TARLOGIC
CYBERSECURITY EXPERTS

Bluetooth Attacks: From theory to practice

www.tarlogic.com

Antonio Vázquez Blanco
Jesús M. Gómez Moreno

TARLOGIC
CYBERSECURITY EXPERTS

$ WHOAMI

# Antonio Vázquez Blanco

@antoniovazquezblanco@mastodon.social

antonio.vazquez@tarlogic.com

#Research Engineer en Tarlogic Security

TARLOGIC
CYBERSECURITY EXPERTS

$ WHOAMI

# Jesús M. Gómez Moreno

@zus_999

@zus@masto.es

jesus.gomez@tarlogic.com

#Research Engineer en Tarlogic Security

TARLOGIC
CYBERSECURITY EXPERTS

$ WHOAMI

Resto del equipo:

- Francisco Manuel Álvarez Wic
- David Sandoval Rodríguez-Bermejo
- Miguel Tarascó Acuña

TARLOGIC
CYBERSECURITY EXPERTS

www.tarlogic.com
29.11.23

BLUETOOTH INTRODUCTION

(IN 5 MINUTES…)

# Bluetooth

Bluetooth®

Bluetooth
Core Specification

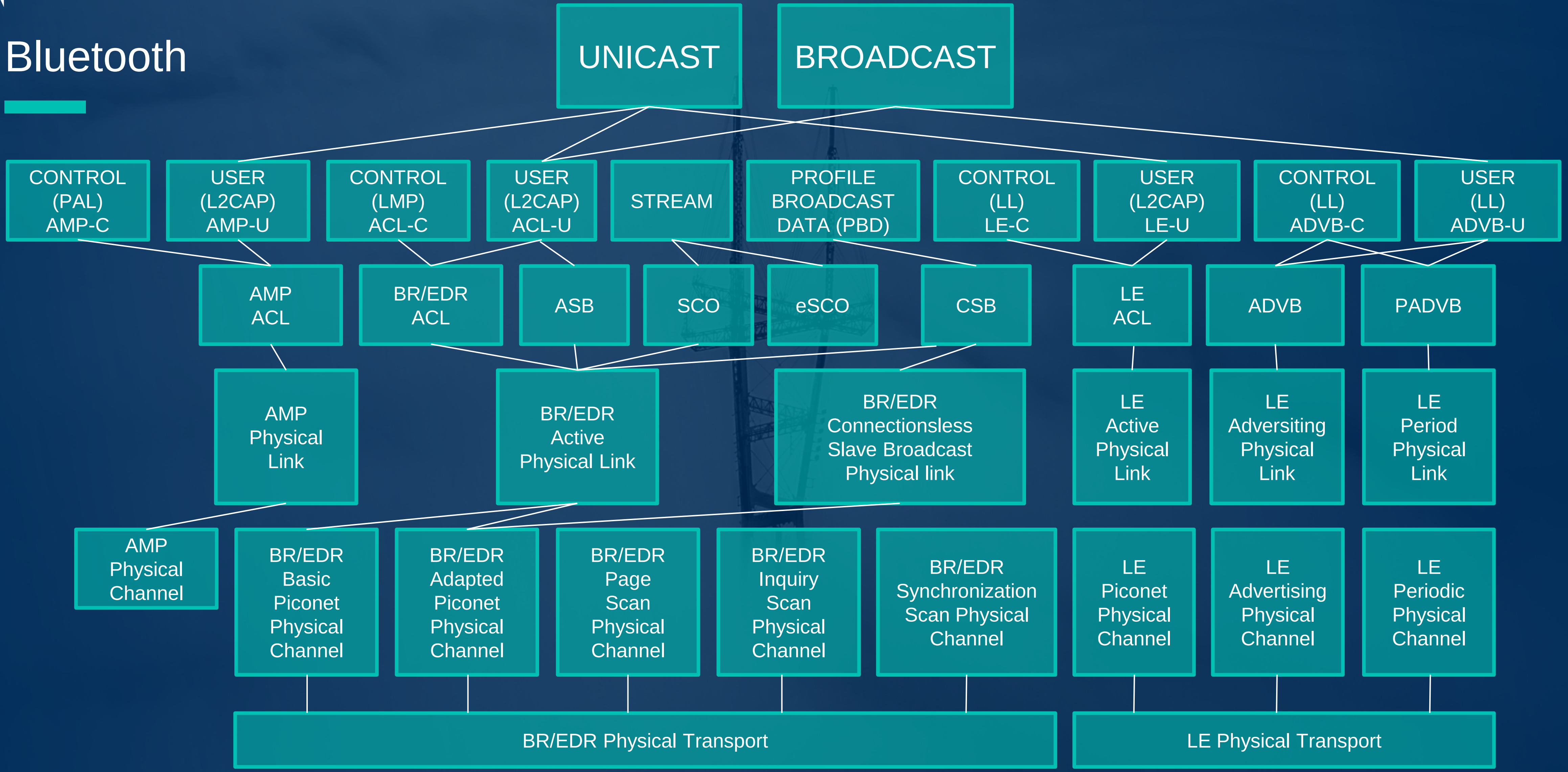
v5.0

Bluetooth SIG Proprietary

# Bluetooth

- Short range (PAN)
- Connects mobile and low power devices
- Uses adaptive frequency-hopping and timeslots
- Has a master/slave architecture
- Master communicates to slaves in a piconet
- Managed by Bluetooth Special Interest Group (SIG)
- Published in the Bluetooth Core Specification

Bluetooth



UNICAST

BROADCAST

CONTROL (PAL) AMP-C

USER (L2CAP) AMP-U

CONTROL (LMP) ACL-C

USER (L2CAP) ACL-U

STREAM

PROFILE BROADCAST DATA (PBD)

CONTROL (LL) LE-C

USER (L2CAP) LE-U

CONTROL (LL) ADVB-C

USER (LL) ADVB-U

AMP ACL

BR/EDR ACL

ASB

SCO

eSCO

CSB

LE ACL

ADVB

PADVB

AMP Physical Link

BR/EDR Active Physical Link

BR/EDR Connectionless Slave Broadcast Physical link

LE Active Physical Link

LE Adversiting Physical Link

LE Period Physical Link

AMP Physical Channel

BR/EDR Basic Piconet Physical Channel

BR/EDR Adapted Piconet Physical Channel

BR/EDR Page Scan Physical Channel

BR/EDR Inquiry Scan Physical Channel

BR/EDR Synchronization Scan Physical Channel

LE Piconet Physical Channel

LE Advertising Physical Channel

LE Periodic Physical Channel

BR/EDR Physical Transport

LE Physical Transport

Bluetooth BR/EDR and Bluetooth LE

# The Bluetooth Core Specification…

- Is created by the Special Interest Group
- Defines Bluetooth BR/EDR and Bluetooth LE

Variant	Bandwidth	Power	Discovery	Encryption
Bluetooth BR/EDR	High	High	Active (paging)	E0\SAFER+
Bluetooth LE	Low	Low	Passive	AES-CCM

Bluetooth BR/EDR and Bluetooth LE

# The Bluetooth Core Specification…

- Is created by the Special Interest Group
- Defines Bluetooth BR/EDR and Bluetooth LE

Variant	Bandwidth	Power	Discovery	Encryption
Bluetooth BR/EDR	High	High	Active (paging)	E0\SAFER+
Bluetooth LE	Low	Low	Passive	AES-CCM

