Connecting ideas, anticipating the future:
collaborative innovation for 5G and 6G networks.

II INTERNATIONAL WORKSHOP xGMobile

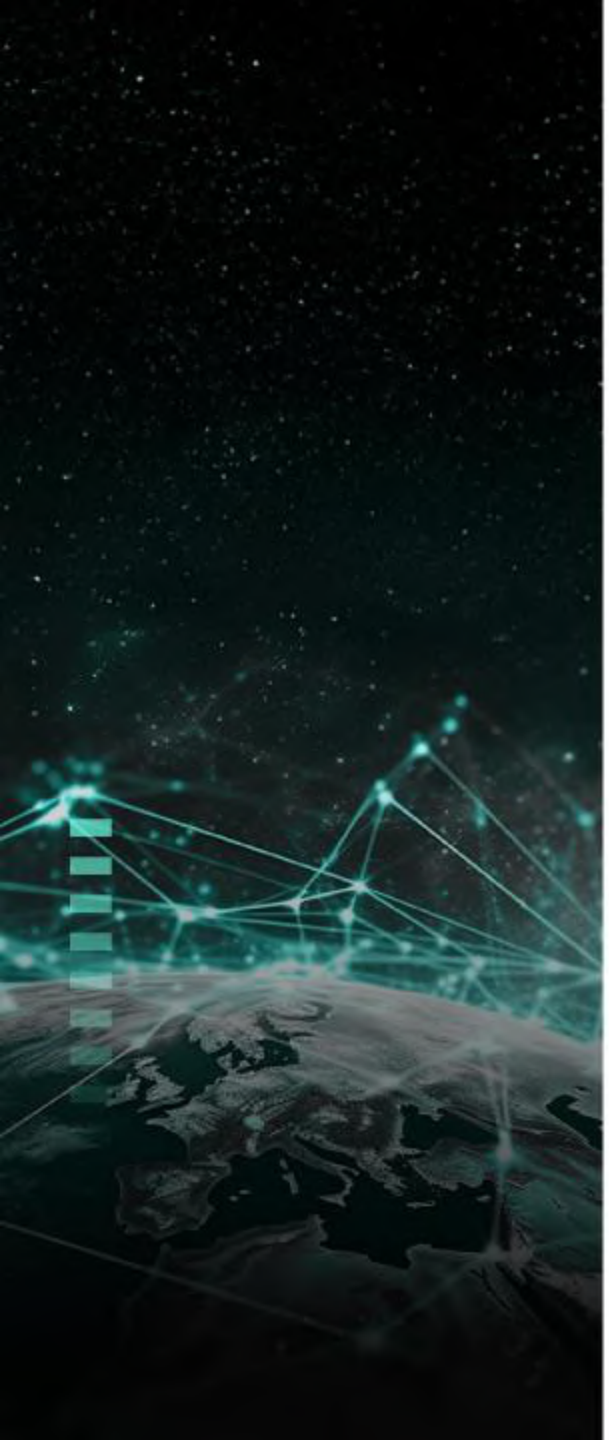
Organized by:

xGMobile · Inatel · FAPEMIG · EMBRAPII · GOVERNO DE MINAS AQUI O TREM PROSPERA. · MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO · GOVERNO DO BRASIL DO LADO DO POVO BRASILEIRO

Bluetooth Vulnerabilities: A Technical Deep Dive

Isabela Ferreira de Vito
CxSC Telecom – Instituto Nacional de Telecomunicações (Inatel)

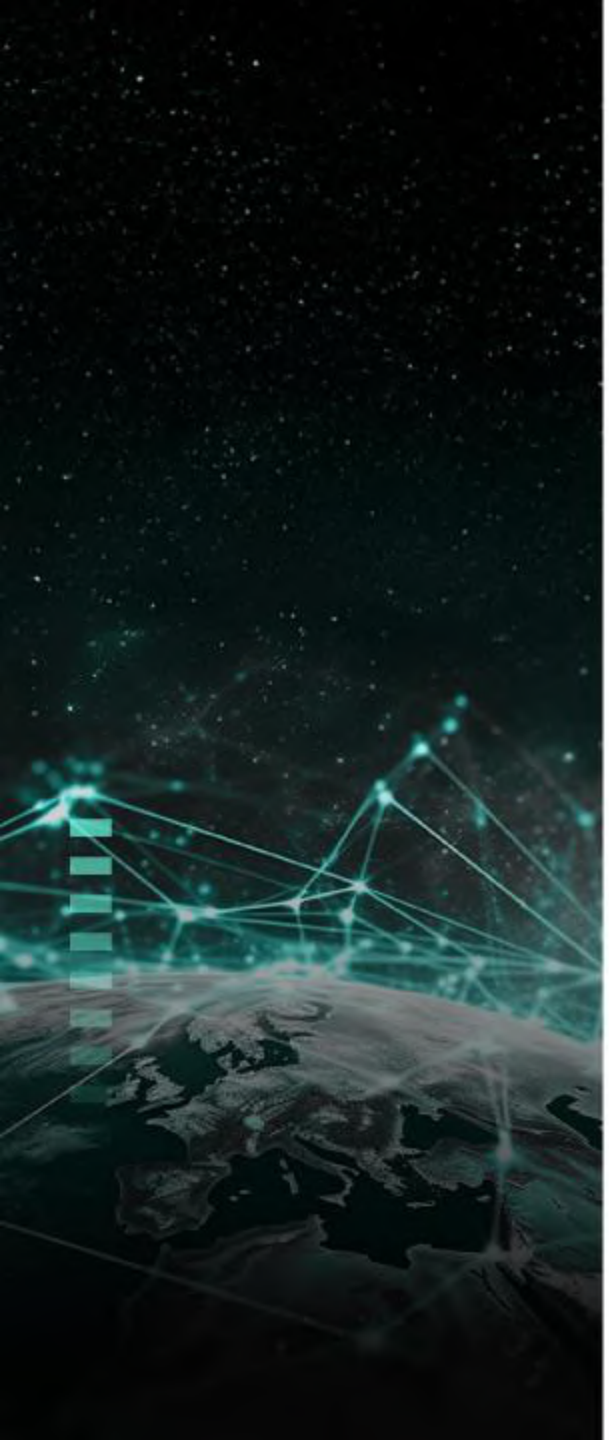
Organized by:
xGMobile Inatel FAPEMIG EMBRAPII GOVERNO DE MINAS AQUI O TREM PROSPERA. MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO DO BRASIL DO LADO DO POVO BRASILEIRO



Goal: to demonstrate the structural problem and the proposed solutions.

Organized by:

xGMobile Inatel FAPEMIG EMBRAPII GOVERNO DE MINAS MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO DO BRASIL



Bluetooth Protocol

- Bluetooth Classic is used by devices that need high-data-rate connections, such as headphones or speakers. As a result, it requires more energy than other Bluetooth versions to transmit larger data packets.

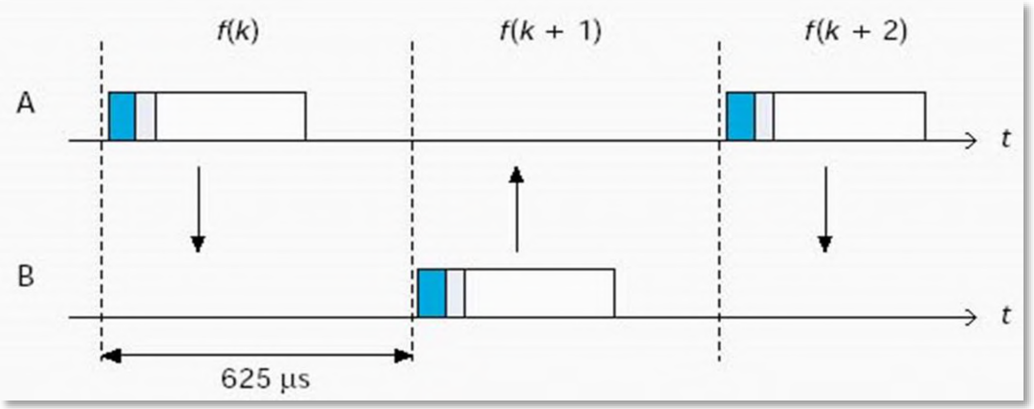
- It operates in the 2.4 GHz band.

- It has 79 channels and operates using frequency hopping. While Bluetooth hops across multiple channels, each channel is divided into time slots of 625 µs (1600 hops/sec). The master and the slave alternate sending data.

Bluetooth Protocol

- It uses Time Division Duplex (TDD), in which data transmission occurs from one device to the other in one time slot, and vice versa.

- Bluetooth 2.0 did not have any real security functionality, and version 2.1 introduced Secure Simple Pairing.

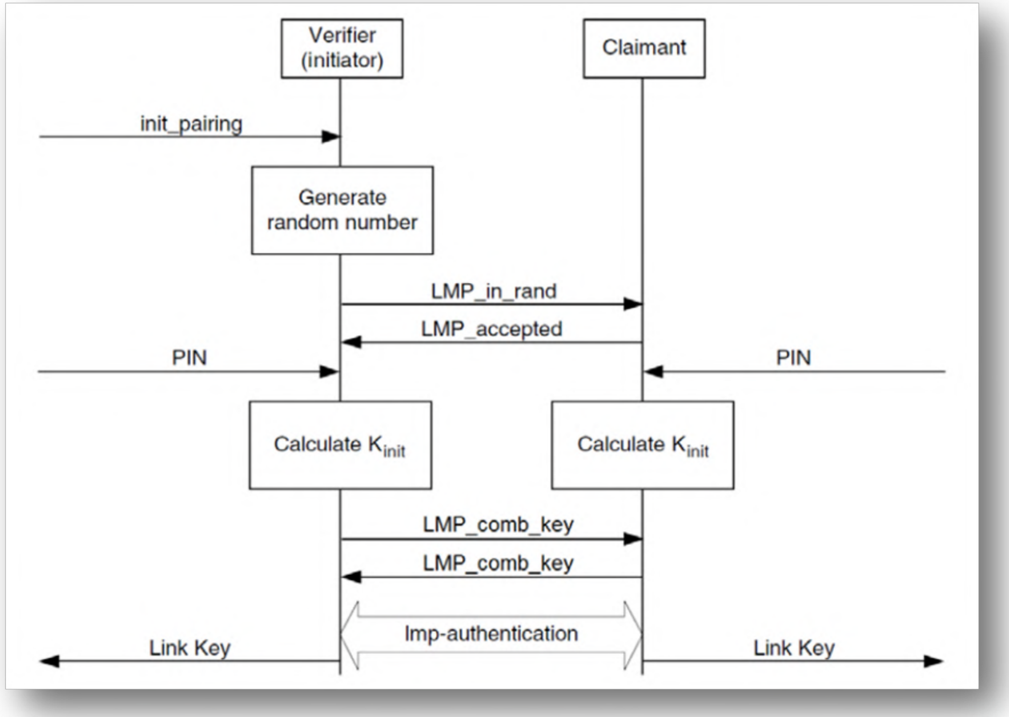


Organized by:

Bluetooth Protocol:

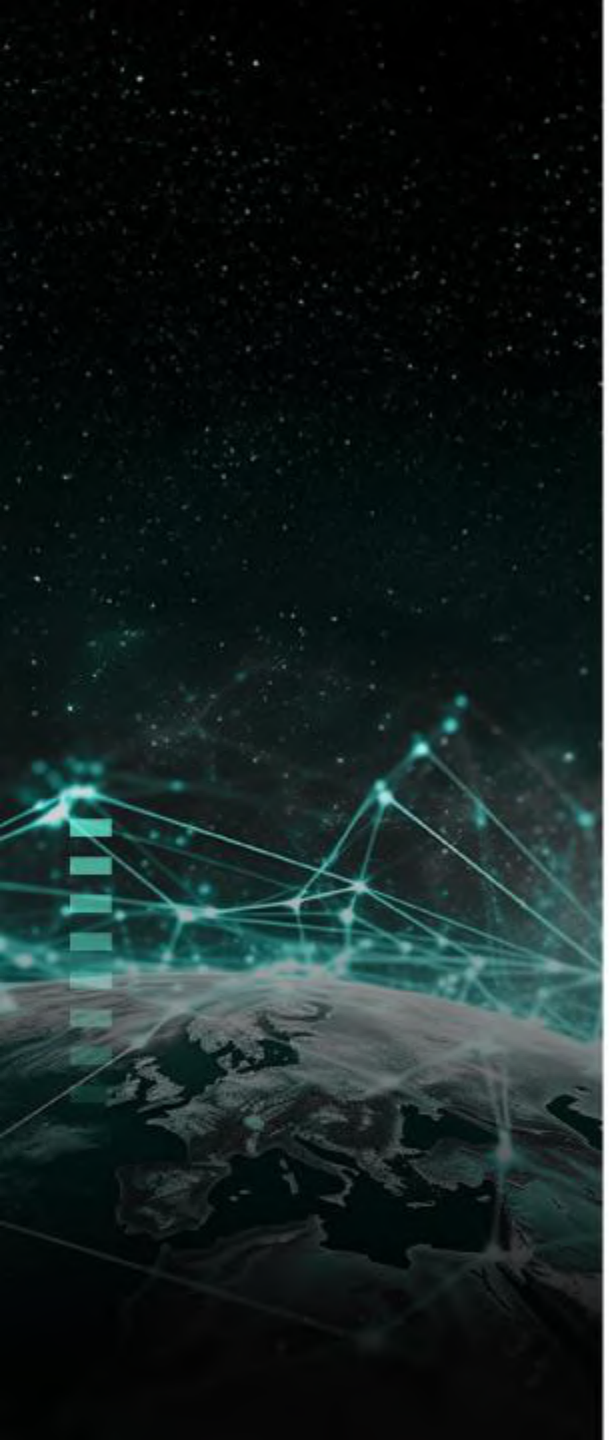
Pairing methods

- LMP Pairing (PIN).



