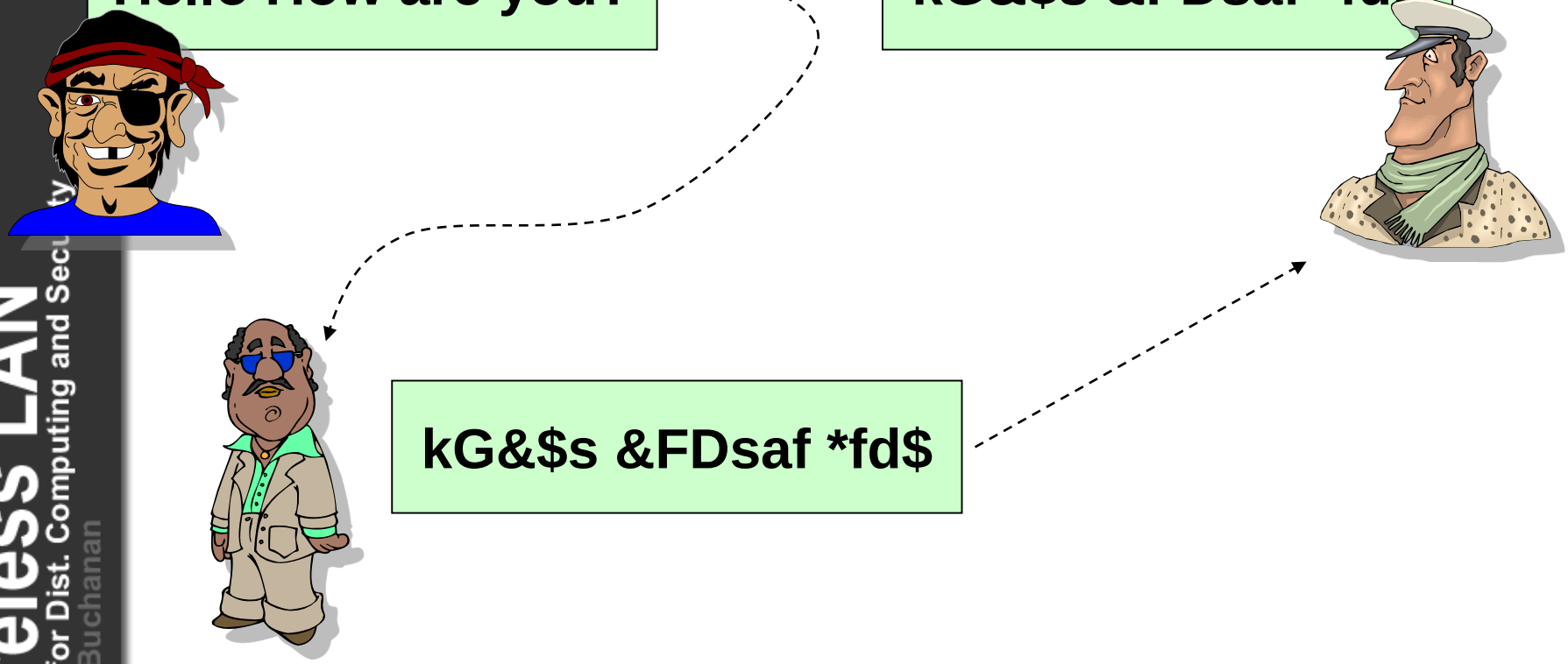
Man-in-the-middle

Man-in-the-middle. Where the hacker is hidden between two parties and impersonates each of them to the other.



Replay system

The replay system. Where the hacker takes a legitimate message and sends it into the network at some future time.



Active attack/cut-and-paste

Active attack. Where the hacker inserts or modifies messages.
Cut and paste. Where the hacker mixes parts of two different encrypted messages and, sometimes, is able to create a new message. This message is likely to make no sense, but may trick the receiver into doing something that helps the hacker.

Hello How are you?

kG&$s &FDsaf *fd$

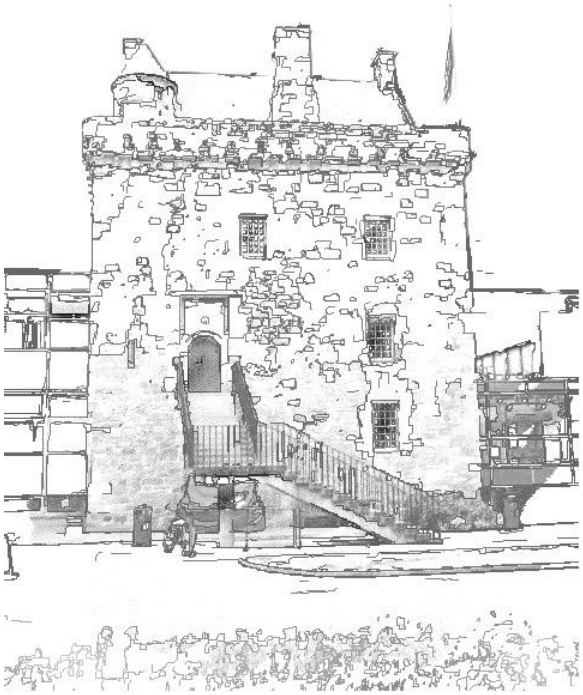
kG&$s

&$s &FDsaf*fd$**kG&$skG**

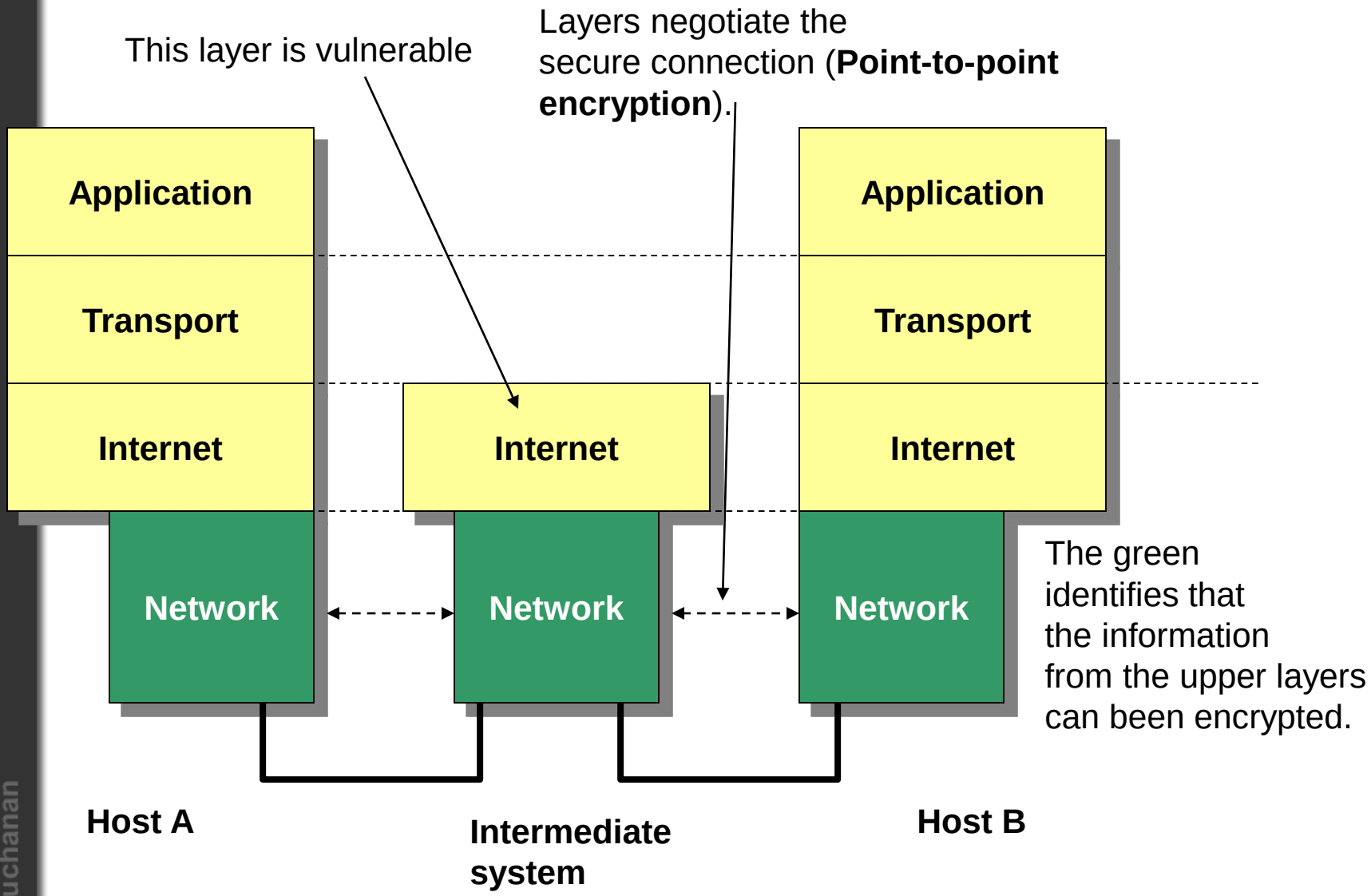
Chosen-ciphertext

Chosen-ciphertext. Where the hacker sends a message to the target, this is then encrypted with the target's private-key and the hacker then analyses the encrypted message. For example, a hacker may send an e-mail to the encryption file server and the hacker spies on the delivered message.

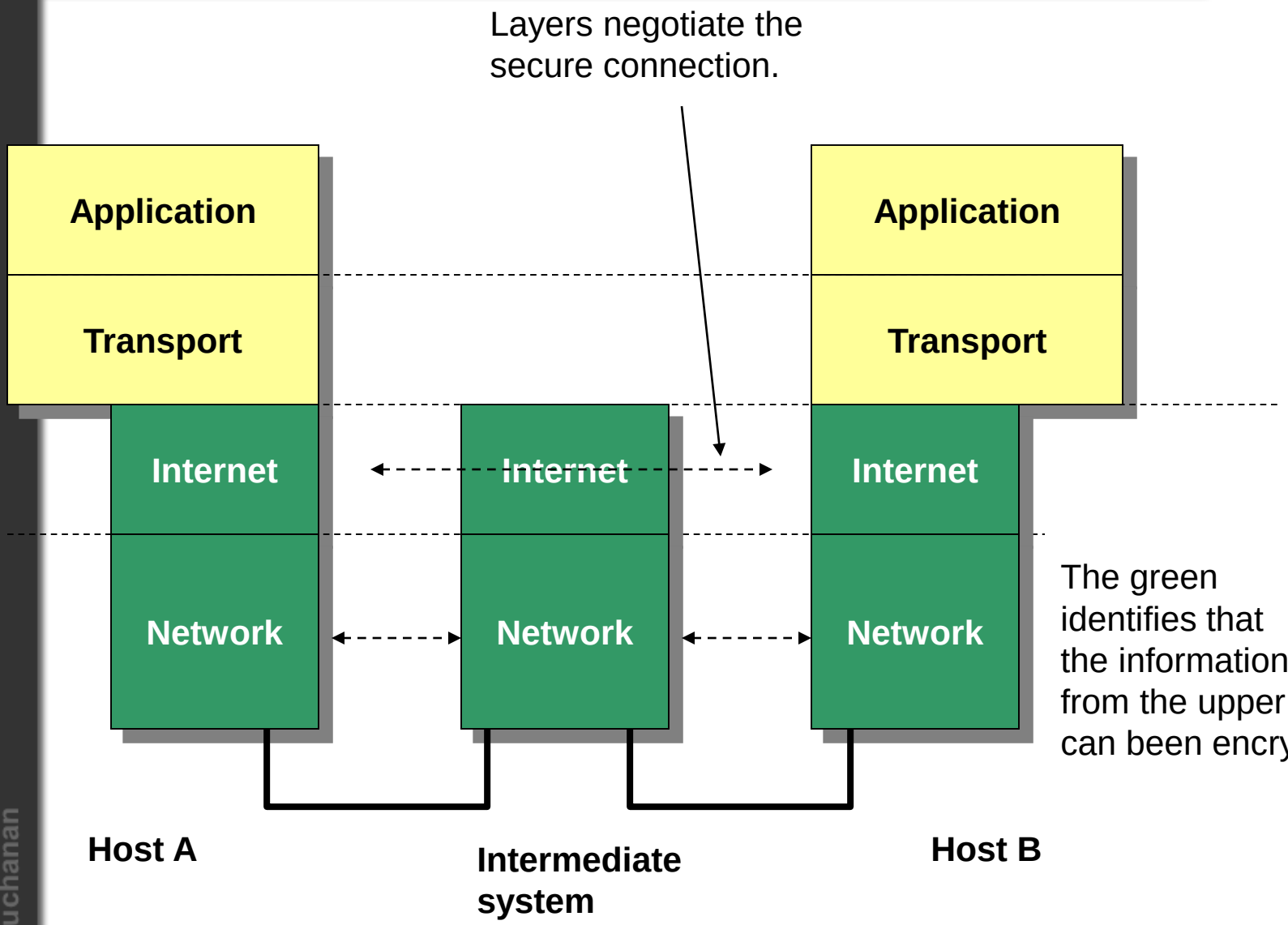
Encryption...



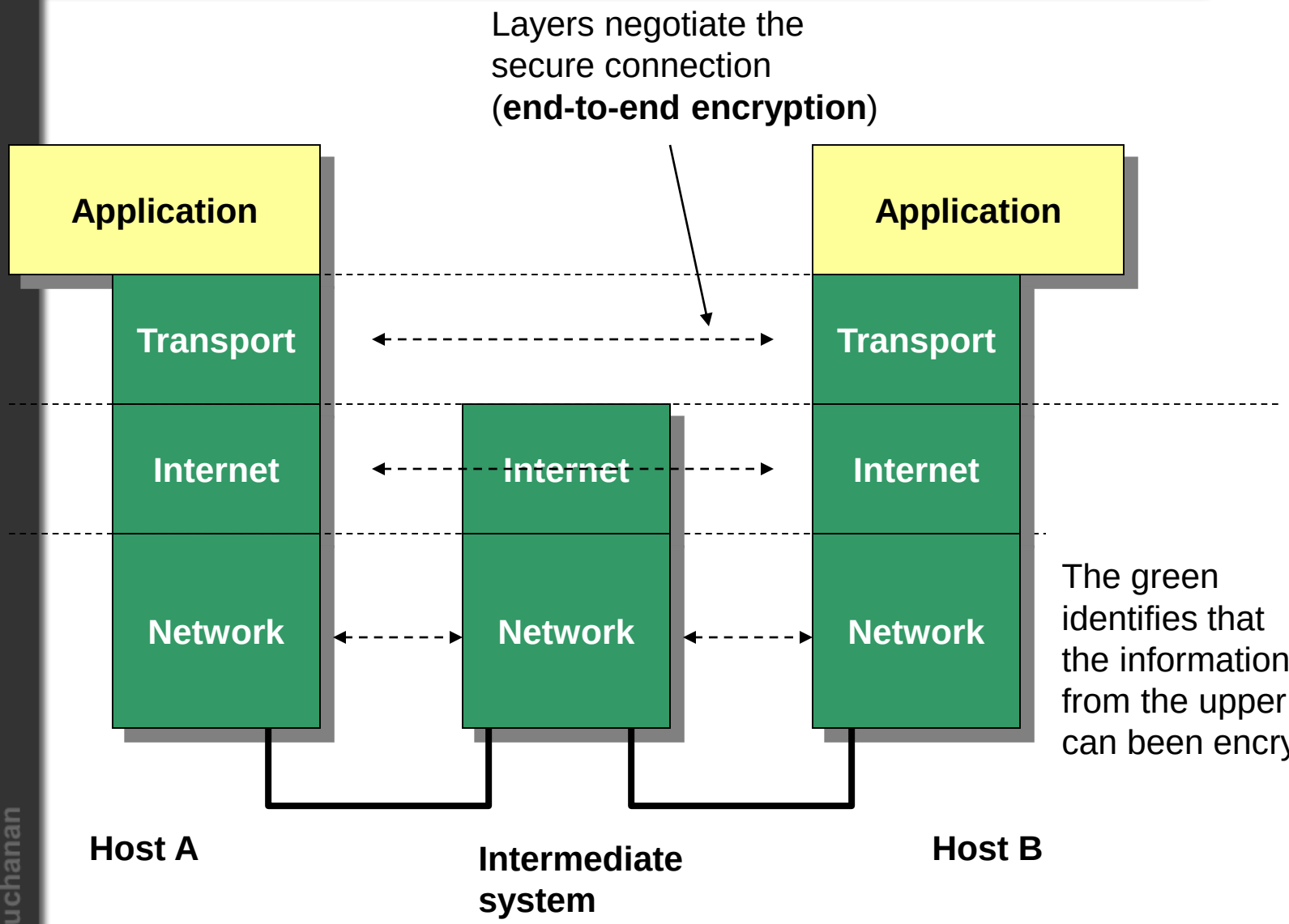
Encryption applied at the Network layer



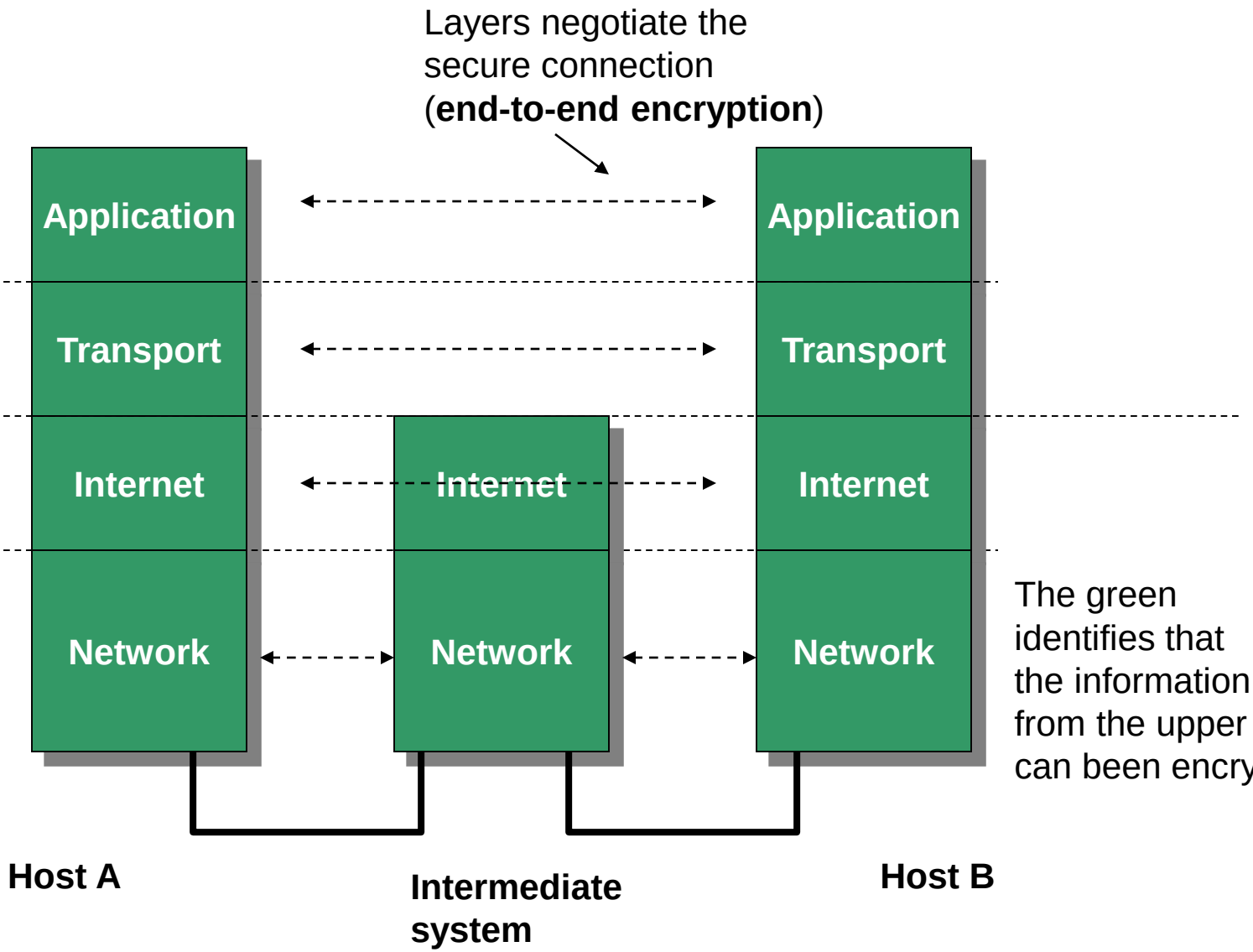
Encryption applied at the Internet layer