Bluetooth Host and Controller

# The Bluetooth core system architecture is divided in …

Bluetooth Host and Controller

# The Bluetooth core system architecture is divided in …

- One host
- One primary controller

Host

- Linux: bluez
- Windows: bluetooth driver stack

Bluetooth Host and Controller

# The Bluetooth core system architecture is divided in …

- One host
- One primary controller

Host

- Linux: bluez
- Windows: bluetooth driver stack

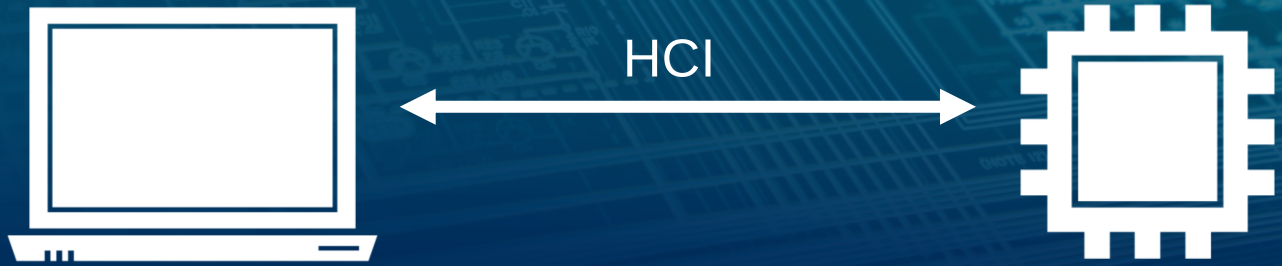
Primary controller

- Device firmware
- BR/EDR, LE or both

Bluetooth Host and Controller

# The Bluetooth core system architecture is divided in …

- One host
- One primary controller



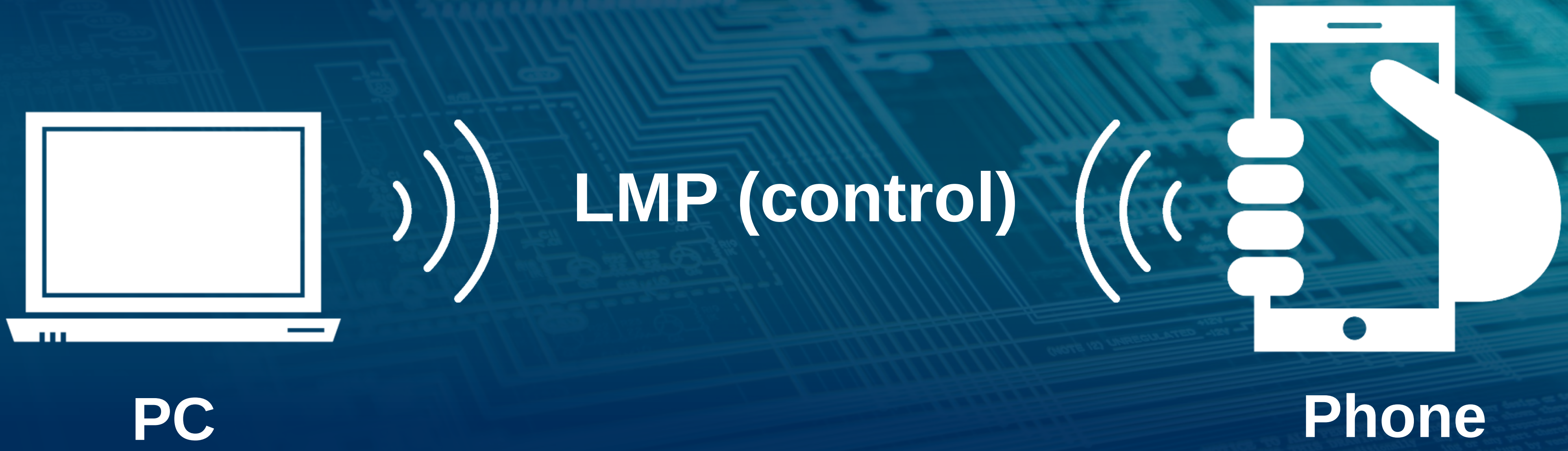
Host

- Linux: bluez
- Windows: bluetooth driver stack

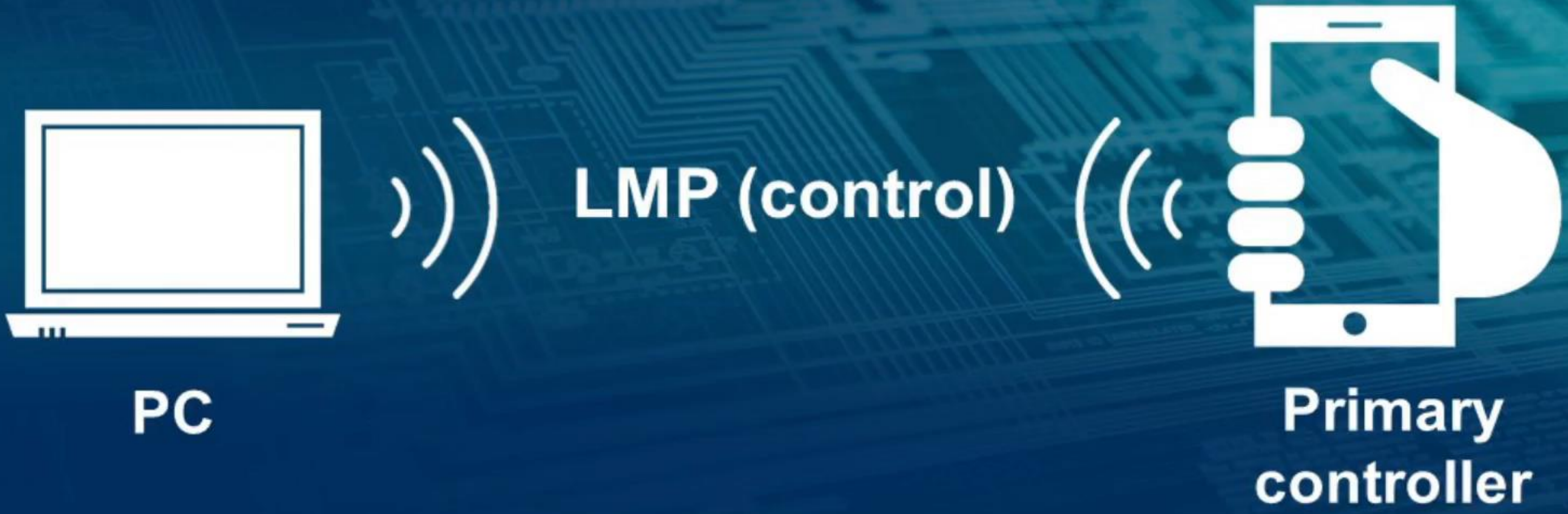
Primary controller

- Device firmware
- BR/EDR, LE or both

Bluetooth Link Management Protocol: LMP



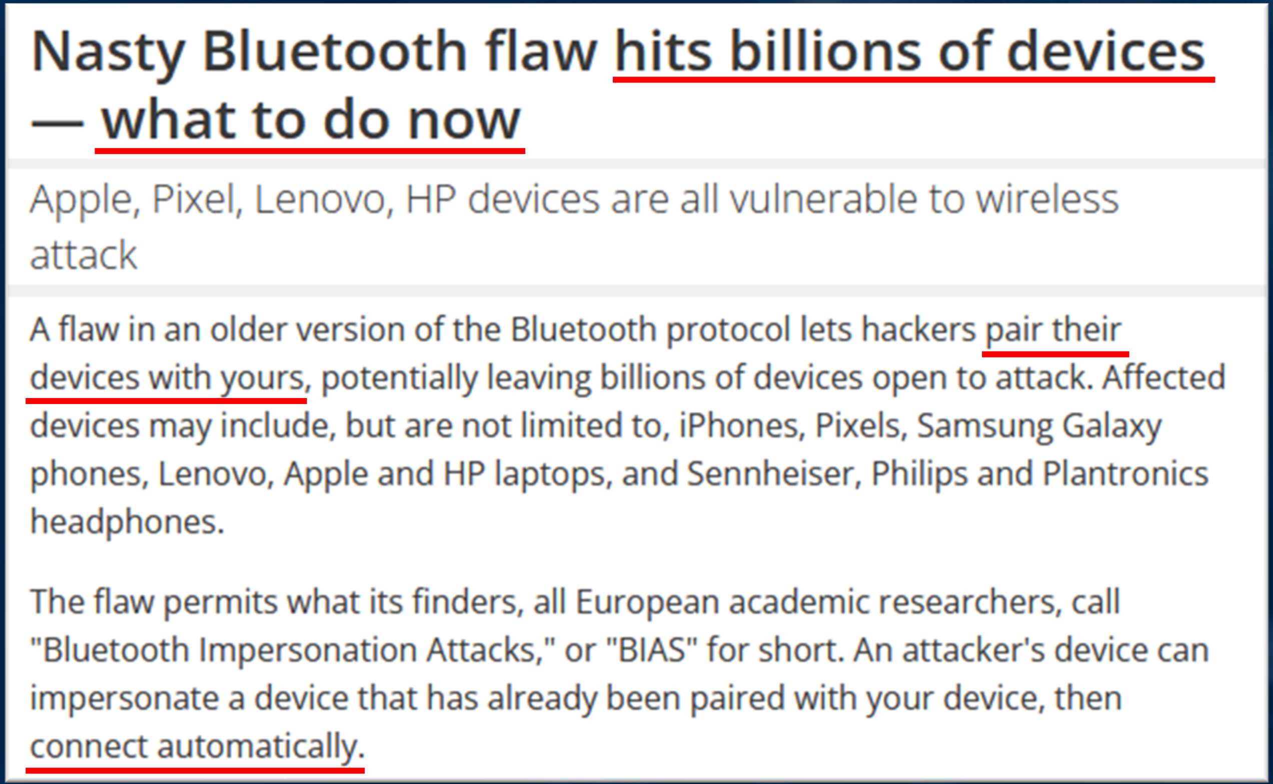
Bluetooth Link Management Protocol: LMP



TARLOGIC
CYBERSECURITY EXPERTS

BIAS ATTACK

BIAS in the media



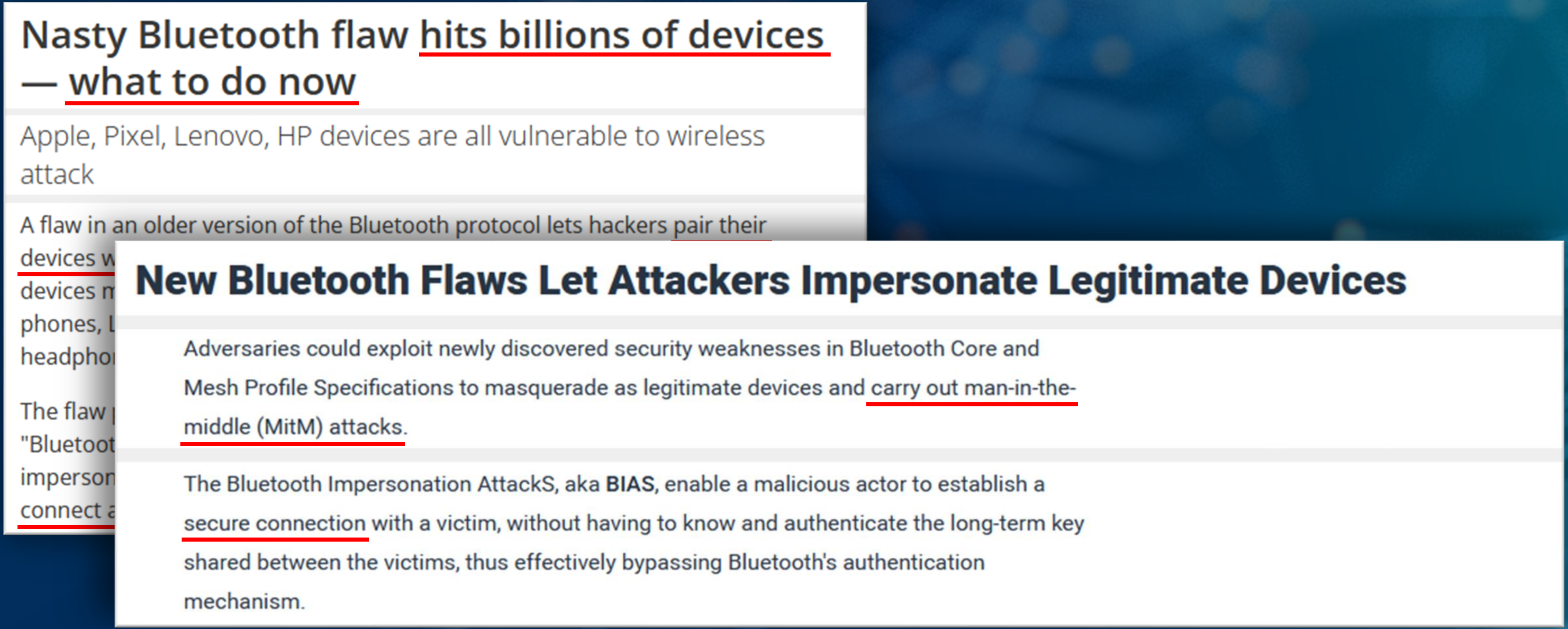
Nasty Bluetooth flaw hits billions of devices — what to do now

Apple, Pixel, Lenovo, HP devices are all vulnerable to wireless attack

A flaw in an older version of the Bluetooth protocol lets hackers pair their devices with yours, potentially leaving billions of devices open to attack. Affected devices may include, but are not limited to, iPhones, Pixels, Samsung Galaxy phones, Lenovo, Apple and HP laptops, and Sennheiser, Philips and Plantronics headphones.

The flaw permits what its finders, all European academic researchers, call "Bluetooth Impersonation Attacks," or "BIAS" for short. An attacker's device can impersonate a device that has already been paired with your device, then connect automatically.

BIAS in the media



Nasty Bluetooth flaw hits billions of devices — what to do now

Apple, Pixel, Lenovo, HP devices are all vulnerable to wireless attack

A flaw in an older version of the Bluetooth protocol lets hackers pair their
devices w
devices m
phones, L
headpho

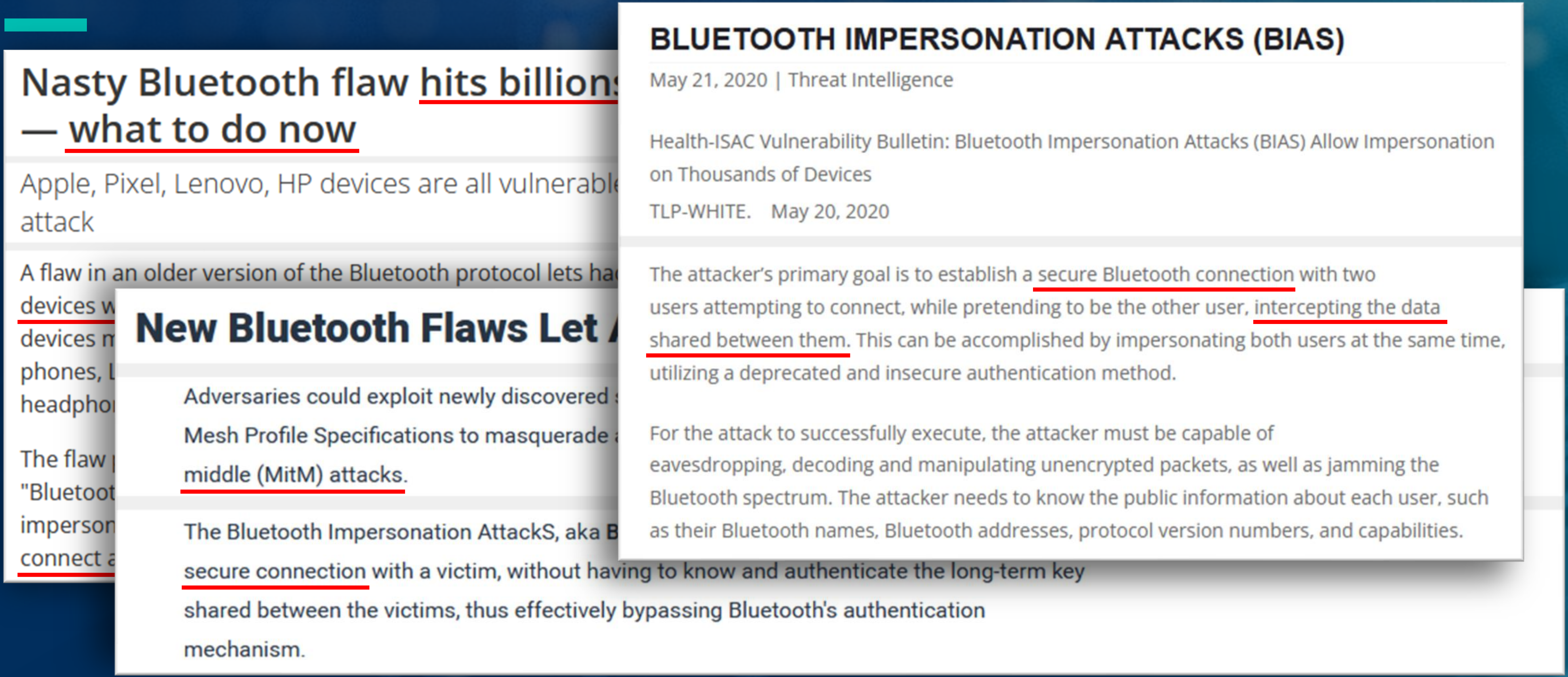
The flaw
"Bluetoot
imperson
connect a

New Bluetooth Flaws Let Attackers Impersonate Legitimate Devices

Adversaries could exploit newly discovered security weaknesses in Bluetooth Core and Mesh Profile Specifications to masquerade as legitimate devices and carry out man-in-the-middle (MitM) attacks.

The Bluetooth Impersonation AttackS, aka **BIAS**, enable a malicious actor to establish a secure connection with a victim, without having to know and authenticate the long-term key shared between the victims, thus effectively bypassing Bluetooth's authentication mechanism.

BIAS in the media



Nasty Bluetooth flaw hits billions — what to do now

Apple, Pixel, Lenovo, HP devices are all vulnerable attack

A flaw in an older version of the Bluetooth protocol lets ha
devices w
devices m
phones, L
headpho

The flaw
"Bluetoot
imperson
connect a

New Bluetooth Flaws Let A

Adversaries could exploit newly discovered s
Mesh Profile Specifications to masquerade a
middle (MitM) attacks.

The Bluetooth Impersonation AttackS, aka B
secure connection with a victim, without having to know and authenticate the long-term key shared between the victims, thus effectively bypassing Bluetooth's authentication mechanism.