Organized by:

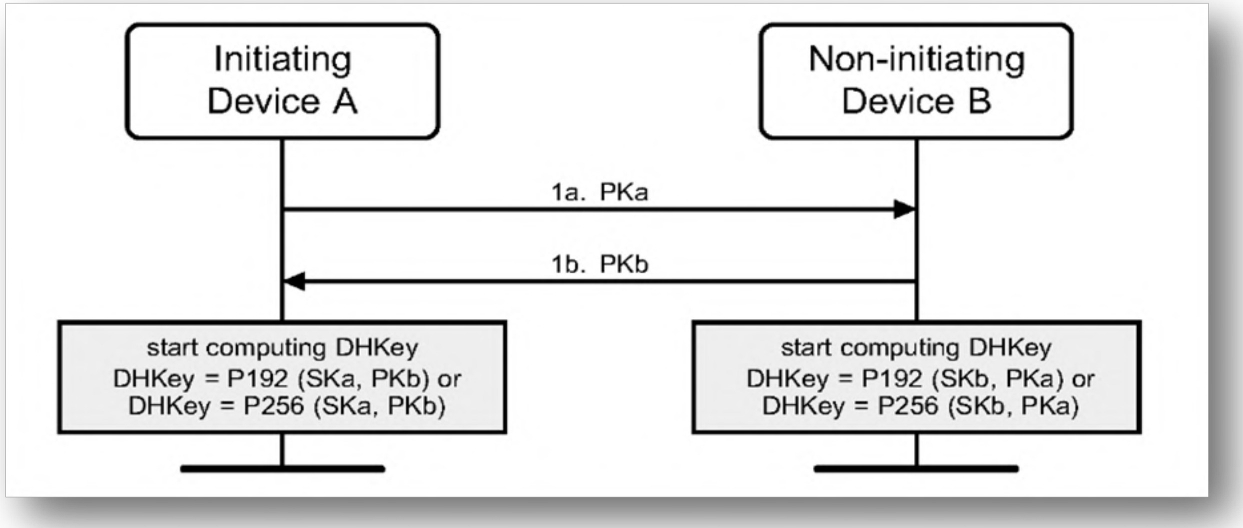
xGMobile Inatel FAPEMIG EMBRAPII GOVERNO DE MINAS AQUI O TREM PROSPERA. MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO DO BRASIL DO LADO DO POVO BRASILEIRO



Bluetooth Protocol:

Pairing methods

- Secure Simple Pairing.



Initiating Device A

Non-initiating Device B

1a. PKa

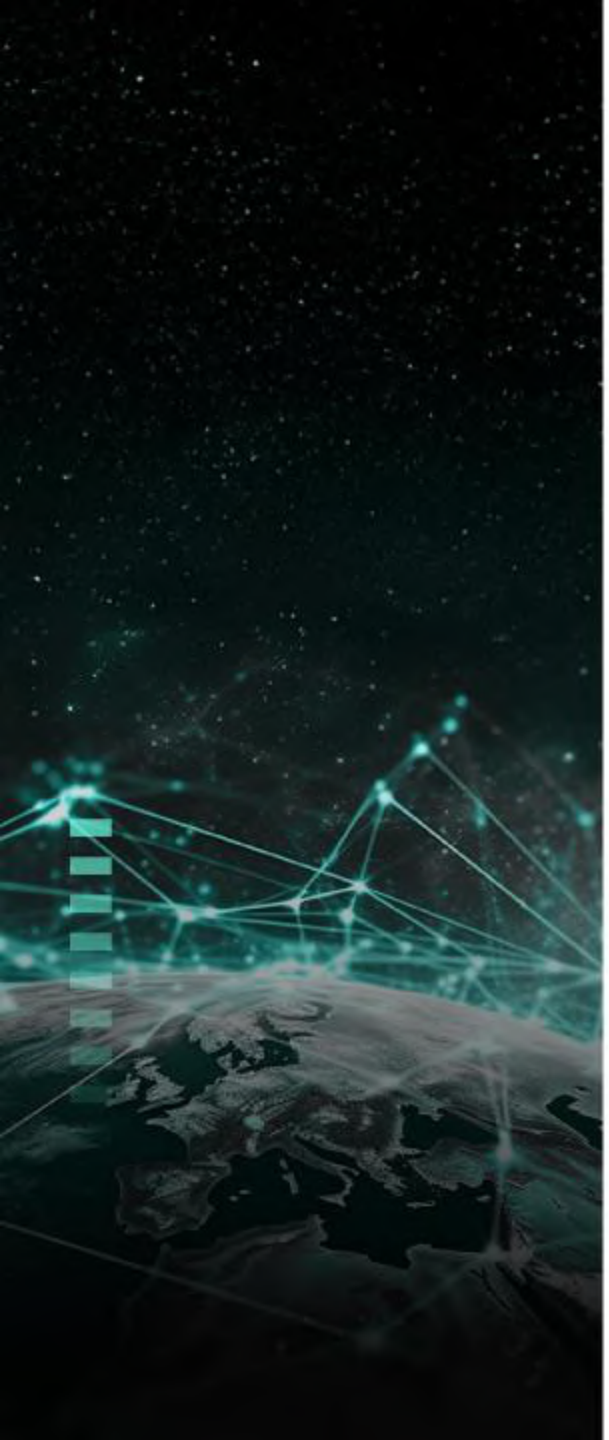
1b. PKb

start computing DHKey
DHKey = P192 (SKa, PKb) or
DHKey = P256 (SKa, PKb)

start computing DHKey
DHKey = P192 (SKb, PKa) or
DHKey = P256 (SKb, PKa)

Organized by:

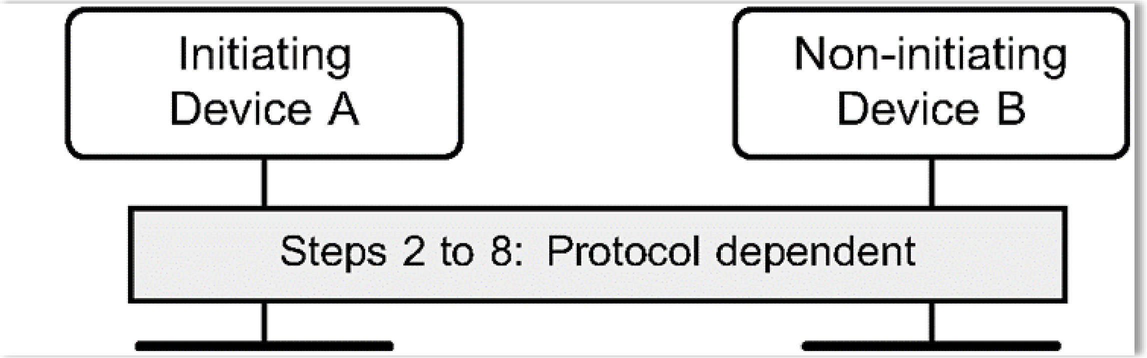
xGMobile Inatel FAPEMIG EMBRAPII GOVERNO DE MINAS MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO DO BRASIL DO LADO DO POVO BRASILEIRO



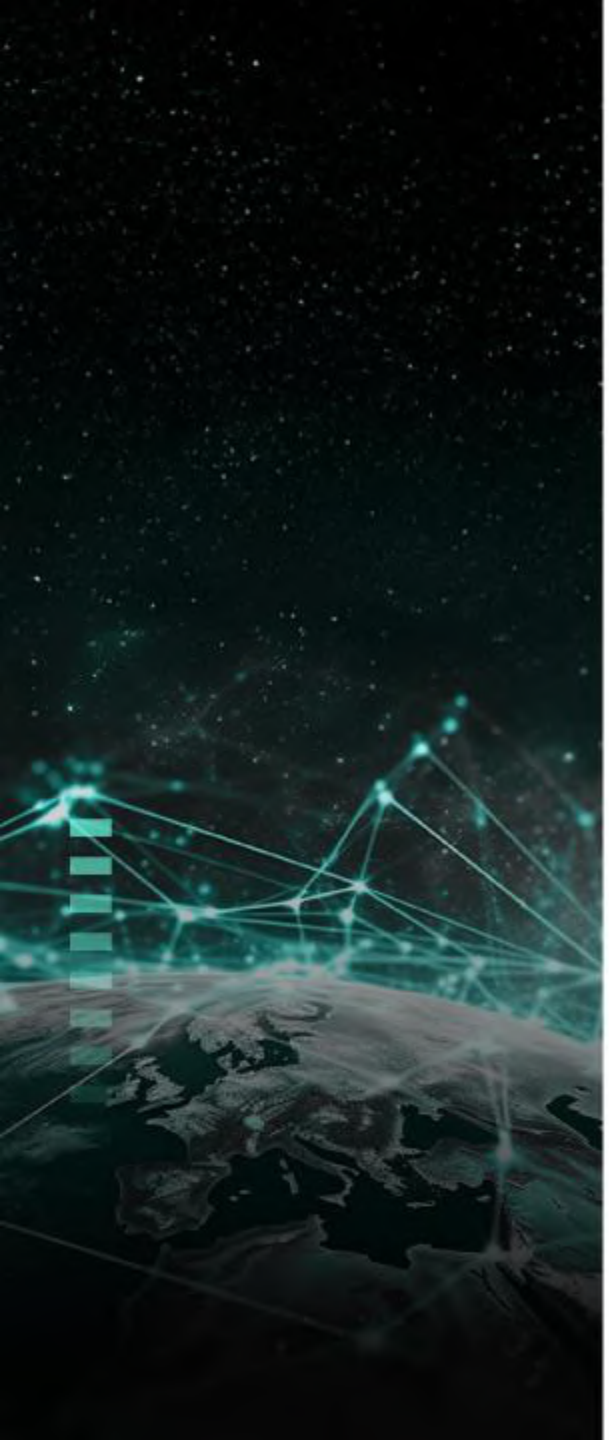
Bluetooth Protocol:

Pairing methods

- Secure Simple Pairing.
  - ✓ Just Works
  - ✓ Numeric comparison.
  - ✓ Passkey entry.
  - ✓ Out Of Band.



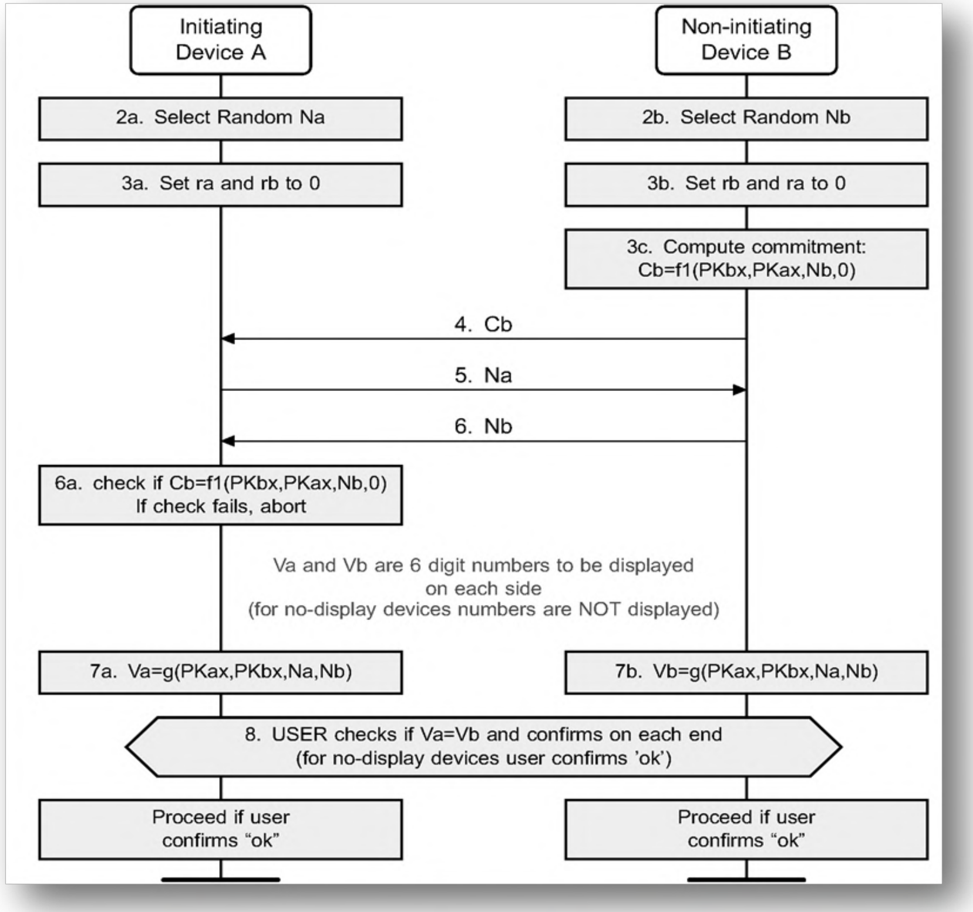
Organized by:



Bluetooth Protocol:

Pairing methods

- Secure Simple Pairing: numeric comparison.



