WiFi and Bluetooth security

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

WiFi networks

- The most common and the most convenient network access method today
- Connect various types of devices (laptop, mobile phone, tablet,…)
- Present “everywhere”: home (in bed…), work, airport, library, shops, city squares, hotels, coffee shops…
- However, not secure: broadcast medium which can be heard by anyone, and where anyone can send transmissions.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

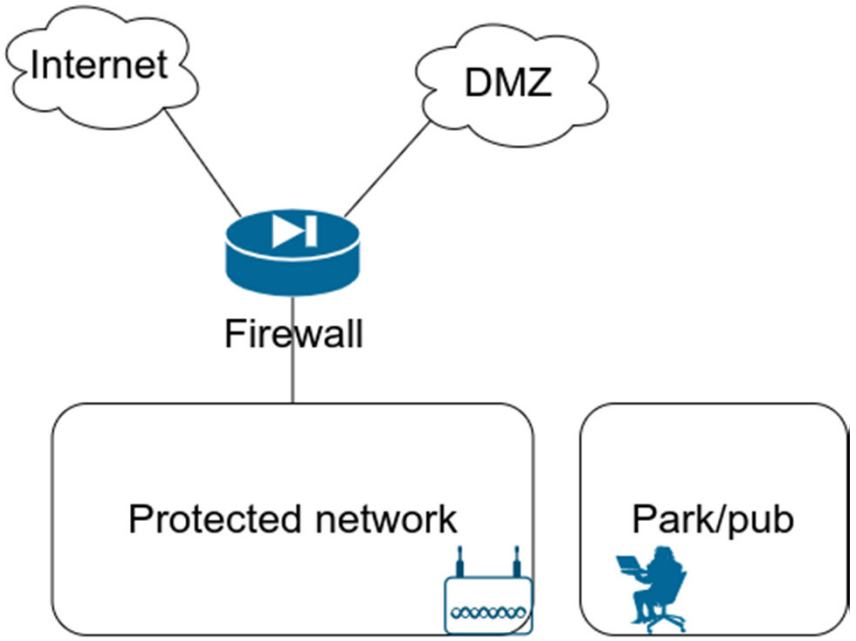
WiFi security

- Eavesdropping is easy (if not encrypted)
- Injecting bogus messages into the network is easy
- Replaying previously recorded messages is easy
- Illegitimate access to the network and its services is easy
- Denial of service is easily achieved by jamming
- Injecting bogus APs is easy

ISSES
Co-funded by the Erasmus+ Programme of the European Union

WiFi presents challenges to the corporate IT security

- No physical control over connectivity
- BYOD can mean unsecure user devices in the offices
- Public WiFi for guests
- Network access behind the firewall (protection policy)
- Strict policy should be imposed



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Mobile device challenges

- Untrusted mobile devices - maintained by the user – lack of physical control
- Use of third-party (potentially unsafe) applications
- Use of devices on untrusted networks
- Use of untrusted content
- Use of location services (GPS, WiFi assisted)

ISSES
Co-funded by the Erasmus+ Programme of the European Union

WiFi standards and concepts

- WiFi generations: 802.11 a/b/g/n/ac/ax
- Work in 2.4 and 5 GHz bands
- Clients associates with some AP
- An access point will continually broadcast an SSID, which will be used by clients to identify and attach to the network.
- The SSID is typically viewed as the text string that end users see when they are searching for a wireless network
- SSID can be hidden, and then client has to know in advanced the SSID of the network to which it connects
- SSID can be sniffed (so hidden SSID isn't a protection)
- BSSID – AP ID - MAC address of the AP

ISSES
Co-funded by the Erasmus+ Programme of the European Union

WiFi sniffing with wireshark (monitoring port)

No.	Time	Source	Destination	Protocol	Length
52	0.699648148	Tp-LinkT_ec:b1:30	Broadcast	802.11	303
53	0.719885455	Tp-LinkT_ec:b1:30	SamsungE_c2:5b:e7	802.11	416
54	0.722973943	Tp-LinkT_ec:b1:30	SamsungE_c2:5b:e7	802.11	416
55	0.726419623	Tp-LinkT_ec:b1:30	SamsungE_c2:5b:e7	802.11	416
56	0.729980983	Tp-LinkT_ec:b1:30	SamsungE_c2:5b:e7	802.11	416

```
    [FCS Status: Good]
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
      Timestamp: 0x0000000105573d80
      Beacon Interval: 0,102400 [Seconds]
    ▶ Capabilities Information: 0x0431
  ▼ Tagged parameters (239 bytes)
    ▼ Tag: SSID parameter set: stanke
        Tag Number: SSID parameter set (0)
        Tag length: 6
        SSID: stanke
    ▼ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
        Tag Number: Supported Rates (1)
        Tag length: 8
        Supported Rates: 1(B) (0x82)
        Supported Rates: 2(B) (0x84)
        Supported Rates: 5.5(B) (0x8b)
        Supported Rates: 11(B) (0x96)
        Supported Rates: 6 (0x0c)
        Supported Rates: 9 (0x12)
        Supported Rates: 12 (0x18)
        Supported Rates: 18 (0x24)
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

WiFi sniffing with wireshark (monitoring port)

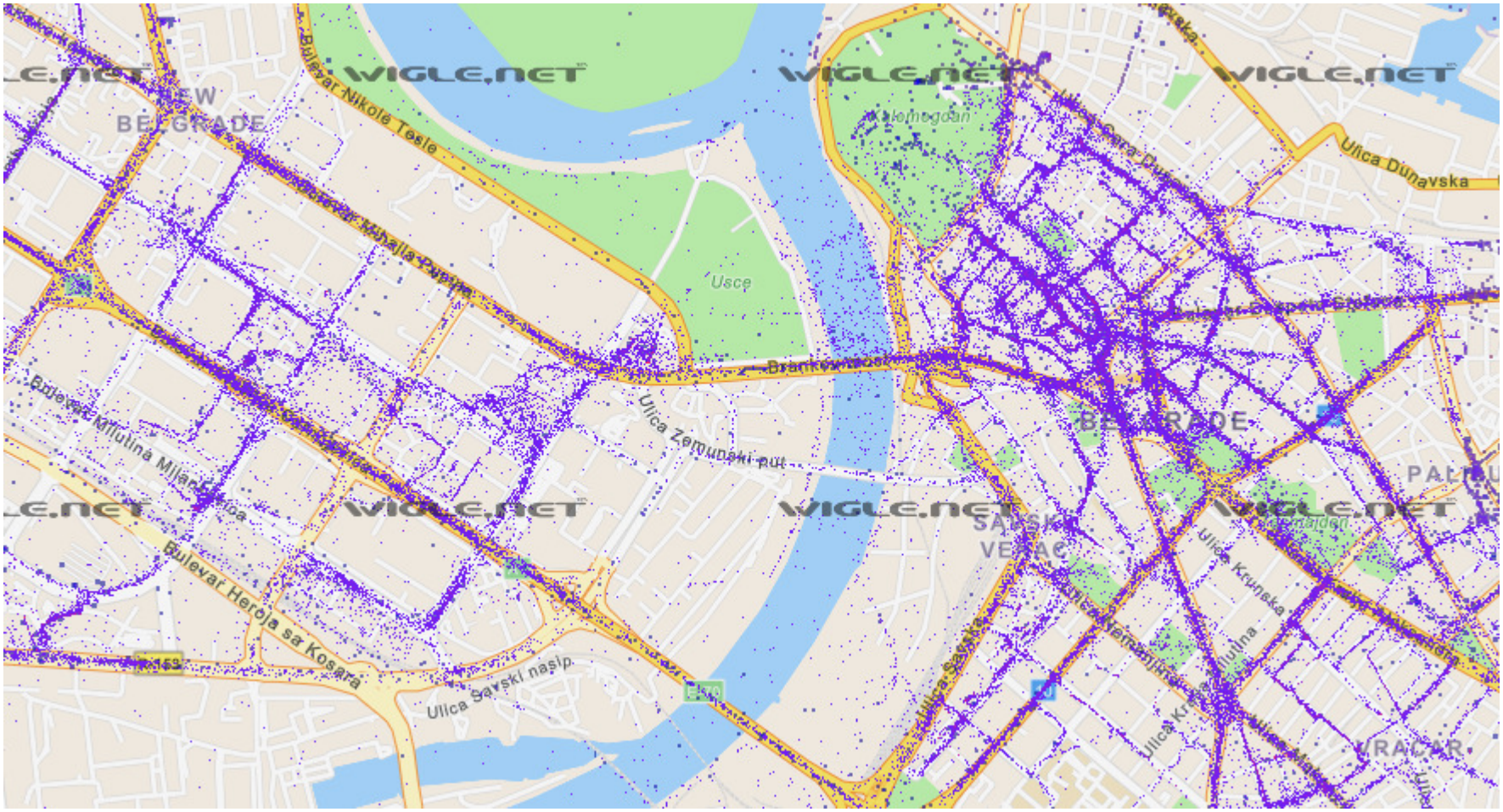
No.	Time	Source	Destination	Protocol
52	0.699648148	Tp-LinkT_ec:b1:30	Broadcast	802.11
53	0.719885455	Tp-LinkT_ec:b1:30	SamsungE_c2:5b:e7	802.11
54	0.722973943	Tp-LinkT_ec:b1:30	SamsungE_c2:5b:e7	802.11
55	0.726419623	Tp-LinkT_ec:b1:30	SamsungE_c2:5b:e7	802.11
56	0.729980983	Tp-LinkT_ec:b1:30	SamsungE_c2:5b:e7	802.11