BLUETOOTH IMPERSONATION ATTACKS (BIAS)

May 21, 2020 | Threat Intelligence

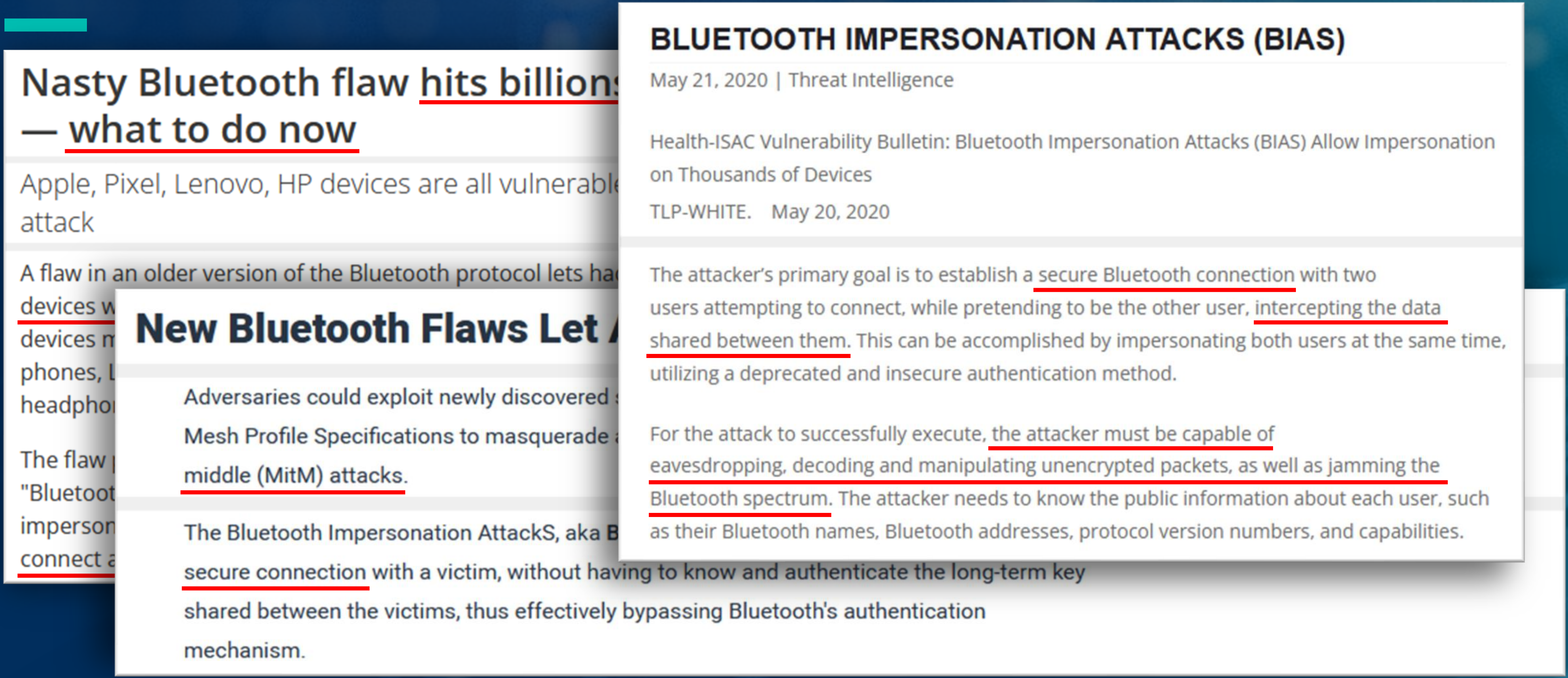
Health-ISAC Vulnerability Bulletin: Bluetooth Impersonation Attacks (BIAS) Allow Impersonation on Thousands of Devices

TLP-WHITE. May 20, 2020

The attacker's primary goal is to establish a secure Bluetooth connection with two users attempting to connect, while pretending to be the other user, intercepting the data shared between them. This can be accomplished by impersonating both users at the same time, utilizing a deprecated and insecure authentication method.

For the attack to successfully execute, the attacker must be capable of eavesdropping, decoding and manipulating unencrypted packets, as well as jamming the Bluetooth spectrum. The attacker needs to know the public information about each user, such as their Bluetooth names, Bluetooth addresses, protocol version numbers, and capabilities.

BIAS in the media



Nasty Bluetooth flaw hits billion
— what to do now

Apple, Pixel, Lenovo, HP devices are all vulnerabl
attack

A flaw in an older version of the Bluetooth protocol lets ha
devices w
devices m
phones, l
headpho

The flaw
"Bluetoot
imperson
connect a

New Bluetooth Flaws Let A

Adversaries could exploit newly discovered s
Mesh Profile Specifications to masquerade a
middle (MitM) attacks.

The Bluetooth Impersonation AttackS, aka B
secure connection with a victim, without having to know and authenticate the long-term key
shared between the victims, thus effectively bypassing Bluetooth's authentication
mechanism.

BLUETOOTH IMPERSONATION ATTACKS (BIAS)

May 21, 2020 | Threat Intelligence

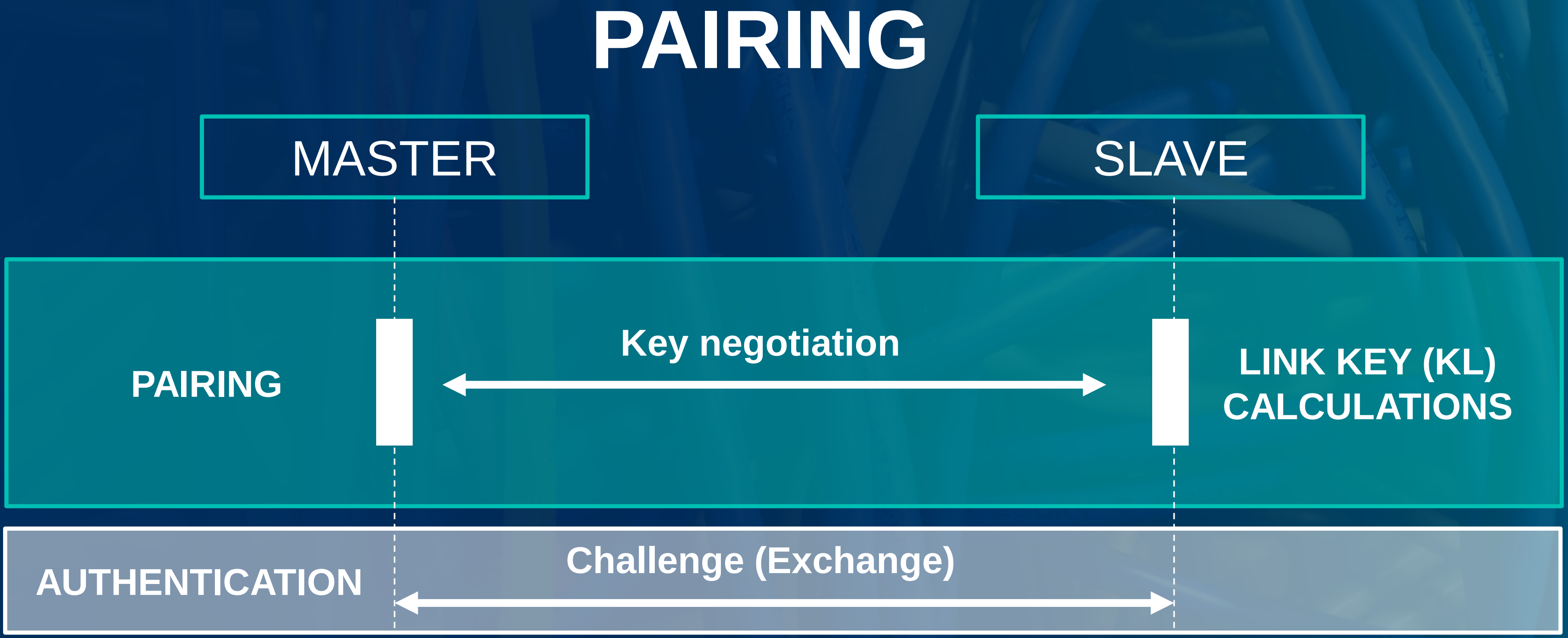
Health-ISAC Vulnerability Bulletin: Bluetooth Impersonation Attacks (BIAS) Allow Impersonation on Thousands of Devices

TLP-WHITE. May 20, 2020

The attacker's primary goal is to establish a secure Bluetooth connection with two users attempting to connect, while pretending to be the other user, intercepting the data shared between them. This can be accomplished by impersonating both users at the same time, utilizing a deprecated and insecure authentication method.

For the attack to successfully execute, the attacker must be capable of eavesdropping, decoding and manipulating unencrypted packets, as well as jamming the Bluetooth spectrum. The attacker needs to know the public information about each user, such as their Bluetooth names, Bluetooth addresses, protocol version numbers, and capabilities.

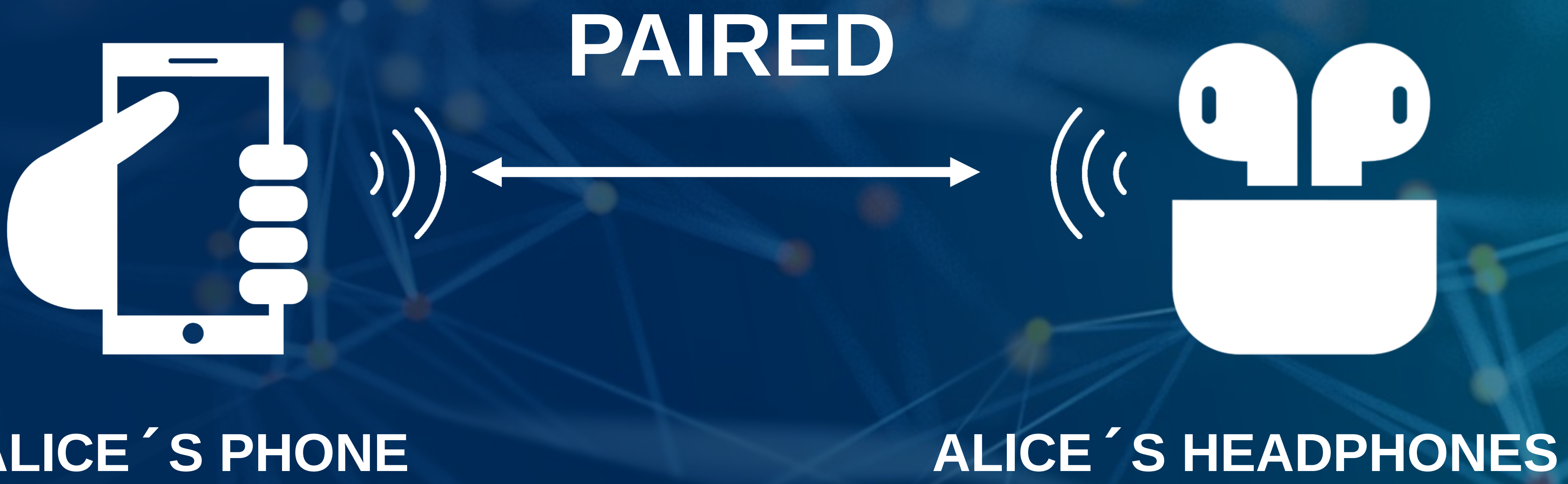
Pairing



(Bluetooth Core, Vol 2, Parte C, Sección 4.2.2)

(Imagen de Gert Skriver)