Initiating Device A

Non-initiating Device B

2a. Select Random Na

2b. Select Random Nb

3a. Set ra and rb to 0

3b. Set rb and ra to 0

3c. Compute commitment: Cb=f1(PKbx,PKax,Nb,0)

4. Cb

5. Na

6. Nb

6a. check if Cb=f1(PKbx,PKax,Nb,0) If check fails, abort

Va and Vb are 6 digit numbers to be displayed on each side (for no-display devices numbers are NOT displayed)

7a. Va=g(PKax,PKbx,Na,Nb)

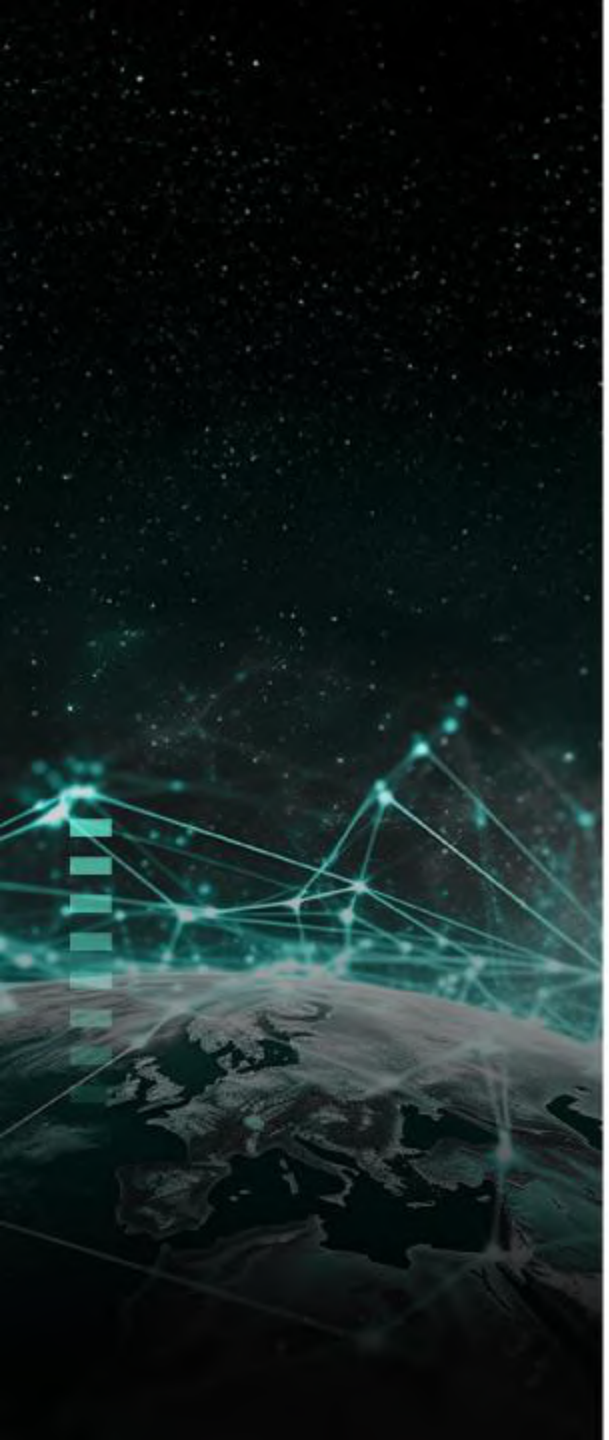
7b. Vb=g(PKax,PKbx,Na,Nb)

8. USER checks if Va=Vb and confirms on each end (for no-display devices user confirms 'ok')

Proceed if user confirms "ok"

Proceed if user confirms "ok"

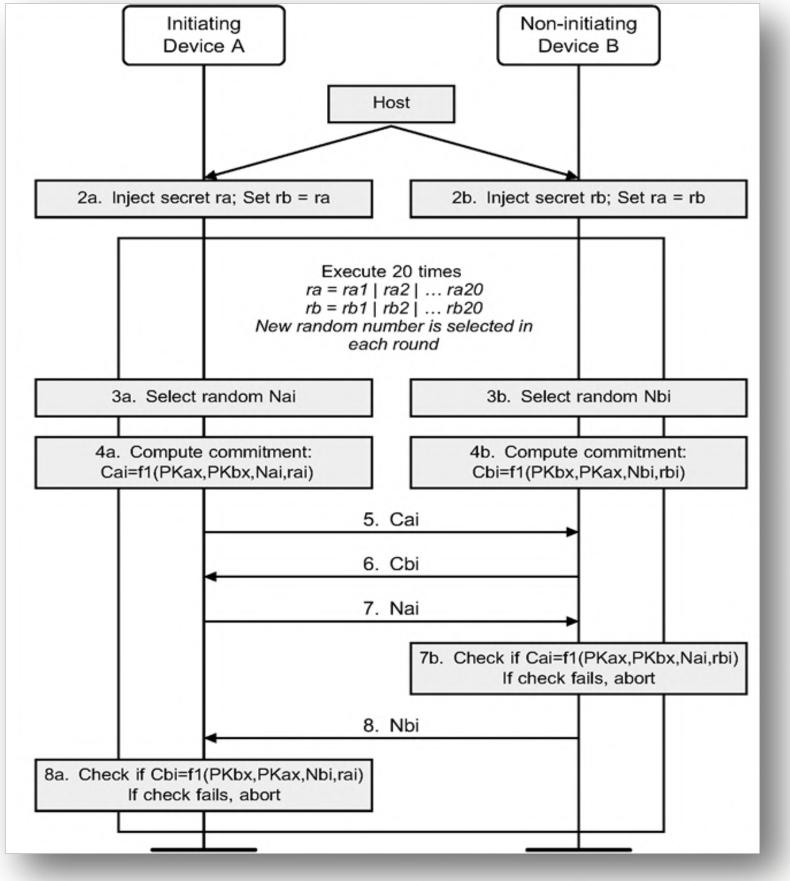
Organized by:



Bluetooth Protocol:

Pairing methods

- Secure Simple Pairing: PasskeyEntry



Initiating Device A

Non-initiating Device B

Host

2a. Inject secret ra; Set rb = ra

2b. Inject secret rb; Set ra = rb

Execute 20 times
ra = ra1 | ra2 | … ra20
rb = rb1 | rb2 | … rb20
New random number is selected in each round

3a. Select random Nai

3b. Select random Nbi

4a. Compute commitment: Cai=f1(PKax,PKbx,Nai,rai)

4b. Compute commitment: Cbi=f1(PKbx,PKax,Nbi,rbi)

5. Cai

6. Cbi

7. Nai

7b. Check if Cai=f1(PKax,PKbx,Nai,rbi)
If check fails, abort

8. Nbi

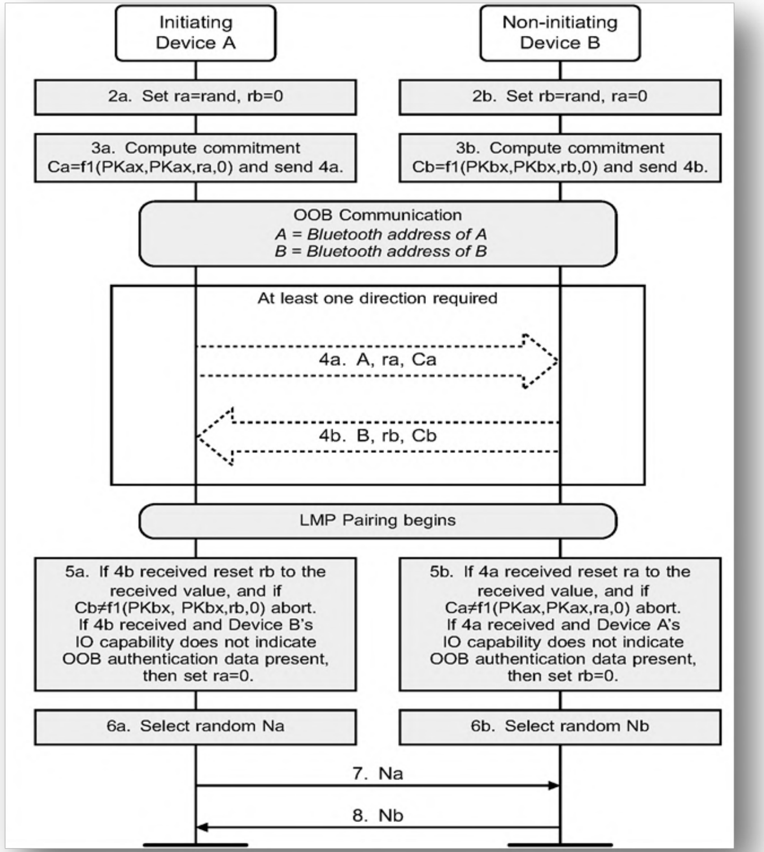
8a. Check if Cbi=f1(PKbx,PKax,Nbi,rai)
If check fails, abort

Organized by:

Bluetooth Protocol:

Pairing methods

- Secure Simple Pairing: Out of Band.



Initiating Device A

Non-initiating Device B

2a. Set ra=rand, rb=0

2b. Set rb=rand, ra=0

3a. Compute commitment Ca=f1(PKax,PKax,ra,0) and send 4a.

3b. Compute commitment Cb=f1(PKbx,PKbx,rb,0) and send 4b.

OOB Communication
A = Bluetooth address of A
B = Bluetooth address of B

At least one direction required

4a. A, ra, Ca

4b. B, rb, Cb

LMP Pairing begins

5a. If 4b received reset rb to the received value, and if Cb≠f1(PKbx, PKbx,rb,0) abort. If 4b received and Device B's IO capability does not indicate OOB authentication data present, then set ra=0.

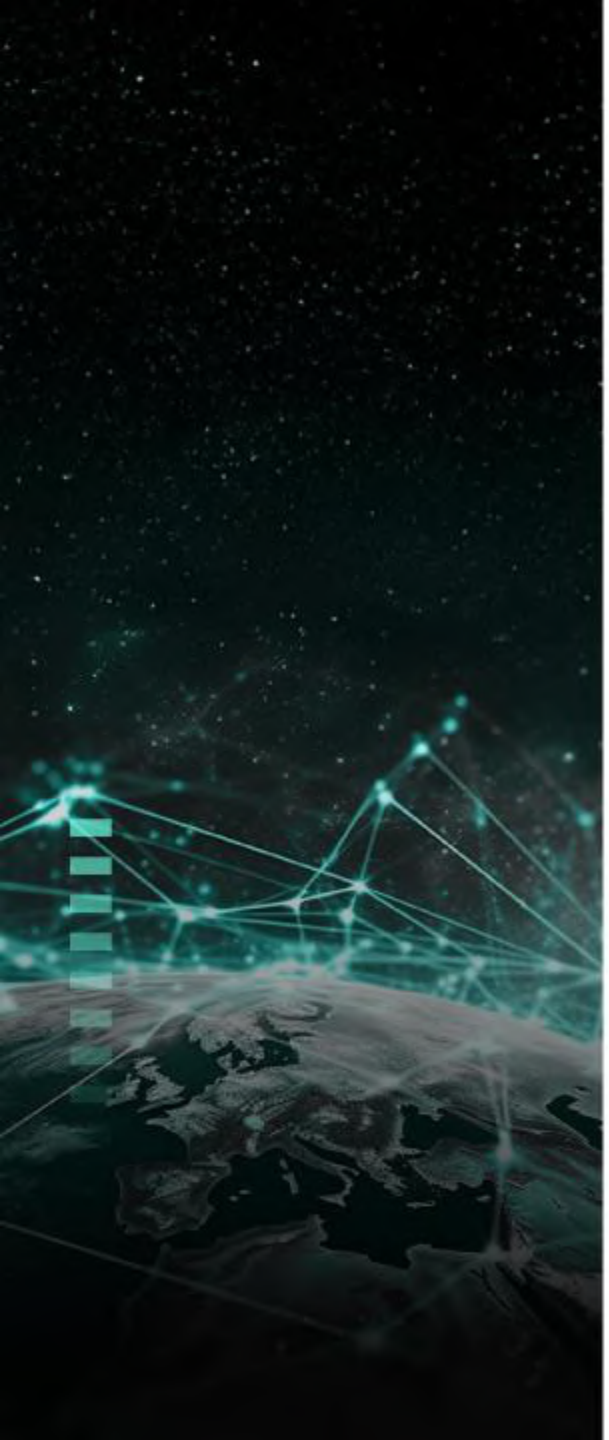
5b. If 4a received reset ra to the received value, and if Ca≠f1(PKax,PKax,ra,0) abort. If 4a received and Device A's IO capability does not indicate OOB authentication data present, then set rb=0.

6a. Select random Na

6b. Select random Nb

7. Na

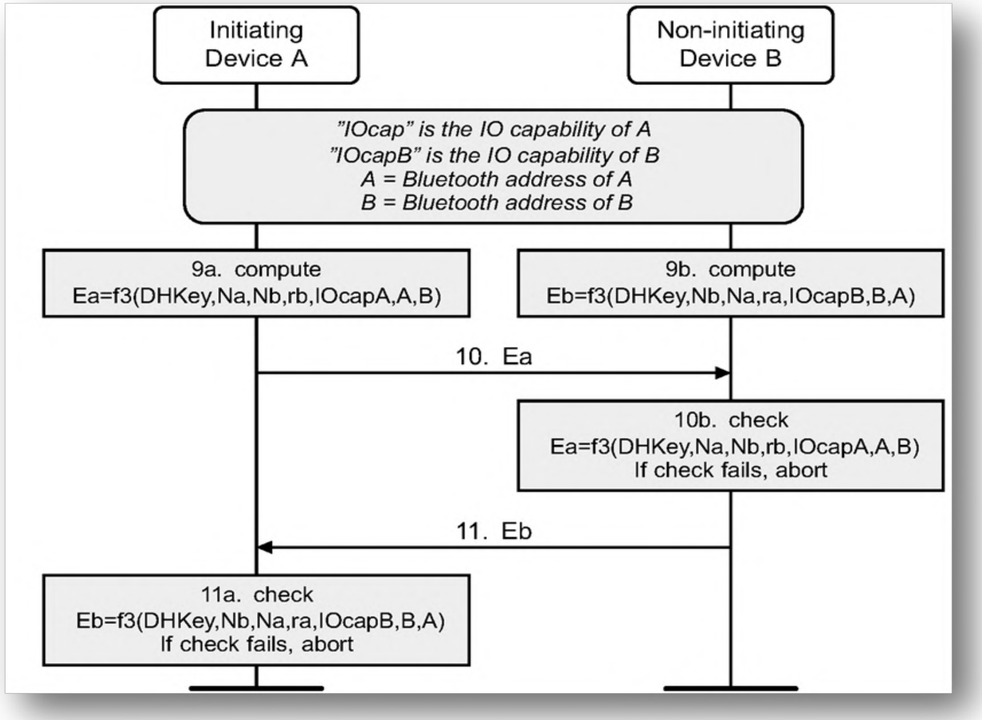
8. Nb



Bluetooth Protocol:

Pairing methods

- Secure Simple Pairing.