```
▼ Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  ▶ Present flags
    MAC timestamp: 9919202327
  ▶ Flags: 0x10
    Channel frequency: 2457 [BG 10]
  ▶ Channel flags: 0x0000
    Antenna signal: -67dBm
▼ 802.11 radio information
    Channel: 10
    Frequency: 2457MHz
    Signal strength (dBm): -67dBm
    TSF timestamp: 9919202327
▼ IEEE 802.11 Probe Response, Flags: ........C
    Type/Subtype: Probe Response (0x0005)
  ▼ Frame Control Field: 0x5000
        .... ..00 = Version: 0
        .... 00.. = Type: Management frame (0)
        0101 .... = Subtype: 5
    ▶ Flags: 0x00
    .000 0001 0011 1010 = Duration: 314 microseconds
    Receiver address: SamsungE_c2:5b:e7 (f4:0e:22:c2:5b:e7)
    Destination address: SamsungE_c2:5b:e7 (f4:0e:22:c2:5b:e7)
    Transmitter address: Tp-LinkT_ec:b1:30 (b0:48:7a:ec:b1:30)
    Source address: Tp-LinkT_ec:b1:30 (b0:48:7a:ec:b1:30)
```

ISSES

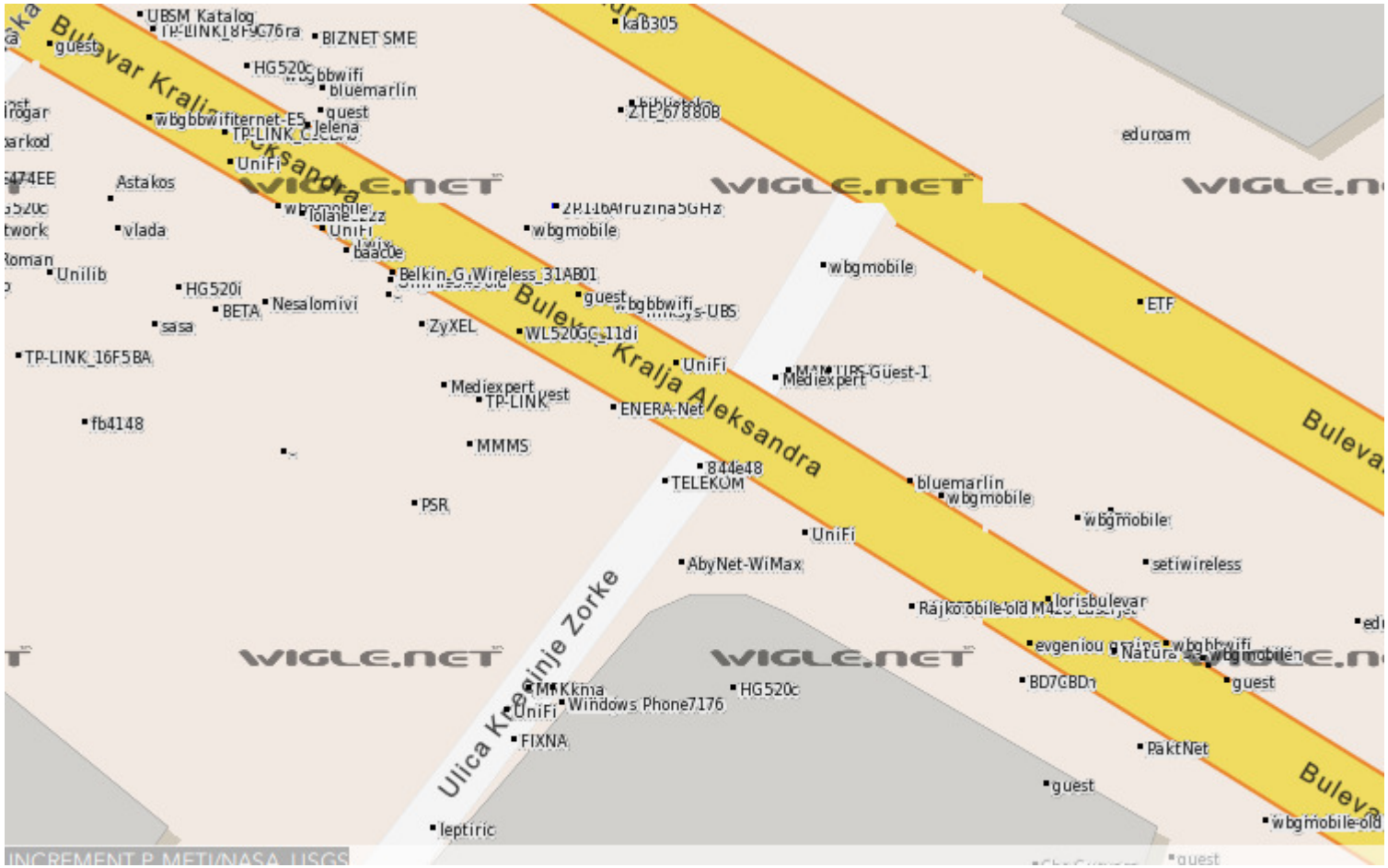
Co-funded by the
Erasmus+ Programme
of the European Union

WiFi geo-location is known



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

Around ETF



ISSES

Co-funded by the Erasmus+ Programme of the European Union

WiFi authentication

1. Open authentication – no authentication, just the SSID has to be matched
2. Shared key authentication (private mode):
   - The client sends an authentication request to the access point.
   - The access point returns a challenge to the client.
   - The client encrypts the challenge using the shared key it is configured with.
   - The access point uses the same shared key to decrypt the challenge; if the responses match, then the client is validated and is given access to the network.
   - Problems – key change, leaving the group, etc.
3. Centralized authentication (EAP) – enterprise mode

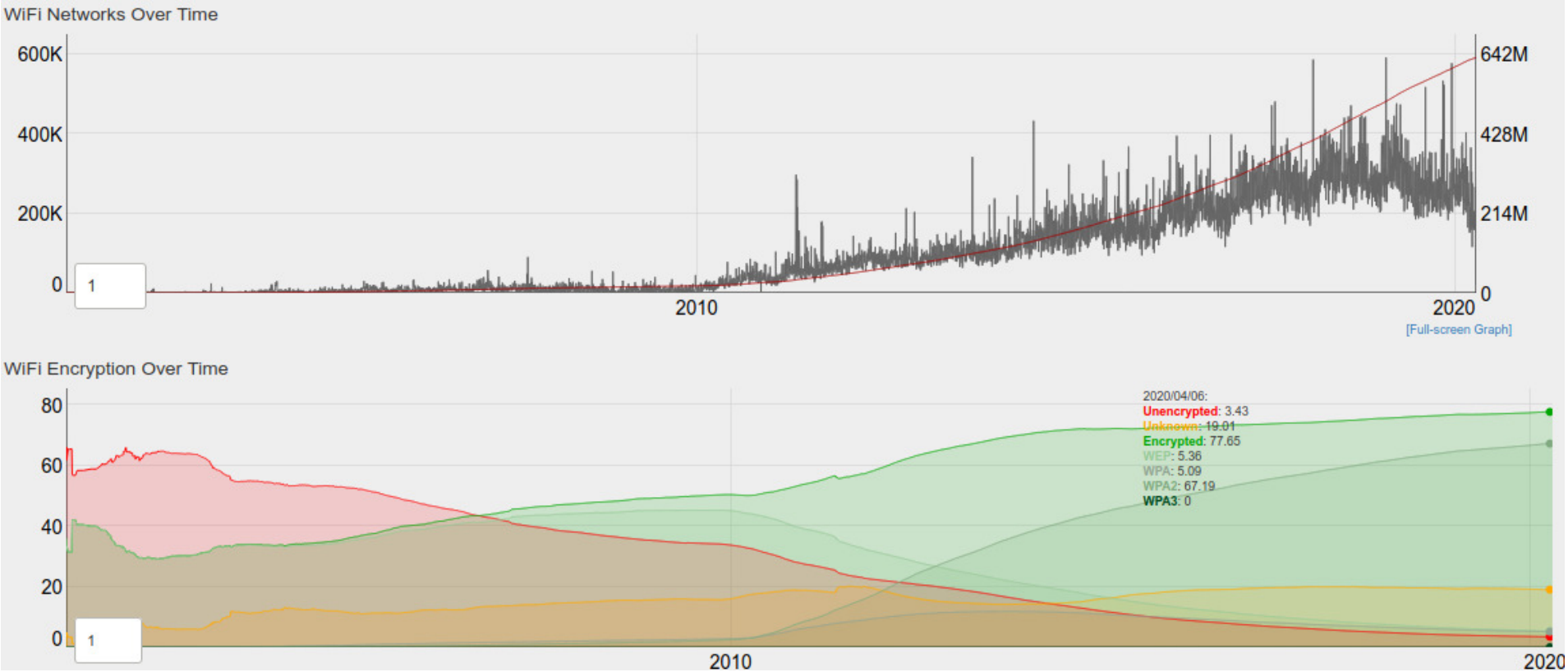
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Traffic encryption

- Everybody can sniff wireless traffic – has to be encrypted
  - WEP – weak – **NOT RECOMMENDED**!
  - WPA - weak – **NOT RECOMMENDED**!
  - WPA2 – the most common today (802.11i - 2004)
  - WPA3 – since 2018

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Number of WiFi networks



ISSES
Co-funded by the Erasmus+ Programme of the European Union

WiFi networks in Serbia (April 2020)

Region	Count
Централна Србија	310,766
Војводина	141,334
u0426u0435u043du0442u0440...	1

Postal Code	Count
11070	43,660
11000	37,102
21101	35,658
21000	22,550
21102	21,914
11102	18,686
11080	17,946
18000	15,181
24000	14,688
11001	12,070
11050	11,042
70857	9,556
21137	9,235
11271	8,749
11108	7,138

Encryption	Count
WPA	311,678
?	62,652
WPA	51,363
WEP	13,405
	13,008

ISSES
Co-funded by the Erasmus+ Programme of the European Union

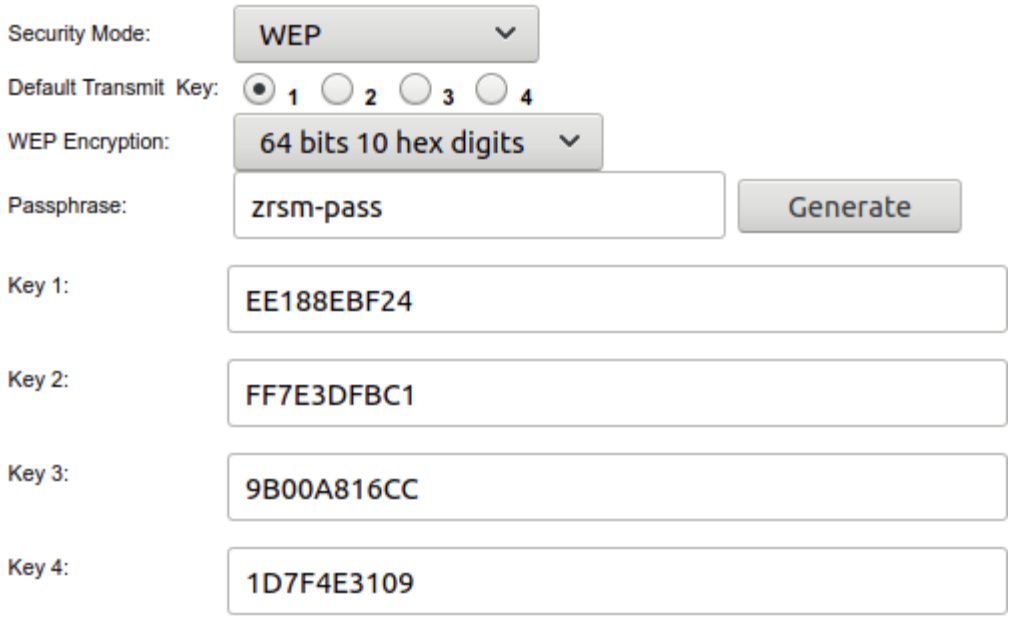
WEP operation

- Authentication
  1. client-> AP: authenticate request
  2. AP -> client: authenticate challenge (r)
  3. client-> AP: authenticate response (encrypted r)
  4. AP -> client: authenticate success/failure
- After successful authentication – association
- WEP uses RC4 stream cypher:
  - 64 bit key = 24bit IV + 40bit key
  - 128 bit WEP key = 24 bit IV + 104 bit key

ISSES
Co-funded by the Erasmus+ Programme of the European Union

WEP configuration

- Old Linksys router
- (demo lab excersise)



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

RC4 (1)

- A variable-length key of from 1 to 256 bytes (8 to 2048 bits) is used to initialize a 256-byte state vector S, with elements S[0], S[1], . . . , S[255].
  - S contains a permutation of all 8-bit numbers from 0 through 255.
  - For encryption and decryption, a byte *k* is generated from S by selecting one of the 255 entries in a systematic fashion.
  - As each value of *k* is generated, the entries in S are once again permuted.