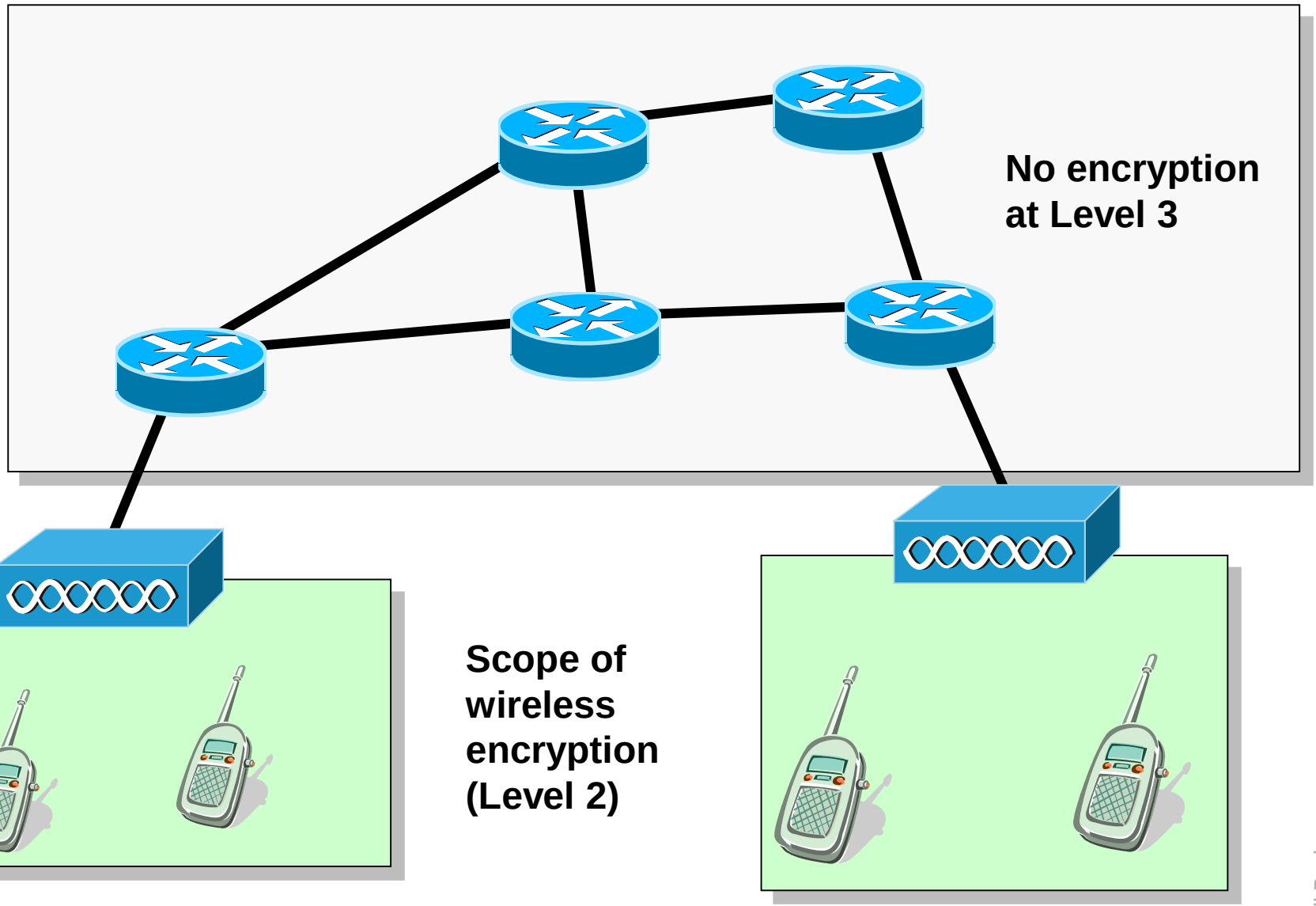
Encryption applied at the Transport layer

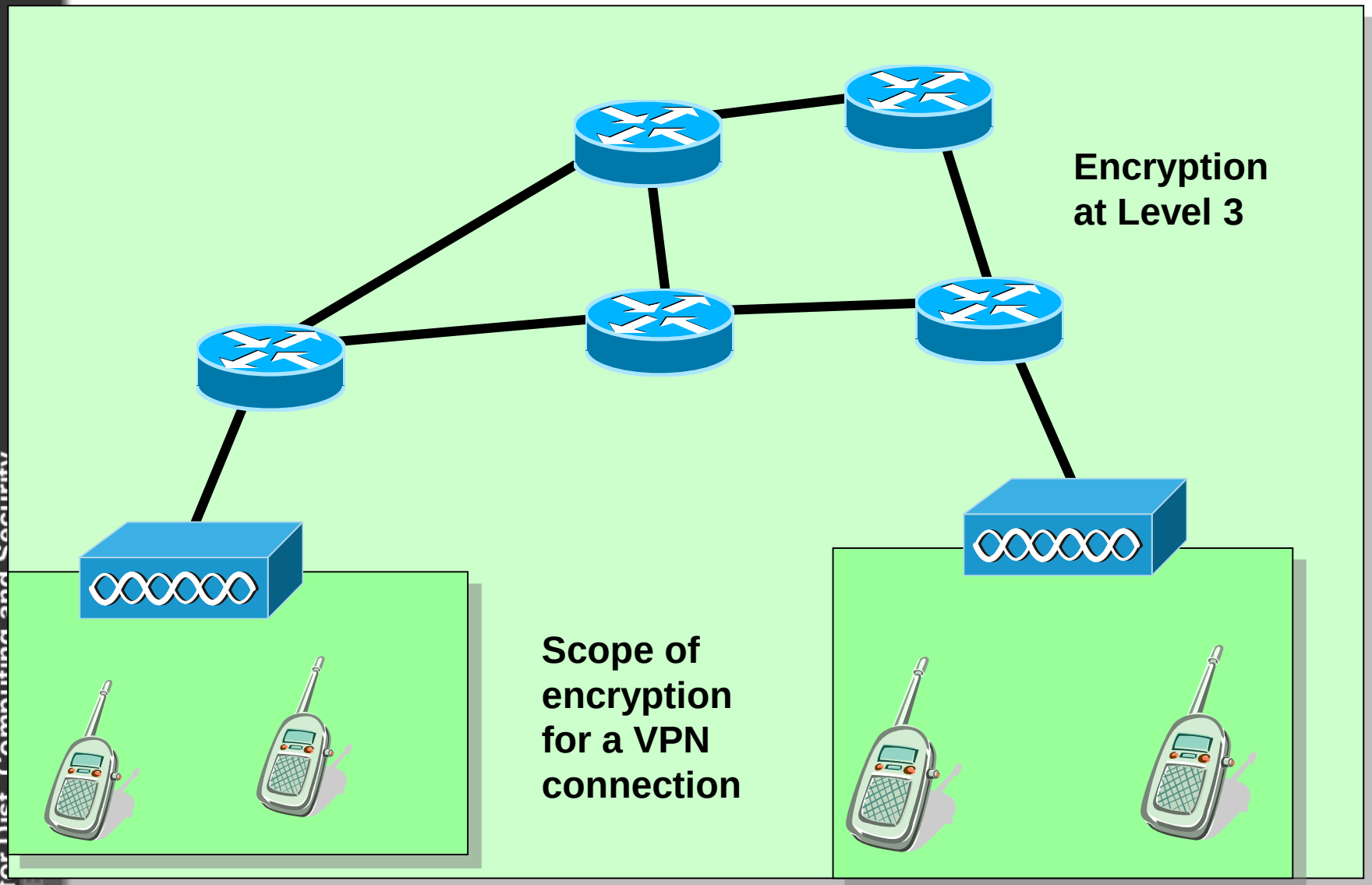


Example of encryption at every layer



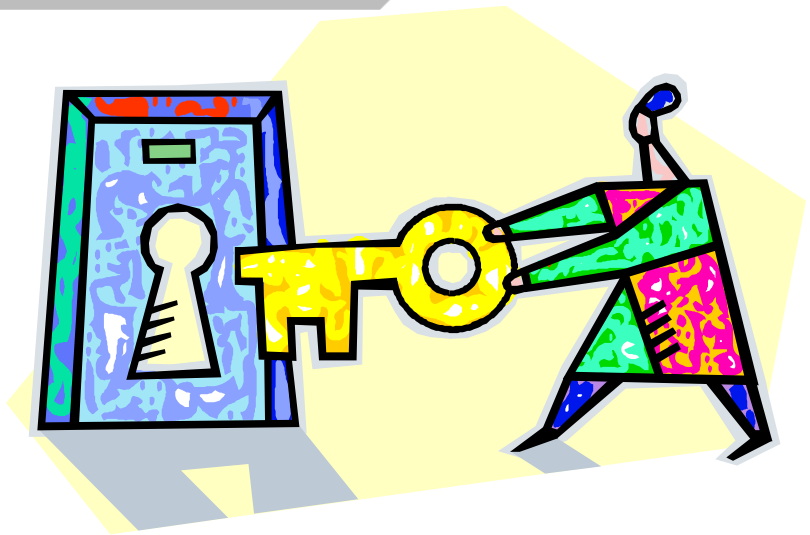
The green identifies that the information from the upper layers can been encrypted.


No encryption
at Level 3
Scope of
wireless
encryption
(Level 2)

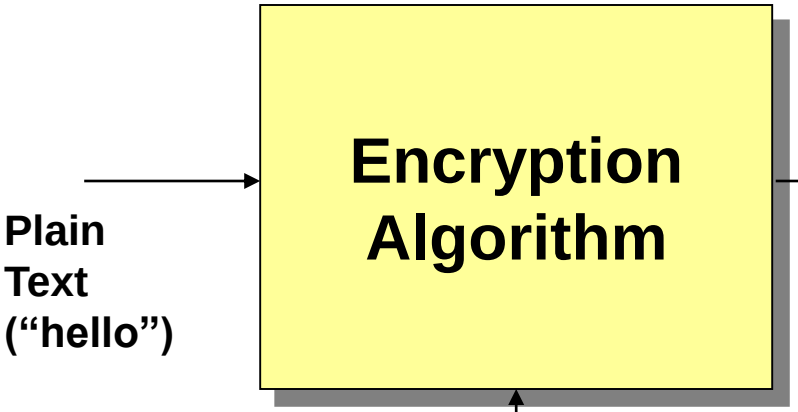

Encryption
at Level 3
Scope of
encryption
for a VPN
connection

Best for security

The optimal form of security is encryption, which uses a fixed encryption algorithm, but differing keys. This can occur at differing levels of the OSI model



Encryption methods



This method makes it difficult to change the algorithm, as someone could be listening.

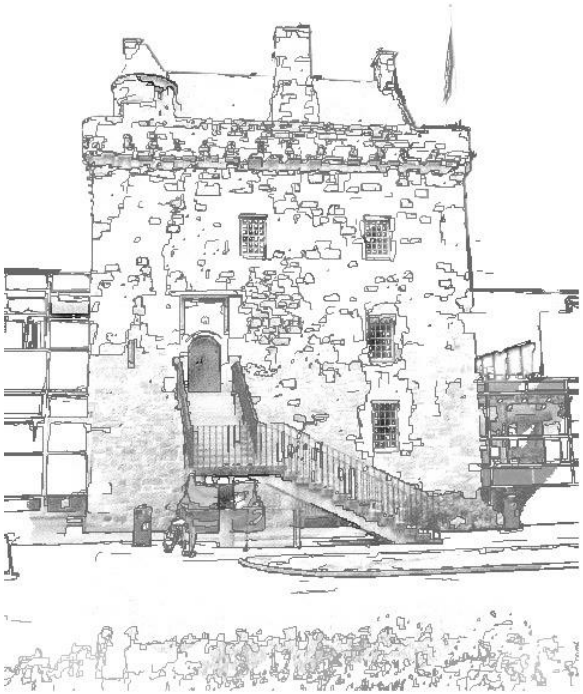
We can either have an encryption algorithm that changes, so that only the sender and receiver know about it.

Or

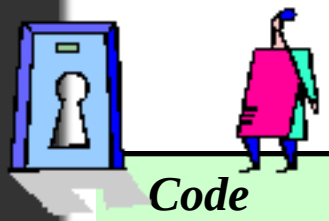
In the case of most encryption techniques, such as RSA, DES, PGP, and so on. The encryption algorithm is known to everyone. It is the key which is secret.

We have a fixed algorithm that everyone knows
About, but vary the key.

Encryption keys

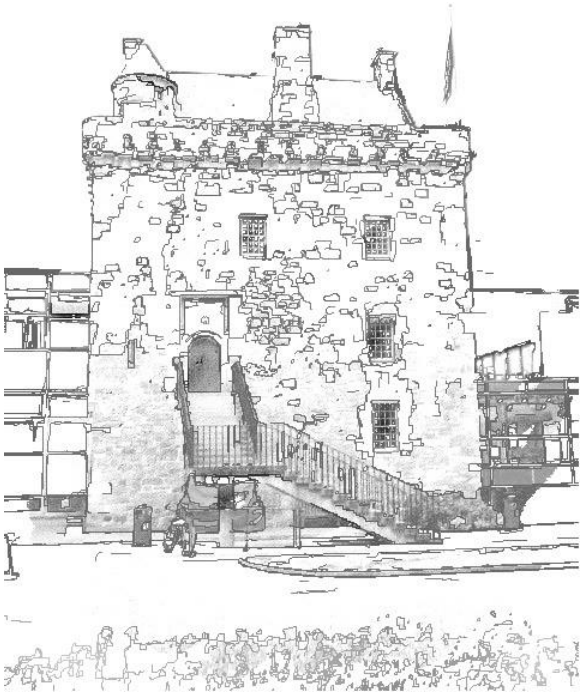


Encryption keys

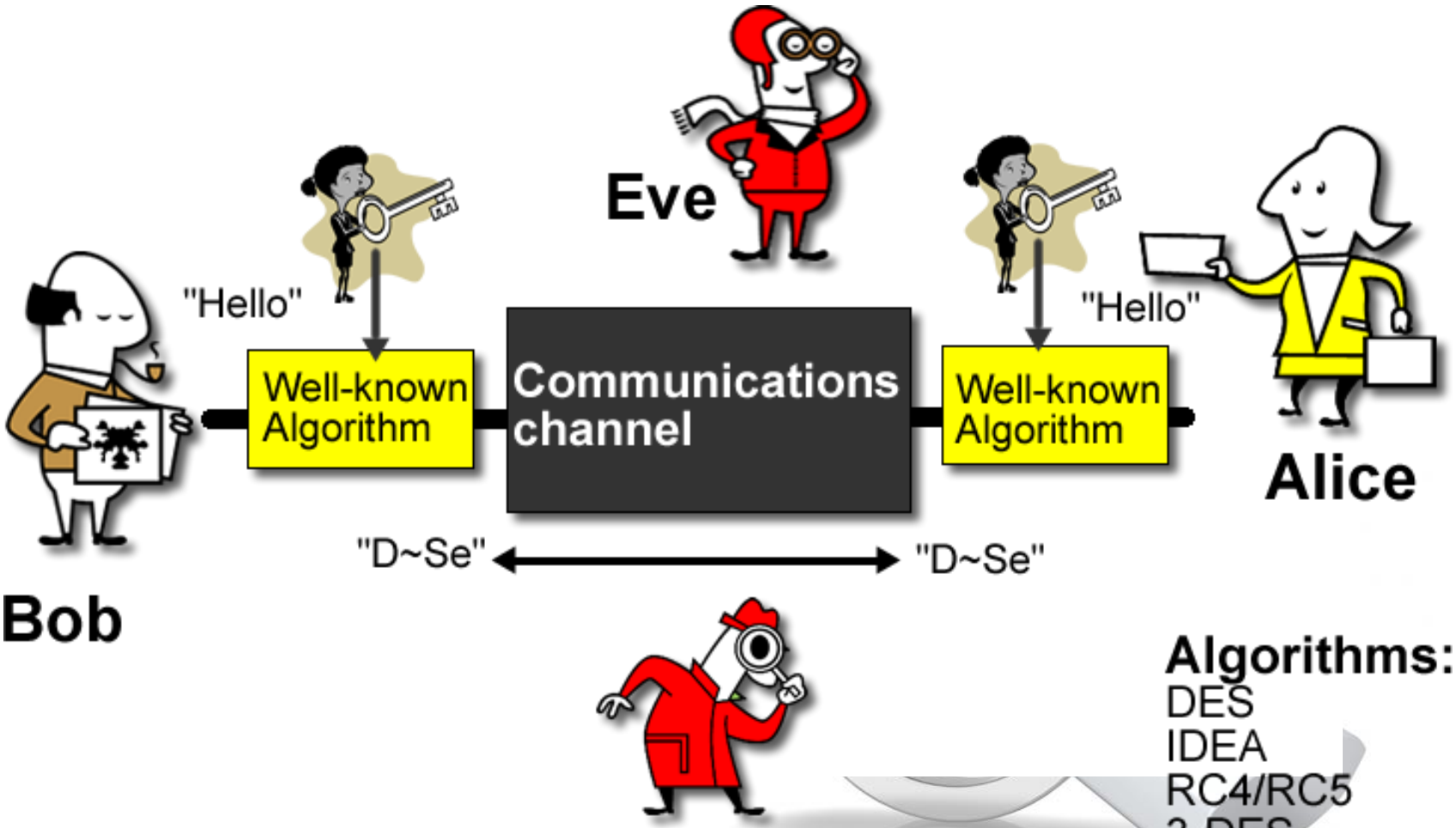


Code size	*Number of keys*	*Code size*	*Number of keys*	*Code size*	*Number of keys*
1	2	12	4096	52	4.5×10^{15}
2	4	16	65536	56	7.21×10^{16}
3	8	20	1048576	60	1.15×10^{18}
4	16	24	16777216	64	1.84×10^{19}
5	32	28	2.68×10^{8}	68	2.95×10^{20}
6	64	32	4.29×10^{9}	72	4.72×10^{21}
7	128	36	6.87×10^{10}	76	7.56×10^{22}
8	256	40	1.1×10^{12}	80	1.21×10^{24}
9	512	44	1.76×10^{13}	84	1.93×10^{25}
10	1024	48	2.81×10^{14}	88	3.09×10^{26}

Public and private keys



Private key encryption



Algorithms:
DES
IDEA
RC4/RC5
3-DES

Public-key ...

Public-key encryption (RSA)

Eve

Alice

Bob

Communications channel

Public key

Public key

Private key

Private key

Public-key ...

Public-key encryption (RSA)

Eve

Alice

Bob

Hello

Communications channel

Public key

Alice's public key is used to encrypt

Public key

Private key

Private key

Public-key ...