Initiating Device A

Non-initiating Device B

"IOcap" is the IO capability of A
"IOcapB" is the IO capability of B
A = Bluetooth address of A
B = Bluetooth address of B

9a. compute
Ea=f3(DHKey,Na,Nb,rb,IOcapA,A,B)

9b. compute
Eb=f3(DHKey,Nb,Na,ra,IOcapB,B,A)

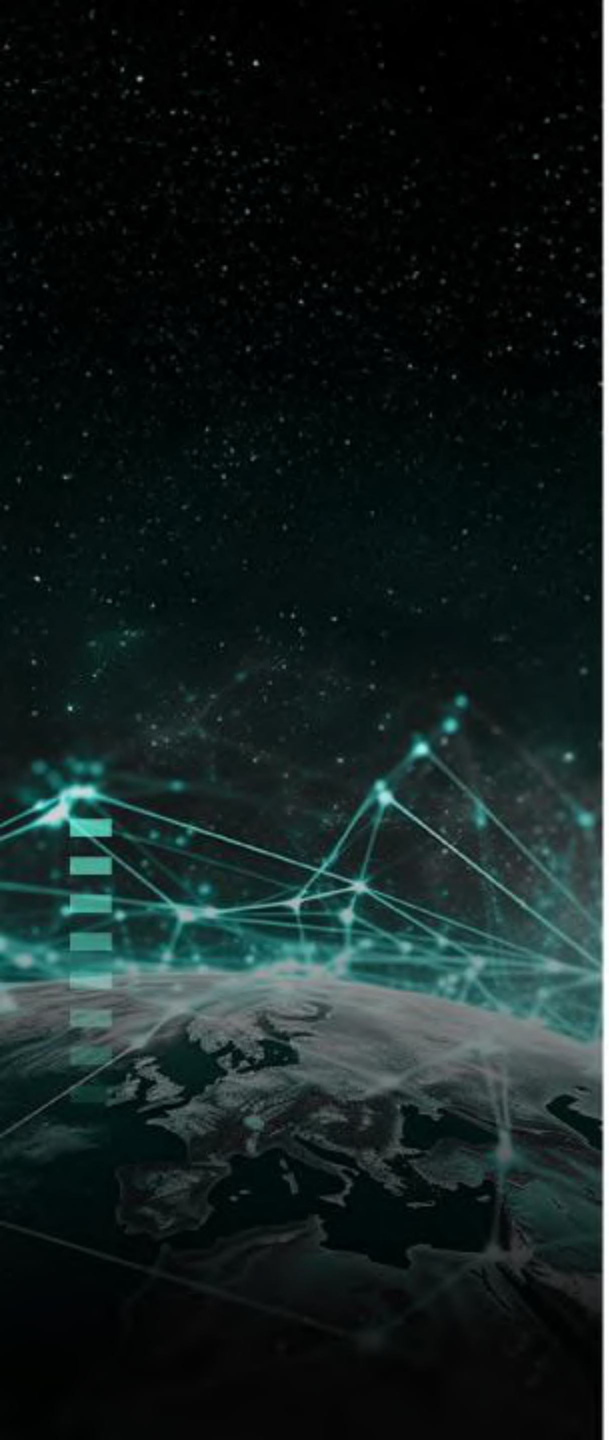
10. Ea

10b. check
Ea=f3(DHKey,Na,Nb,rb,IOcapA,A,B)
If check fails, abort

11. Eb

11a. check
Eb=f3(DHKey,Nb,Na,ra,IOcapB,B,A)
If check fails, abort

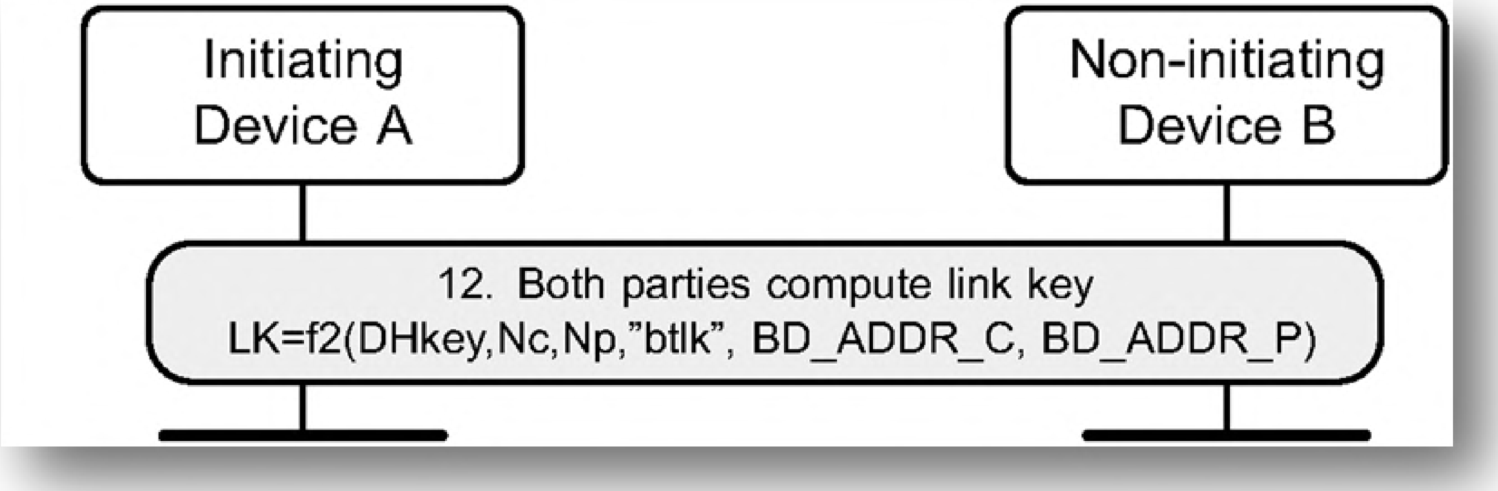
Organized by:



Bluetooth Protocol:

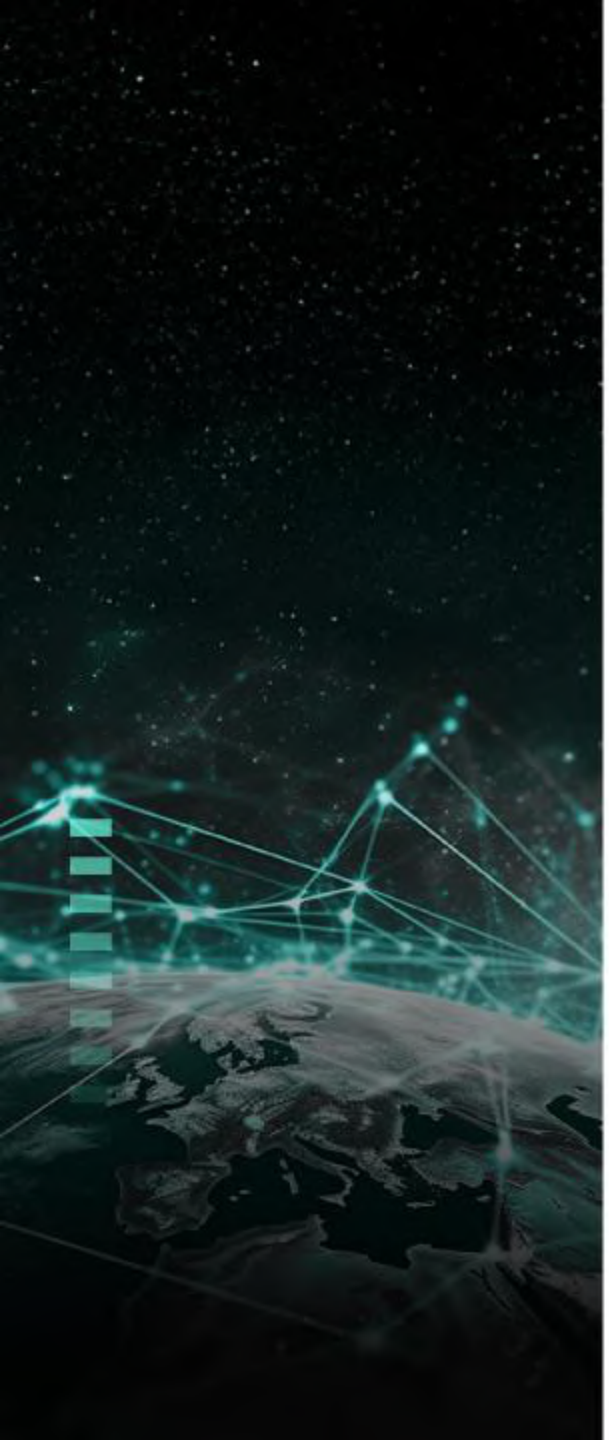
Pairing methods

- Secure Simple Pairing.



12. Both parties compute link key
LK=f2(DHkey,Nc,Np,"btlk", BD_ADDR_C, BD_ADDR_P)

Organized by:

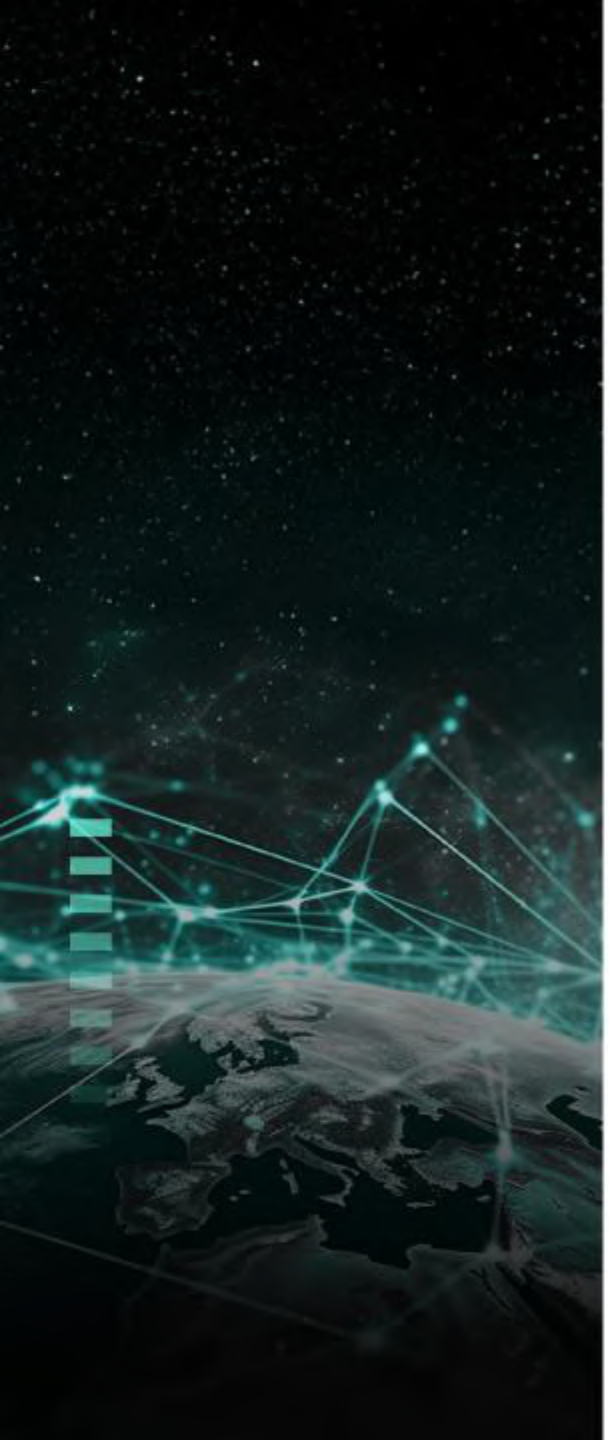


Bluetooth Low Energy:

- Bluetooth Low Energy is an extension of the Bluetooth protocol created with the purpose of providing a low-energy solution for control and monitoring applications, also aimed at IoT applications.

- As such, it does not support high data rates compared to Bluetooth Classic.

- It was initially specified with a focus on efficiency and low power consumption, with security mechanisms introduced as optional.

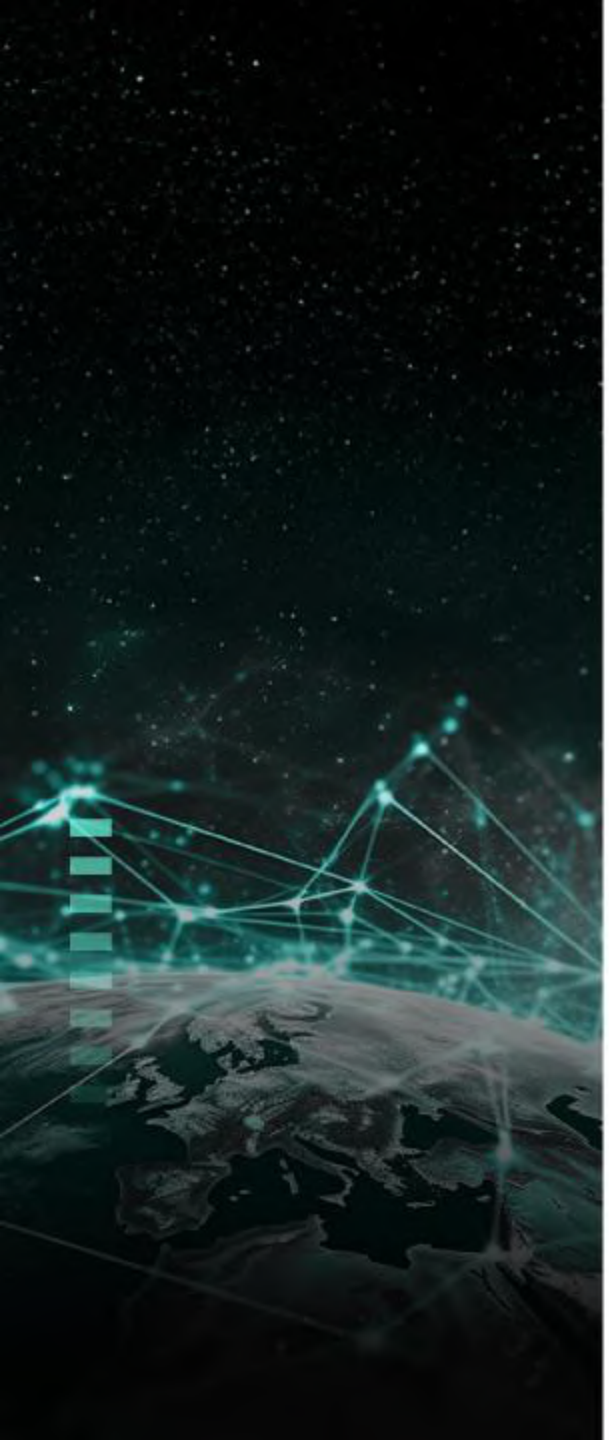


Bluetooth Low Energy:

- **Battery consumption**: it operates at lower energy levels, allowing device batteries to have a longer lifespan. Much of BLE’s battery life comes from its ability to remain in standby mode until a data transfer is needed.