```
/* Initialization */
for i = 0 to 255 do
 S[i] = i;
 T[i] = K[i mod keylen];
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

RC4 (2)

- A temporary vector, T, is also created from key and IV.
  - If the length of the key K is 256 bytes, then K is transferred to T.
  - Otherwise, for a key of length *keylen* bytes, the first *keylen* elements of T are copied from K, and then K is repeated as many times as necessary to fill out T.
- T is used to produce initial permutation of S

```
/* Initial Permutation of S */
j = 0;
for i = 0 to 255 do
    j = (j + S[i] + T[i]) mod 256;
    Swap (S[i], S[j]);
```

ISSES
Co-funded by the Erasmus+ Programme of the European Union

RC4 (3)

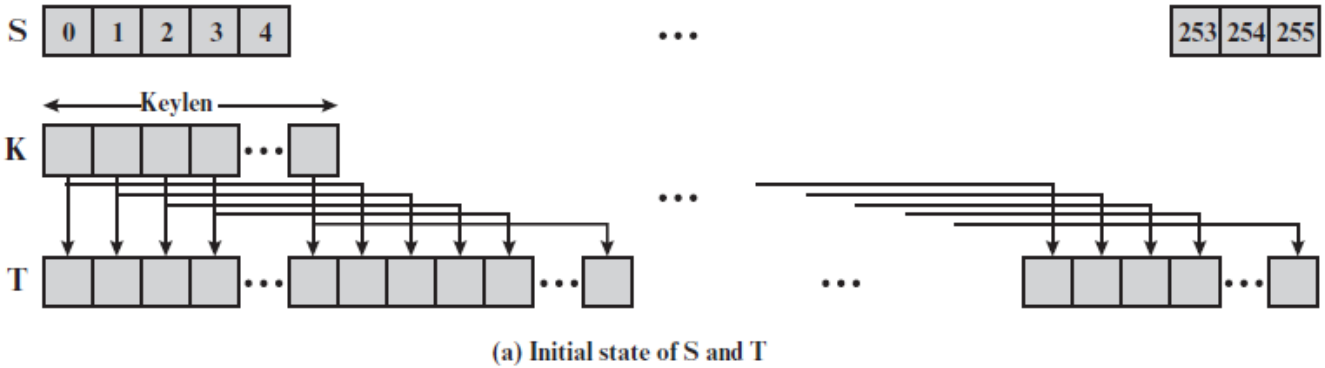
- Once the S vector is initialized, the input key is no longer used.
- Stream generation involves cycling through all the elements of S[i], and for each S[i], swapping S[i] with another byte in S according to a scheme dictated by the current configuration of S.
- After S[255] is reached, the process continues, starting over again at S[0]
- **To encrypt, XOR the value k with the next byte of plaintext.**
- **To decrypt, XOR the value *k* with the next byte of ciphertext.**

```
/* Stream Generation */
i, j = 0;
while (true)
  i = (i + 1) mod 256;
  j = (j + S[i]) mod 256;
  Swap (S[i], S[j]);
  t = (S[i] + S[j]) mod 256;
  k = S[t];
```

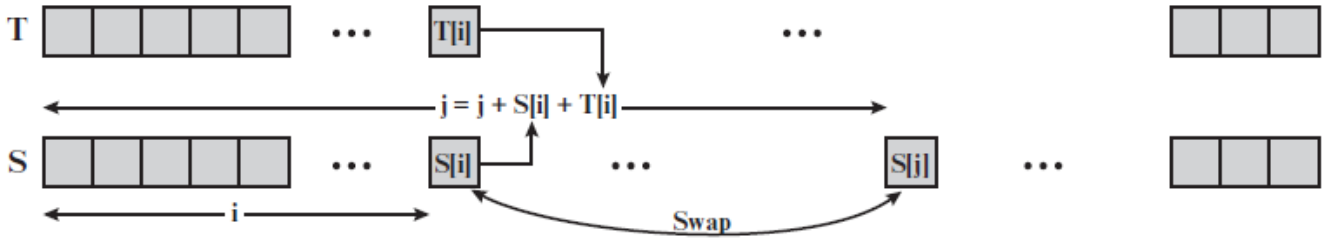
ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

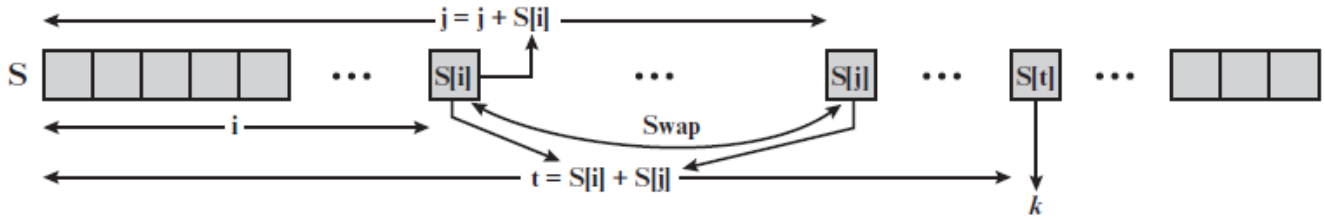
RC4 (4)



(a) Initial state of S and T



(b) Initial permutation of S

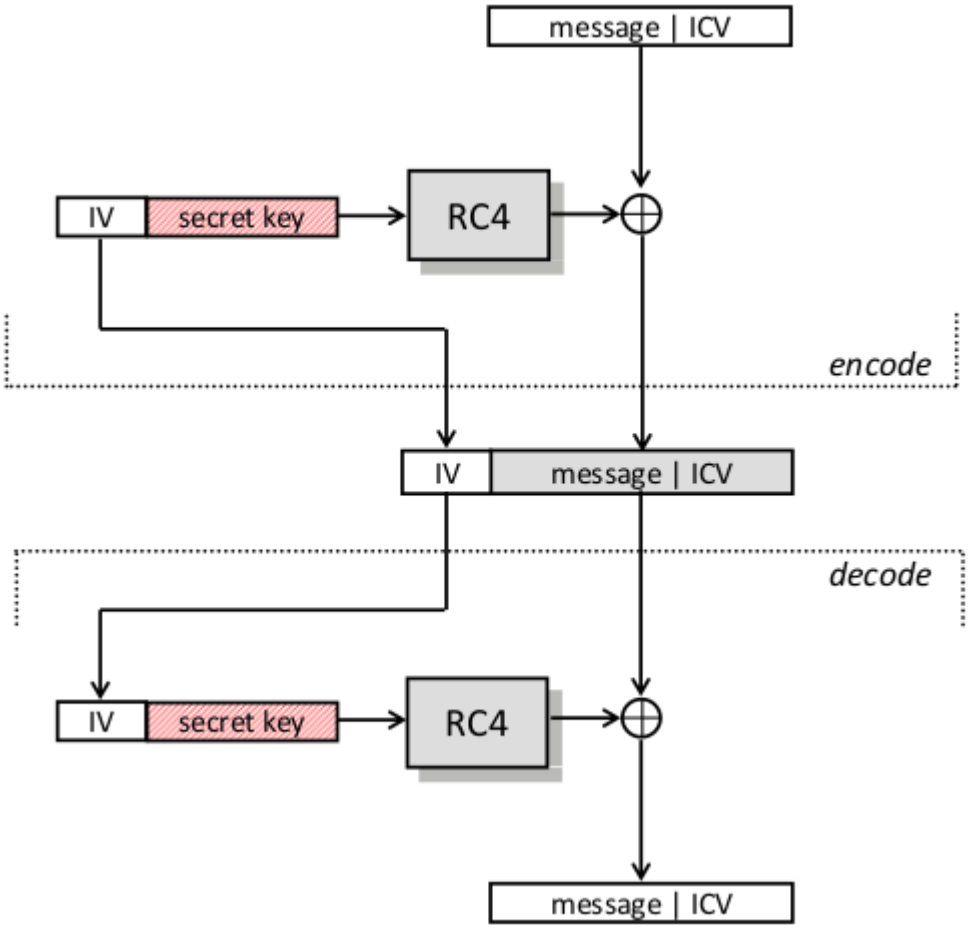


(c) Stream generation

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

WEP encryption



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

WEP vulnerabilities

- CRC32 (Cyclic Redundancy Check), used in integrity checking, is flawed, and with slight modifications packets may be modified consistently by attackers to produce their desired results.
- Initialization vectors (IVs) are only 24 bits in length, meaning that an entire pool of IVs can be exhausted by a mildly active network in 5 hours or less.
- WEP is susceptible to known plaintext attacks through the analysis of packets.
- Keys may be uncovered through the analysis of packets, allowing for the creation of a decryption table.
- WEP is susceptible to denial-of-service (DoS) attacks through the use of associate and disassociate messages, which are not authenticated by WEP.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Breaking WEP

- The important part of breaking the WEP protocol is intercepting as many IVs as possible before attempting to recover the key.
- The collection of IVs is done through the process of sniffing or capturing.
- Collecting and saving IVs allows you to perform analysis: The more packets, the easier it becomes to retrieve the keys. (but it can take time…)

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

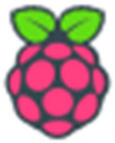
Breaking WEP steps

1. Start the wireless interface on the attacking system in **monitor mode** on the specific access point channel. This mode is used to listen to all the packets in the air.
2. Probe the target network with the wireless device to determine if packet injection can be performed.
3. Select a tool such as aireplay-ng to perform a fake authentication with the access point.
4. Start the Wi-Fi sniffing tool to **capture IVs**. If you're using aireplay-ng, ARP request packets can be intercepted and re-injected back into the network, causing more packets to be generated and then captured.
5. Run a tool such as Cain & Abel or **aircrack-ng** to extract the encryption keys from the IVs.

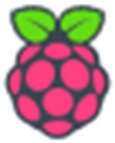
ISSES
Co-funded by the Erasmus+ Programme of the European Union