Normal pair of bluetooth devices

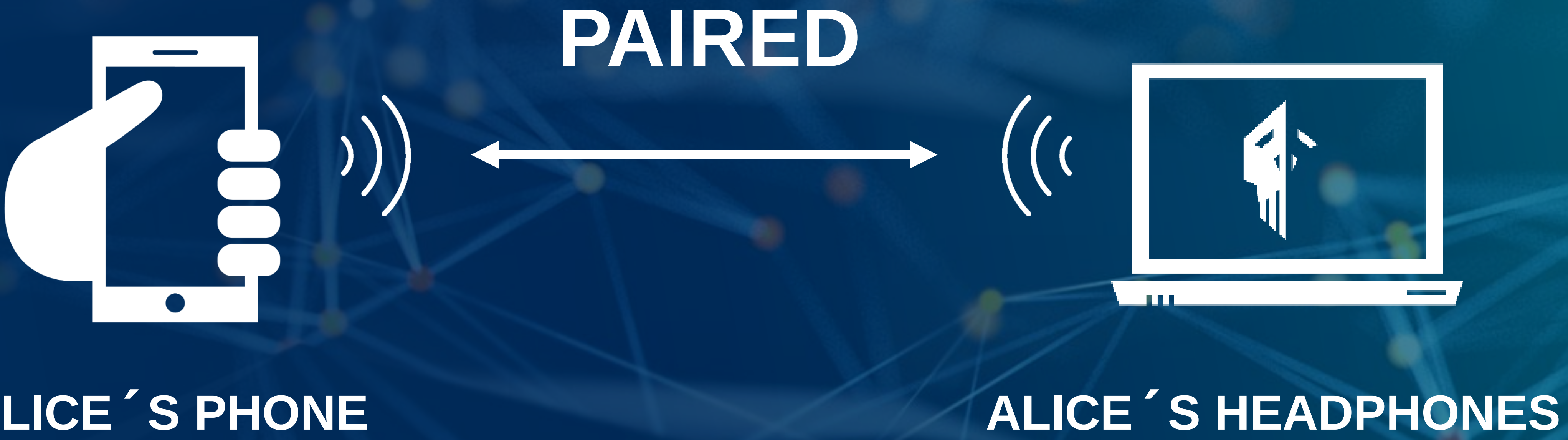


PAIRED

ALICE´S PHONE

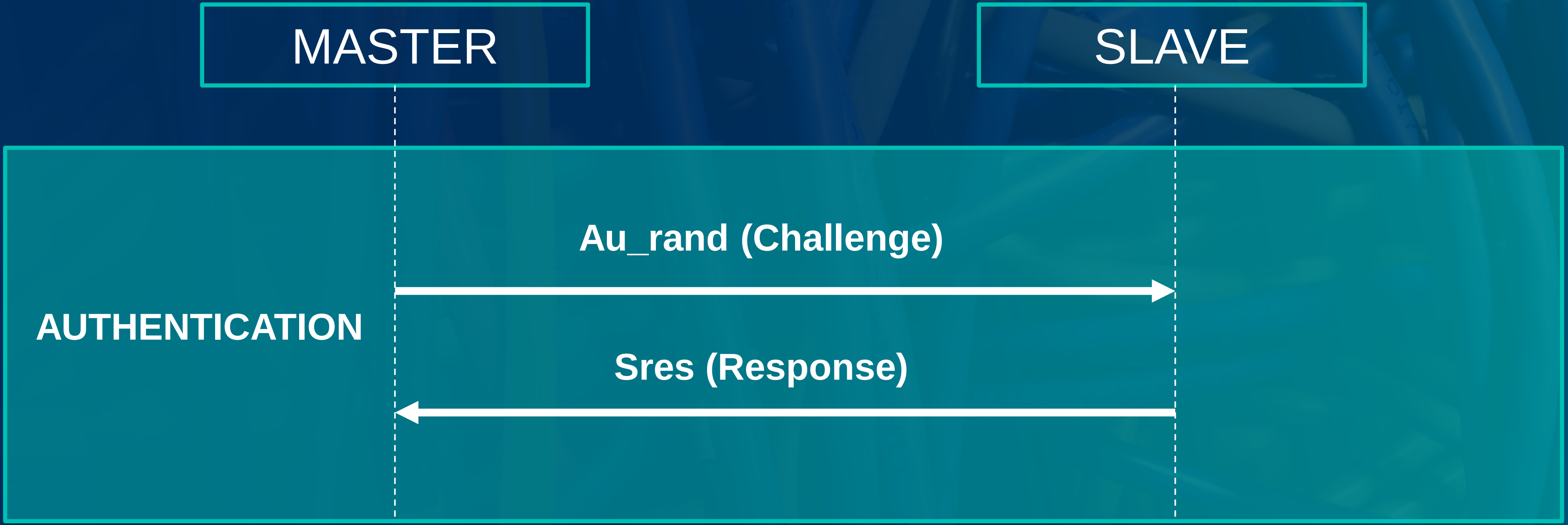
ALICE´S HEADPHONES

BIAS Attack



Authentication

LEGACY AUTHENTICATION

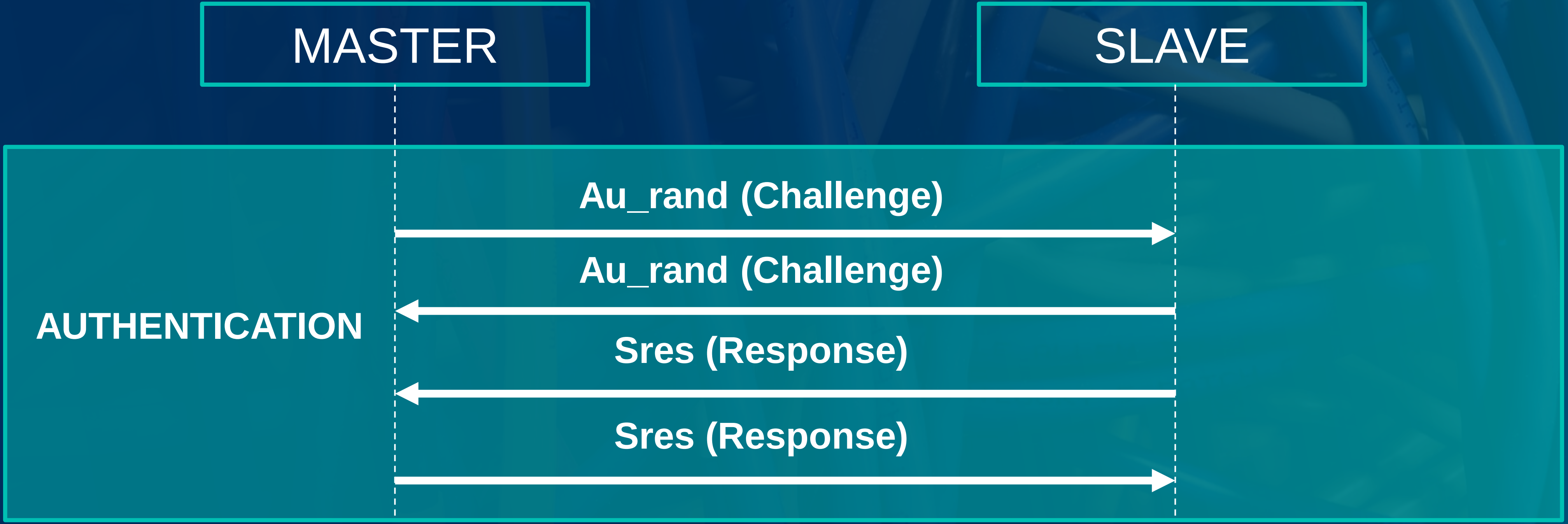


(Bluetooth Core, Vol 2, Parte C, Sección 4.2)

(Imagen de Gert Skriver)

Authentication

SECURE AUTHENTICATION

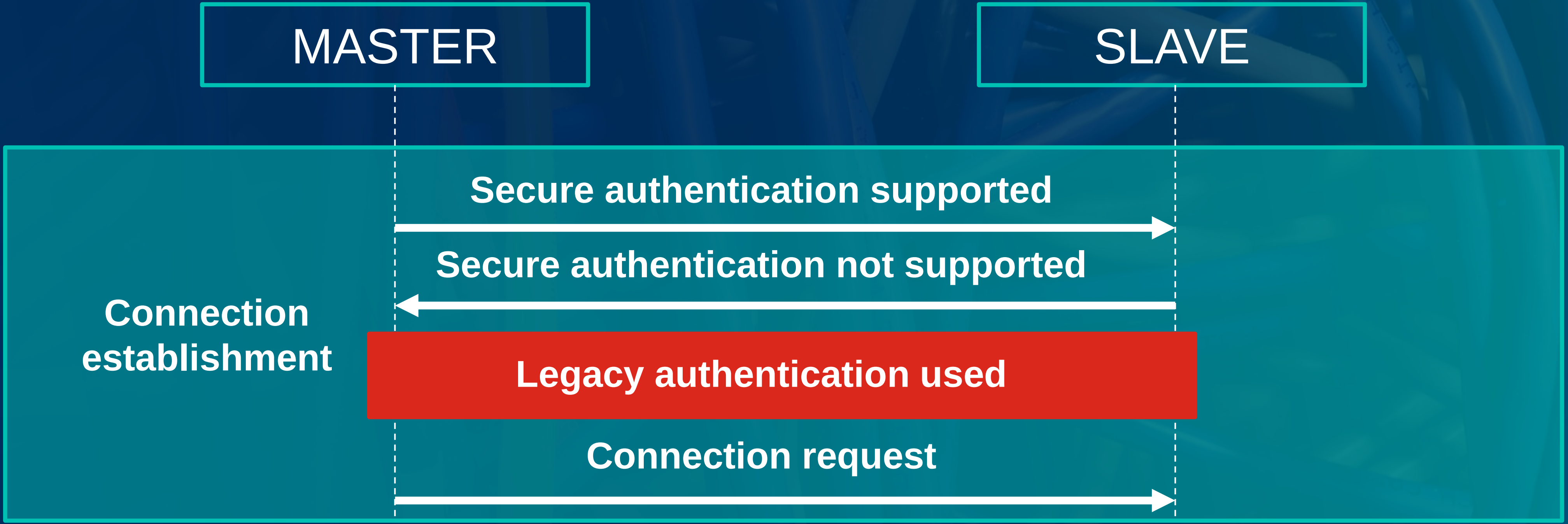


(Bluetooth Core, Vol 2, Parte C, Sección 4.2)

(Imagen de Gert Skriver)