Public-key encryption (RSA)

Eve

Alice

Bob

G#~$

Hello

Hello

Communications channel

Public key

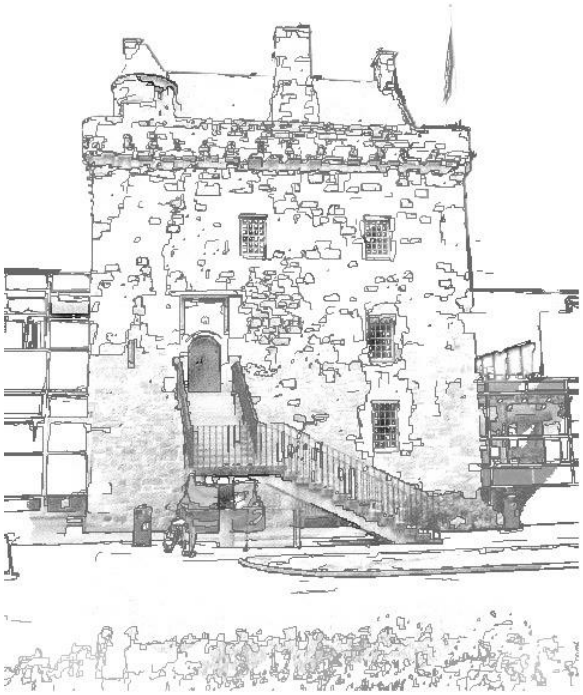
Private key

Alice's public key is used to encrypt

Public key

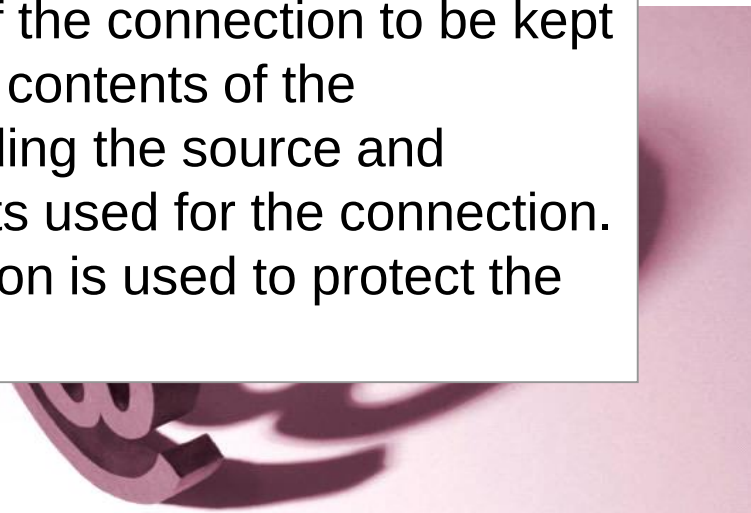
Private key

Security



Fundamental Elements of Security

Authentication. This is used to identify the user, the wireless client and the wireless access point.
Authorization. This is used to determine that users and wireless devices have the authorization to connect to the network.
Accounting. This is used to log information on the usage of the network, and may set restrictions of the access.
Assurance. This defines that the data that is received and transmitted has not been changed in any way. This is often known as Integrity.
Confidentiality. This allows the details of the connection to be kept secret. It typically involves preserving the contents of the transmitted data, but may also include hiding the source and destinations addresses, and the TCP ports used for the connection. Most often, in wireless networks, encryption is used to protect the confidentiality.

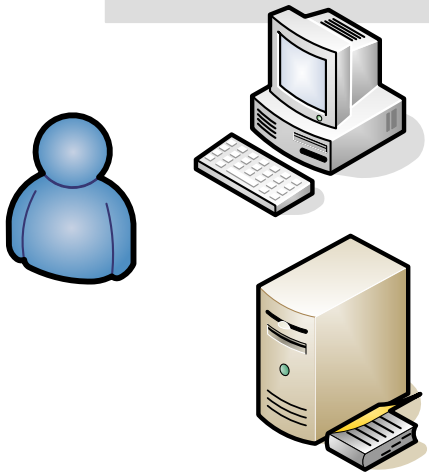


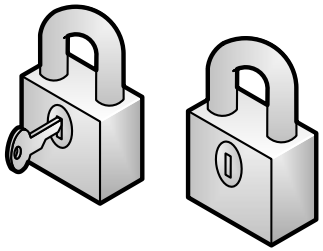
Fundamental Principles of Security

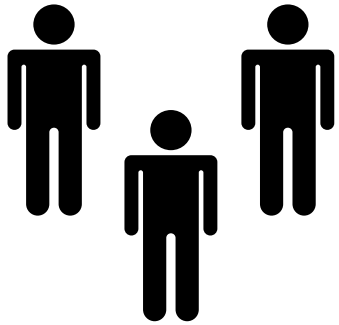
Authentication (Device, User, Servers, Connections, etc)

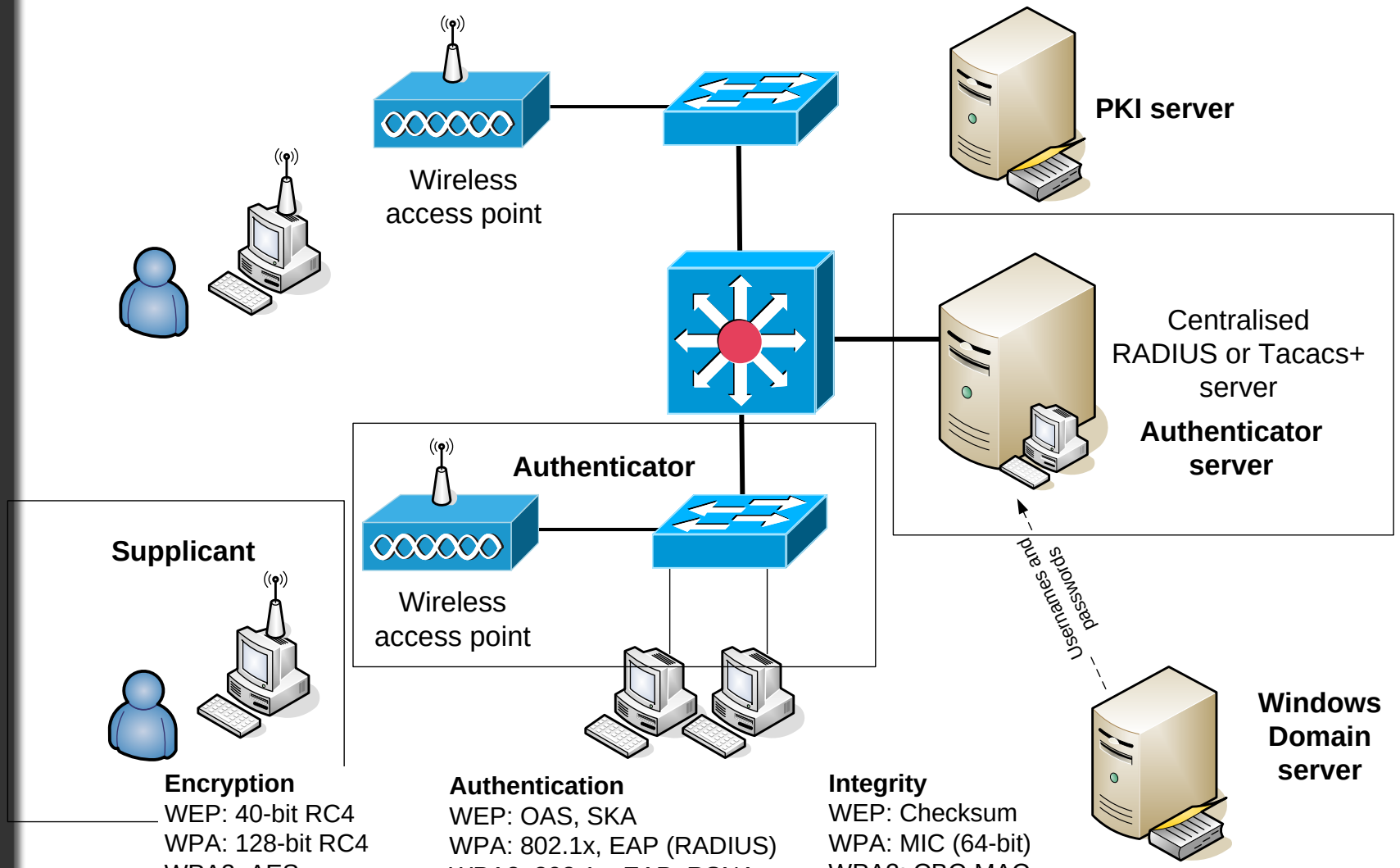
Confidentiality (Encryption)

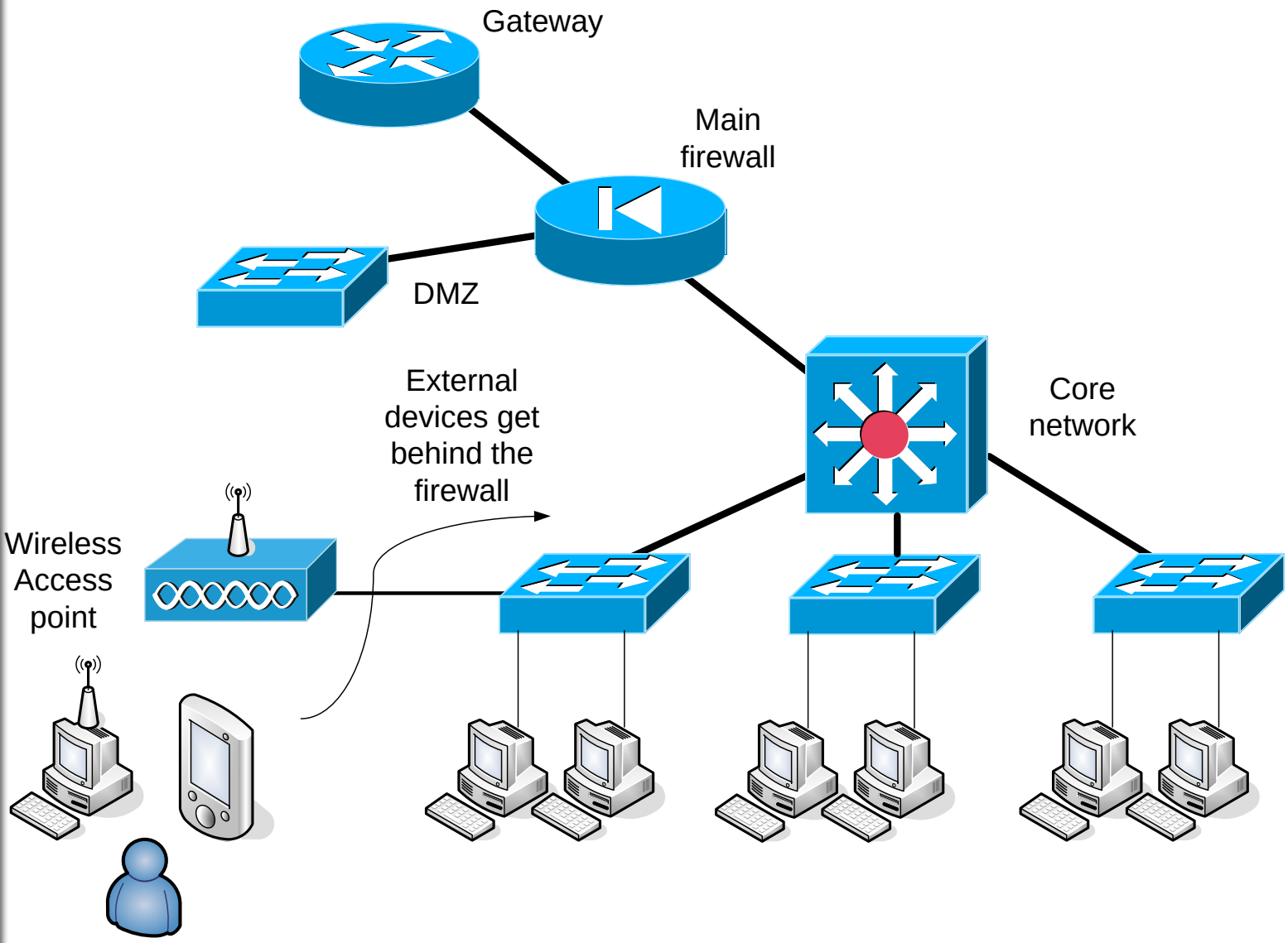
Assurance (Integrity)

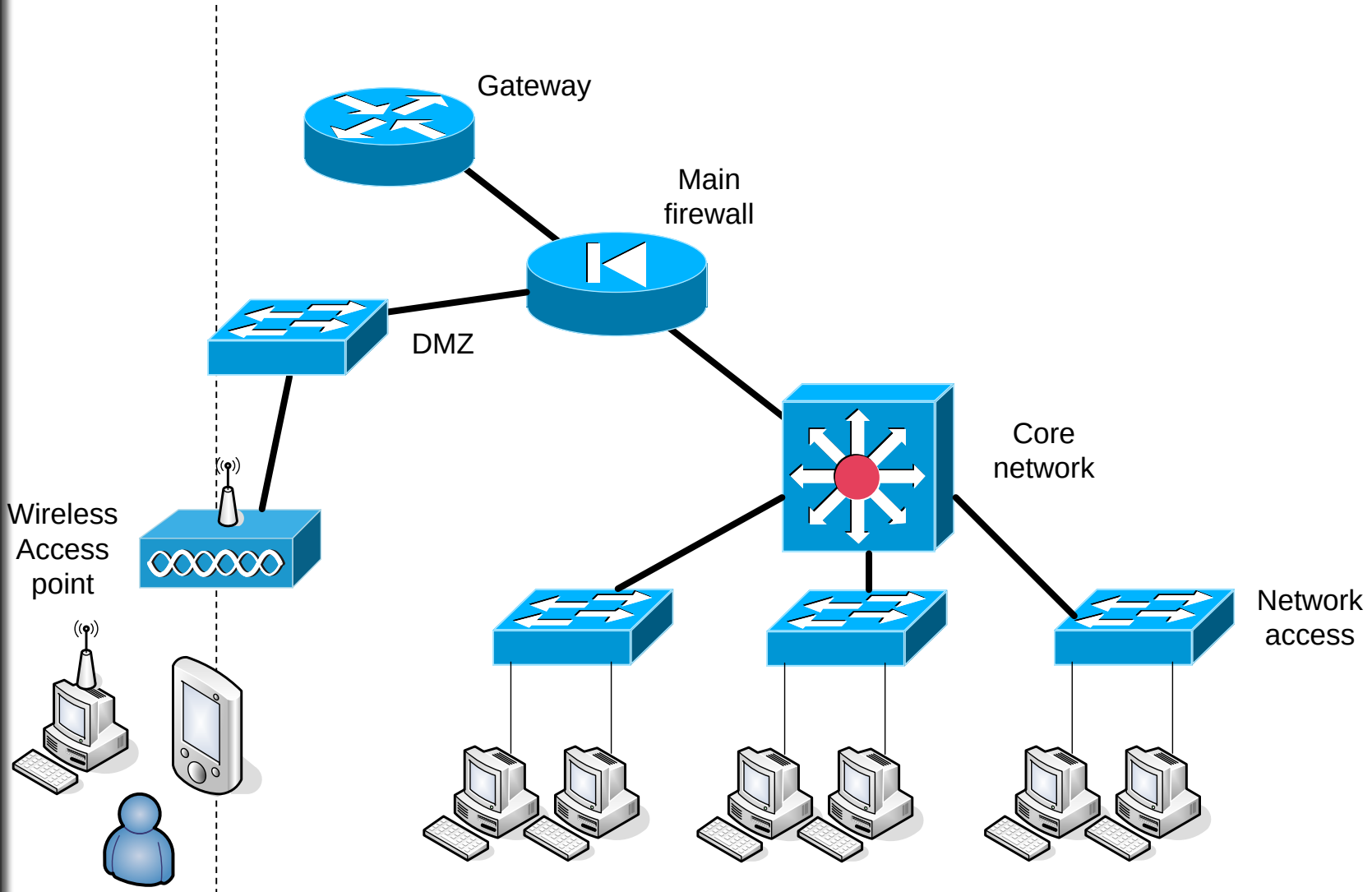




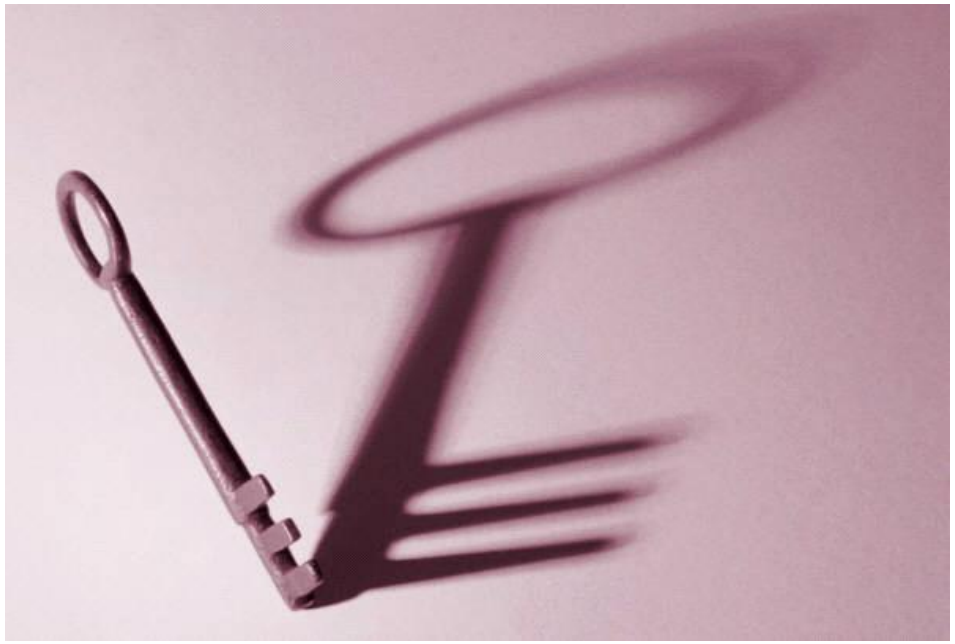


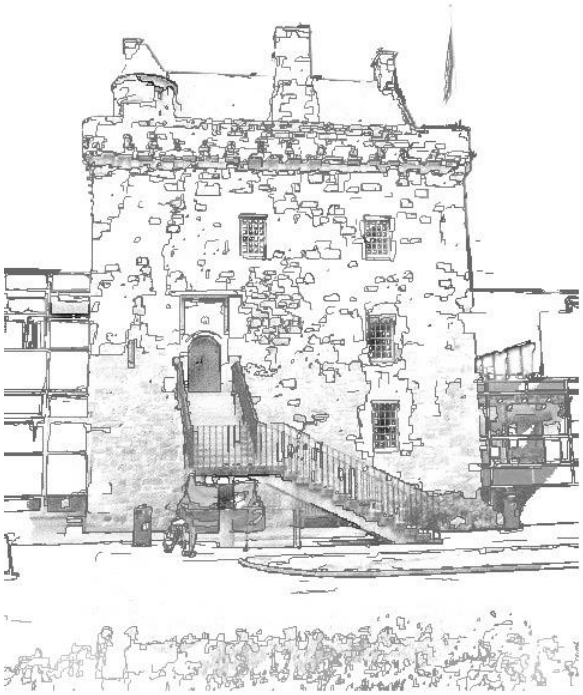

Wireless access point
PKI server
Centralised RADIUS or Tacacs+ server
Authenticator server
Authenticator
Supplicant
Wireless access point
Usernames and passwords
Windows Domain server
Encryption
WEP: 40-bit RC4
WPA: 128-bit RC4
WPA2: AES
Authentication
WEP: OAS, SKA
WPA: 802.1x, EAP (RADIUS)
WPA2: 802.1x, EAP, RSNA
Integrity
WEP: Checksum
WPA: MIC (64-bit)
WPA2: CBC-MAC