WEP crack demo lab

Linksys WRT54G



Kali
Attacker



Normal traffic
generator

ISSES

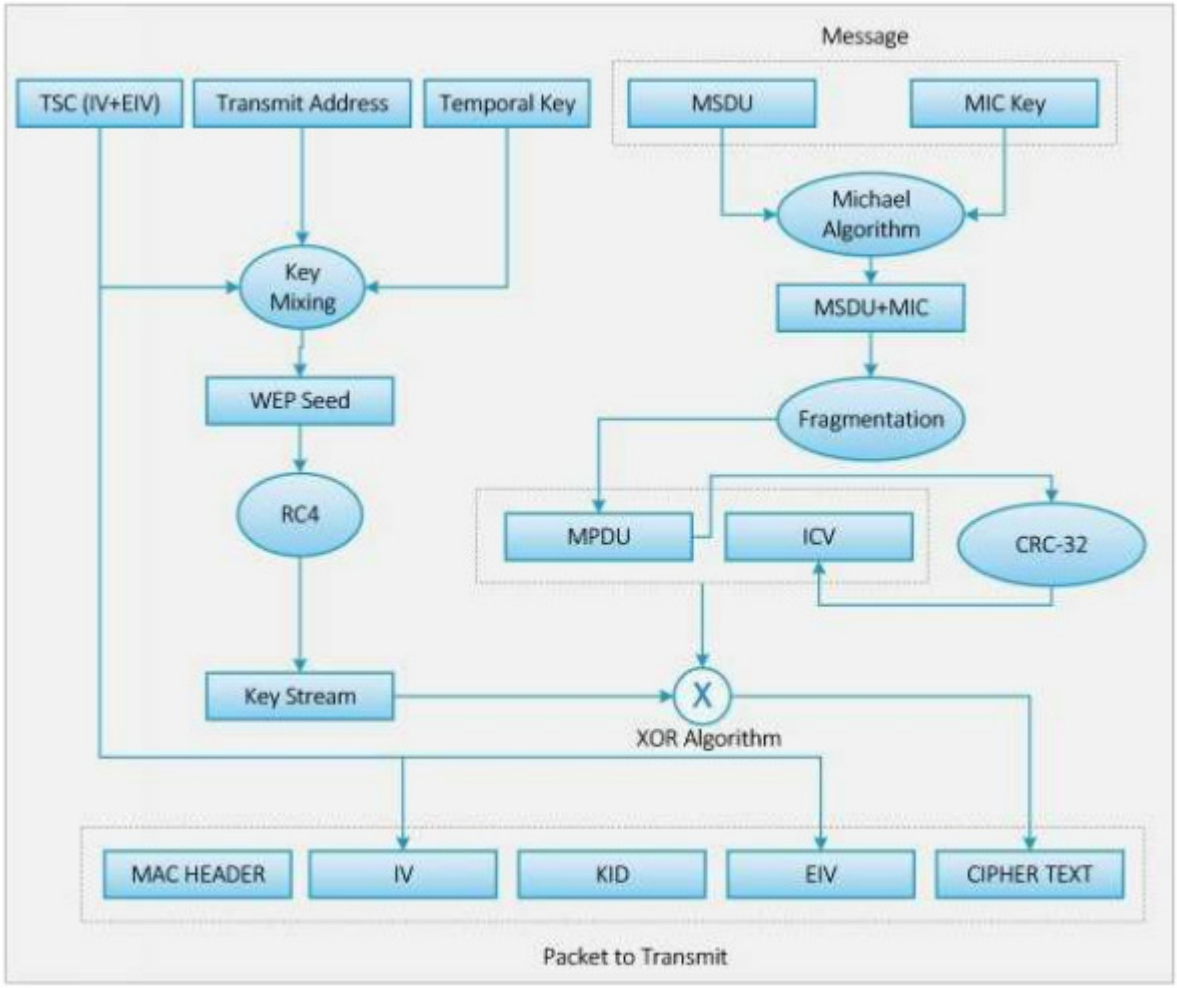
Co-funded by the
Erasmus+ Programme
of the European Union

WPA (Wi-Fi Protected Access)

- The most significant development introduced with the WPA protocol was the TKIP (Temporal Key Integrity Protocol) system, whose purpose is to improve data encryption.
- TKIP improves on the WEP protocol (where a static unchanging key is used for every frame transmitted) by changing the key after every frame.
- This dynamic changing of keys makes WPA much more difficult to crack than WEP.
- IV – 48 bits
- 64 bit Message Integrity Check instead of CRC-32
- WPA suffers from the following flaws:
  - Weak keys chosen by the user
  - Packet spoofing
  - Authentication issues with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAP v2)

ISSES
Co-funded by the Erasmus+ Programme of the European Union

WPA encryption flow



ISSES

Co-funded by the Erasmus+ Programme of the European Union

Cracking WPA

- **Reaver** tool exploits holes in wireless routers in an attempt to retrieve information about the WPA preshared key that is used to access the network
- WPA was much more complex to configure than WEP. WPS (Wi-Fi Protected Setup) was introduced to make the configuration less complex.
- WPS allowed a push button which for a brief period allowed devices in range can connect to the wireless network without entering a passphrase
- Anyone with the physical access to the AP can push the button…

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Cracking WPA

- WPS also has a PIN code which is only 8 characters
- When the router checks the eight-digit PIN, it only checks the first four digits to verify that they are correct before moving to the second set of four.
- An attacker can brute force the PIN code by cracking only four digits at a time, of which only about 11,000 combinations are possible. (no block after x attempts)
- Ultimately for WPA – password dictionary attacks or forced handshaking

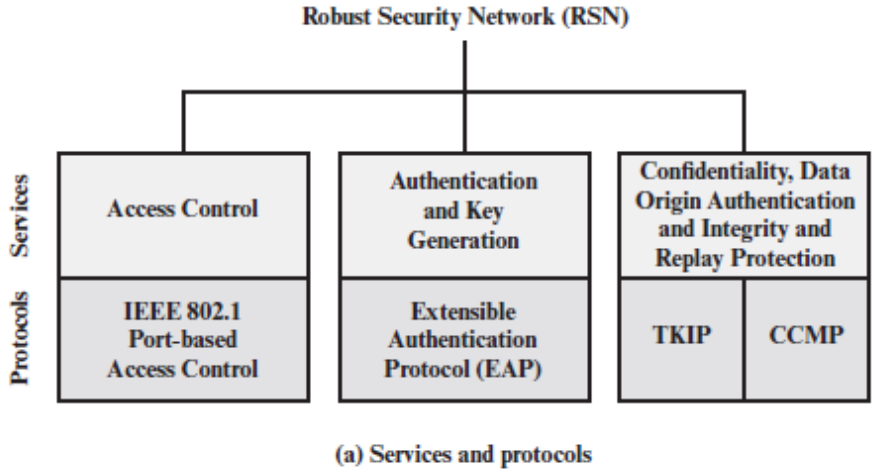
ISSES
Co-funded by the Erasmus+ Programme of the European Union

WLAN security - 802.11i

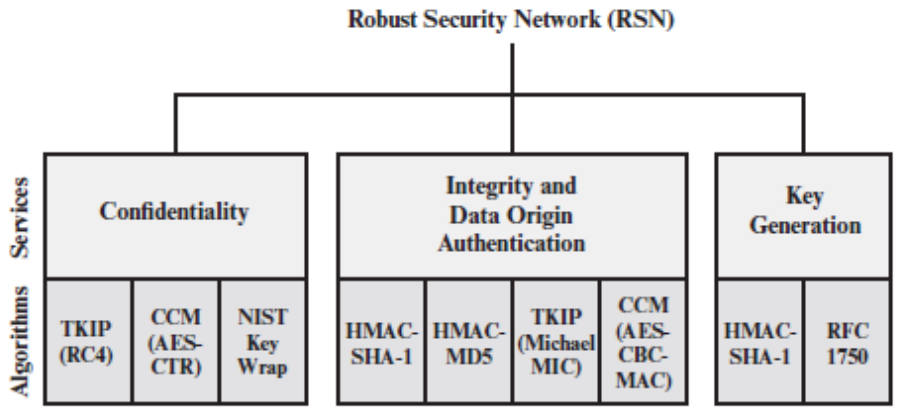
- **802.11i services (AP – WiFi device):**
  - **Authentication:** A protocol is used to define an exchange between a user and an AS that provides mutual authentication and generates temporary keys to be used between the client and the AP over the wireless link.
  - **Access control:** This function enforces the use of the authentication function, routes the messages properly, and facilitates key exchange. It can work with a variety of authentication protocols.
  - **Privacy with message integrity:** MAC-level data (e.g., an LLC PDU) are encrypted along with a message integrity code that ensures that the data have not been altered