BIAS – Authentication bypass

SECURE AUTHENTICATION DOWNGRADE



MASTER

SLAVE

Connection establishment

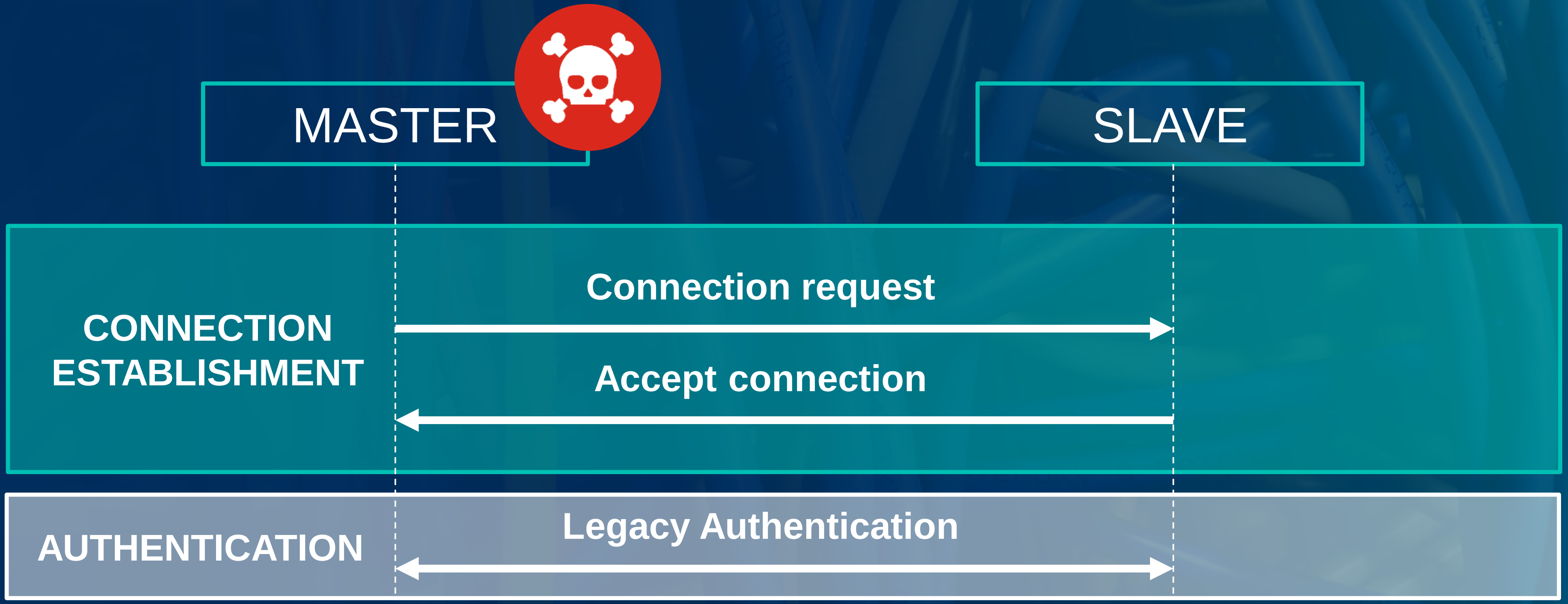
Secure authentication supported

Secure authentication not supported

Legacy authentication used

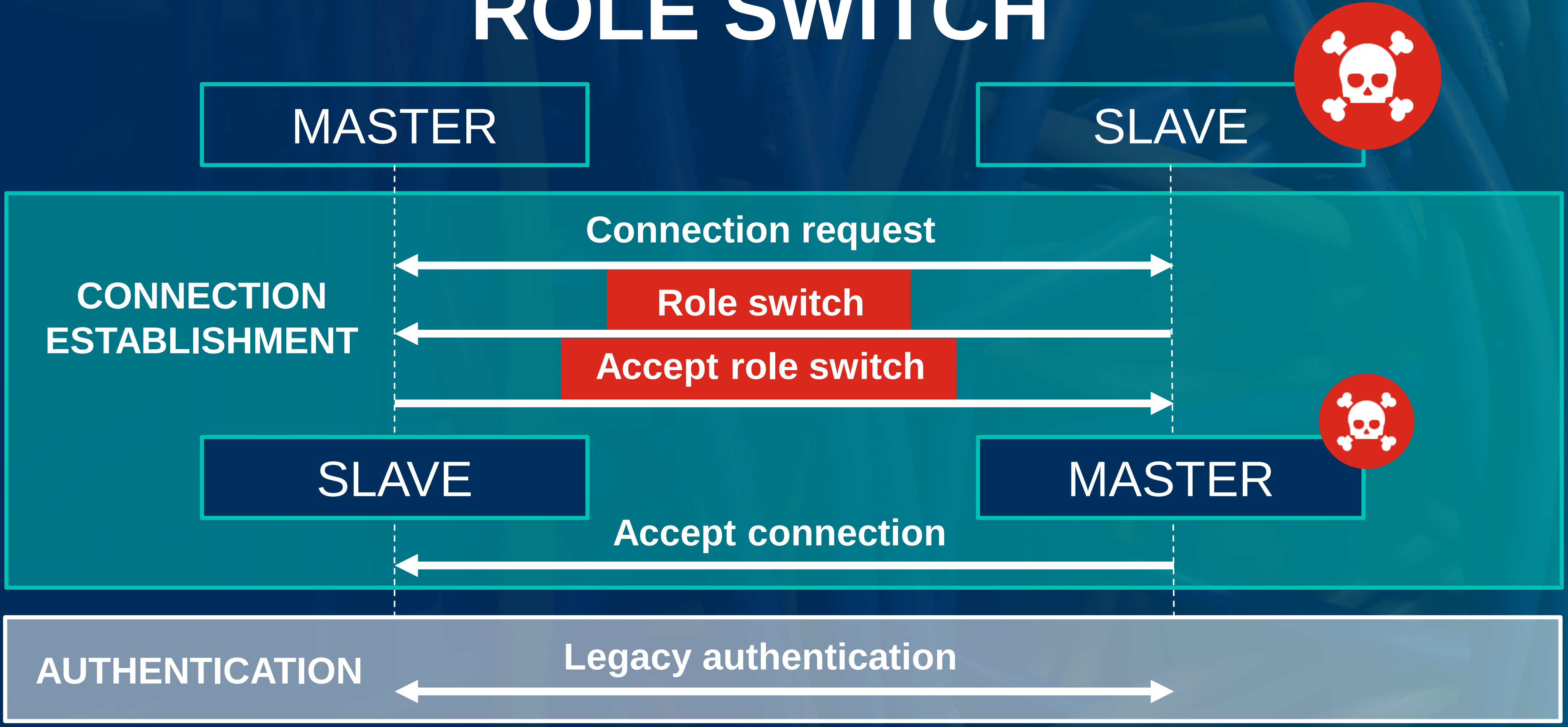
Connection request

BIAS – Authentication bypass



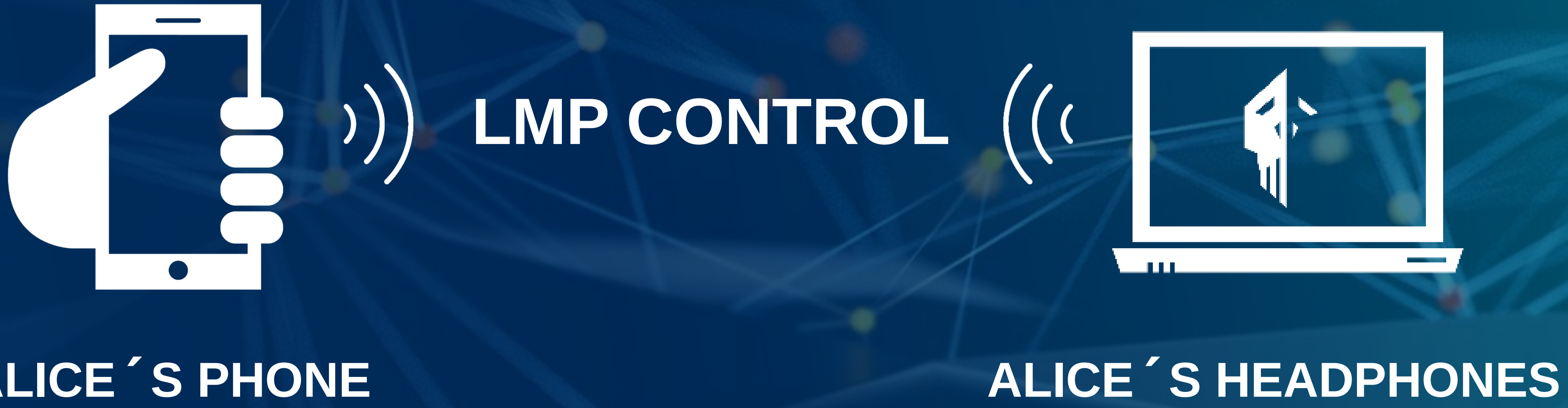
BIAS – Authentication bypass

ROLE SWITCH



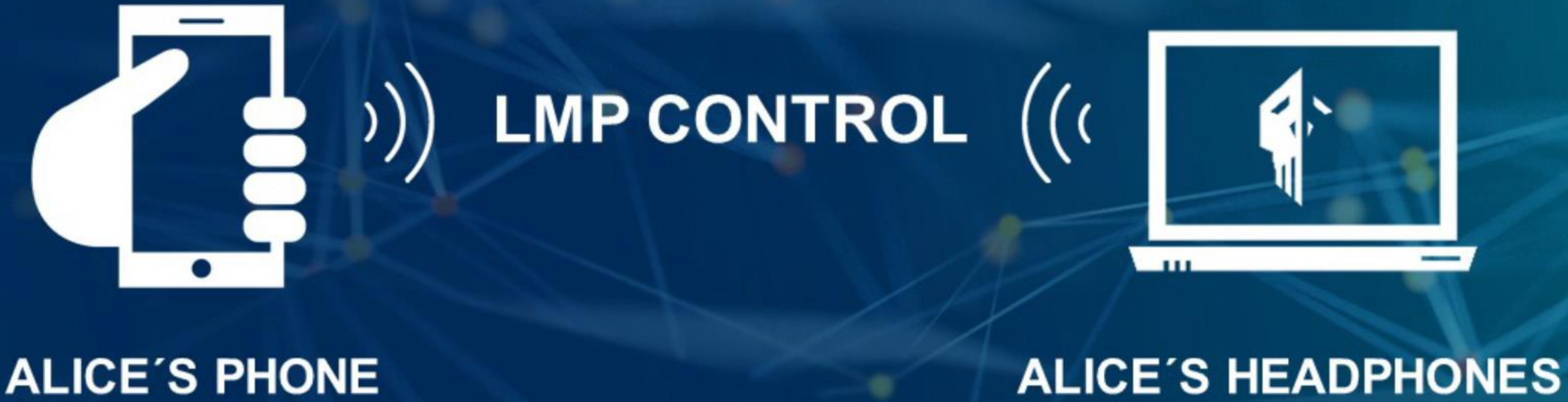
BIAS Attack

# The attack modifies the LMP message sequence



BIAS Attack

# The attack modifies the LMP message sequence



LMP CONTROL

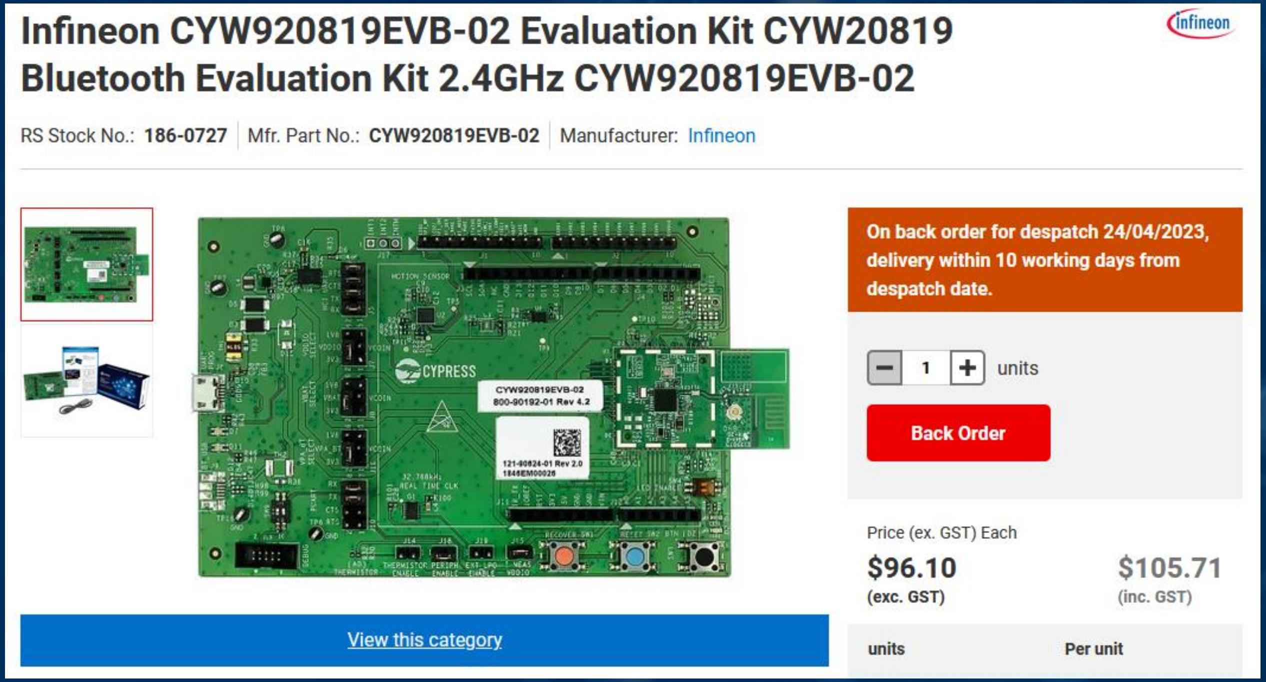
ALICE´S PHONE

ALICE´S HEADPHONES

THE FIRMWARE MUST BE MODIFIED!

BIAS – The PoC

# Getting the hardware!



Infineon CYW920819EVB-02 Evaluation Kit CYW20819 Bluetooth Evaluation Kit 2.4GHz CYW920819EVB-02

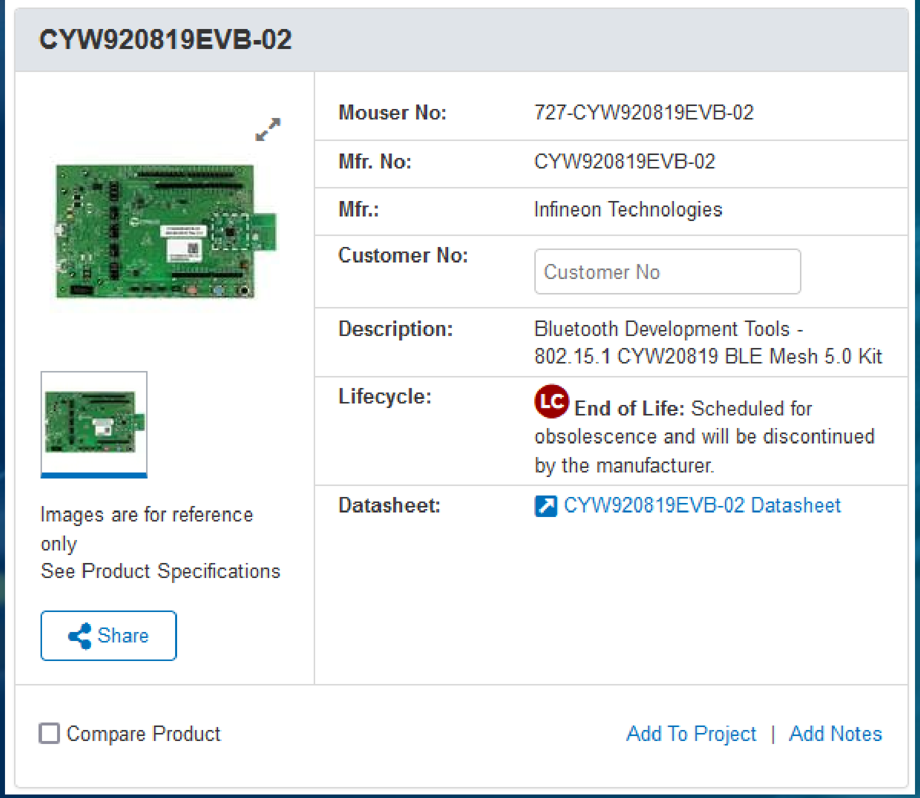
RS Stock No.: **186-0727** | Mfr. Part No.: **CYW920819EVB-02** | Manufacturer: Infineon

On back order for despatch 24/04/2023, delivery within 10 working days from despatch date.