- **Data transfer**: BLE operates at a rate of 1 Mbps, while Bluetooth Classic works with higher transmission rates. This aspect was deprioritized in BLE due to the goals of the technology.

Organized by:



Bluetooth Low Energy:

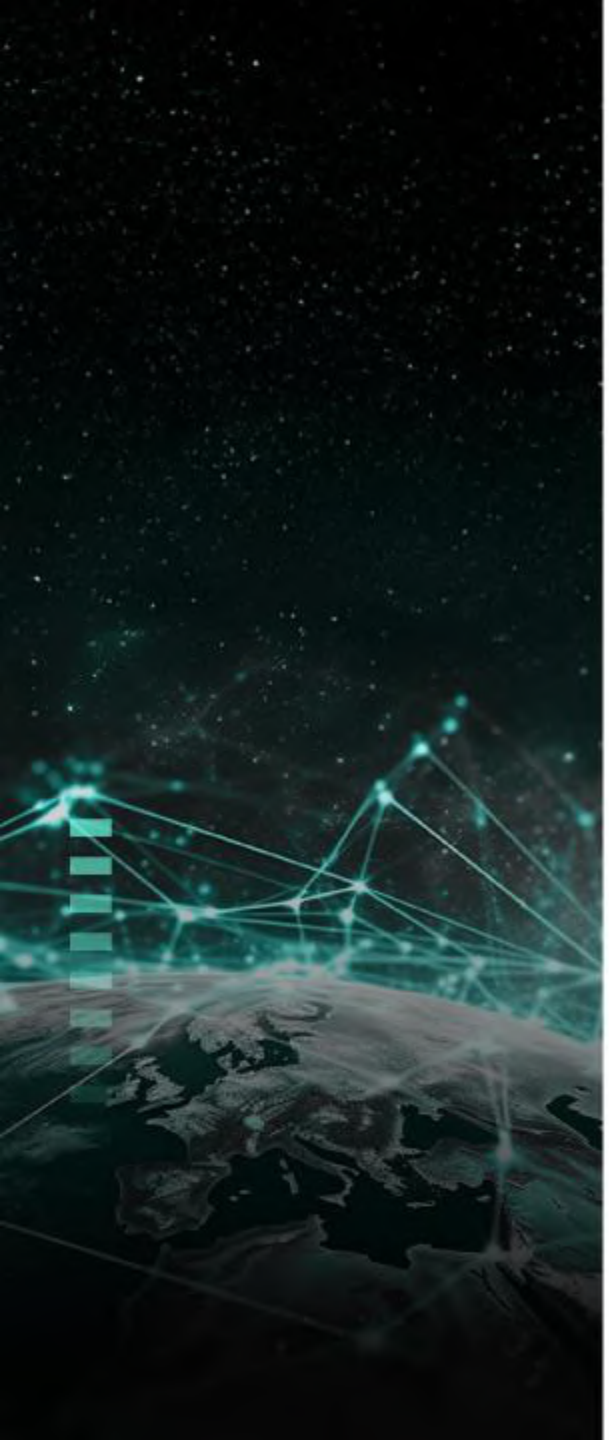
Pairing methods

Pairing involves the first phase of establishing a connection using BLE. The process is divided into three phases:

1. The devices exchange pairing request and response messages, communicating their capabilities and determining the pairing method.

2. Parameter exchange that results in the derivation of a temporary encryption key (TK) for the connection.

3. The devices exchange random values and use them, along with the TK, to generate the STK. The STK is used to distribute the LTK, IRK, and CSRK.

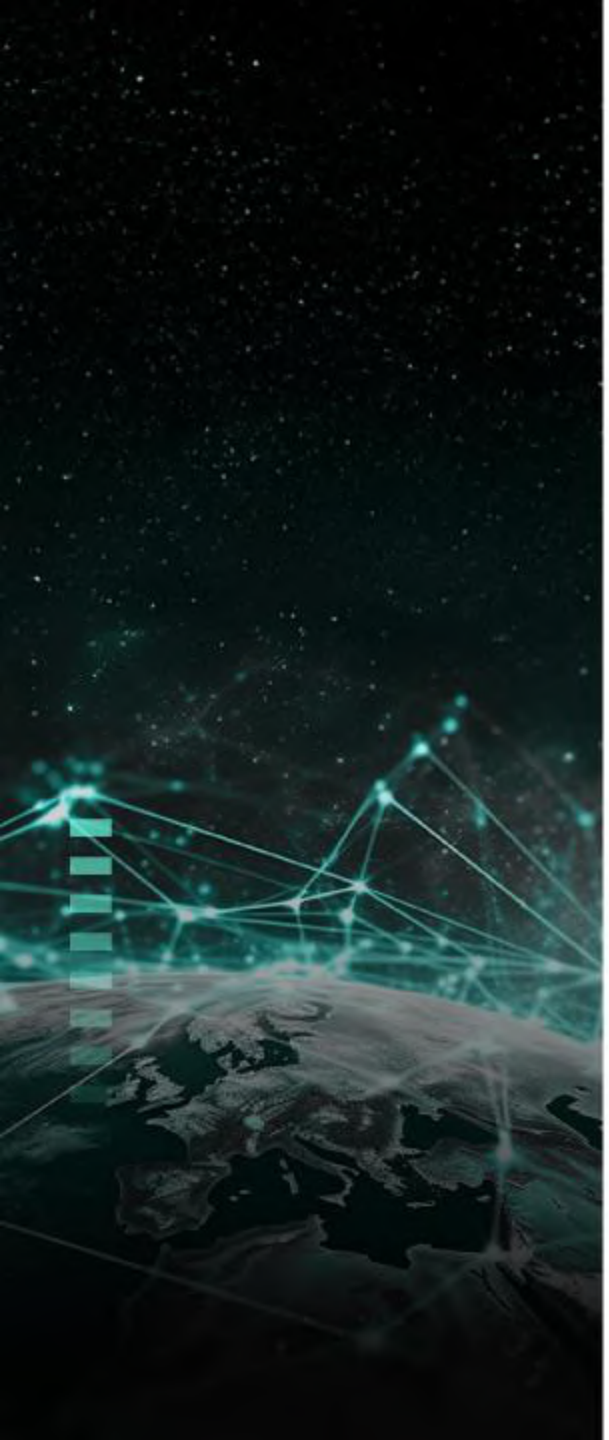


Bluetooth Low Energy:

Pairing methods

The second-stage pairing methods are defined according to the Bluetooth protocol specification version, as either legacy pairing or secure connections.

- **Legacy pairing**: the devices exchange a Temporary Key (TK) through pairing methods defined as Just Works, Passkey Entry, or Out-of-Band. They then use the TK to derive a Short-Term Key, which is used to encrypt the connection.

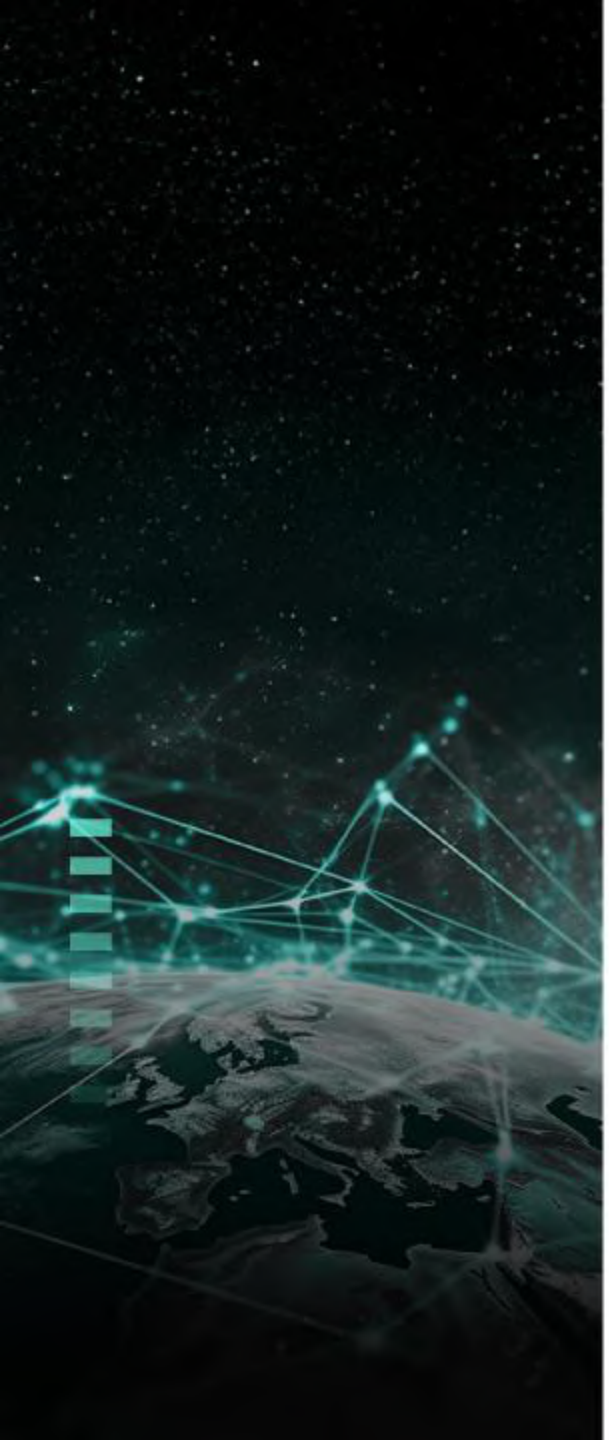


Bluetooth Low Energy:

Pairing methods

Legacy pairing methods:

- **Just Works**: sets the TK to a null or fixed value, compromising the confidentiality of the communication and making it susceptible to brute-force attacks, eavesdropping, and MITM (Man-in-the-Middle) attacks.
- **Passkey Entry**: one of the devices generates and displays a six-digit numeric TK that must be entered on the second device. Although it provides a basic level of security, breaking this code through brute force is relatively easy, allowing an attacker to use the TK to derive the STK corresponding to the Bluetooth link.
- **Out of Band**: enables pairing and sending of the TK through an external channel, using a wireless technology other than Bluetooth (e.g., NFC, Near Field Communication).



Bluetooth Low Energy:

Pairing methods

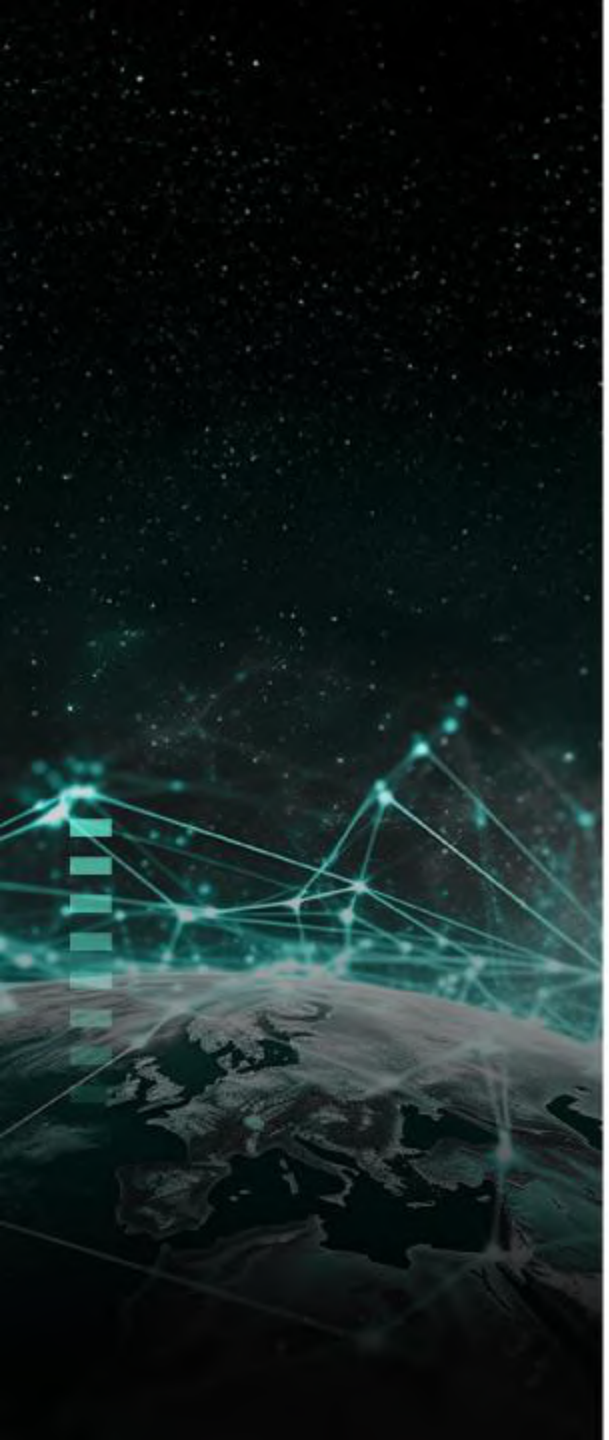
Secure Connections methods:

- ✓ LE Secure Connections uses the **ECDH (Elliptic-curve Diffie–Hellman) protocol** to derive public and private keys, which are exchanged to implement the Diffie–Hellman key agreement. Afterwards, a pairing method is used to authenticate the connection, and the long-term key (LTK) is generated directly to encrypt the connection.
- ✓ The previously mentioned pairing methods are adopted by LE Secure Connections, including a fourth variation called Numerical Comparison. In this case, a six-digit number is displayed on both devices, and the user must confirm whether the two numbers are identical.