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Elements of 802.11i



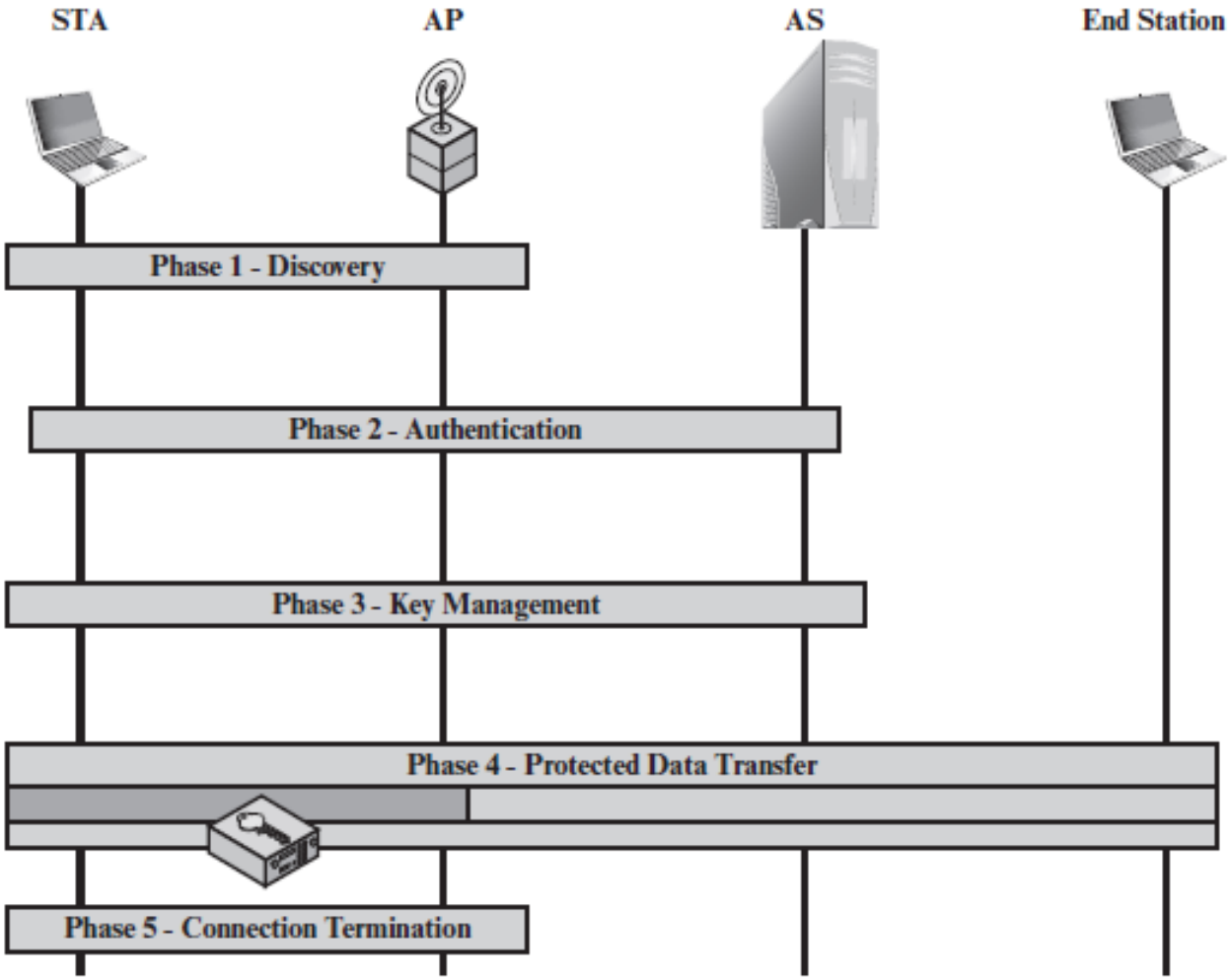
(a) Services and protocols



(b) Cryptographic algorithms

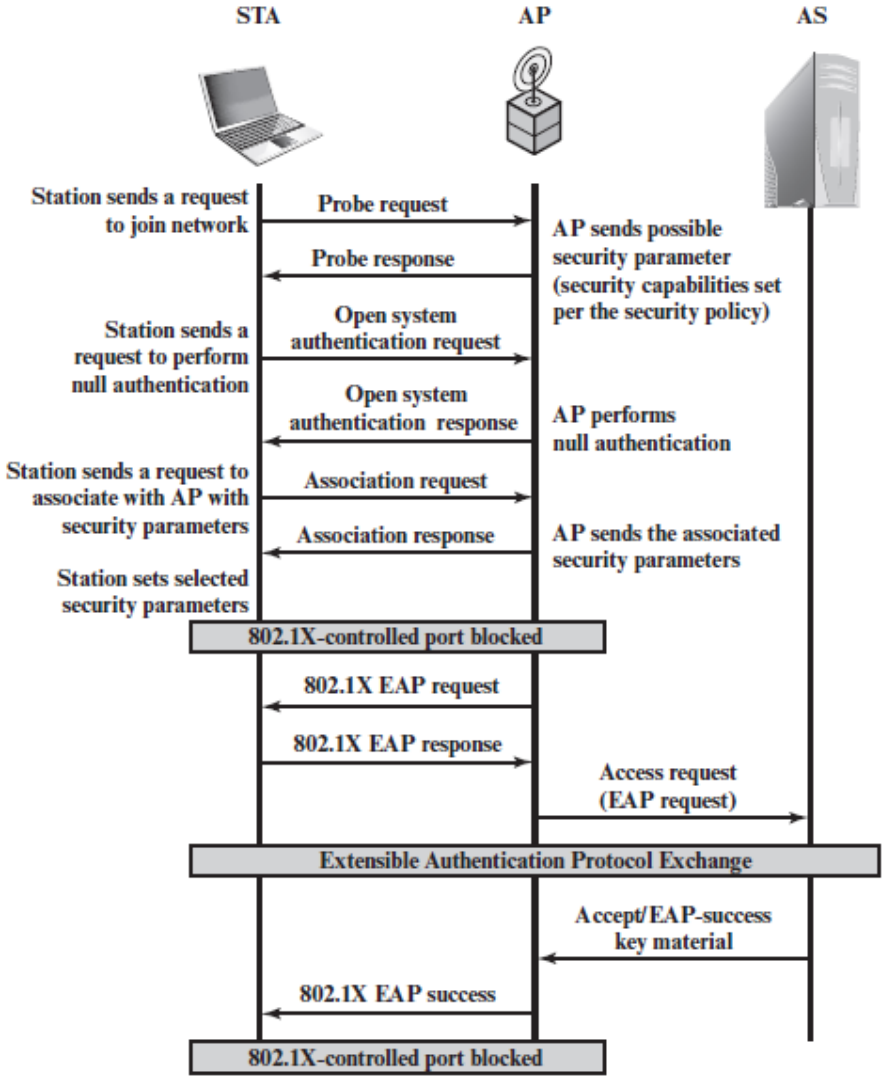
ISSES
Co-funded by the Erasmus+ Programme of the European Union

802.11i phases of operation



ISSES
Co-funded by the Erasmus+ Programme of the European Union

802.11i discovery phase



ISSES
Co-funded by the Erasmus+ Programme of the European Union

EAP

- The authentication protocol that is used, the Extensible Authentication Protocol (EAP), is defined in the IEEE 802.1X standard.
- IEEE 802.1X uses the terms **supplicant**, **authenticator**, and **authentication server** (AS).
- Enterprise mode

ISSES
Co-funded by the Erasmus+ Programme of the European Union

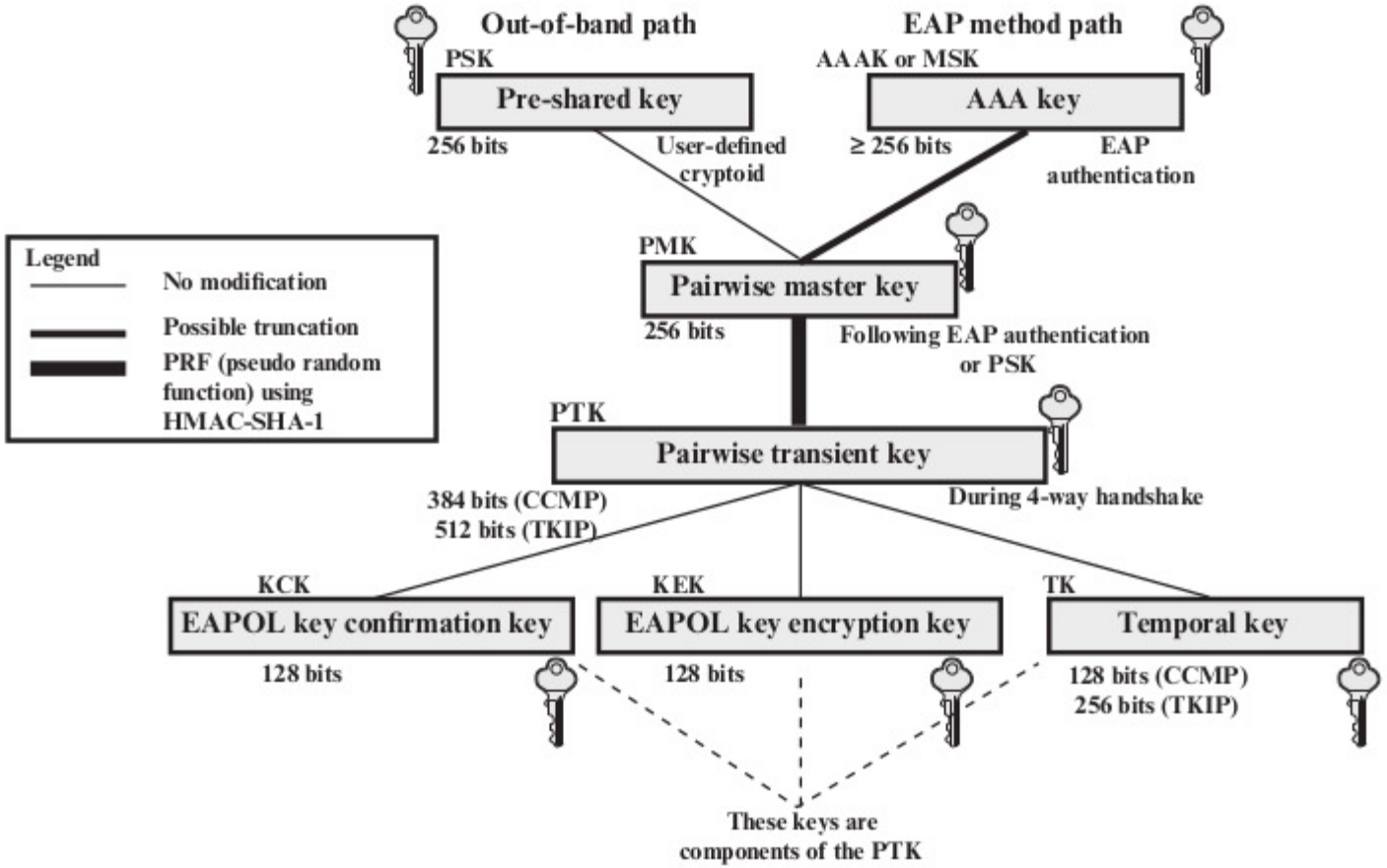
EAP exchange

- 1. The EAP exchange begins with the AP issuing an EAP-Request/Identity frame to the **supplicant**.
- 2. The **supplicant** replies with an EAP-Response/Identity frame, which the AP receives over the uncontrolled port. The packet is then encapsulated in RADIUS over EAP and passed on to the RADIUS server as a RADIUS-Access-Request packet.
- 3. The AAA server replies with a RADIUS-Access-Challenge packet, which is passed on to the **supplicant** as an EAP-Request. This request is of the appropriate authentication type and contains relevant challenge information.
- 4. The **supplicant** formulates an EAP-Response message and sends it to the AS. The response is translated by the AP into a Radius-Access-Request with the response to the challenge as a data field. Steps 3 and 4 may be repeated multiple times, depending on the EAP method in use. For TLS tunneling methods, it is common for authentication to require 10 to 20 round trips.
- 5. The AAA server grants access with a Radius-Access-Accept packet. The AP issues an EAP-Success frame. (Some protocols require confirmation of the EAP success inside the TLS tunnel for authenticity validation.) The controlled port is authorized, and the user may begin to access the network.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Key management