Price (ex. GST) Each

$96.10 (exc. GST) $105.71 (inc. GST)

units	Per unit



CYW920819EVB-02

Mouser No:	727-CYW920819EVB-02
Mfr. No:	CYW920819EVB-02
Mfr.:	Infineon Technologies
Customer No:	Customer No
Description:	Bluetooth Development Tools - 802.15.1 CYW20819 BLE Mesh 5.0 Kit
Lifecycle:	LC **End of Life:** Scheduled for obsolescence and will be discontinued by the manufacturer.
Datasheet:	CYW920819EVB-02 Datasheet

Images are for reference only
See Product Specifications

BIAS – The PoC

# The impersonation requires some data about the device: A PROFILE

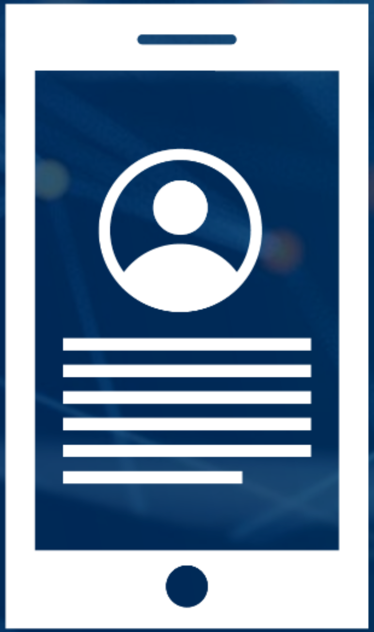
Name	**phone**
MAC addres	**00:11:22:33:44:55**
Device Class	**0x0c025a**
Version	**9**
Features	**0xfffe8ffed83f5b87**
IO Capability	**1**
Auth. Req.	**5**

BIAS – The PoC

# The PoC just provides profiles for some models

USEFUL TOOLS:

- bluetoothctl
- hciconfig
- wireshark



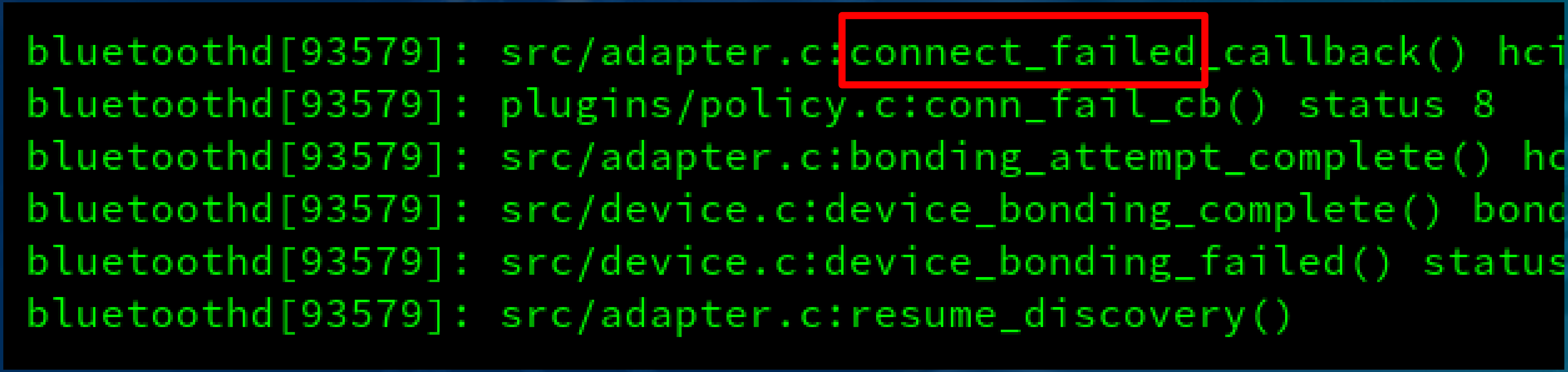
Name	**phone**
MAC addres	**00:11:22:33:44:55**
Device Class	**?**
Version	**?**
Features	**?**
IO Capability	**?**
Auth. Req.	**?**

BIAS – The PoC

# We finally run the attack and…

BIAS – The PoC

# We finally run the attack and…



```
bluetoothd[93579]: src/adapter.c:connect_failed_callback() hci
bluetoothd[93579]: plugins/policy.c:conn_fail_cb() status 8
bluetoothd[93579]: src/adapter.c:bonding_attempt_complete() hc
bluetoothd[93579]: src/device.c:device_bonding_complete() bonc
bluetoothd[93579]: src/device.c:device_bonding_failed() status
bluetoothd[93579]: src/adapter.c:resume_discovery()
```

BIAS – Authentication bypass

# Next try

BIAS – Authentication bypass

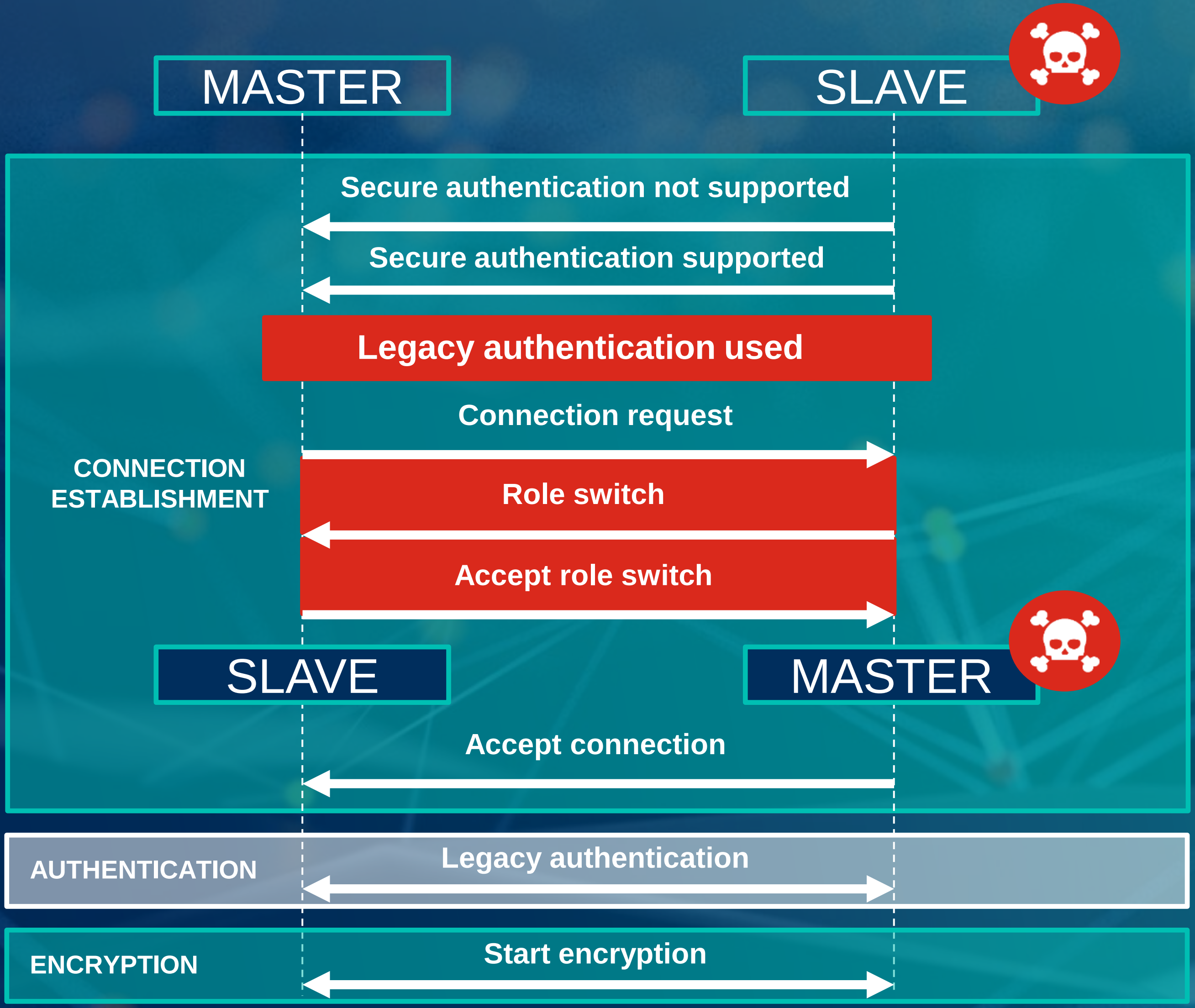
# Next try

- Capture the info from a device ☑

BIAS – Authentication bypass

# Next try

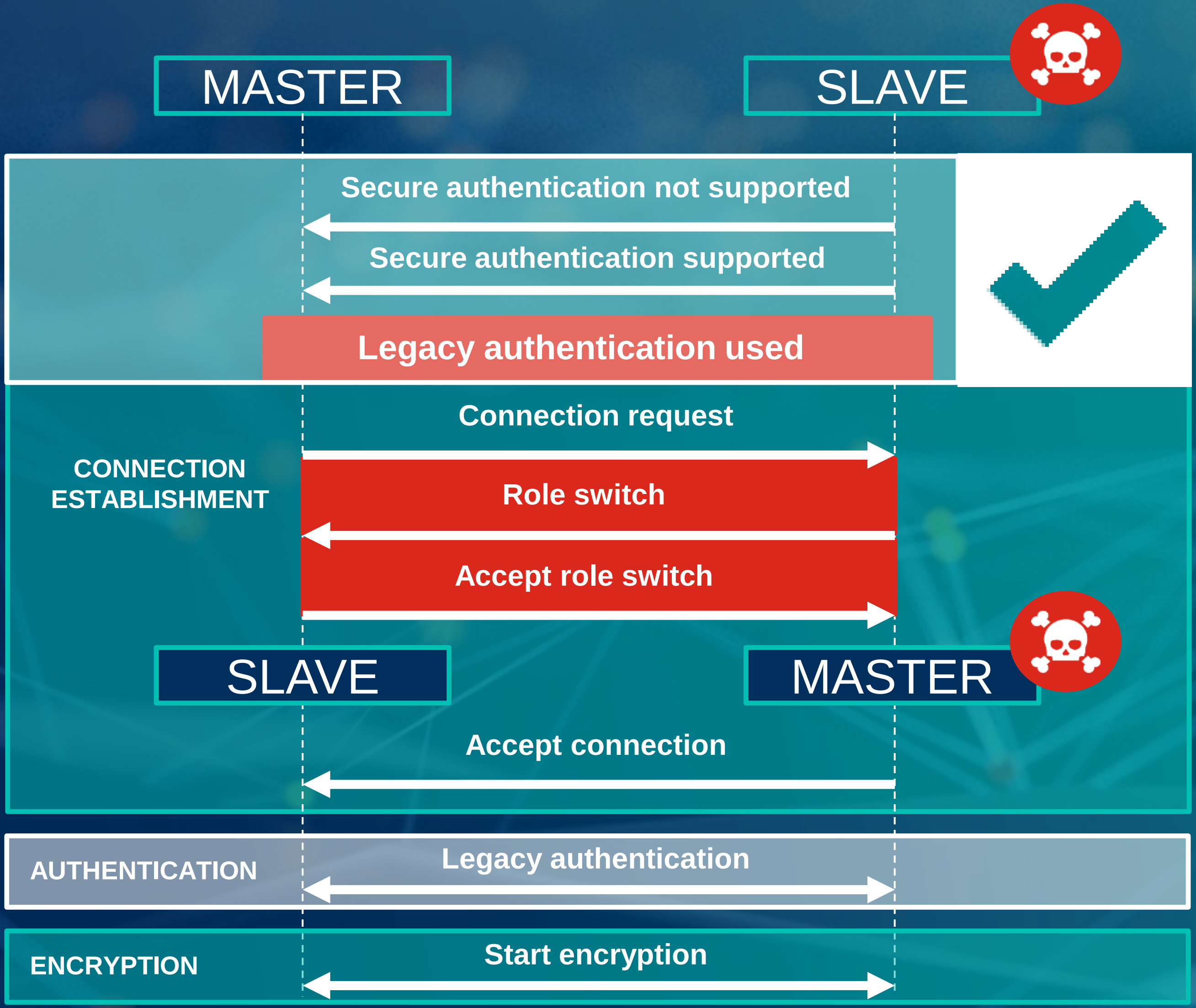
- Capture the info from a device ☑
- Impersonate that device ☑



BIAS – Authentication bypass

# Next try

- › Capture the info from a device ☑
- › Impersonate that device ☑
- › Downgrade authentication ☑