Gateway
Main firewall
DMZ
External devices get behind the firewall
Core network
Wireless Access point
Network access

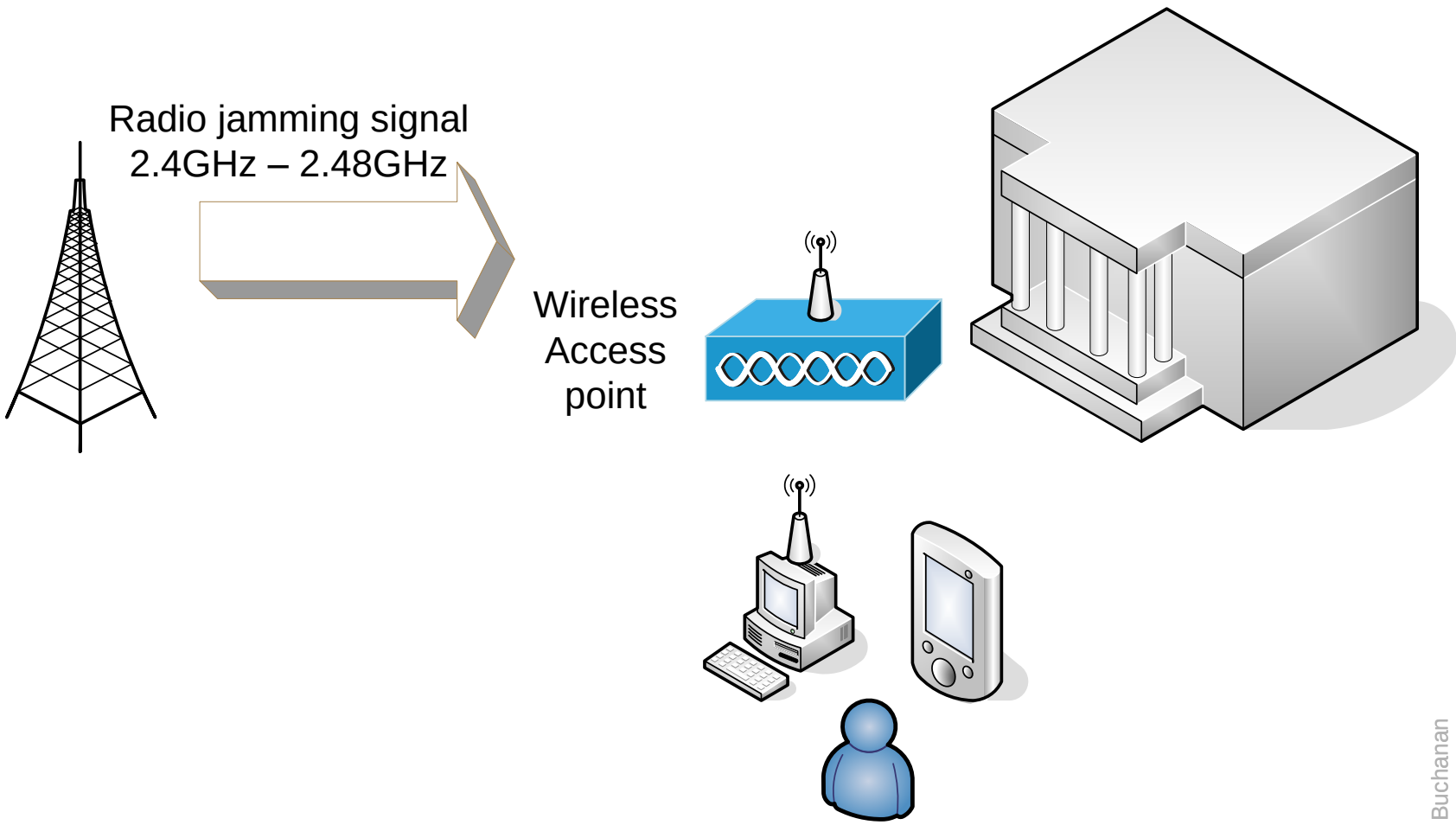

Gateway
Main
firewall
DMZ
Core
network
Wireless
Access
point
Network
access

Radio Frequency Problems

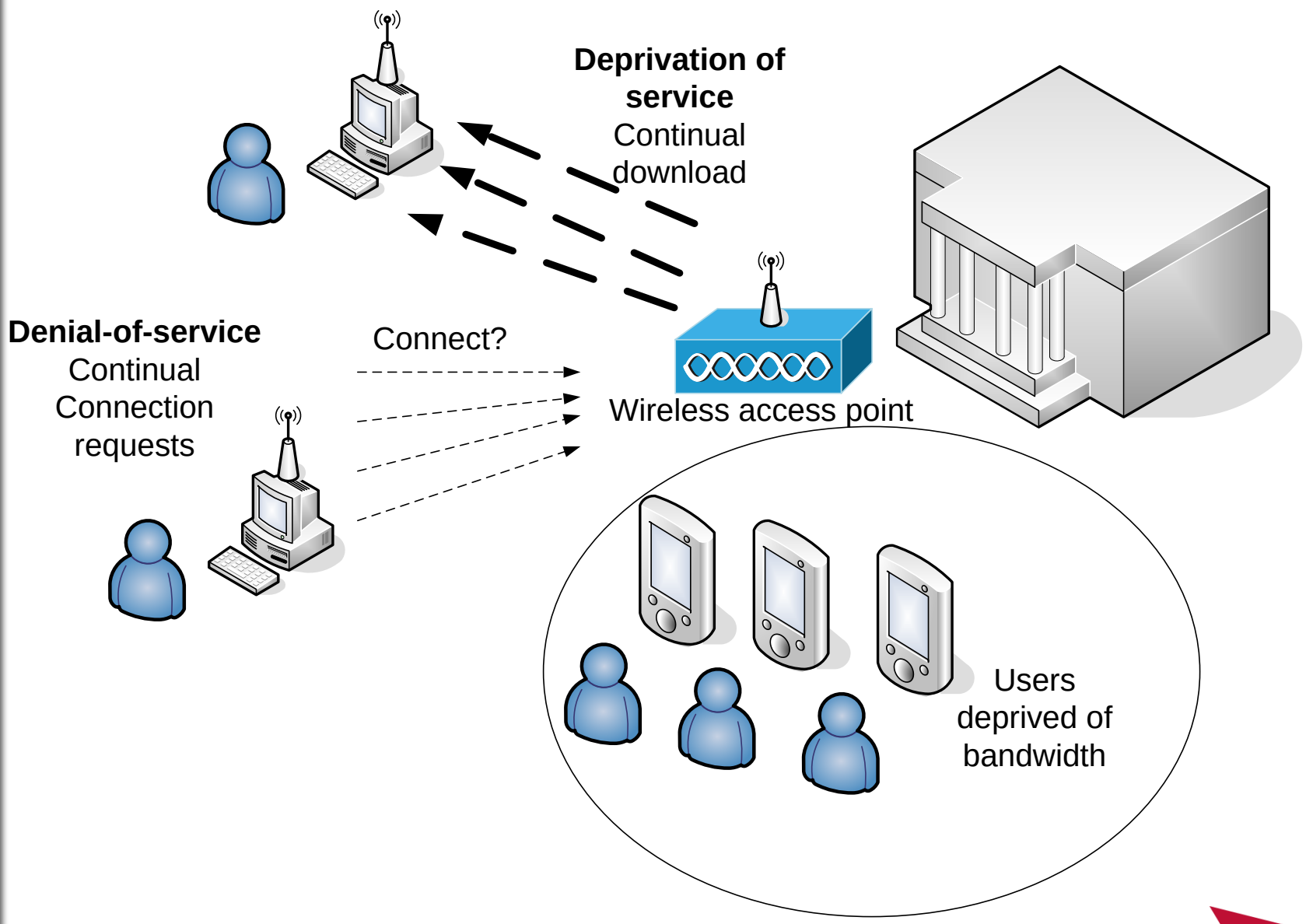




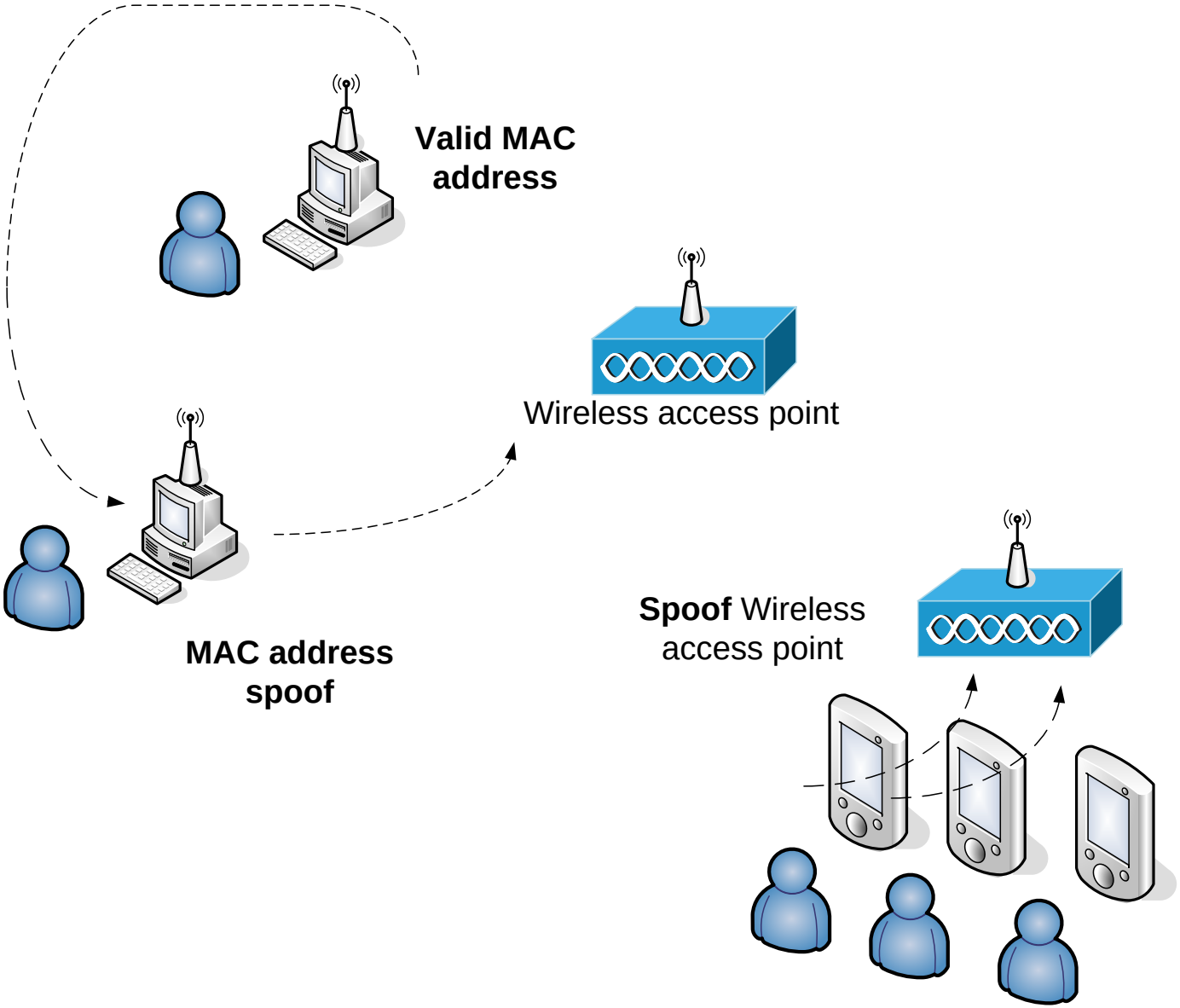
Jamming

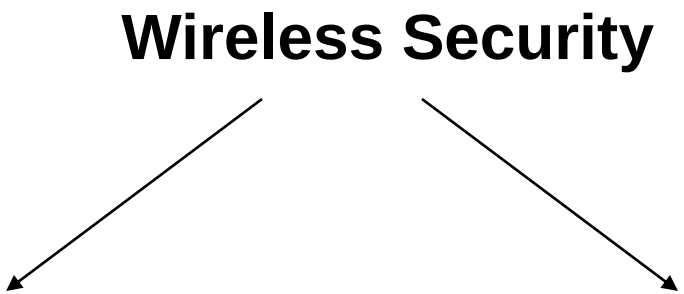


DoS


Deprivation of service
Continual download
Denial-of-service
Continual Connection requests
Connect?
Wireless access point
Users deprived of bandwidth

Spoofing


Valid MAC address
Wireless access point
MAC address spoof
Spoof Wireless access point



IPSec standards for VPN's

- Limited to IP
- Required for public access systems.

Wireless Security Standards

Encryption

WEP - Wireless Encryption Protocol

WPA - Wireless Protected Access

IEEE 802.11i

Authentication

802.1x/EAP:

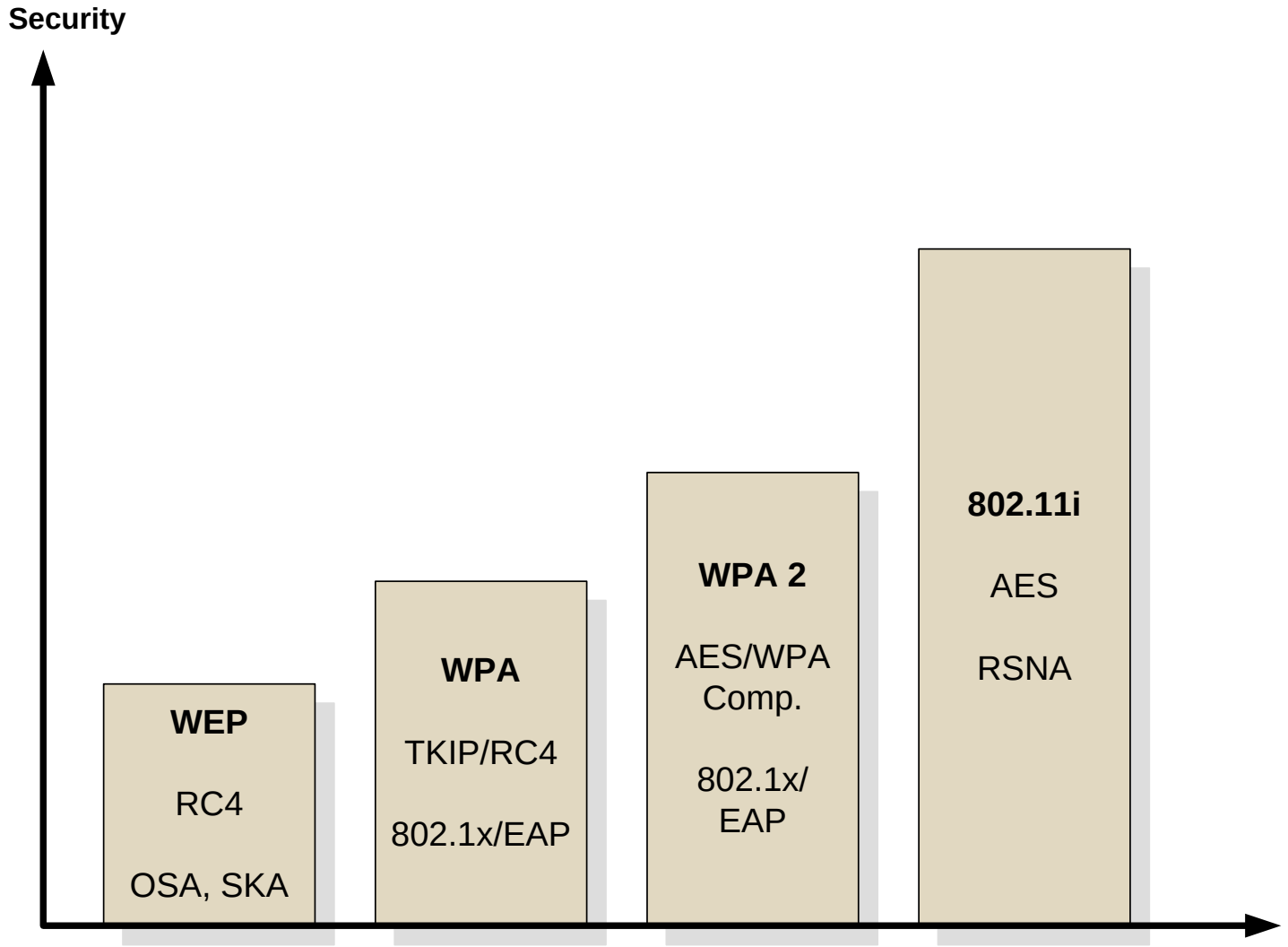
EAPS - Extensible Authentication Protocol

LEAP - Lightweight EAP

EAP-TLS - EAP - Transport Layer Security

EAP-TTLS - Tunnelled TLS

PEAP - Protected EAP



WEP – Wireless Equivalent Protocol
OSA – Open System Auth.
SKA – Shared Key Auth.