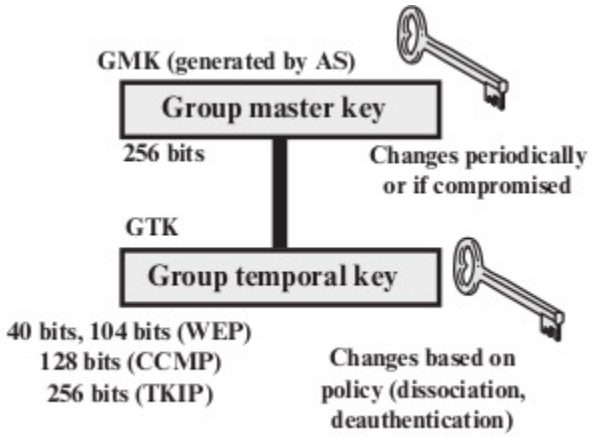
- Pairwise key management



ISSES
Co-funded by the Erasmus+ Programme of the European Union

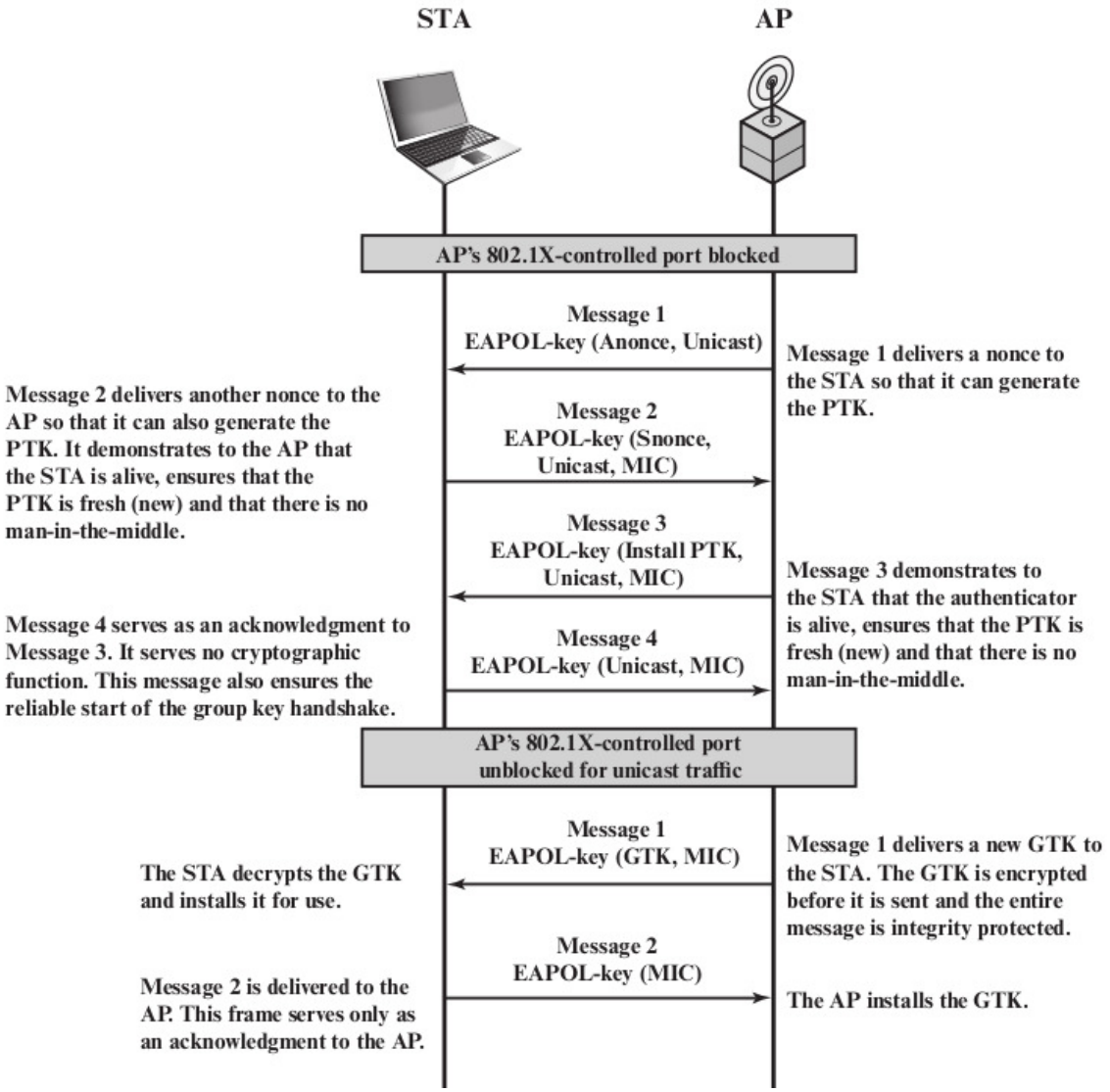
Key management

- Group key hierarchy



ISSES
Co-funded by the
Erasmus+ Programme
of the European Union

802.11i 4-way key exchange handshake



ISS

EAP and crypto protocols

- EAP-TLS
- EAP-TTLS/PAP
- PEAP (Protected EAP)
- (EAP-IKEv2, Eap-MSCHAPv2, LEAP)

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Wardriving

- A wardriving attack is one of the most common forms of action targeting wireless networks.
- It consists of an attacker driving around an area with a computing or mobile device that has both a wireless card and software designed to detect wireless clients or access points.
- What makes this type of attack possible is that wireless detection software will either listen for the beacon of a network or send off a probe request designed to detect the network.
- Once a network is detected, it can be singled out for later attack by the intruder.
- Some of the software packages that are used to perform this type of attack are KisMAC, NetStumbler, Kismet, WaveStumbler, and InSSIDer.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Rogue access point

- A rogue access point is another effective way of breaching a network by violating trust.
- The attacker installs a new access point that is completely unsecured behind a company firewall.
- The attacker can then connect with relative impunity to the target network, extracting information or carrying out further attacks.
- This type of attack has been made relatively easy to perform through the use of more compact hardware access points and software designed to create an access point.
- A savvy attacker will either hide the access point from being readily observed or will configure the SSID to appear as a corporate access point.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Jamming attack

- DoS attack.
- Although there are many ways to do this, one of the easiest is to just jam the network, thus preventing it from being used.
- It is possible to use a specially designed jammer that will transmit signals that can overwhelm and deny the use of the access point by legitimate clients.
- To perform this type of attack, one can use a specially designed hardware device that can transmit signals that interfere with 802.11 networks.
- These devices are easy to find online and can be used to jam any type of wireless network.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

BLUETOOTH HACKING

Bluetooth

- Bluetooth is an open standard for short-range radio frequency (RF) communication
- Bluetooth technology is used primarily to establish wireless personal area networks (WPANs).
- Bluetooth operates in the unlicensed 2.4000gigahertz (GHz) to 2.4835 GHz Industrial, Scientific, and Medical (ISM)frequency band
- Bluetooth technology has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, medical devices, printers, keyboards, mice, and headsets.
- This allows users to form ad hoc networks between a wide variety of devices to transfer voice and data.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Bluetooth versions

Table 2-1. Bluetooth Device Classes of Power Management

Type	Power	Max Power Level	Designed Operating Range	Sample Devices
Class 1	High	100 mW (20 dBm)	Up to 100 meters (328 feet)	USB adapters, access points
Class 2	Medium	2.5 mW (4 dBm)	Up to 10 meters (33 feet)	Mobile devices, Bluetooth adapters, smart card readers
Class 3	Low	1 mW (0 dBm)	Up to 1 meter (3 feet)	Bluetooth adapters

- 1.0
- 1.1
- 1.2
- 2.0 – 2005
- 2.1 – 2007 - Secure simple pairing
- 3.0 – 2009 – AMP link key derivation
- 4.0 - 2010
- 4.1 - 2013
- 4.2 – 2014 – Secure LE pairing
- 5.0 - 2016
- 5.1 – Jan 2019
- 5.2 – Jan 2020
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf

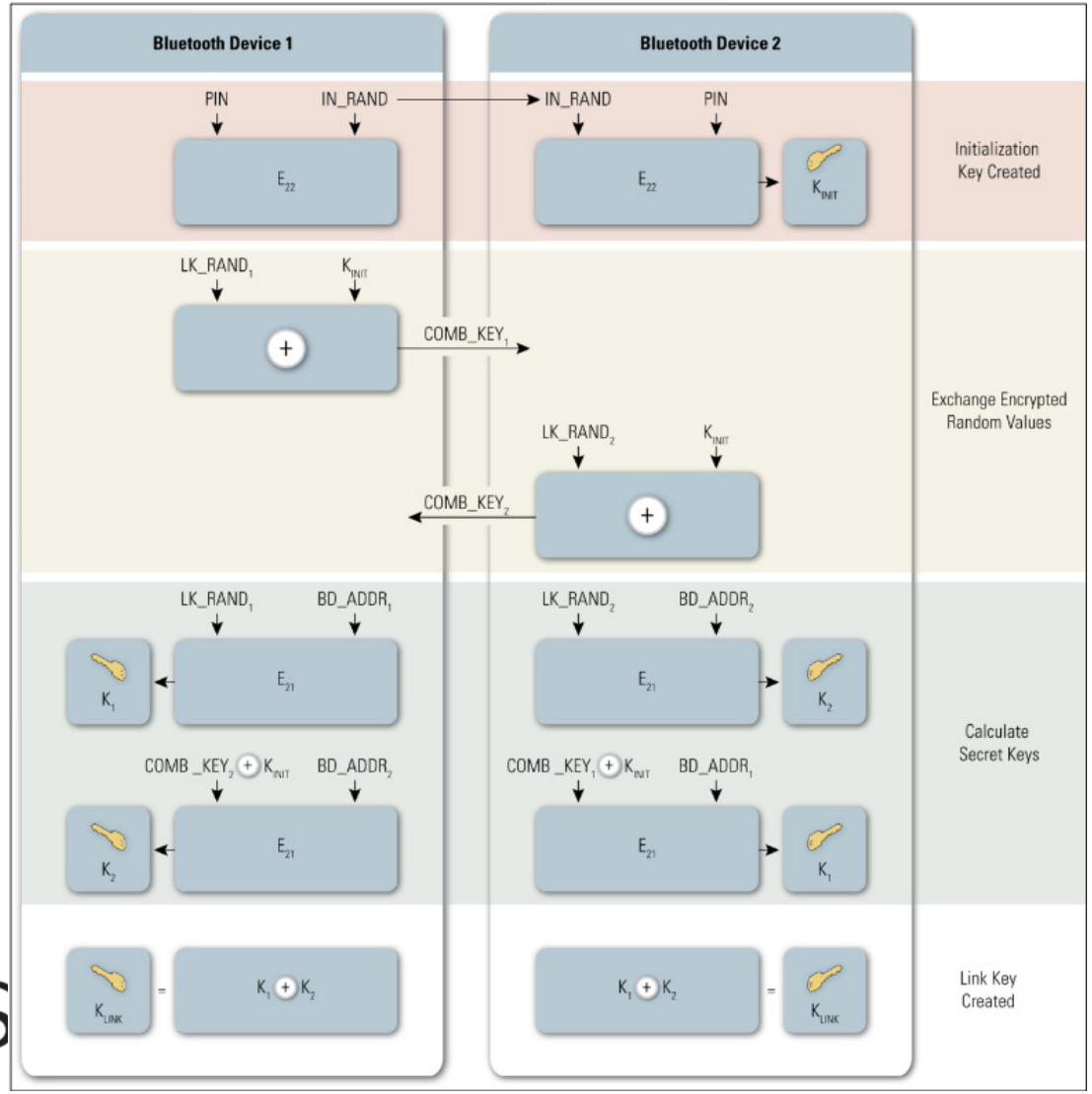
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Bluetooth security modes

- **Security Mode 1** supports communication without security at all, and applies to any Bluetooth communication - unpaired communications – NOT RECOMMENDED
- **Security Mode 2** service level-enforced security mode, security procedures may be initiated after link establishment but before logical channel establishment. SM2 supports AES-CMAC encryption (aka AES-128 via RFC 4493, which is FIPS-compliant).
- **Security Mode 3** Bluetooth device initiates security procedures before the physical link is fully established. Bluetooth devices operating in Security Mode 3 mandate authentication and encryption for all connections to and from the device.
- **Security Mode 4** supports uses in which Elliptic Curve Diffie-Hellman (ECDH) key agreement replaces legacy key agreement for link key generation.

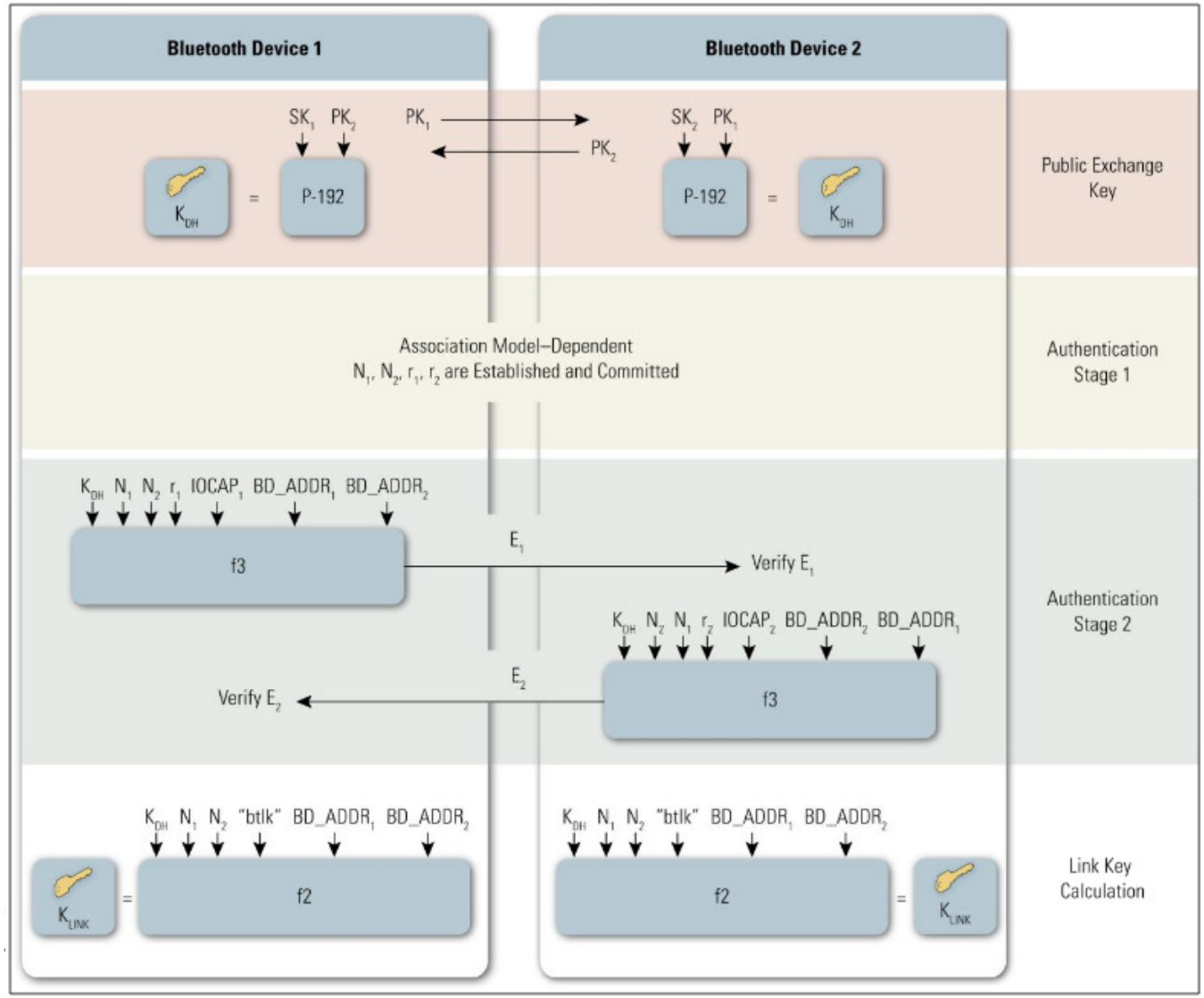
ISSES
Co-funded by the Erasmus+ Programme of the European Union