MASTER

SLAVE

Secure authentication not supported

Secure authentication supported

Legacy authentication used

CONNECTION ESTABLISHMENT

Connection request

Role switch

Accept role switch

SLAVE

MASTER

Accept connection

AUTHENTICATION

Legacy authentication

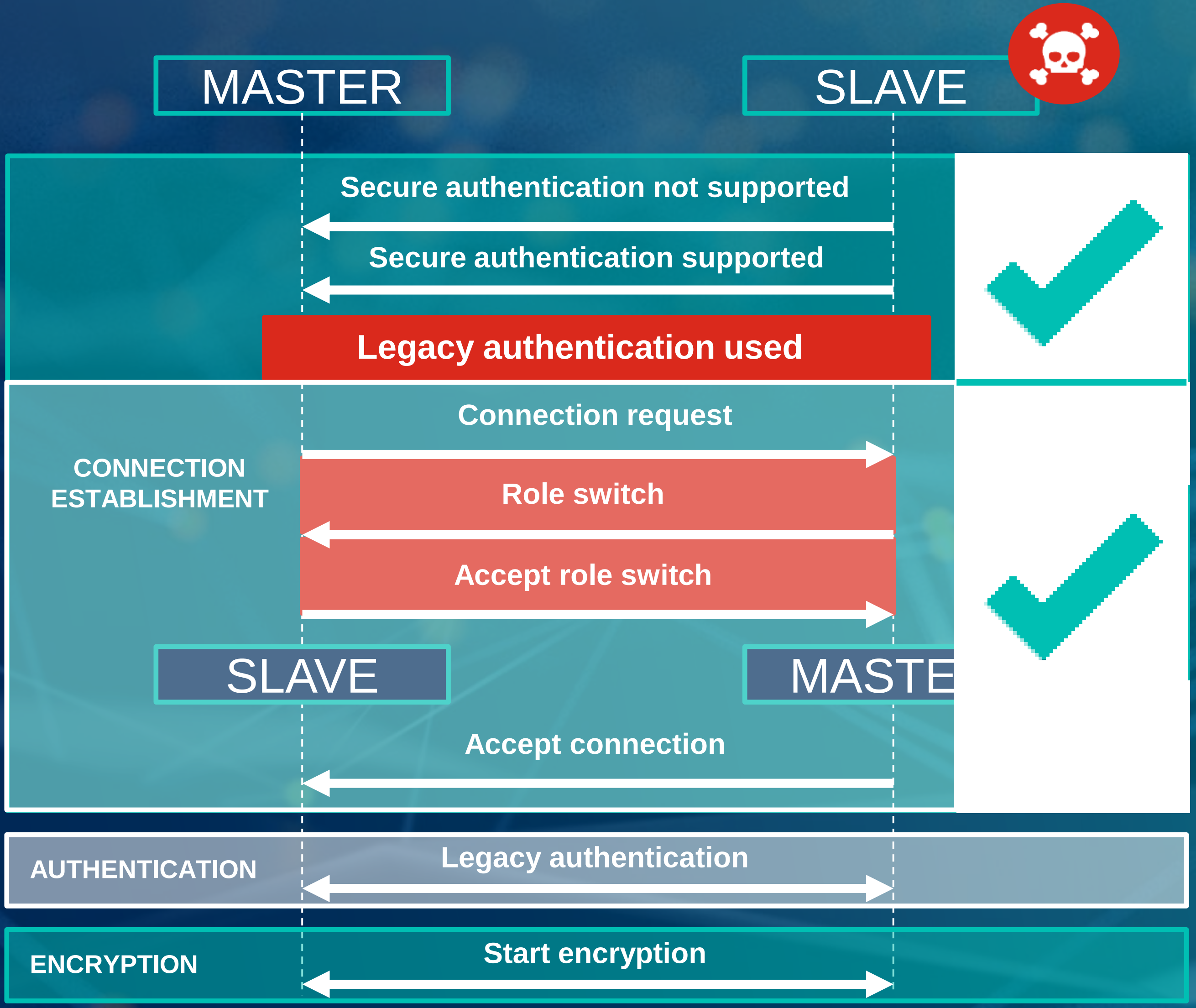
ENCRYPTION

Start encryption

BIAS – Authentication bypass

# Next try

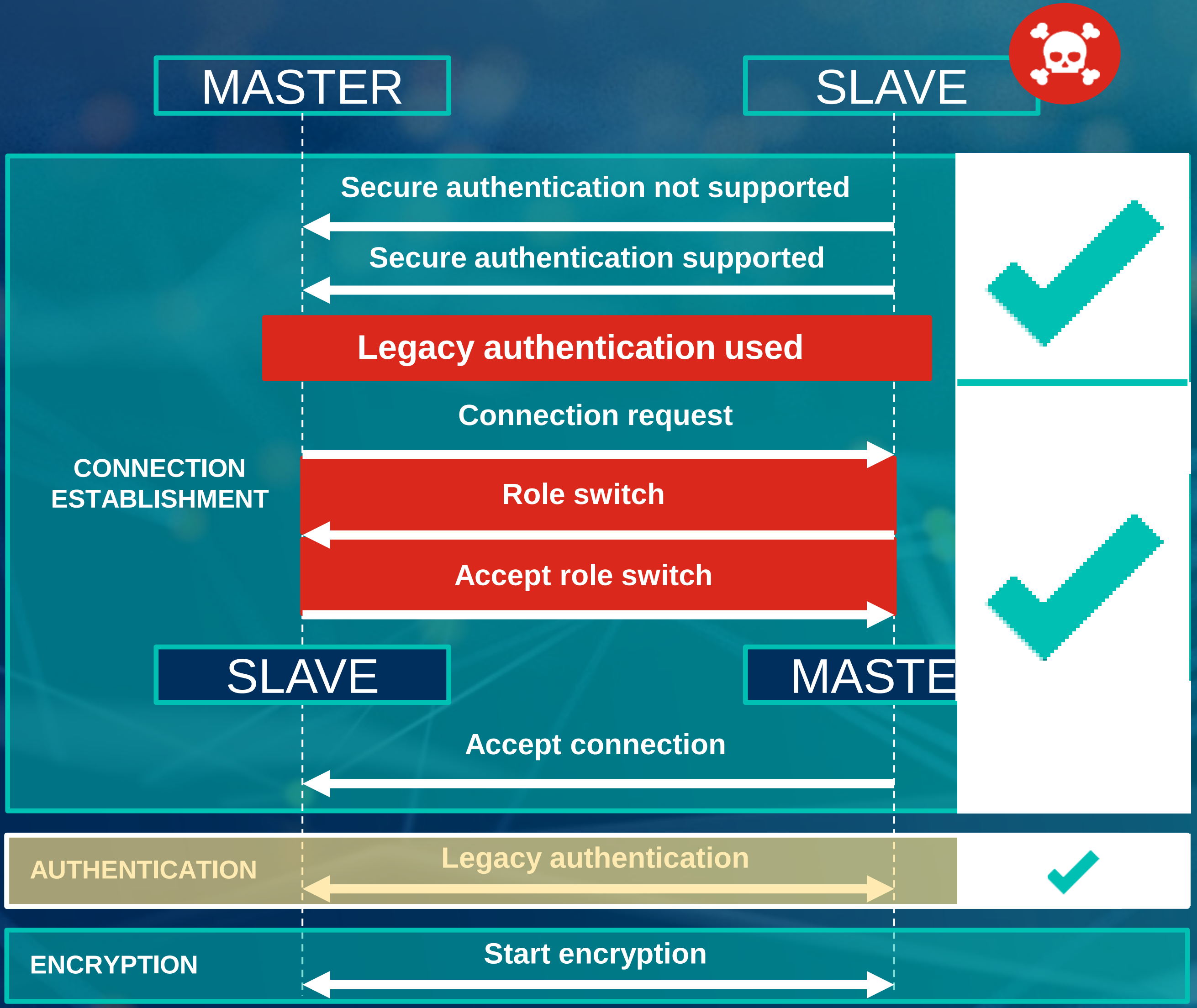
- Capture the info from a device ☑
- Impersonate that device ☑
- Downgrade authentication ☑
- Role switch ☑



BIAS – Authentication bypass

# Next try

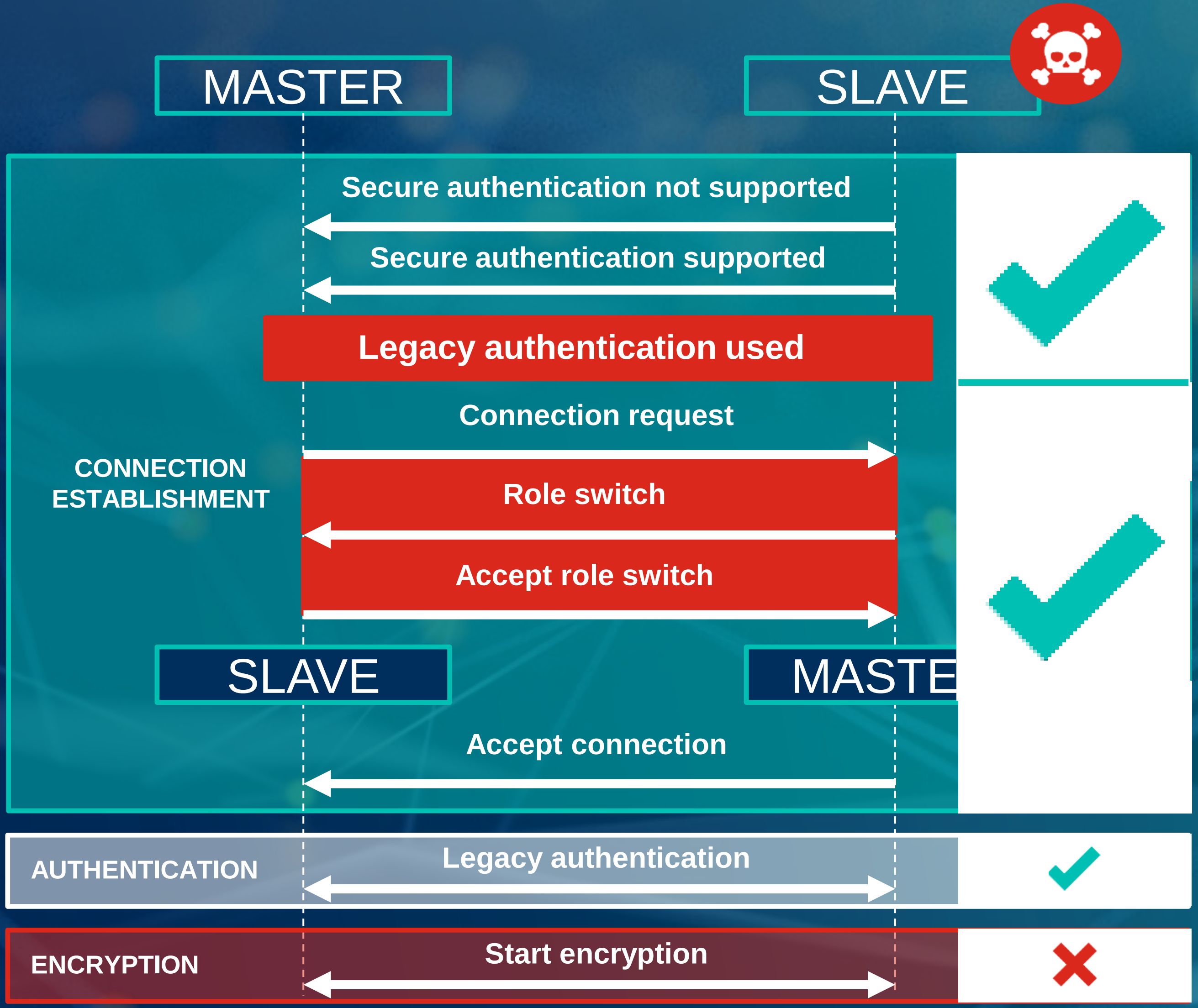
- Capture the info from a device ☑
- Impersonate that device ☑
- Downgrade authentication ☑
- Role switch ☑
- Bypass the authentication!!!! ☑



BIAS – Authentication bypass

# Next try

- Capture the info from a device ☑
- Impersonate that device ☑
- Downgrade authentication ☑
- Role switch ☑
- Bypass the authentication!!!! ☑
- FAIL TO ENCRYPT… :(☒