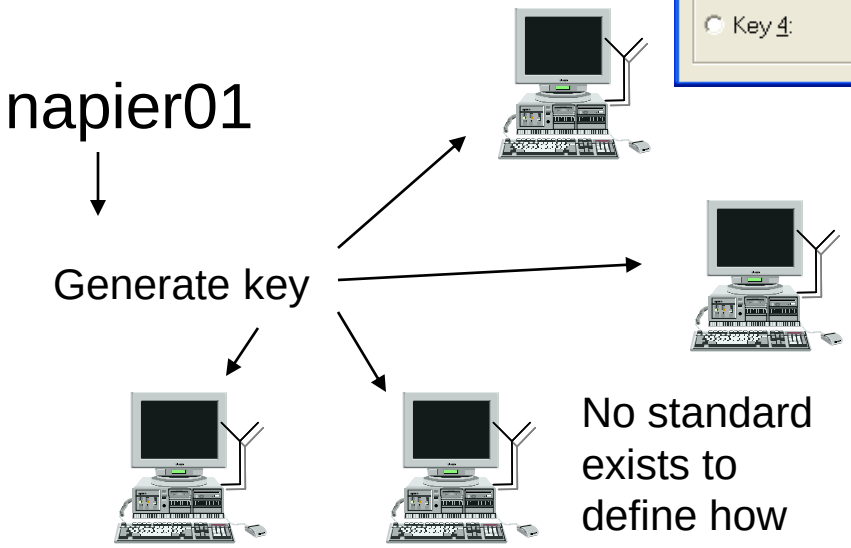
WPA – Wi-Fi Protected Access

RSNA – Robust Security Network Association
AES – Advanced Encryption Standard

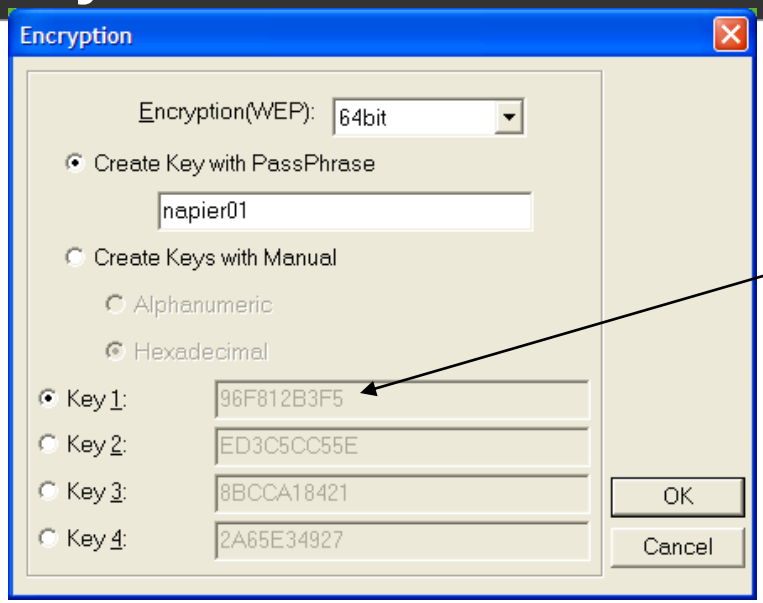
Generating the WEP key

WEP encryption key reduces eavesdropping

It stops unauthorized access to a Wireless Access Point (along with the SSID, of course)

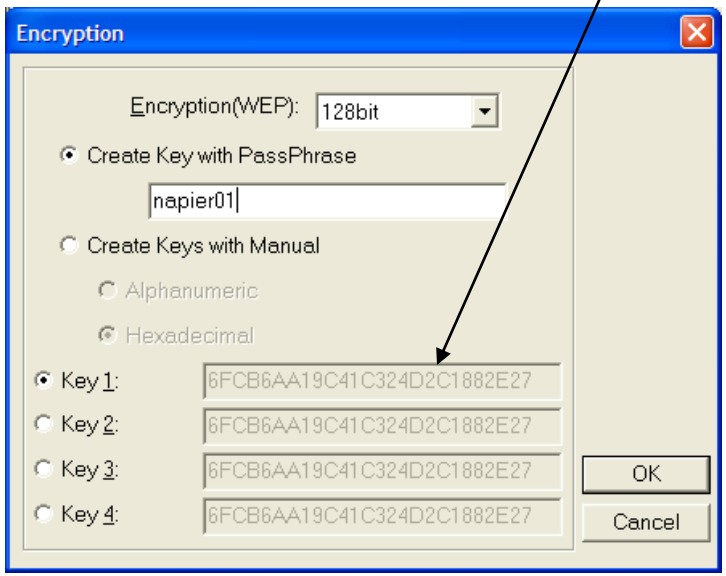


No standard exists to define how the WEP key is created

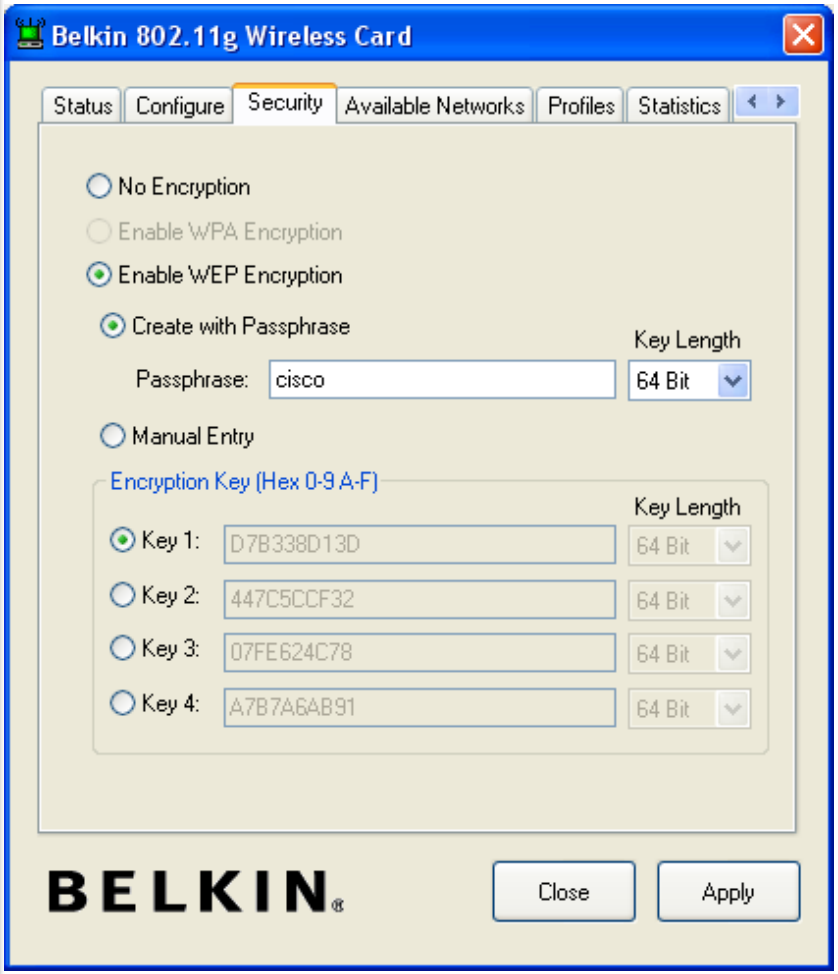


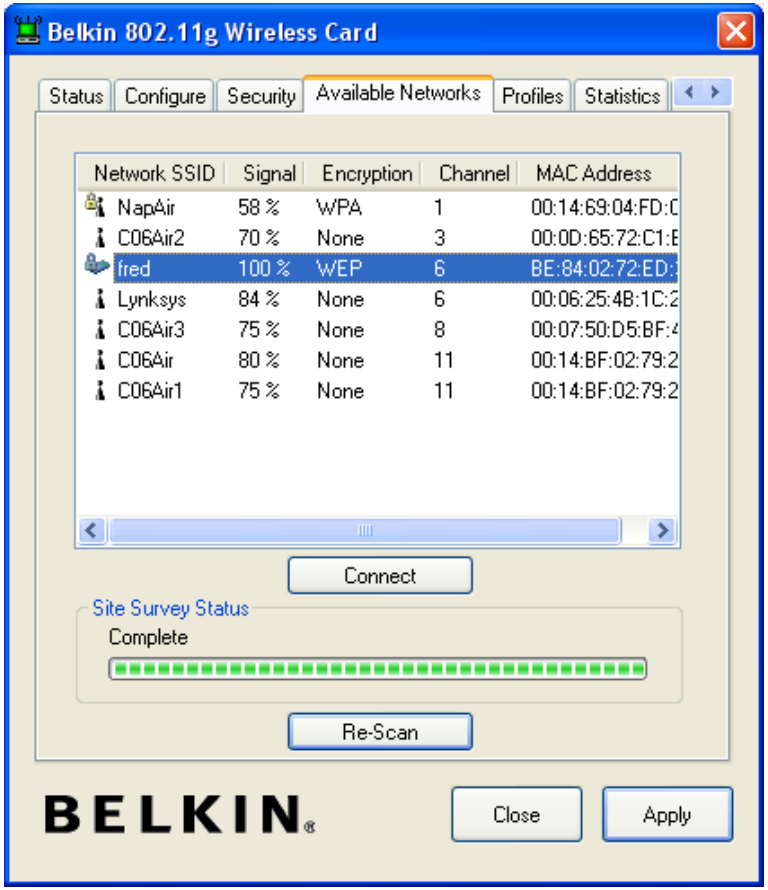
40-bit Keys (24 bits for IV)

104-bit Keys (24 bits for IV)

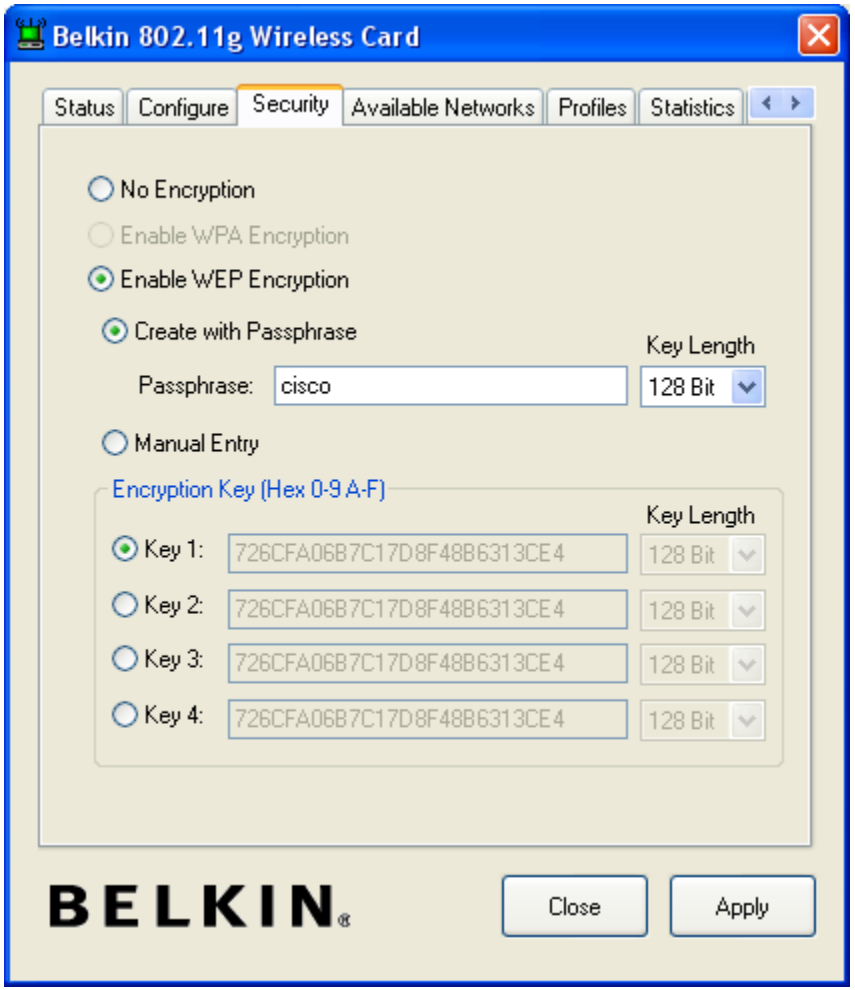


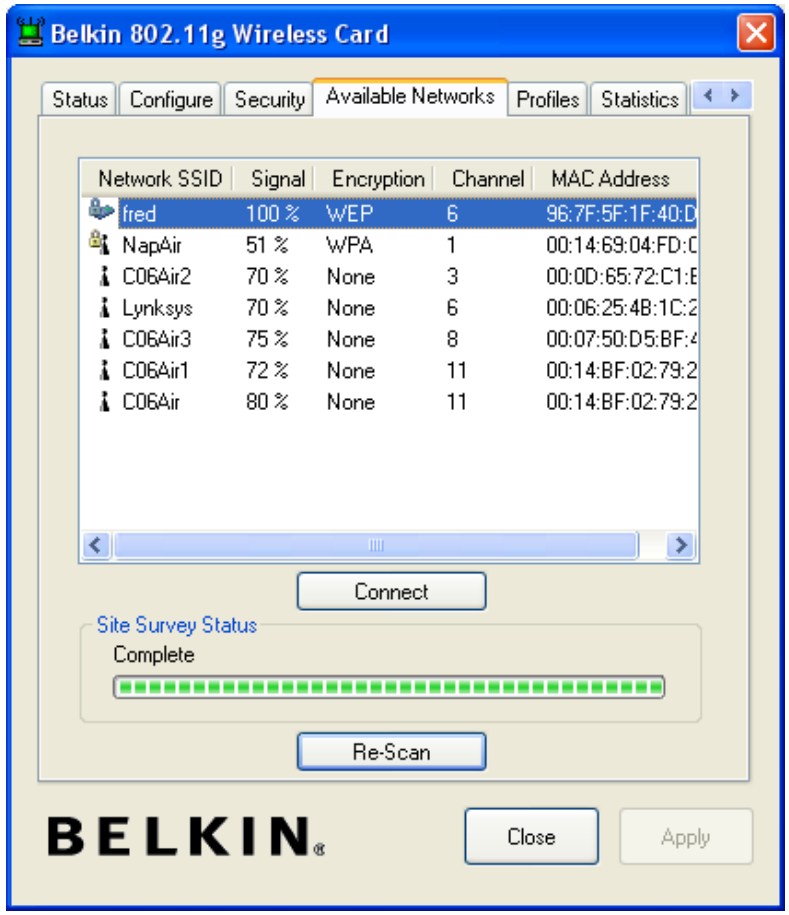
64-bit WEP key



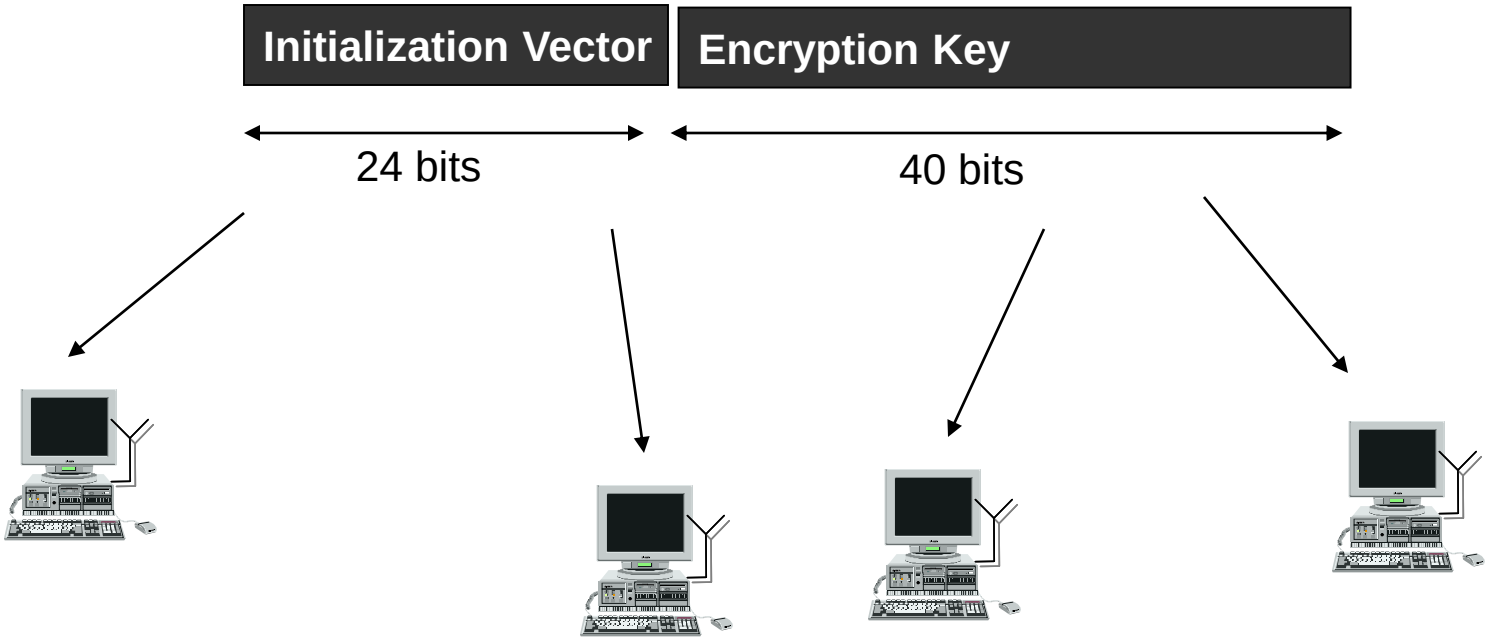


128-bit WEP key





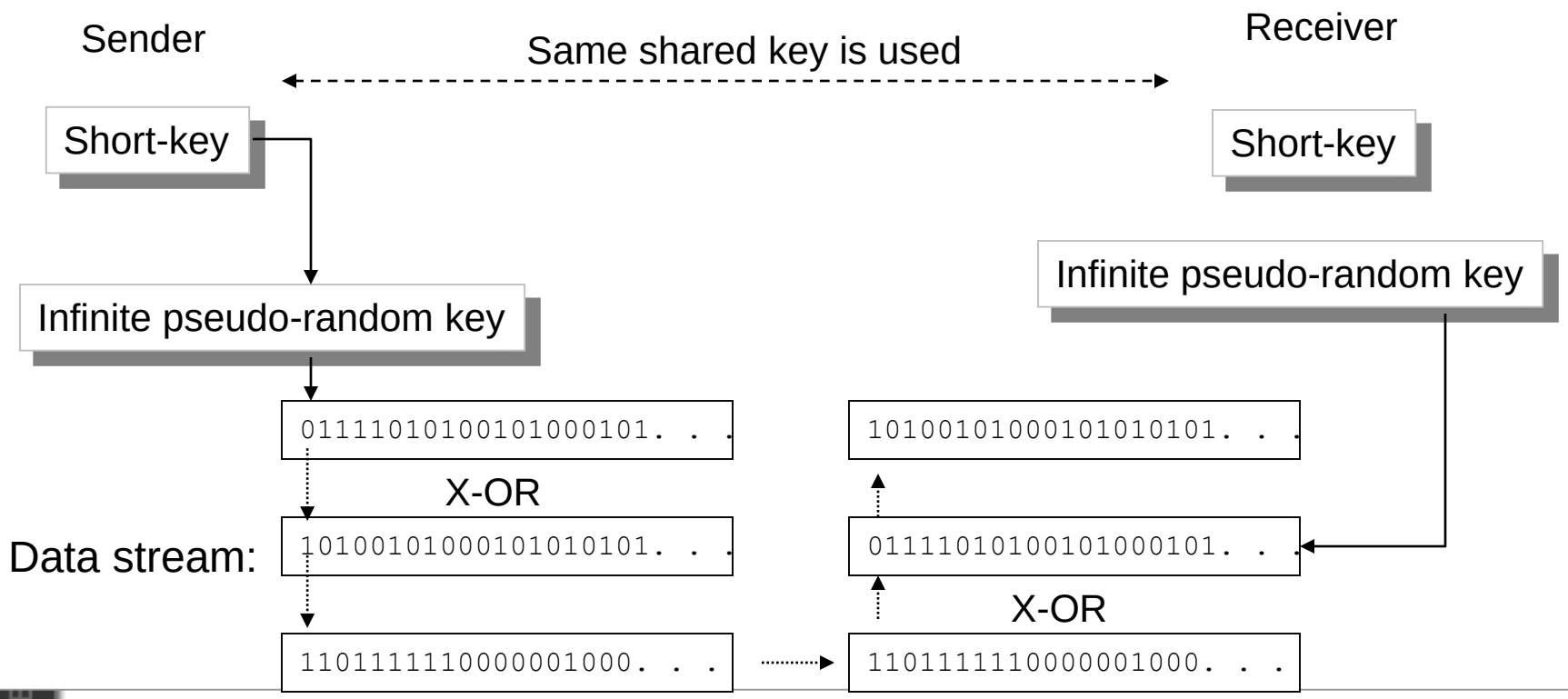
Same key is used for all nodes. Thus an eavesdropper can eventually gain the key