Organized by:

Hardware/Software limitations in IoT devices

Lack of security at the application layer



Bluetooth Low Energy:

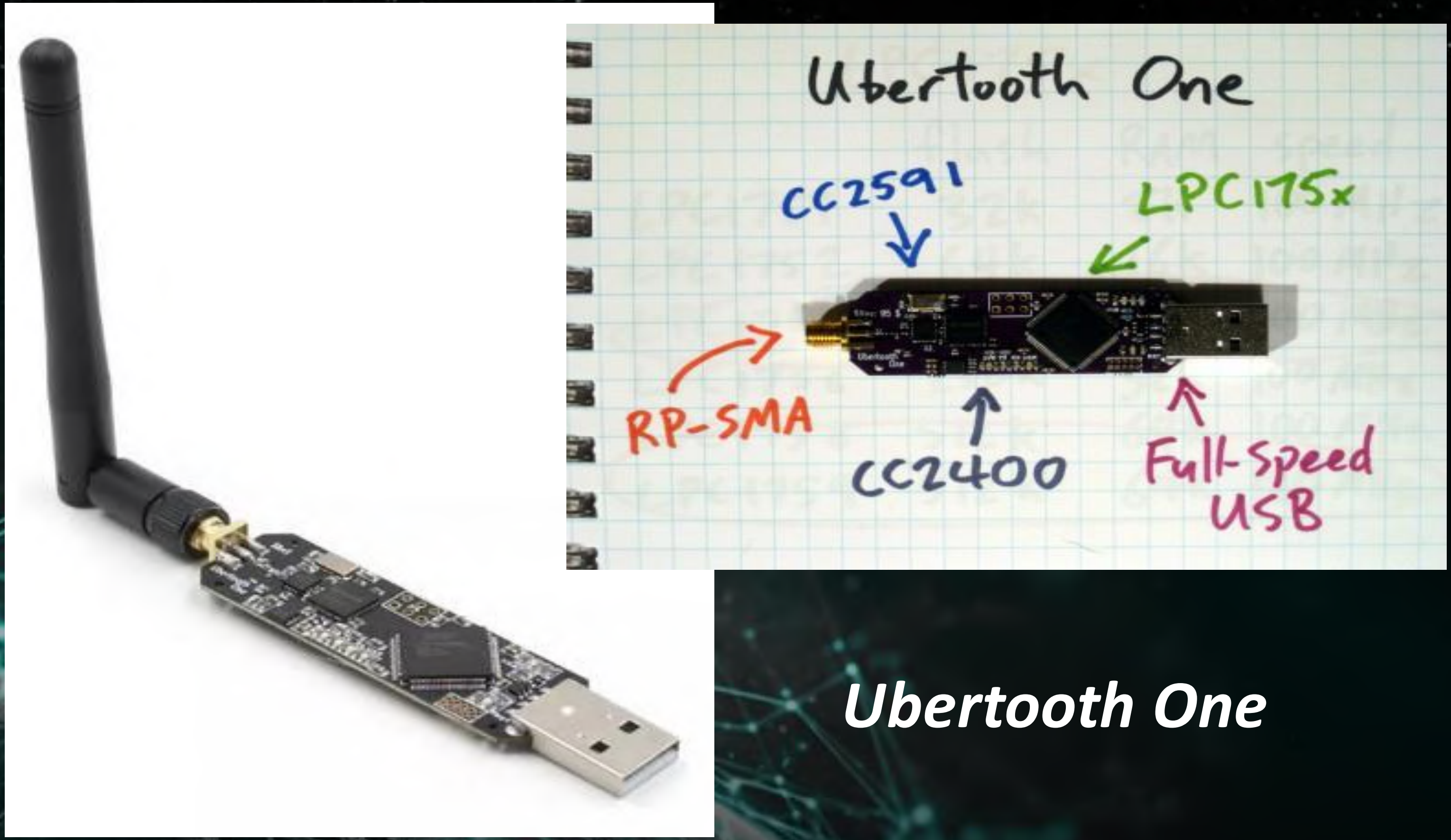
Vulnerabilities

The security risks to which Bluetooth devices and communication are exposed can be summarized as follows:

- ➢ Eavesdropping (traffic interception)
- ➢ Impersonation and communication tampering attacks
- ➢ Replay attacks

Organized by:

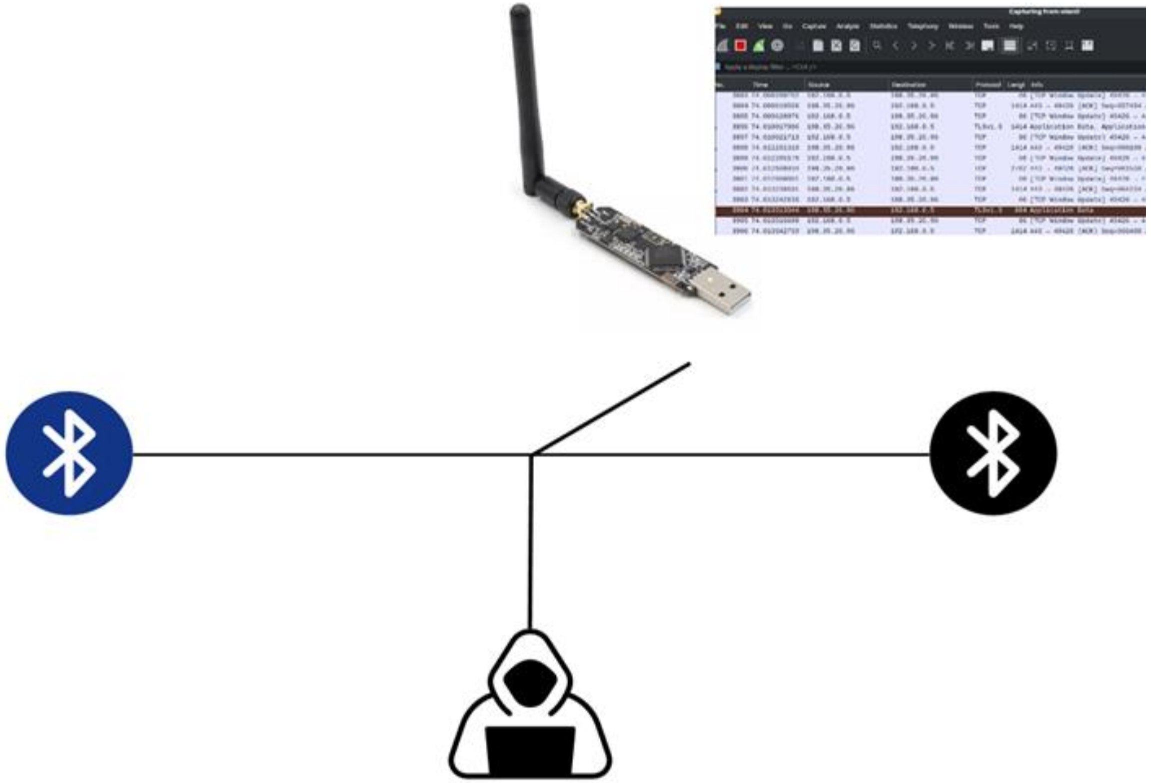
Practical demonstration



Ubertooth One

Practical demonstration

eavesdropping



Organized by:

xGMobile Centro de Competência EMBRAPII Inatel em Redes 5G e 6G

Inatel

FAPEMIG

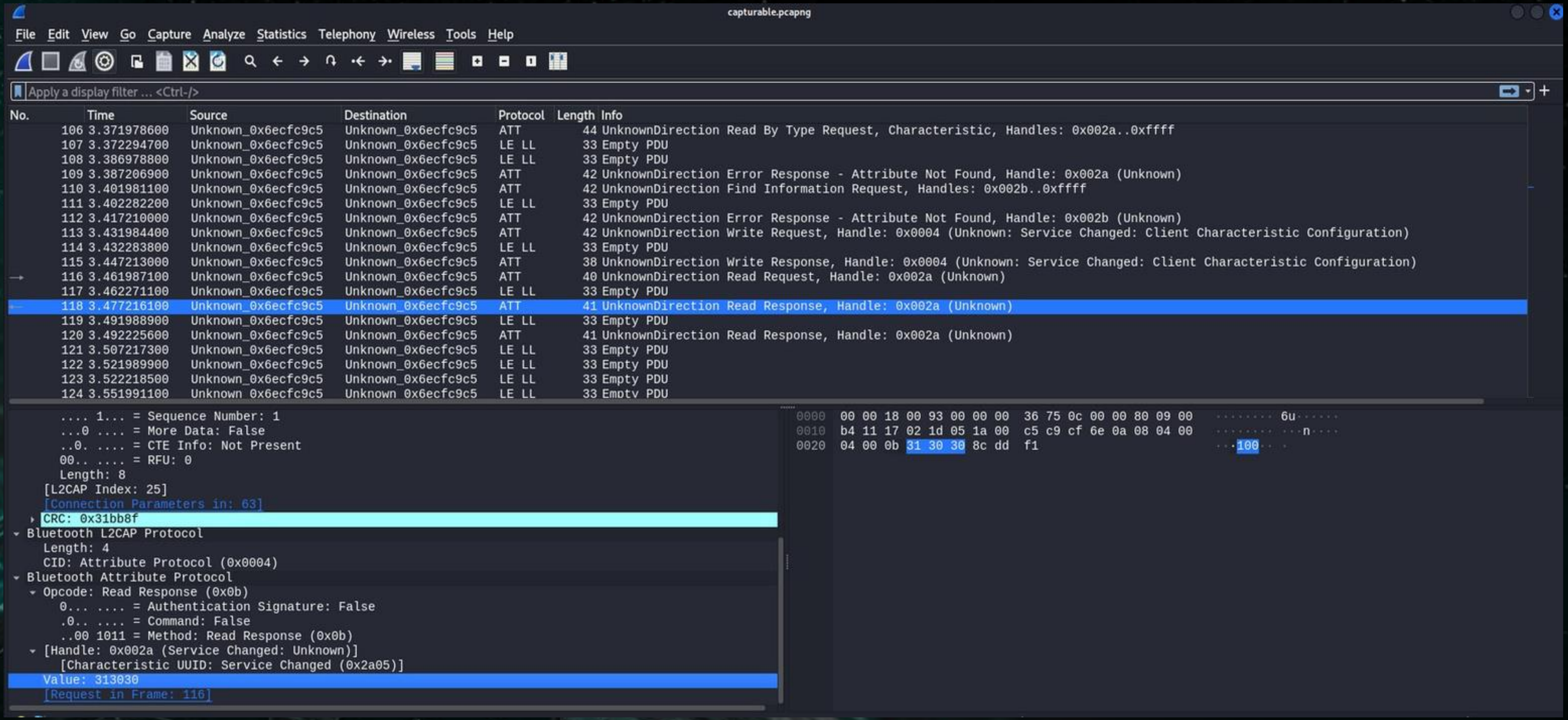
EMBRAPII

GOVERNO DE MINAS
AQUI O TREM PROSPERA.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO

Practical demonstration: eavesdropping



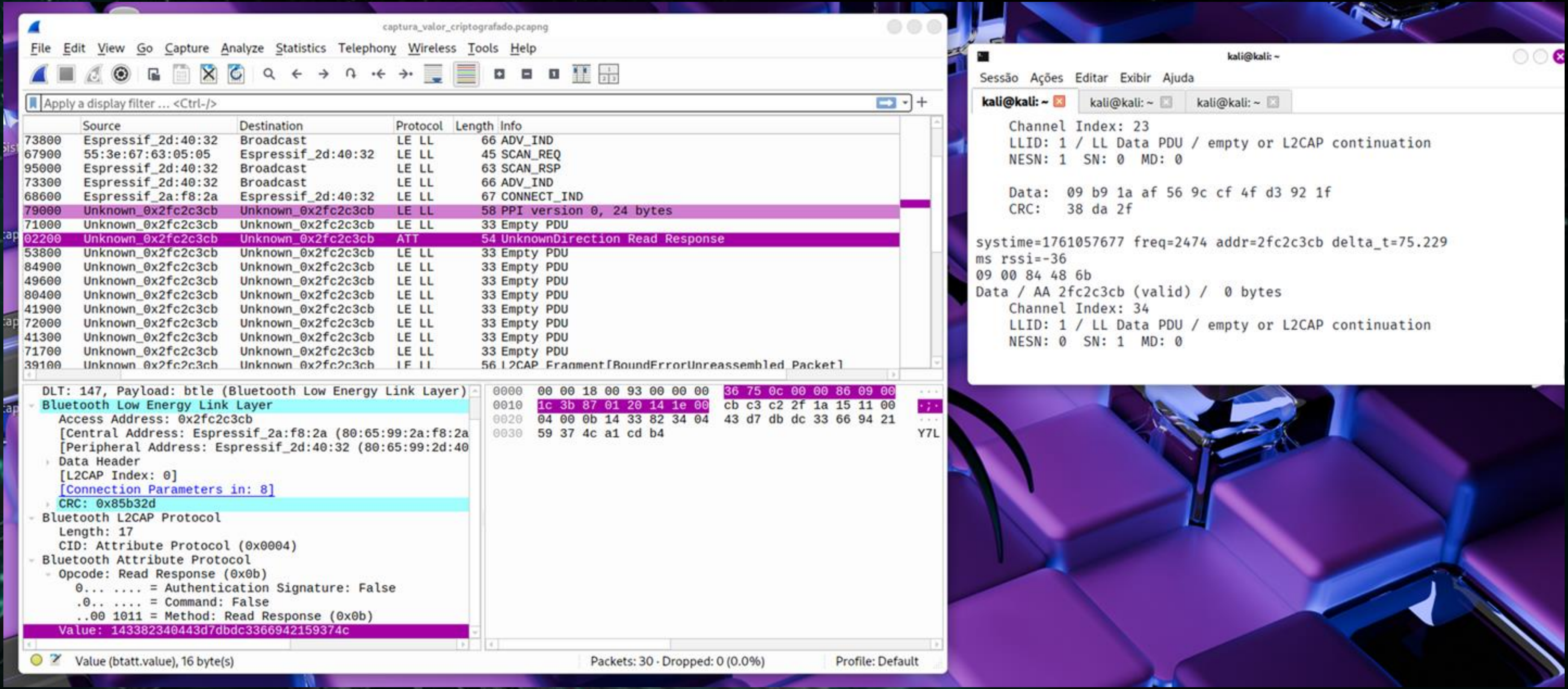
capturable.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time        Source               Destination          Protocol Length Info
    106 3.371978600 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   ATT        44 UnknownDirection Read By Type Request, Characteristic, Handles: 0x002a..0xffff
    107 3.372294700 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   LE LL      33 Empty PDU
    108 3.386978800 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   LE LL      33 Empty PDU
    109 3.387206900 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   ATT        42 UnknownDirection Error Response - Attribute Not Found, Handle: 0x002a (Unknown)
    110 3.401981100 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   ATT        42 UnknownDirection Find Information Request, Handles: 0x002b..0xffff
    111 3.402282200 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   LE LL      33 Empty PDU
    112 3.417210000 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   ATT        42 UnknownDirection Error Response - Attribute Not Found, Handle: 0x002b (Unknown)
    113 3.431984400 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   ATT        42 UnknownDirection Write Request, Handle: 0x0004 (Unknown: Service Changed: Client Characteristic Configuration)
    114 3.432283800 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   LE LL      33 Empty PDU
    115 3.447213000 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   ATT        38 UnknownDirection Write Response, Handle: 0x0004 (Unknown: Service Changed: Client Characteristic Configuration)
→   116 3.461987100 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   ATT        40 UnknownDirection Read Request, Handle: 0x002a (Unknown)
    117 3.462271100 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   LE LL      33 Empty PDU
←   118 3.477216100 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   ATT        41 UnknownDirection Read Response, Handle: 0x002a (Unknown)
    119 3.491988900 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   LE LL      33 Empty PDU
    120 3.492225600 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   ATT        41 UnknownDirection Read Response, Handle: 0x002a (Unknown)
    121 3.507217300 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   LE LL      33 Empty PDU
    122 3.521989900 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   LE LL      33 Empty PDU
    123 3.522218500 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   LE LL      33 Empty PDU
    124 3.551991100 Unknown_0x6ecfc9c5   Unknown_0x6ecfc9c5   LE LL      33 Empty PDU
```

```
      .... 1... = Sequence Number: 1
      ...0 .... = More Data: False
      ..0. .... = CTE Info: Not Present
      00.. .... = RFU: 0
      Length: 8
    [L2CAP Index: 25]
    [Connection Parameters in: 63]
  › CRC: 0x31bb8f
⌄ Bluetooth L2CAP Protocol
    Length: 4
    CID: Attribute Protocol (0x0004)
⌄ Bluetooth Attribute Protocol
  ⌄ Opcode: Read Response (0x0b)
      0... .... = Authentication Signature: False
      .0.. .... = Command: False
      ..00 1011 = Method: Read Response (0x0b)
  ⌄ [Handle: 0x002a (Service Changed: Unknown)]
      [Characteristic UUID: Service Changed (0x2a05)]
    Value: 313030
    [Request in Frame: 116]
```

```
0000  00 00 18 00 93 00 00 00  36 75 0c 00 00 80 09 00   ········6u······
0010  b4 11 17 02 1d 05 1a 00  c5 c9 cf 6e 0a 08 04 00   ···········n····
0020  04 00 0b 31 30 30 8c dd  f1                        ···100···
```

Practical demonstration: eavesdropping


captura_valor_criptografado.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
kali@kali: ~
Sessão Ações Editar Exibir Ajuda
kali@kali: ~
kali@kali: ~
kali@kali: ~

```
       Source                Destination           Protocol Length Info
73800  Espressif_2d:40:32    Broadcast             LE LL        66 ADV_IND
67900  55:3e:67:63:05:05     Espressif_2d:40:32    LE LL        45 SCAN_REQ
95000  Espressif_2d:40:32    Broadcast             LE LL        63 SCAN_RSP
73300  Espressif_2d:40:32    Broadcast             LE LL        66 ADV_IND
68600  Espressif_2a:f8:2a    Espressif_2d:40:32    LE LL        67 CONNECT_IND
79000  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    LE LL        58 PPI version 0, 24 bytes
71000  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    LE LL        33 Empty PDU
02200  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    ATT          54 UnknownDirection Read Response
53800  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    LE LL        33 Empty PDU
84900  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    LE LL        33 Empty PDU
49600  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    LE LL        33 Empty PDU
80400  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    LE LL        33 Empty PDU
41900  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    LE LL        33 Empty PDU
72000  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    LE LL        33 Empty PDU
41300  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    LE LL        33 Empty PDU
71700  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    LE LL        33 Empty PDU
39100  Unknown_0x2fc2c3cb    Unknown_0x2fc2c3cb    LE LL        56 L2CAP Fragment[BoundErrorUnreassembled Packet]
```

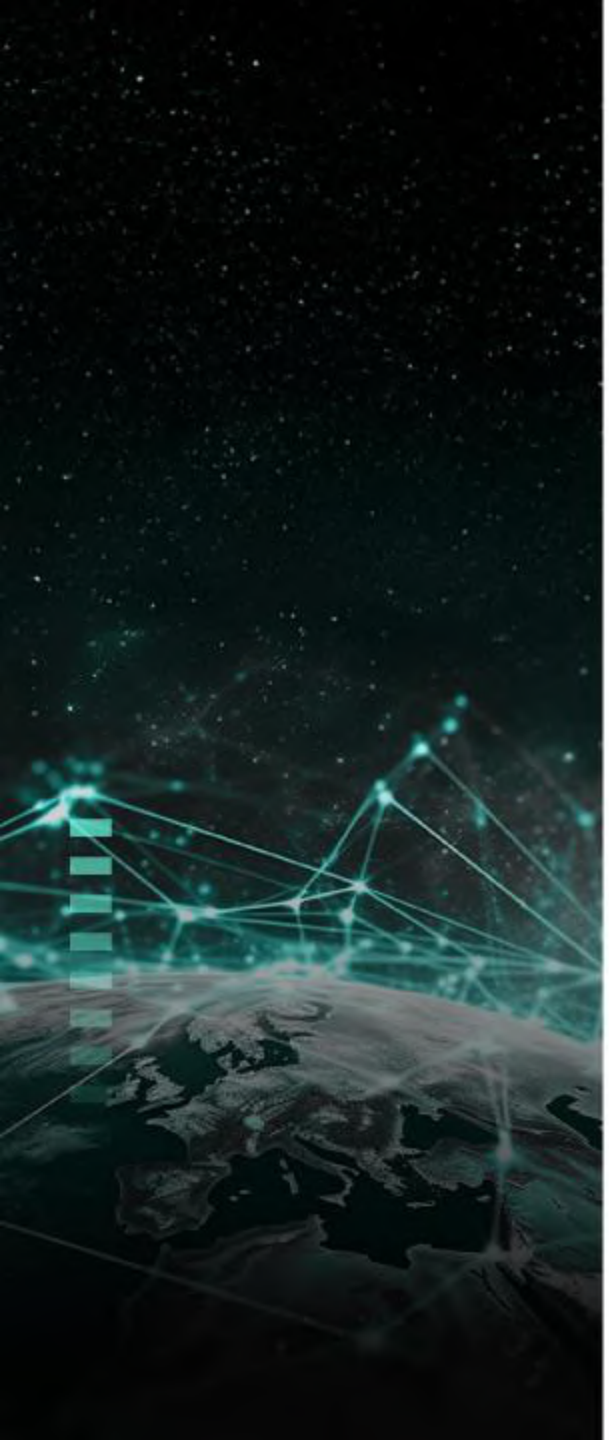
```
DLT: 147, Payload: btle (Bluetooth Low Energy Link Layer)
Bluetooth Low Energy Link Layer
  Access Address: 0x2fc2c3cb
  [Central Address: Espressif_2a:f8:2a (80:65:99:2a:f8:2a
  [Peripheral Address: Espressif_2d:40:32 (80:65:99:2d:40
  Data Header
  [L2CAP Index: 0]
  [Connection Parameters in: 8]
  CRC: 0x85b32d
Bluetooth L2CAP Protocol
  Length: 17
  CID: Attribute Protocol (0x0004)
Bluetooth Attribute Protocol
  Opcode: Read Response (0x0b)
    0... .... = Authentication Signature: False
    .0.. .... = Command: False
    ..00 1011 = Method: Read Response (0x0b)
  Value: 143382340443d7dbdc3366942159374c
```

```
0000  00 00 18 00 93 00 00 00  36 75 0c 00 00 86 09 00   ···
0010  1c 3b 87 01 20 14 1e 00  cb c3 c2 2f 1a 15 11 00   ·;·
0020  04 00 0b 14 33 82 34 04  43 d7 db dc 33 66 94 21   ···
0030  59 37 4c a1 cd b4                                  Y7L
```

Value (btatt.value), 16 byte(s)   Packets: 30 · Dropped: 0 (0.0%)   Profile: Default

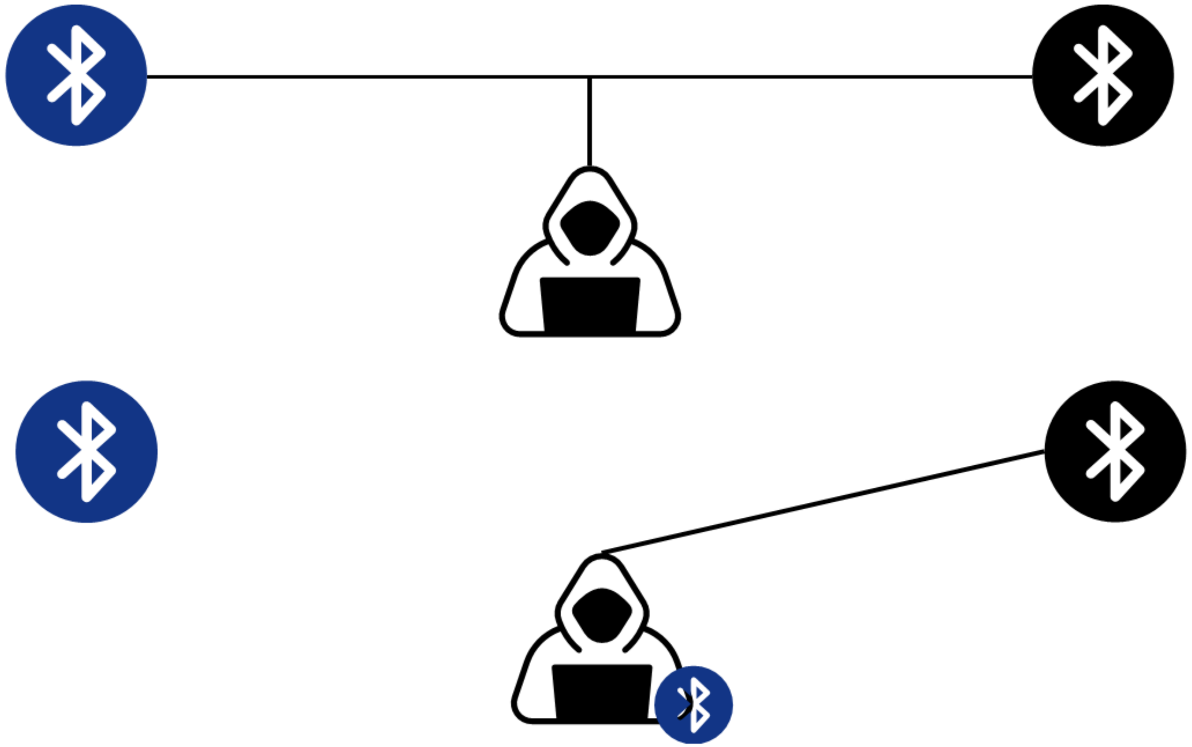
```
    Channel Index: 23
    LLID: 1 / LL Data PDU / empty or L2CAP continuation
    NESN: 1  SN: 0  MD: 0