Bluetooth key generation SM2 & SM3 (from PIN)

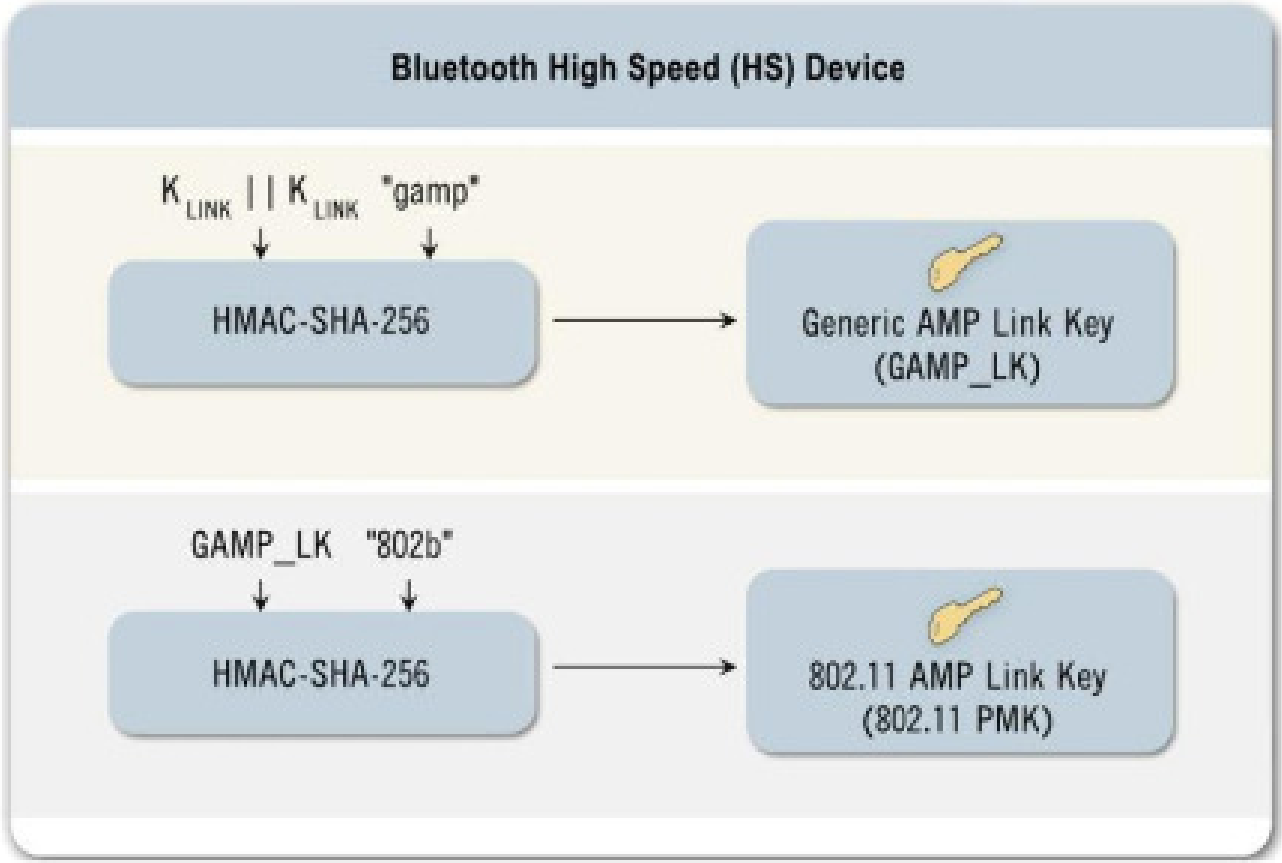


ISSES

Bluetooth key generation – SM4 (Secure Simple Pairing)



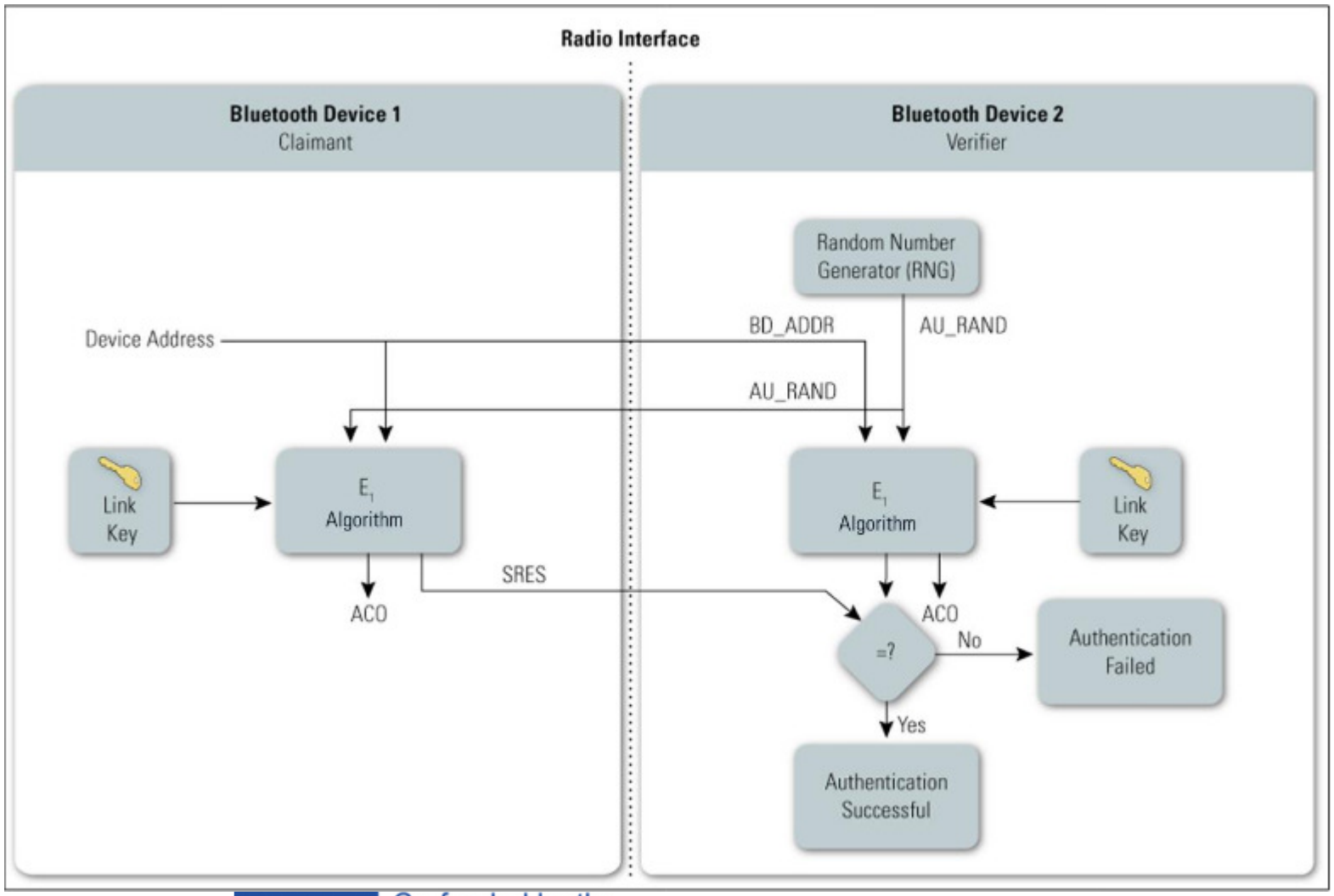
AMP link key derivation



ISSES

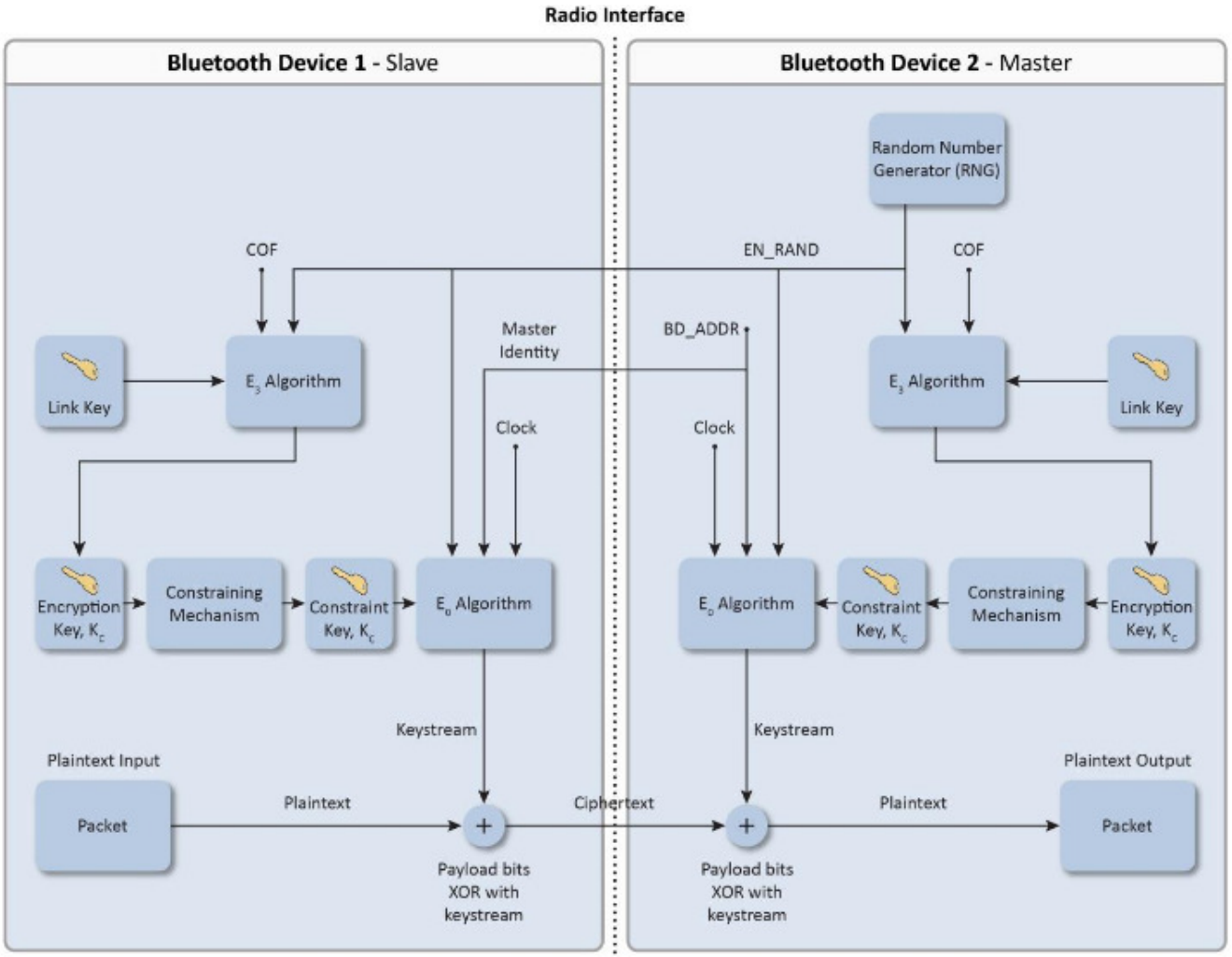
Co-funded by the
Erasmus+ Programme
of the European Union