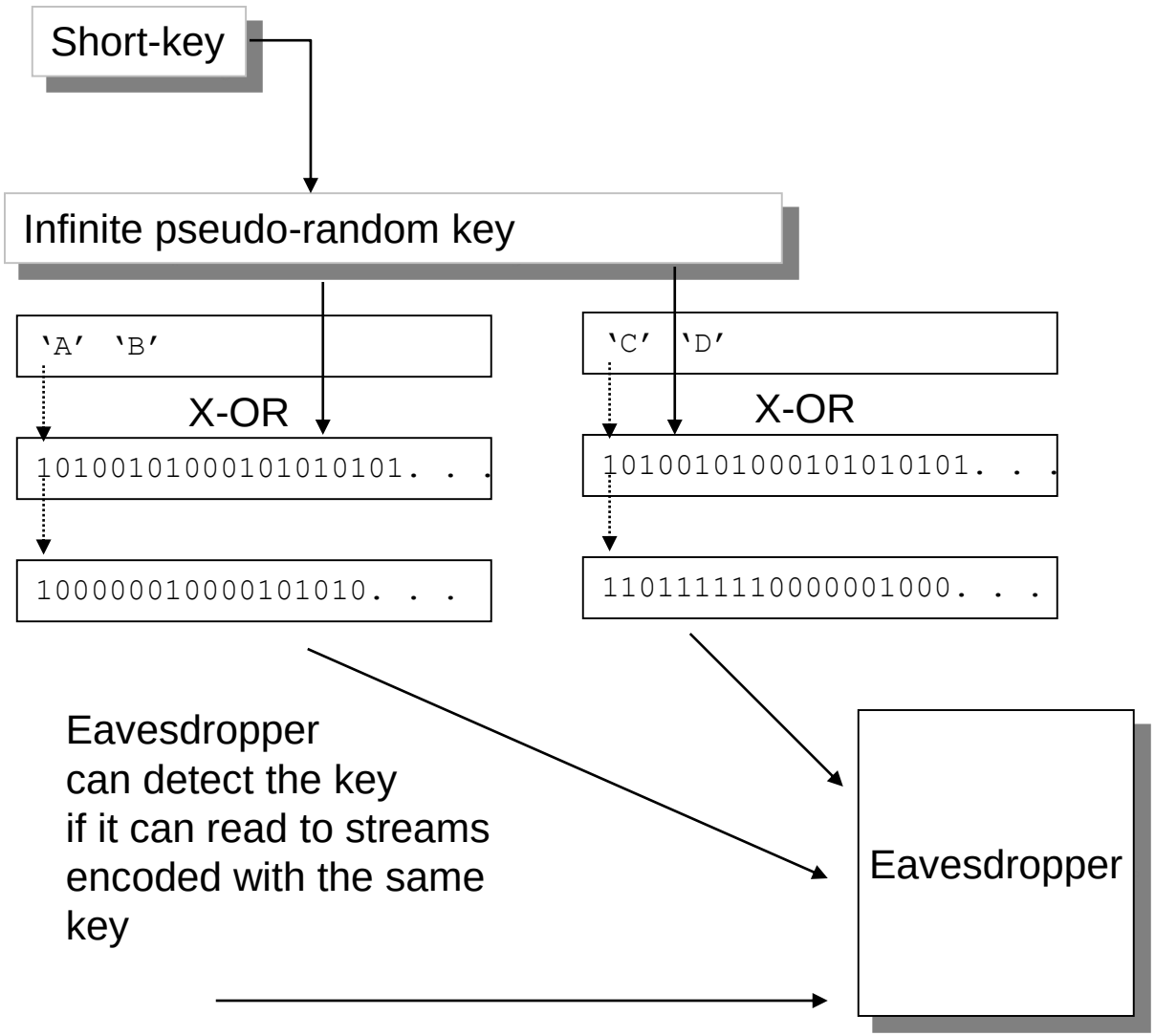
This key is used for encryption of all the data in the domain

WEP uses a stream cipher based on the RC4 algorithm.

- Expands a short key into an infinite pseudo-random key.

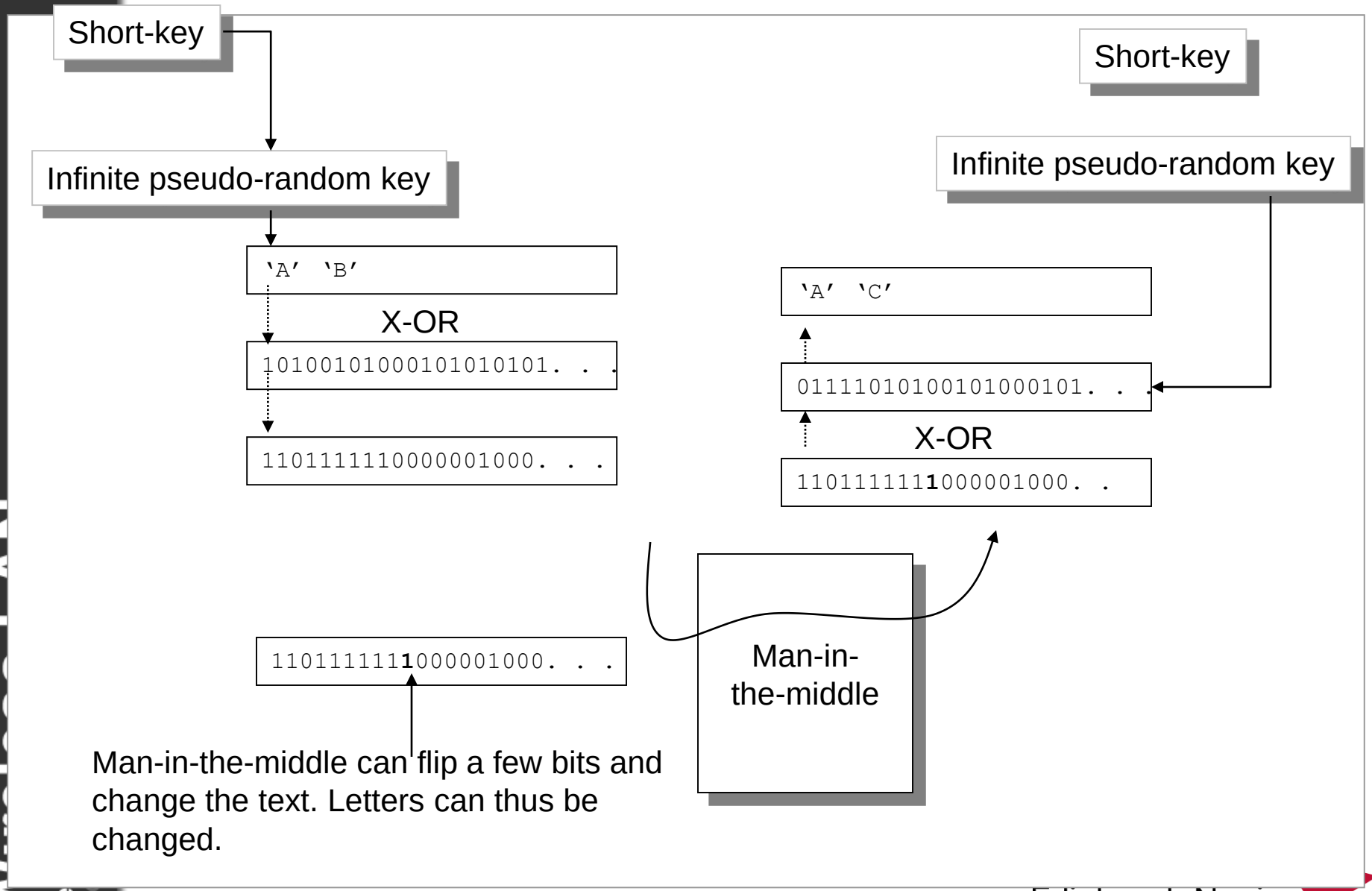


WEP - Possible Problem? Statistical Analysis



Author: Bill Buchanan

WEP - Possible Problem? Man-in-the-Middle



IV and IC

WEP guards against these attacks with:

An **Initialization Vector** (IV). This is a secret key which varies the key for every data packet.
An **Integrity Checker** (IC). This is a 32-bit CRC (Cyclic Redundancy Check). If bits are flipped, it will not give the same CRC value. Thus an error is caused.

Unfortunately both methods have not been implemented properly!!! Which leads to lots of problems.

Weakness of the Integrity Checker

01010101 10101010 01010101 01010101
11010101 10101010 01010101 01010111
01010101 10111010 01010101 01110111

01010101 10101**1**10 01010101 01010101
11010101 10101**1**10 01010101 01010111
01010101 10111010 01010101 01110111

Bits are flipped over consecutive bit positions, so that the overall CRC stays the same.

The IV is a 24-bit value, which is sent as **cleartext**.

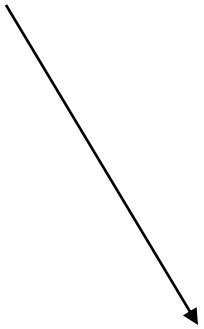
There can only be 2^{24} vectors (16,777,216)

If we use 1500 byte packets, the time to send each packet is 1500×8/11e6 = 1.1ms

Thus, if the device is continually sending the same vector will repeat after:

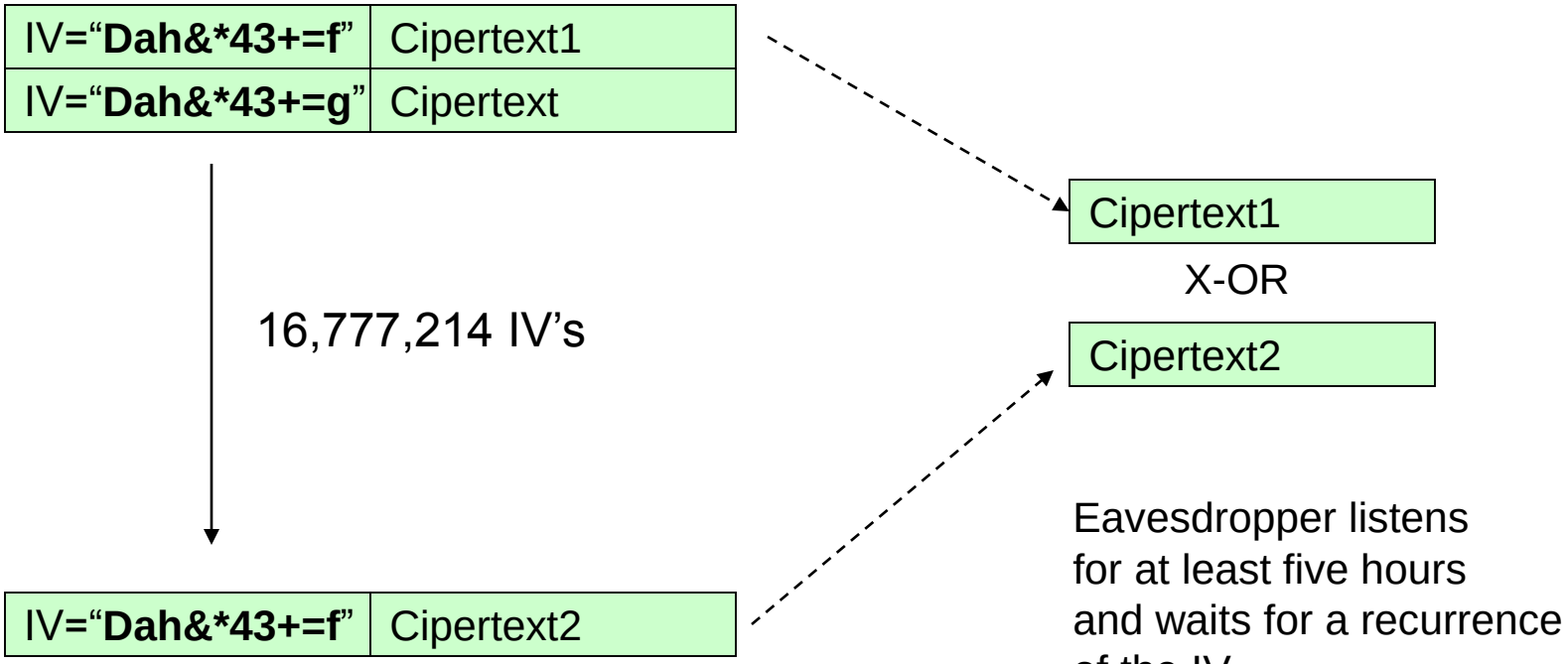
1.1ms × 16,777,216 = 18,302.4 seconds

which is **5 hours**



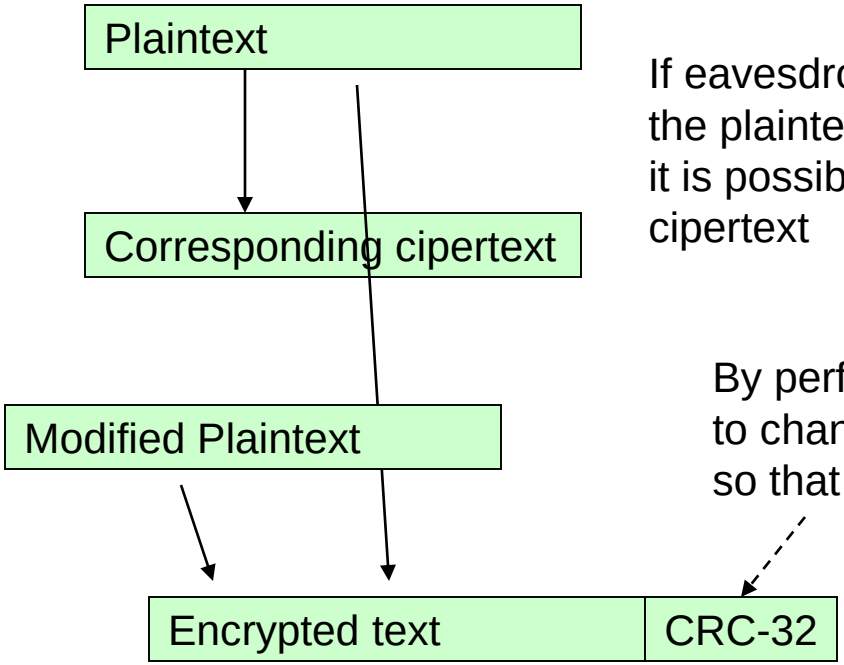
The attacker then takes the two cipertexts which have been encrypted with the same key, and performs a statistical analysis on it.

Passive Attack to Decrypt Traffic



Some network cards actually initial at zero, and then increment by 1 each time (in fact the standard does not even specify that the IV should change, at all.

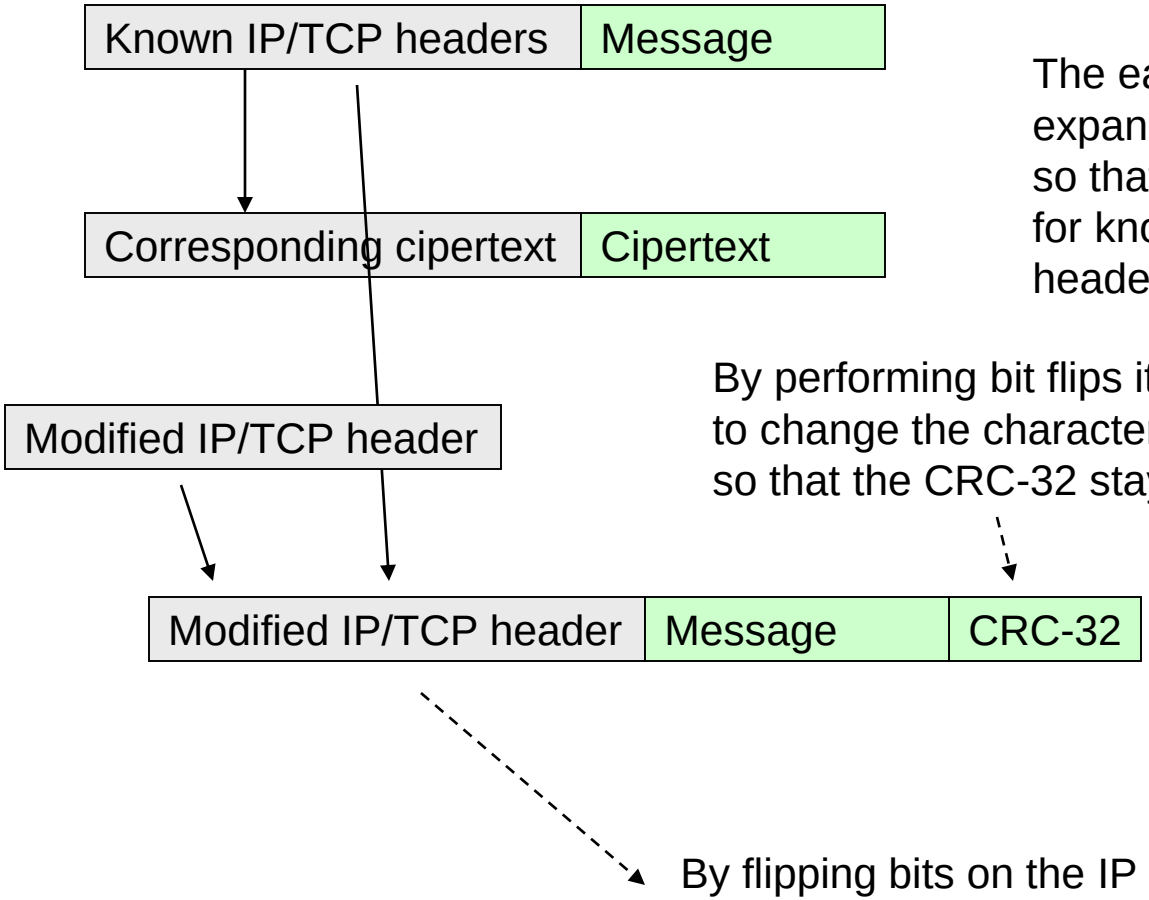
Active Attack to Inject Traffic



If eavesdropper knows part of the plaintext for a corresponding cipertext it is possible to build a correctly encrypted cipertext

By performing bit flips it is possible to change the characters in the plain-text so that the CRC-32 stays the same.

Active Attack from Both Ends

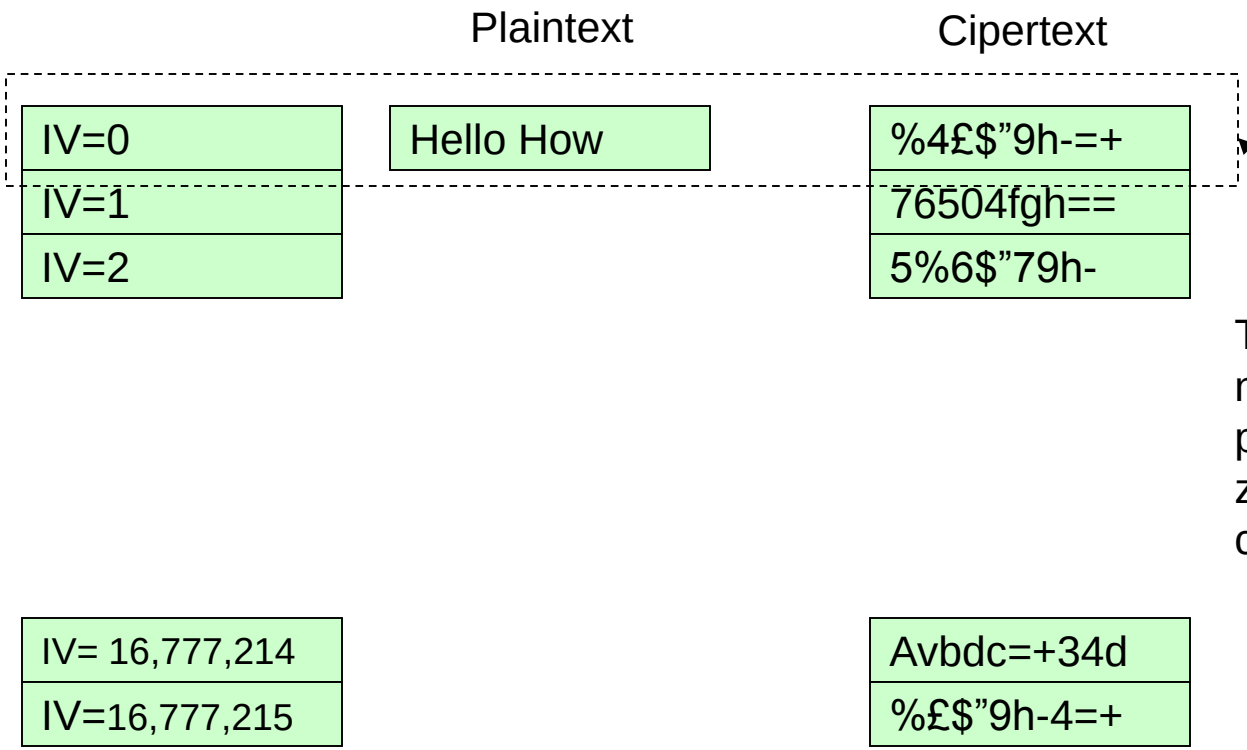


The eavesdropper can expand the method so that they can examine for know IP and TCP headers.