    Data:  09 b9 1a af 56 9c cf 4f d3 92 1f
    CRC:   38 da 2f

systime=1761057677 freq=2474 addr=2fc2c3cb delta_t=75.229
ms rssi=-36
09 00 84 48 6b
Data / AA 2fc2c3cb (valid) /  0 bytes
    Channel Index: 34
    LLID: 1 / LL Data PDU / empty or L2CAP continuation
    NESN: 0  SN: 1  MD: 0
```

Organized by:



Practical demonstration

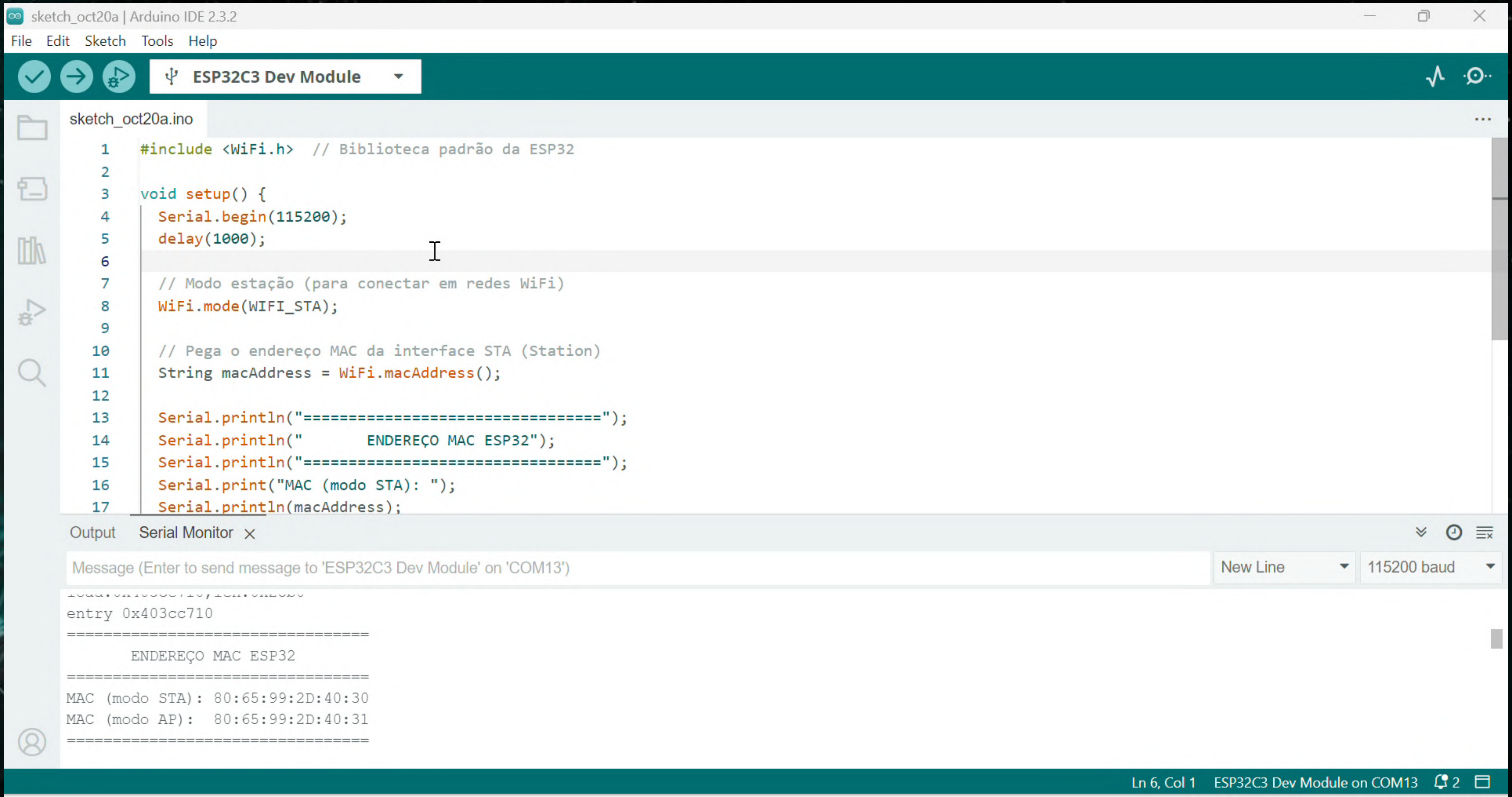
Impersonation and replay



Organized by:

xGMobile Inatel FAPEMIG EMBRAPII GOVERNO DE MINAS AQUI O TREM PROSPERA. MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO DO BRASIL DO LADO DO POVO BRASILEIRO

Practical demonstration: Impersonation and replay

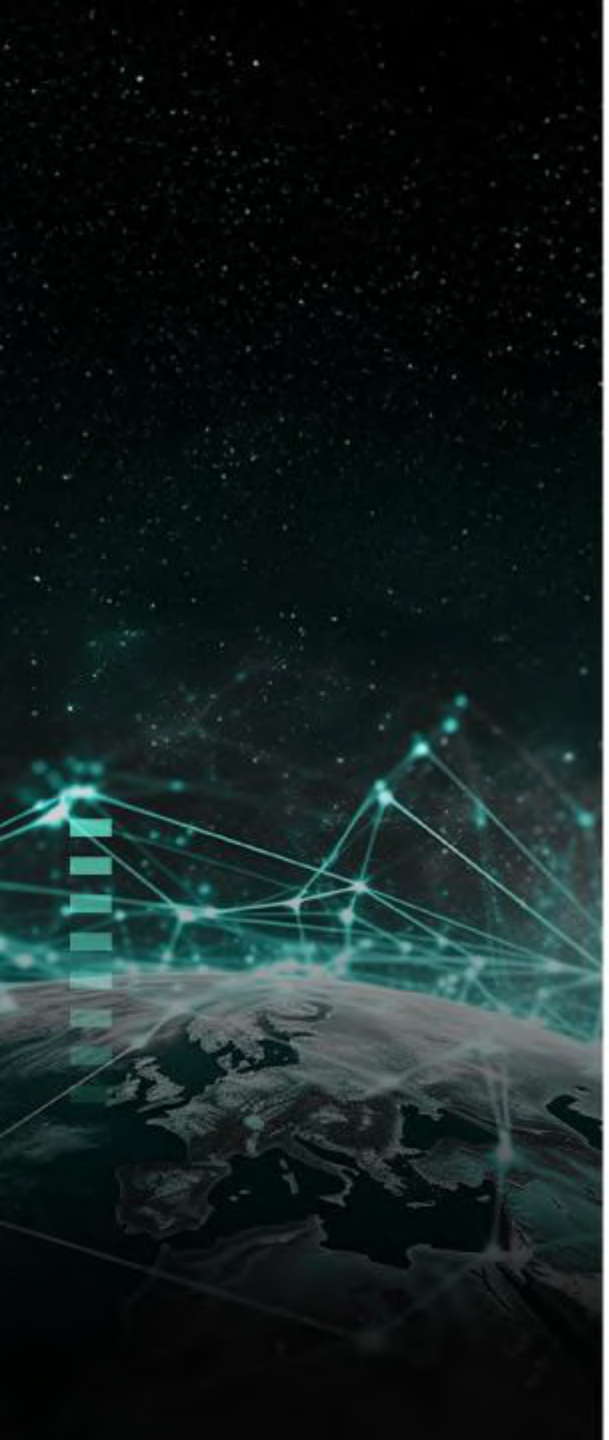

sketch_oct20a | Arduino IDE 2.3.2
File Edit Sketch Tools Help
ESP32C3 Dev Module
sketch_oct20a.ino
Output
Serial Monitor
Message (Enter to send message to 'ESP32C3 Dev Module' on 'COM13')
New Line
115200 baud
Ln 6, Col 1 ESP32C3 Dev Module on COM13 2

```
#include <WiFi.h>  // Biblioteca padrão da ESP32

void setup() {
  Serial.begin(115200);
  delay(1000);

  // Modo estação (para conectar em redes WiFi)
  WiFi.mode(WIFI_STA);

  // Pega o endereço MAC da interface STA (Station)
  String macAddress = WiFi.macAddress();

  Serial.println("=================================");
  Serial.println("       ENDEREÇO MAC ESP32");
  Serial.println("=================================");
  Serial.print("MAC (modo STA): ");
  Serial.println(macAddress);
```

```
entry 0x403cc710
=================================
       ENDEREÇO MAC ESP32
=================================
MAC (modo STA): 80:65:99:2D:40:30
MAC (modo AP):  80:65:99:2D:40:31
=================================
```

Organized by:

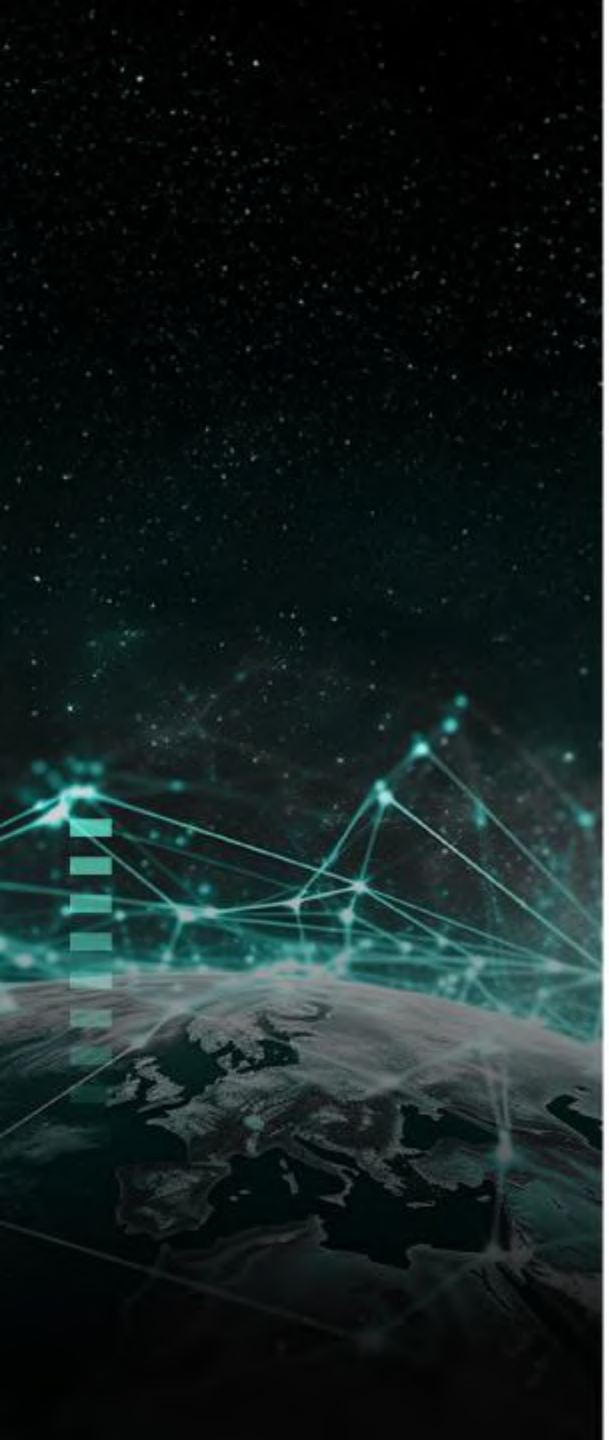
xGMobile Inatel FAPEMIG EMBRAPII GOVERNO DE MINAS AQUI O TREM PROSPERA. MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO DO BRASIL DO LADO DO POVO BRASILEIRO



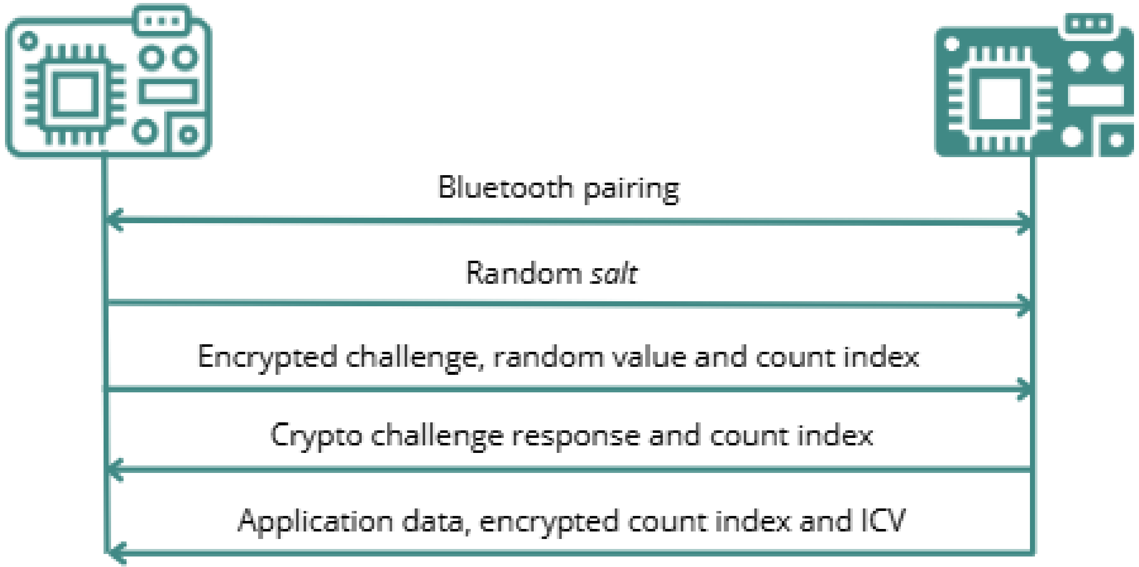
Real-world scenario

Platform developed for industries, where the main devices communicated via BLE. Vulnerabilities found:

- The central device was susceptible to impersonation and replay attacks.
- Even with an already established connection to the legitimate peripheral, creating a fake impersonated device caused the central to connect to the falsified device.
- Replay attacks were not necessary, as the encryption and security mechanisms implemented in the system relied on the BLE protocol itself.



Proposed secure implementation model



Bluetooth pairing

Random *salt*

Encrypted challenge, random value and count index

Crypto challenge response and count index

Application data, encrypted count index and ICV

(PDF) A Novel Secure Communication Scheme for...

PDF | This work presents a new approach to implementing a secure communication model for devices operating based on th...

researchgate.net

Organized by:

xGMobile Inatel FAPEMIG EMBRAPII GOVERNO DE MINAS AQUI O TREM PROSPERA. MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO DO BRASIL DO LADO DO POVO BRASILEIRO

Connecting ideas, anticipating the future:
collaborative innovation for 5G and 6G networks.

II INTERNATIONAL WORKSHOP xGMobile

Organized by:

xGMobile
Centro de Competência EMBRAPII Inatel em Redes 5G e 6G

Inatel

FAPEMIG

EMBRAPII

GOVERNO DE MINAS
AQUI O TREM PROSPERA.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

GOVERNO DO BRASIL
DO LADO DO POVO BRASILEIRO