Bluetooth authentication



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Bluetooth encryption



ISSES

Co-funded by the Erasmus+ Programme of the European Union

Bluetooth LE

- Low Energy – devices with constrained CPU and storage capacities
- No Link Key – LTK – Long Term Key
- Uses “key transport” - one device determines the LTK and securely sends it over to the other device during pairing
- Uses Advanced Encryption Standard–Counter with CBC-MAC (AES-CCM)
- LE Security modes:
  - SM1 has multiple levels associated with encryption. Level 1 specifies no security, meaning no authentication and no encryption will be initiated. Level 2 requires unauthenticated pairing with encryption. Level 3 requires authenticated pairing with encryption.
  - SM2 has multiple levels associated with data signing. Data signing provides strong data integrity but not confidentiality. Level 1 requires unauthenticated pairing with data signing. Level 2 requires authenticated pairing with data signing.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

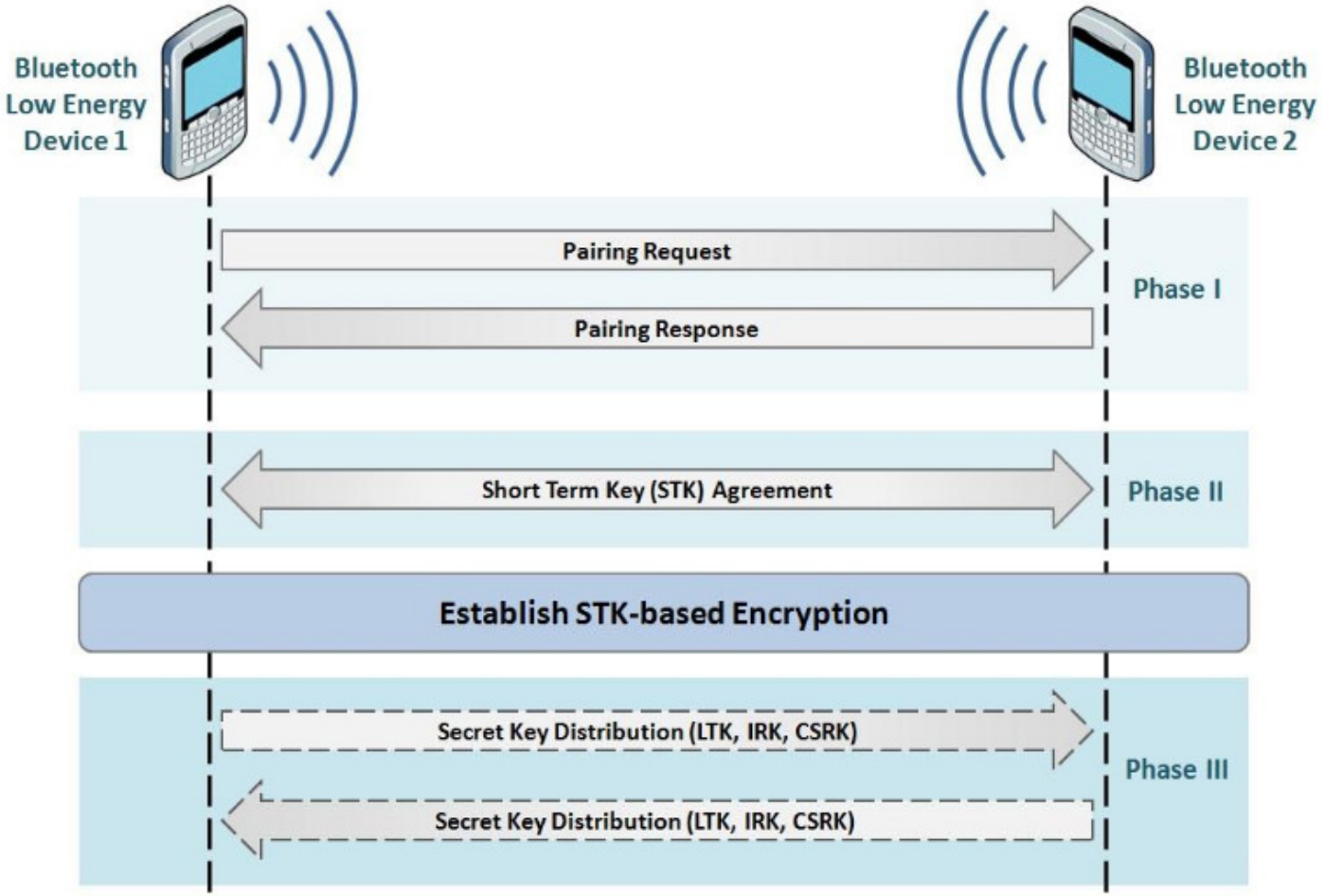
LE pairing methods (before 4.2)

- Does not use ECDH-based cryptography and provides no eavesdropping protection.
- If an attacker can capture the LE pairing frames, he/she may be able to determine the resulting LTK.
- LE pairing begins with the two devices agreeing on a Temporary Key (TK), whose value depends on the pairing method being used.
- The devices then exchange random values and generate a Short Term Key (STK) based on these values and the TK.
- The link is then encrypted using the STK, which allows secure key distribution of the LTK, IRK, and CSRK

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Bluetooth (legacy) LE pairing



ISSES
Co-funded by the Erasmus+ Programme of the European Union

Legacy LE pairing methods

- Out of band
  - Common OOB technology, such as NFC or tethering
  - TK is passed over the OOB technology from one device to the other
  - TK should be unique, random, and equivalent to six decimal digits
- Passkey entry
  - In this model, the TK is generated from the passkey generated and/or entered in each device. The specification requires the passkey size tobe6 numeric digits; therefore,a maximum of 20 bits of entropy can be provided.
- Just works
  - Just Works pairing method for LE is the weakest of the pairing options from a security perspective. In this model, the TK is set to all zeros (0x00). Therefore, an eavesdropper or MITM attacker does not need to guess the TK to generate the STK.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Ver 4.2 LE pairing

- Secure Connection pairing which upgraded low energy pairing to utilize FIPS-approved algorithms (AES-CMAC and P-256 elliptic curve).
- 4.0 and 4.1 low energy pairing was renamed to low energy Legacy Pairing in 4.2.
- Additional method – numeric comparison: If both devices are capable of displaying a six-digit number and both are capable of having the user enter “yes” or “no”, then numeric comparison can be used.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Bluetooth can be sniffed with wireshark

Length	Info
8	Rcvd Number of Completed Packets
19	Rcvd Configure Response - Success (SCID: 0x0040)
36	Rcvd Service Search Attribute Request : Headset: [Service Class ID List 0x0001] [Pro
130	Sent Service Search Attribute Response
8	Rcvd Number of Completed Packets
17	Rcvd Disconnection Request (SCID: 0x0042, DCID: 0x0040, PSM: 0x0001, Service: SDP)
17	Sent Disconnection Response (SCID: 0x0042, DCID: 0x0040, PSM: 0x0001, Service: SDP)
8	Rcvd Number of Completed Packets
9	Rcvd Link Key Request
26	Sent Link Key Request Reply
13	Rcvd Command Complete (Link Key Request Reply)
7	Rcvd Encryption Change
6	Sent Read Encryption Key Size
17	Rcvd Connection Request (RFCOMM, SCID: 0x0043)
21	Sent Connection Response - Success (SCID: 0x0043, DCID: 0x0040)

```
▸ Frame 174: 10 bytes on wire (80 bits), 10 bytes captured (80 bits) on interface 0
▾ Bluetooth
    [Source: controller]
    [Destination: host]
▾ Bluetooth HCI H4
    [Direction: Rcvd (0x01)]
    HCI Packet Type: HCI Event (0x04)
▾ Bluetooth HCI Event - Command Complete
    Event Code: Command Complete (0x0e)
    Parameter Total Length: 7
    Number of Allowed Command Packets: 1
  ▸ Command Opcode: Read Encryption Key Size (0x1408)
    Status: Success (0x00)
    Connection Handle: 0x0001
    Encryption Key Size: 16
    [Command in frame: 170]
    [Command-Response Delta: 0,807ms]
```

ISSES

Co-funded by the Erasmus+ Programme of the European Union

Bluetooth threats

- Leaking calendars and address books or other information is possible through the Bluetooth protocol.
- Creation of bugging devices has been a problem with Bluetooth devices because software has been made available that can remotely activate cameras and microphones.
- An attacker can remotely control a phone to make phone calls or connect to the Internet.
- Attackers have been known to fool victims into disabling security for Bluetooth connections in order to pair with them and steal information.
- Mobile phone worms can exploit a Bluetooth connection to replicate and spread.

ISSES

Co-funded by the
Erasmus+ Programme
of the European Union

Bluejacking

- Sending an anonymous text message via Bluetooth to a victim.
- Use the following steps to bluejack a victim or a device:
  - 1. Locate an area with a high density of mobile users such as a mall or convention center.
  - 2. Go to the contacts in your device's address book.
  - 3. Create a new contact and enter a message.
  - 4. Save the contact with a name but without a phone number.
  - 5. Choose Send Via Bluetooth.
  - 6. Choose a phone from the list of devices and send the message.

ISSES
Co-funded by the Erasmus+ Programme of the European Union

Bluesnarfing

- Bluesnarfing enables attackers to gain access to a Bluetooth-enabled device by exploiting a firmware flaw in older devices. This attack forces a connection to a Bluetooth device, allowing access to data stored on the device including the device's international mobile equipment identity (IMEI). The IMEI is a unique identifier for each device that an attacker could potentially use to route all incoming calls from the user's device to the attacker's device.
- This attack is designed to extract information at a distance from a Bluetooth device.
- The attacker can access the address book, call information, text information, and other data from the device.
- Nowadays the user has to accept pairing with the device which is preventing this type of attack.
- Bluesnipping – long range snarfing
- Blueballing – break pairing of two devices

ISSES
Co-funded by the Erasmus+ Programme of the European Union