By performing bit flips it is possible to change the characters in the plain-text so that the CRC-32 stays the same.

By flipping bits on the IP address, the eavesdropper can send all data packets to their machine.

Table-based

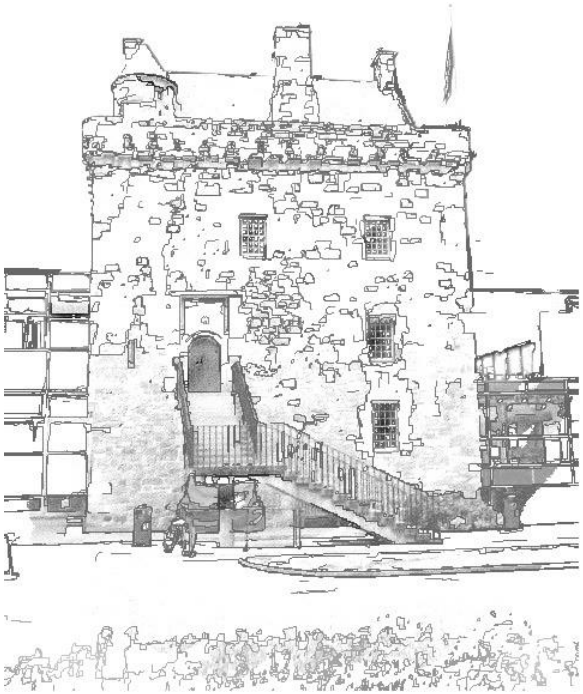

Plaintext
Cipertext
IV=0
Hello How
%4£$”9h-=+
IV=1
76504fgh==
IV=2
5%6$”79h-
The eavesdropper can now decrypt all the data packets with the IV of zero. Over time others can be learnt.
IV= 16,777,214
Avbdc=+34d
IV=16,777,215
%£$”9h-4=+
Eavesdropper stores a table of known keys for each IV (15GB)

```
# config t
(config)# int dot11radio0
(config-if)# encryption ?
(config-if)# encryption mode wep optional
(config-if)# encryption key 1 size 40bit 1122334455 transmit-key
(config)# exit


# config t
(config)# int dot11radio0
(config-if)# encryption mode wep optional
(config-if)# encryption key 1 size 128bit 12345678901234567890123456
   transmit-key
(config)# exit

(config)# int dot11radio0
(config-if)# encryption mode cipher tkip wep128
(config-if)# encryption key ?
(config-if)# encryption key 3 size 128bit 12345678901234567890123456
transmit-key
```

IEEE 802.11i



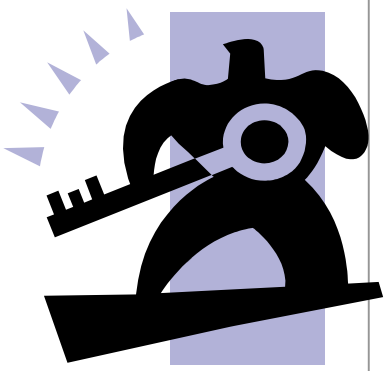
EAP - Efficient Application Protocols

It has been developed by the IEEE 802.11i Task Group as an end-to-end framework and uses 802.1X and EAP.

This is:

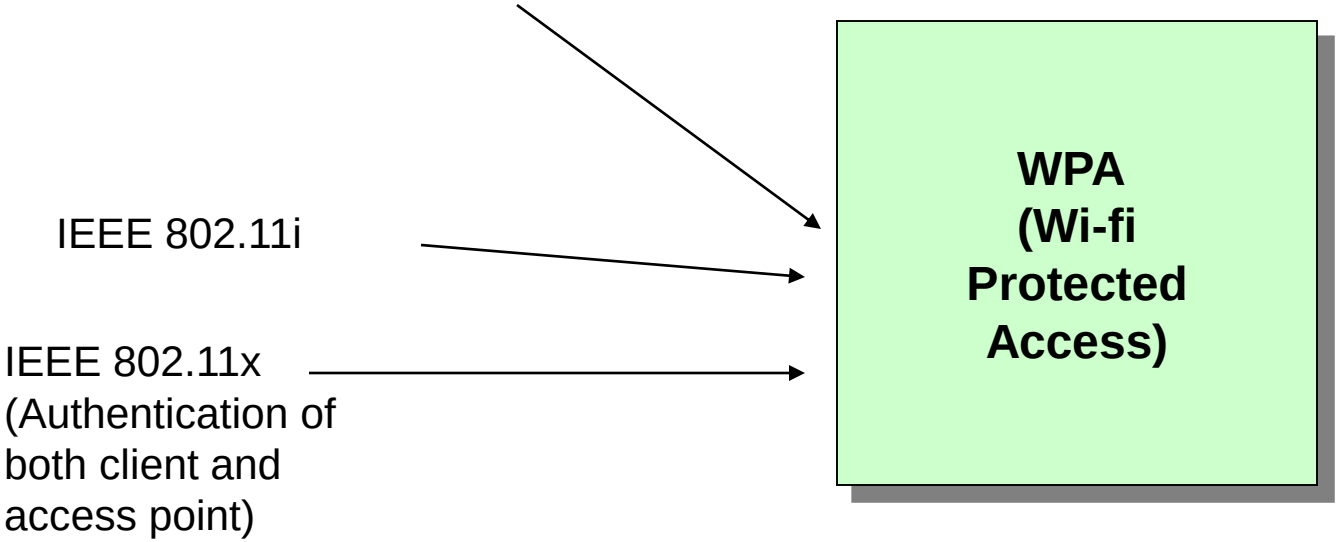
- **Authentication**. This is of both the client and the authentication server (such as a RADIUS server).
- **Encryption keys**. These are dynamically created after authentication. They are not common to the whole network.
- **Centralized policy control**. A session time-out generates a reauthentication and the generation of new encryption keys.

A wireless client cannot gain access to the network, unless it has been authenticated by the access point or a RADIUS server, and has encryption keys.

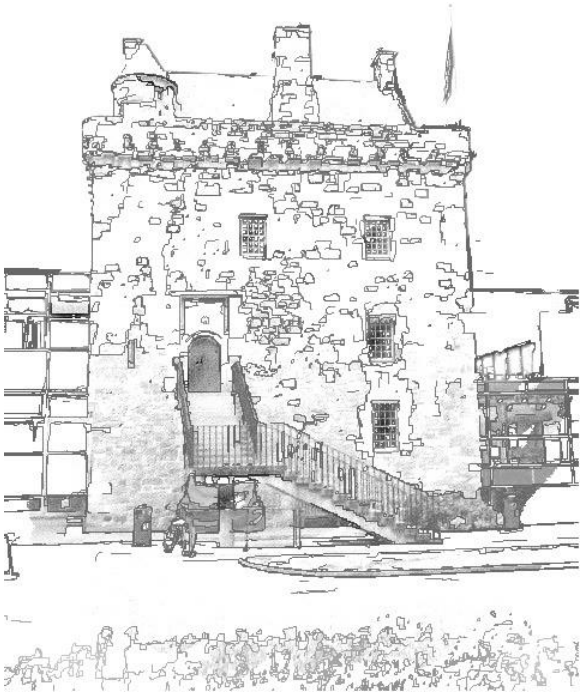


The new enhancements for WLAN are:

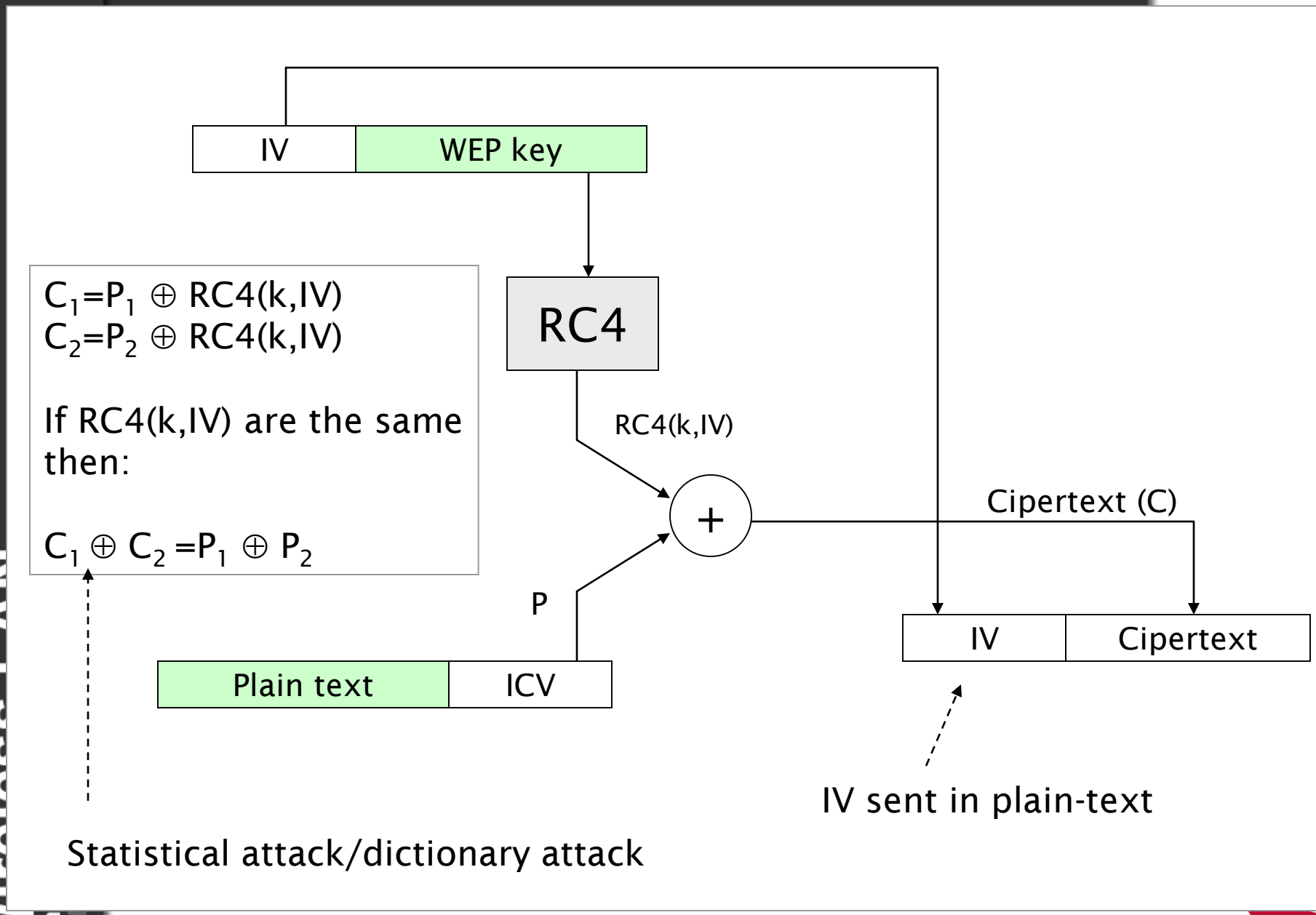
TKIP (Temporal Key Integrity Protocol) which are enhancements to RC4-based WEP. The IV has been increased to 48 bits (rather that 24 bits), and the Integrety Checker has been improved.
AES, which is a stronger alternative to RC4.



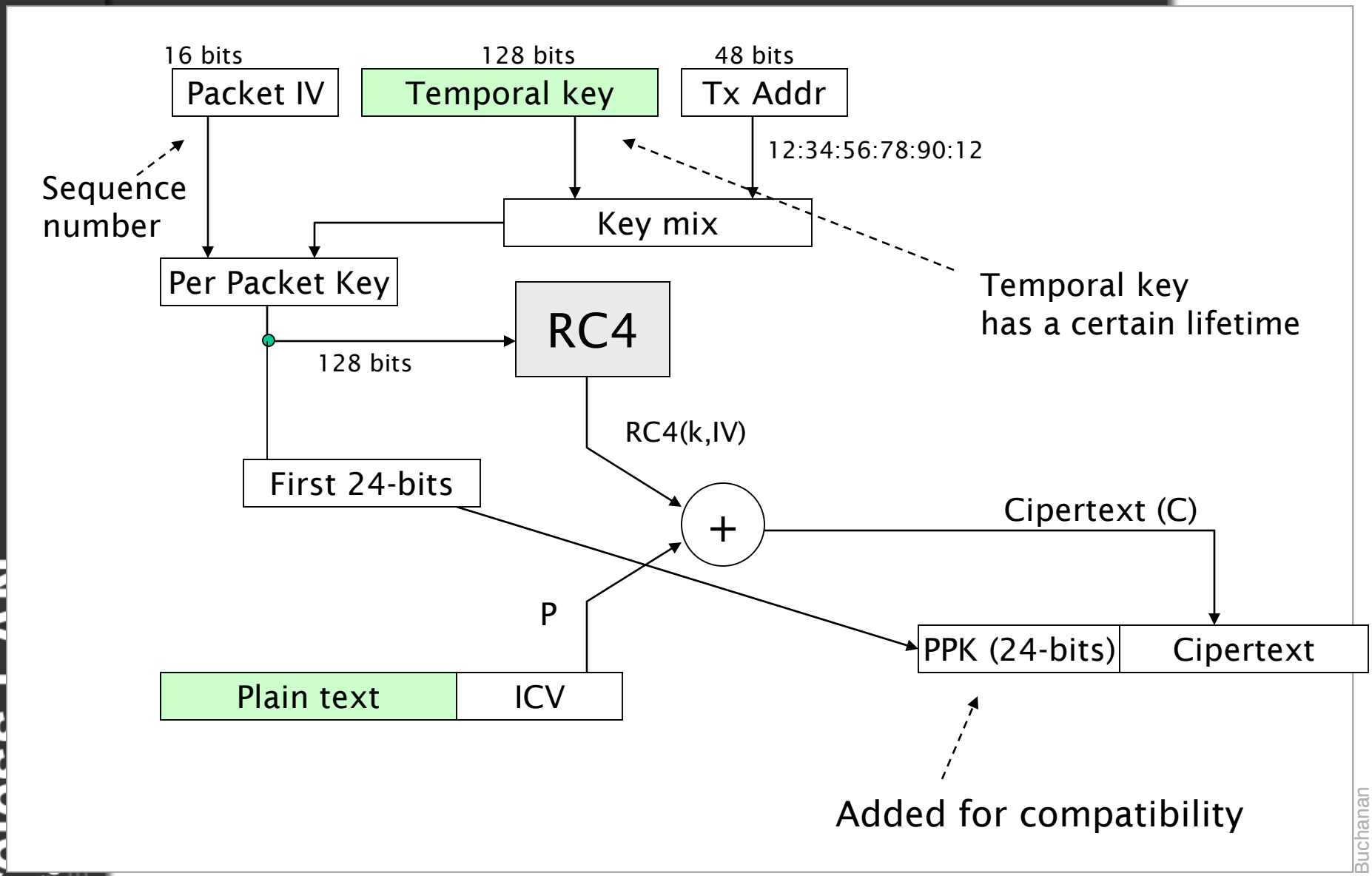
TKIP



Standard WEP



TKIP


16 bits
Packet IV
128 bits
Temporal key
48 bits
Tx Addr
12:34:56:78:90:12
Sequence number
Key mix
Per Packet Key
RC4
128 bits
Temporal key has a certain lifetime
RC4(k,IV)
First 24-bits
+
Cipertext (C)
P
PPK (24-bits)
Cipertext
Plain text
ICV
Added for compatibility

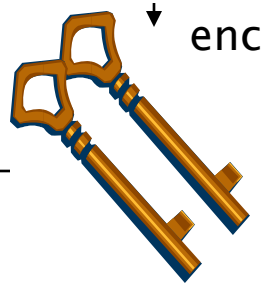
Re-keying

Master key

shared secret-key (generated for each session)

shared secret-key (generated for each session)

Used to pass encryption keys



Wireless Access Point

Temporal key (sending)

Temporal key (receiving)

Temporal key (sending)

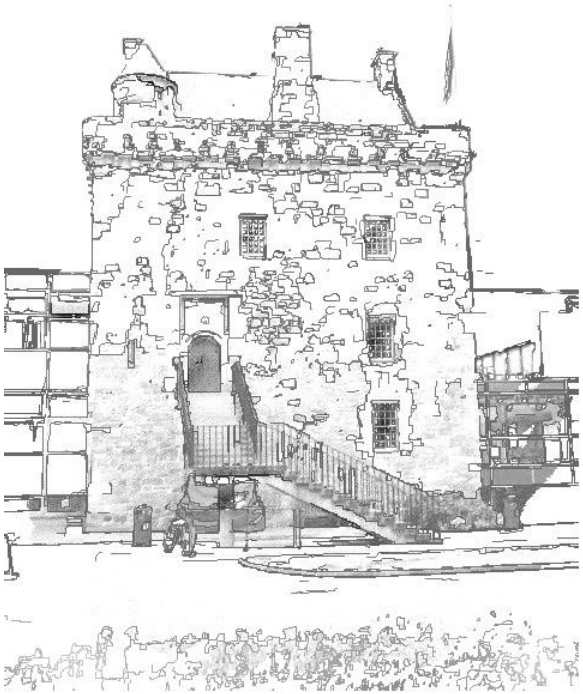
Temporal key (receiving)

Master key must be refreshed every 2^{16} packets

16 bits	128 bits	48 bits
Packet IV	Temporal key	Tx Addr

```
(config-if)# encryption mode ?
  ciphers  Optional data ciphers
  wep      Classic 802.11 privacy algorithm
(config-if)# encryption mode ciphers ?
  aes-ccm    WPA AES CCMP
  ckip       Cisco Per packet key hashing
  ckip-cmic  Cisco Per packet key hashing and MIC (MMH)
  cmic       Cisco MIC (MMH)
  tkip       WPA Temporal Key encryption
  wep128     128 bit key
  wep40      40 bit key
(config-if)# encryption mode ciphers tkip ?
  aes-ccm  WPA AES CCMP
  wep128   128 bit key
  wep40    40 bit key
  <cr>
(config-if)# encryption key 1 size
        128 12345678901234567890123456 transmit-key
```

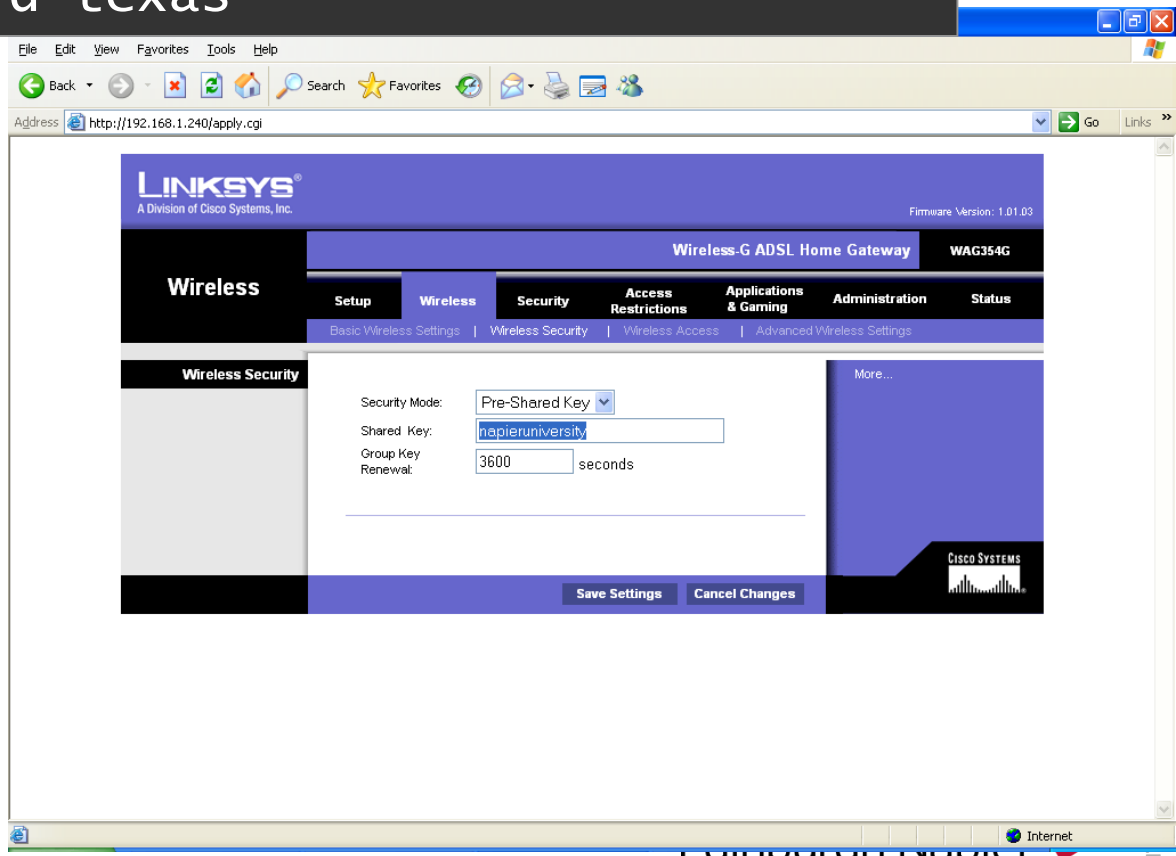
WPA-PSK



NAPIER UNIVERSITY
EDINBURGH

Author: Bill Buchanan

```
> enable
# config t
(config)# dot11 ssid texas
(config-ssid)# wpa-psk ascii napieruniversity
(config-ssid)# exit
(config)# int d0
(config-if)# ssid texas
```



```
> enable
# config t
(config)# dot11 ssid texas
(config-ssid)# wpa-psk ascii napieruniversity
(config-ssid)# exit
(config)# int d0
(config-if)# ssid texas
```

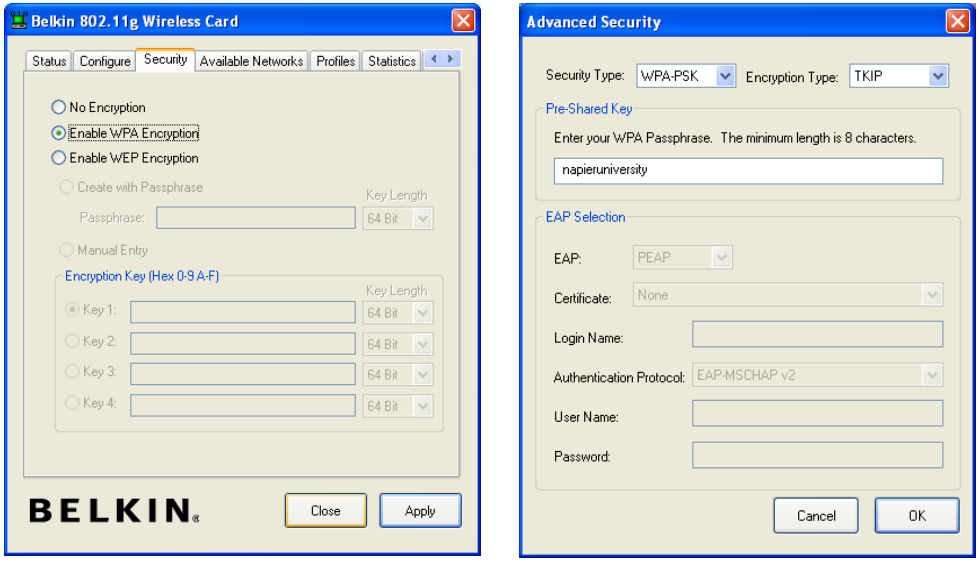


Figure 2: WPA-PSK (client)

```
> enable
# config t
(config)# dot11 ssid texas
(config-ssid)# wpa-psk ascii napieruniversity
(config-ssid)# exit
(config)# int d0
(config-if)# ssid texas
```

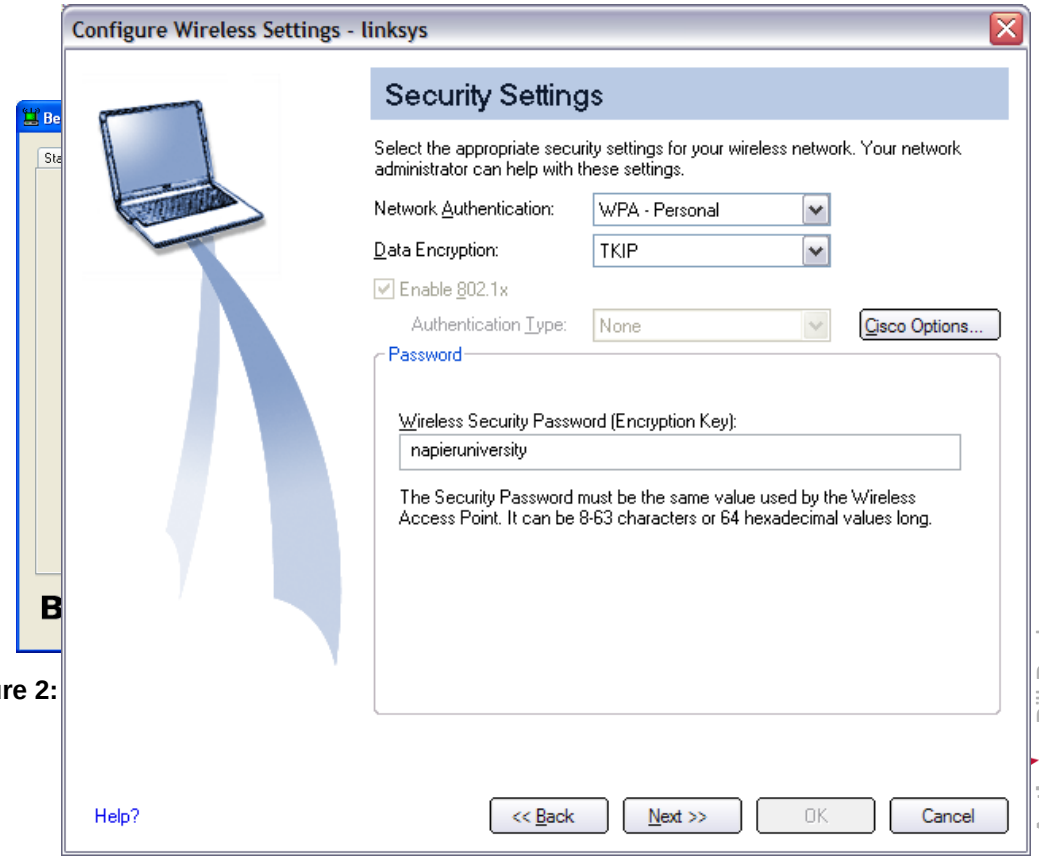
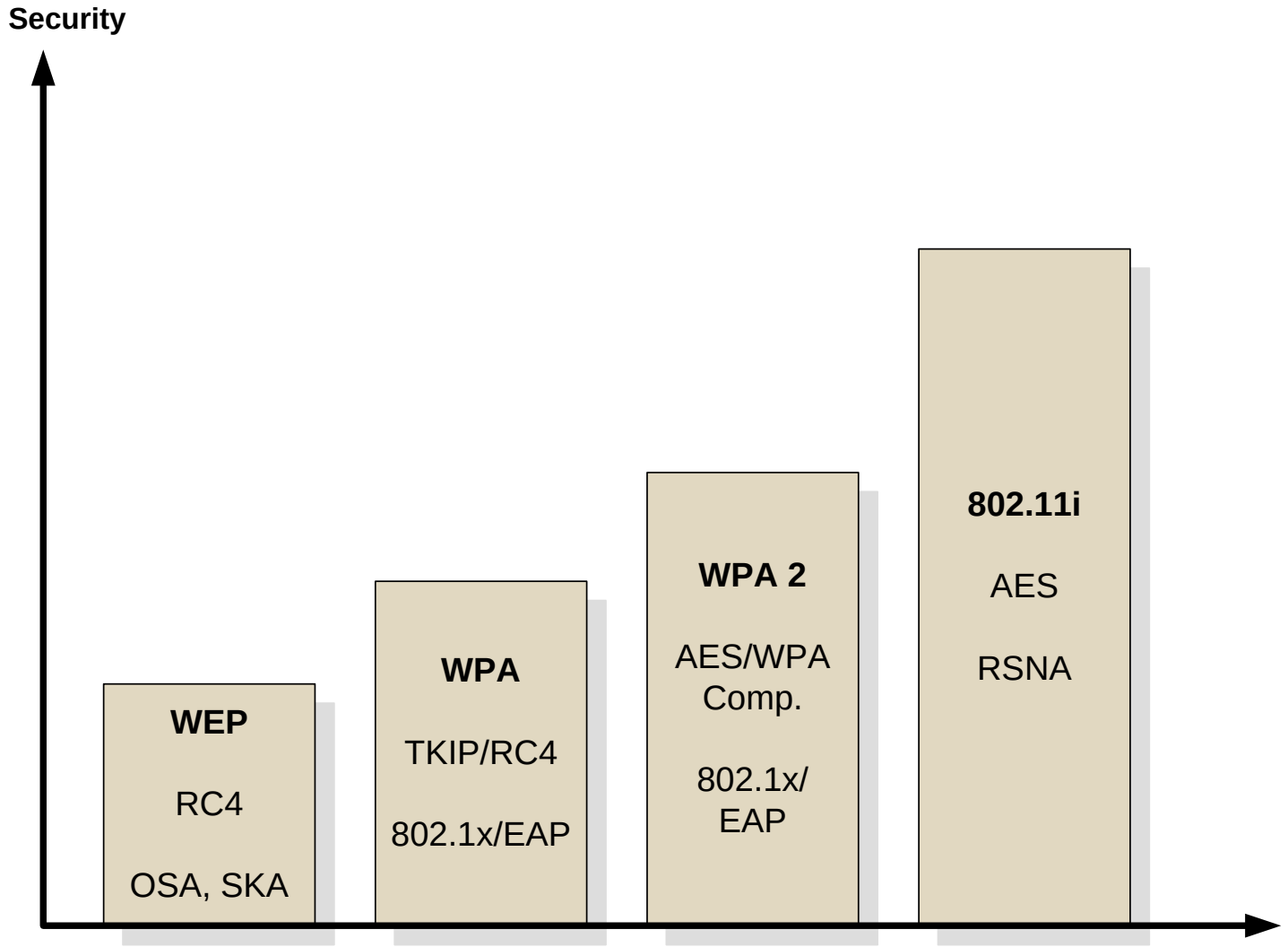


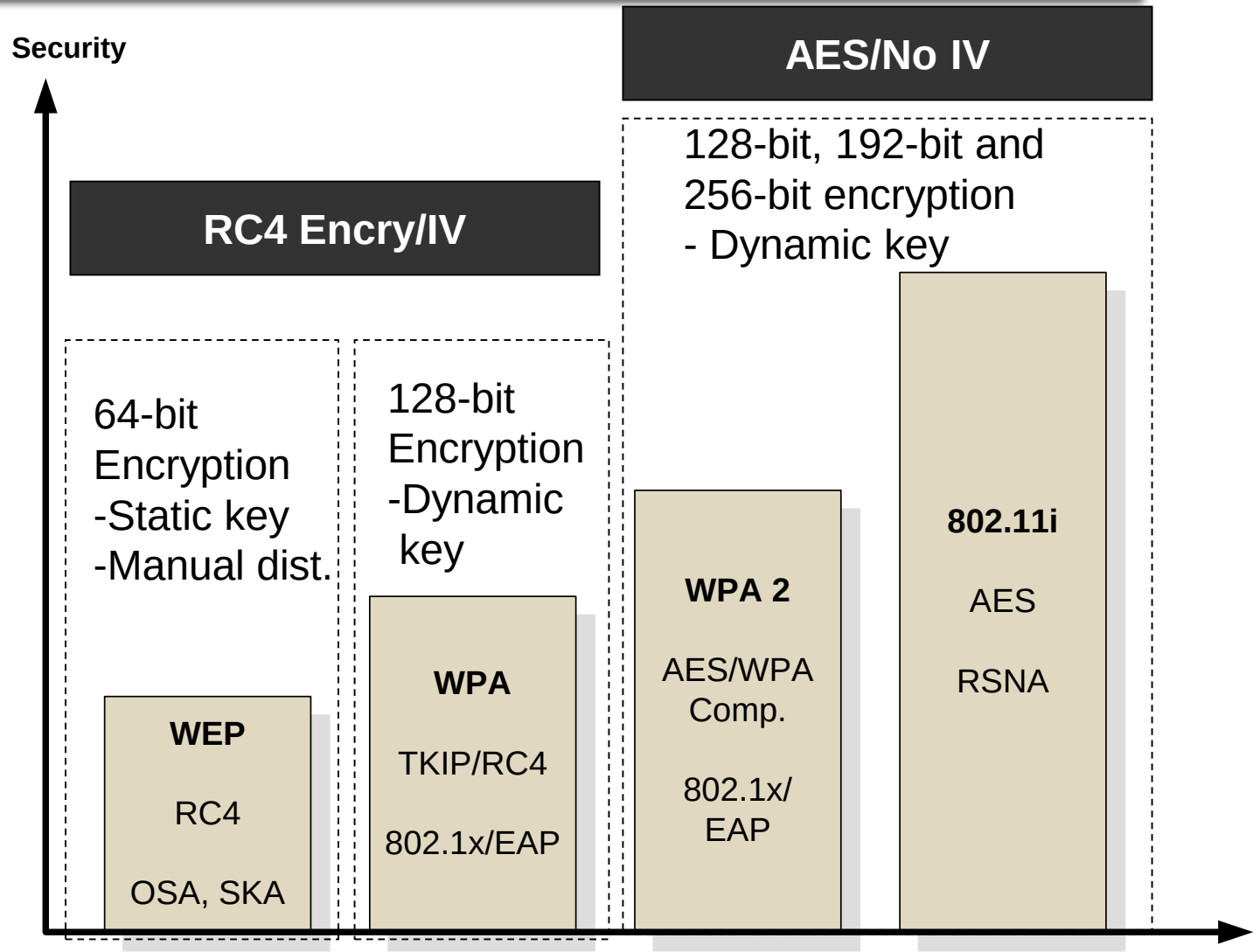
Figure 2:



WEP – Wireless Equivalent Protocol
OSA – Open System Auth.
SKA – Shared Key Auth.

WPA – Wi-Fi Protected Access

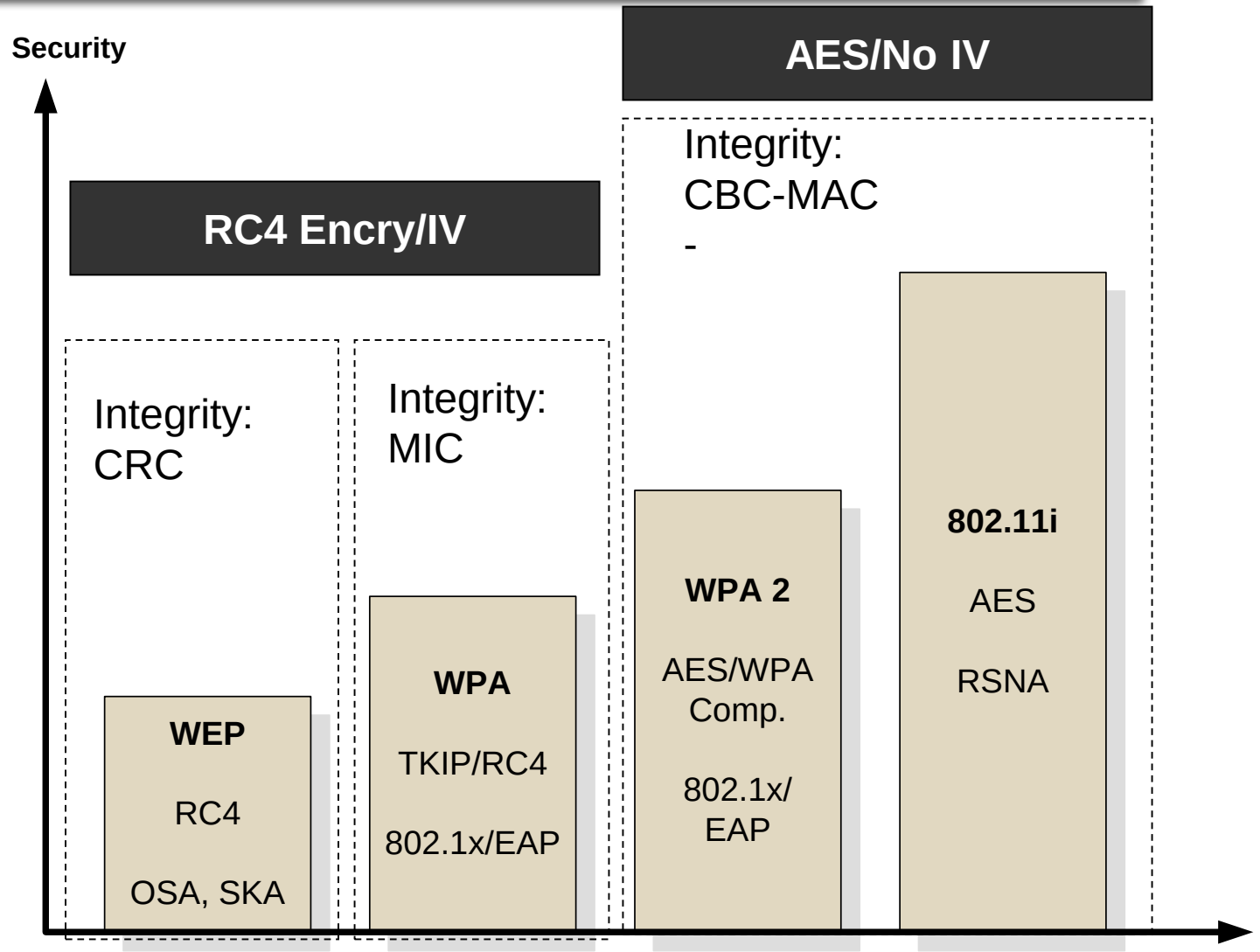
RSNA – Robust Security Network Association
AES – Advanced Encryption Standard



WEP – Wireless Equivalent Protocol
OSA – Open System Auth.
SKA – Shared Key Auth.

WPA – Wi-Fi Protected Access

RSNA – Robust Security Network Association
AES – Advanced Encryption Standard



WEP – Wireless Equivalent Protocol
OSA – Open System Auth.
SKA – Shared Key Auth.

WPA – Wi-Fi Protected Access

RSNA – Robust Security Network Association
AES – Advanced Encryption Standard