TARLOGIC

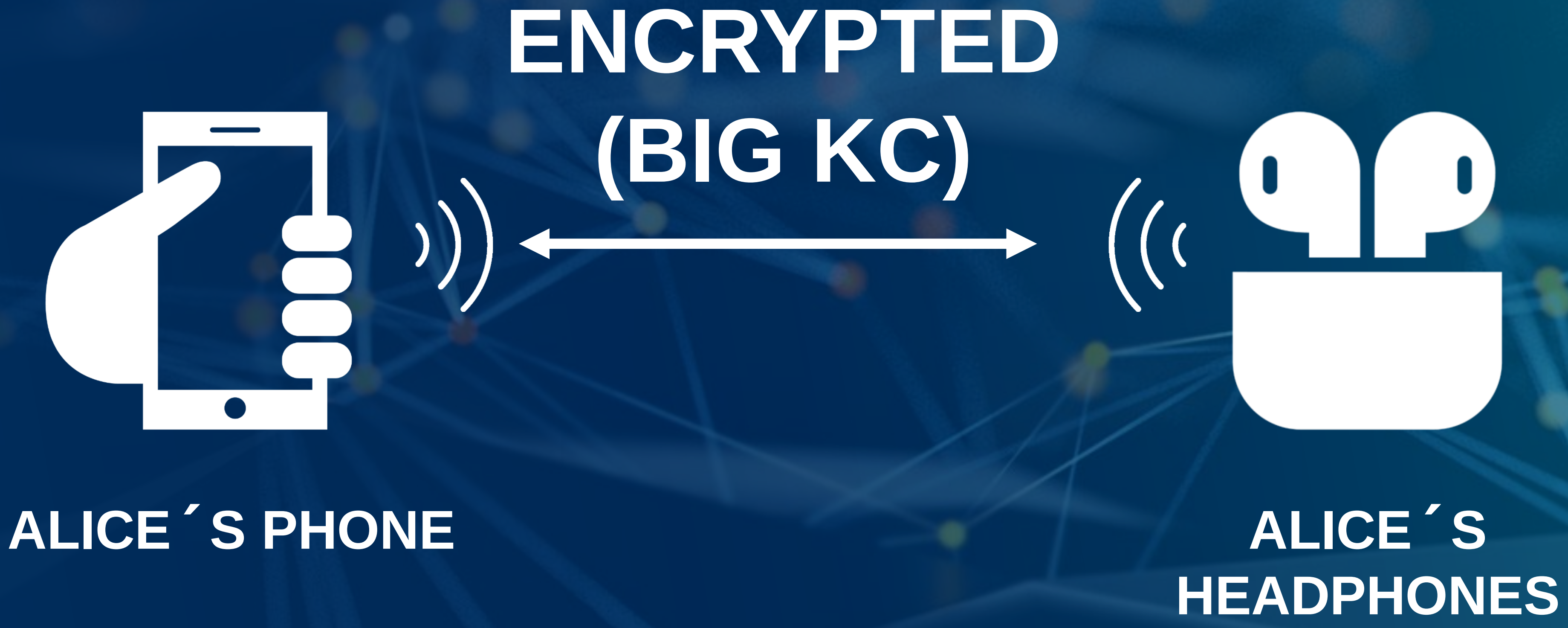
CYBERSECURITY EXPERTS

www.tarlogic.com

29.11.23

KNOB ATTACK

KNOB Attacks

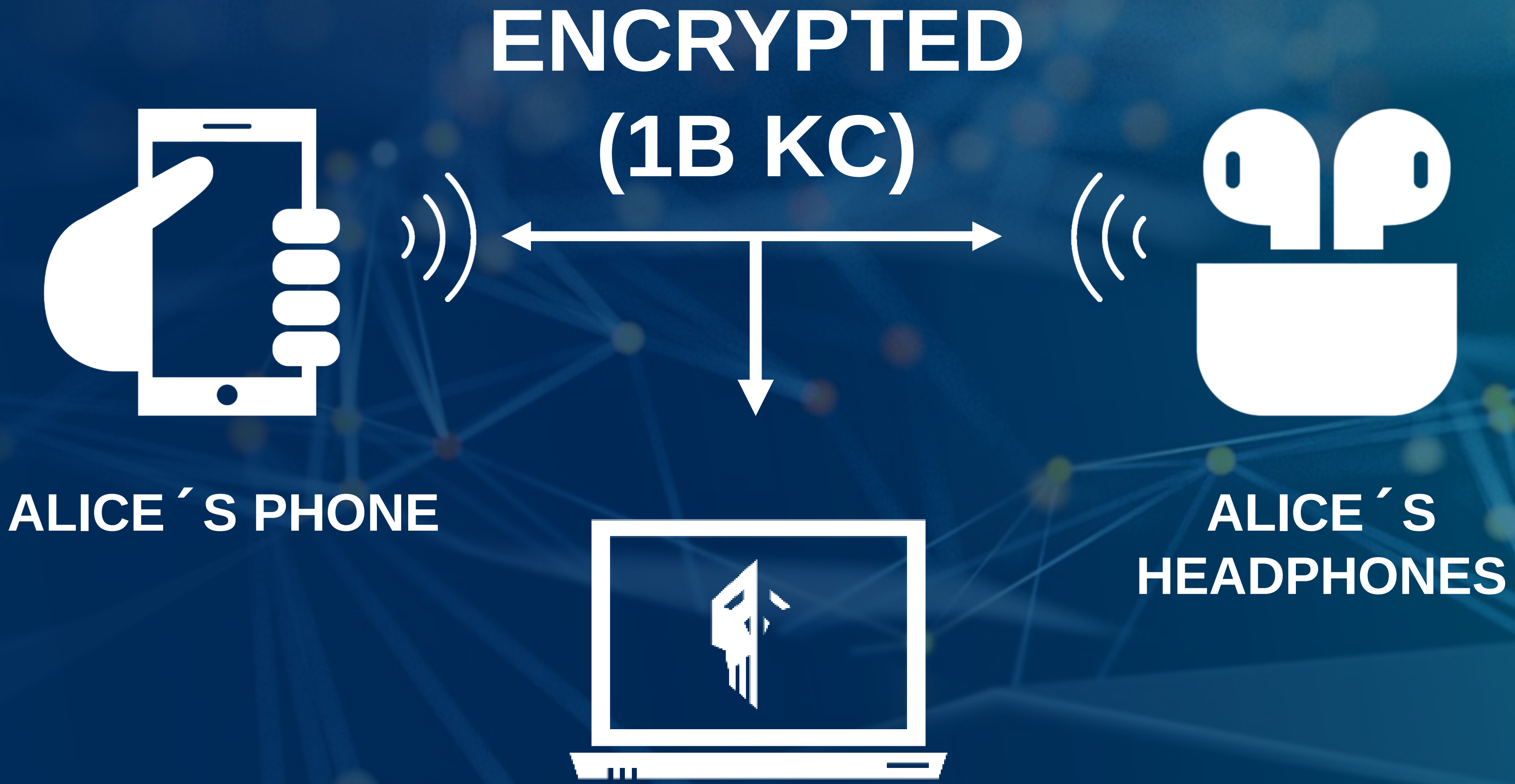


ENCRYPTED (BIG KC)

ALICE´S PHONE

ALICE´S HEADPHONES

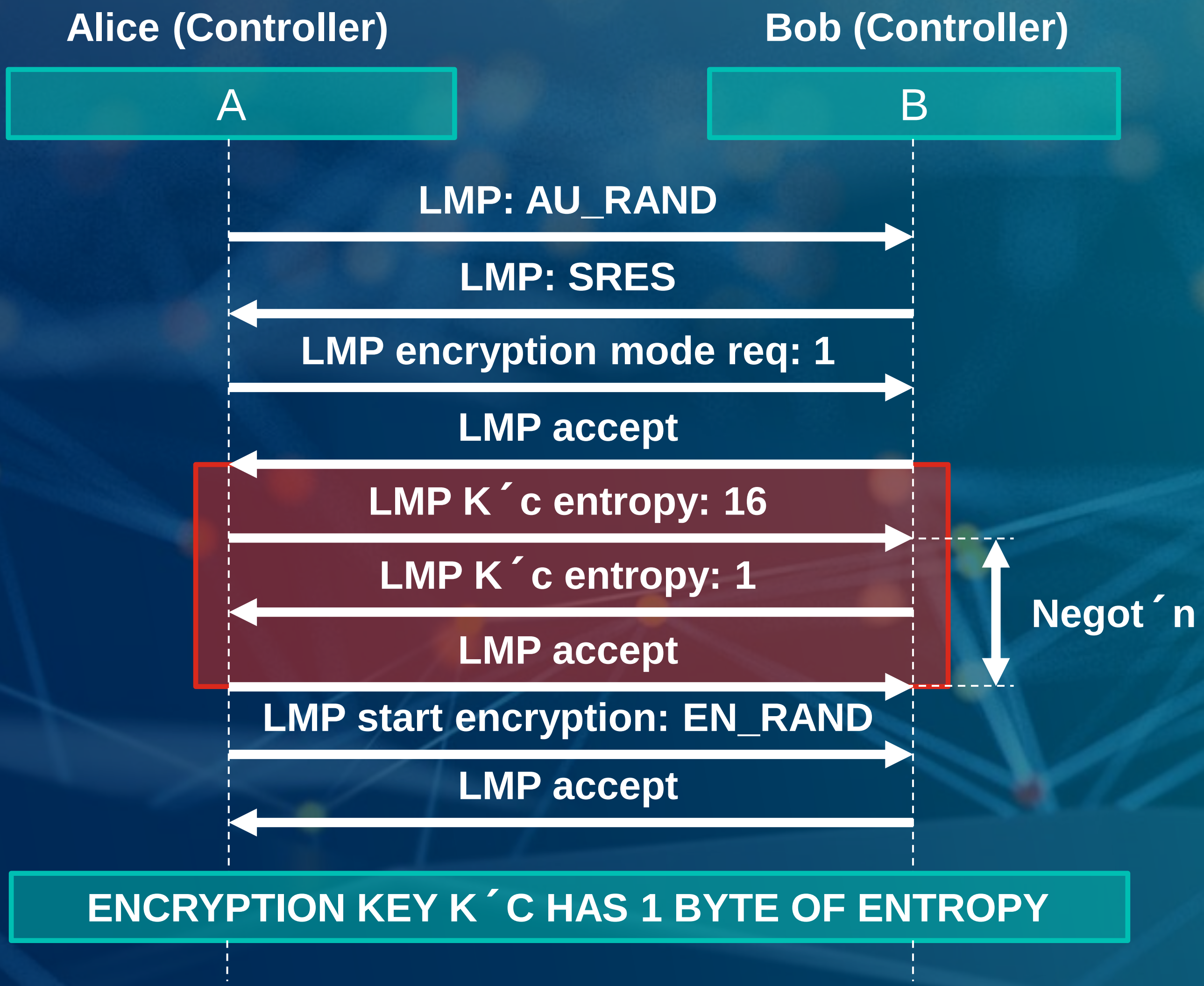
KNOB Attacks



Knob

# The Attack…

- Uses LMP key size negotiation
- Allows bruteforcing the low entropy key



Alice (Controller)

Bob (Controller)

A

B

LMP: AU_RAND

LMP: SRES

LMP encryption mode req: 1

LMP accept

LMP K´c entropy: 16

LMP K´c entropy: 1

LMP accept

Negot´n

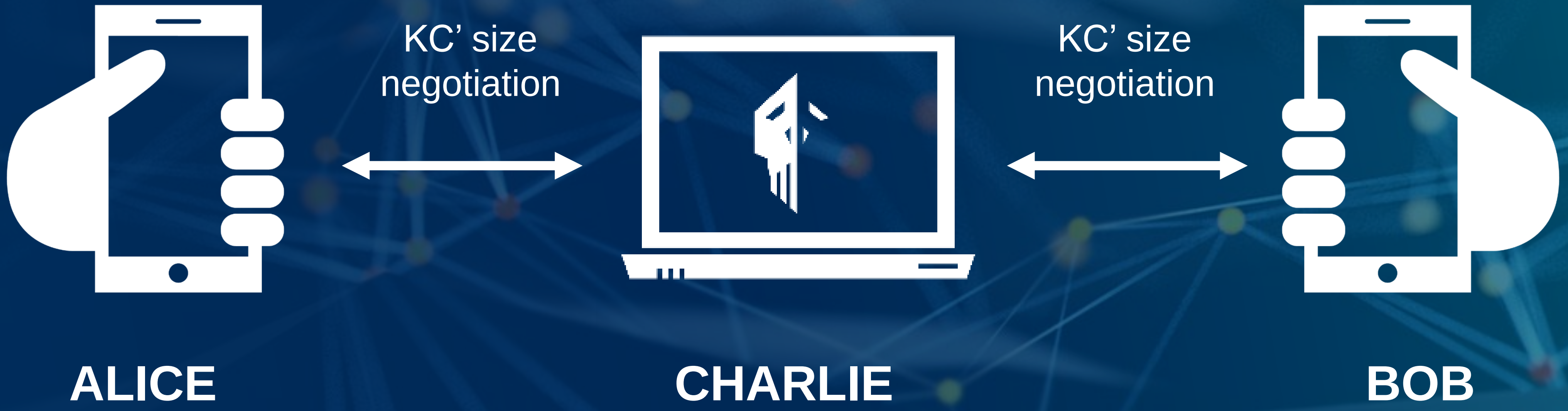
LMP start encryption: EN_RAND

LMP accept

ENCRYPTION KEY K´C HAS 1 BYTE OF ENTROPY

Knob

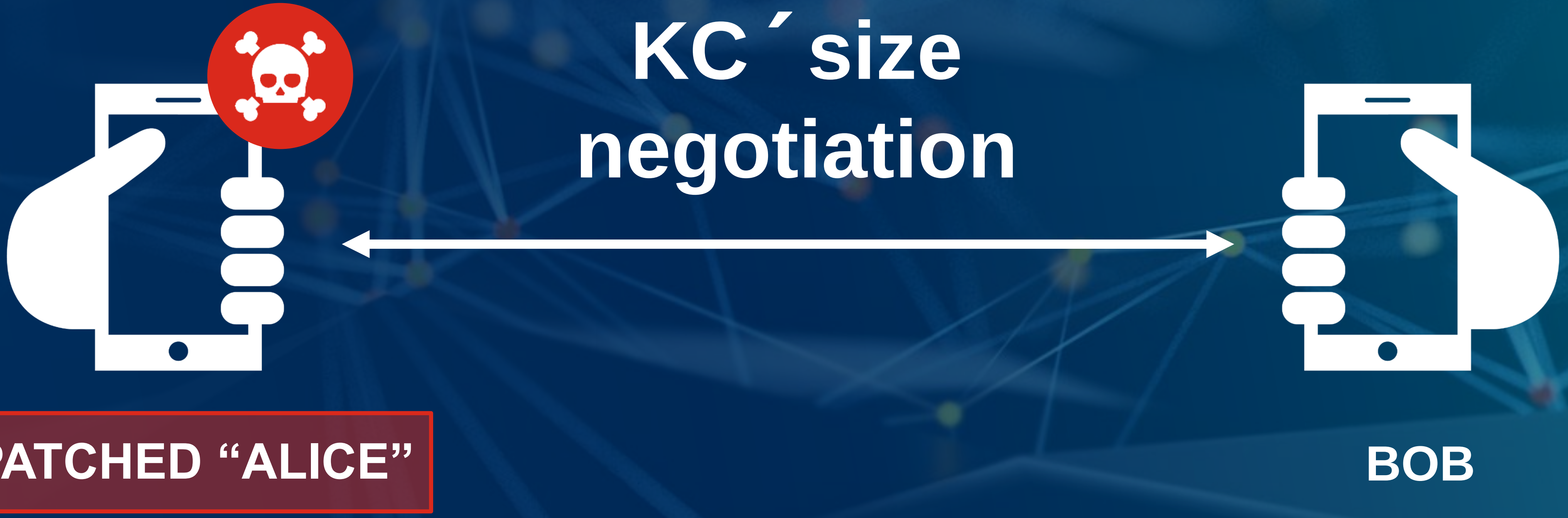
# MitM needed



BUT...

Knob

# Actual MitM



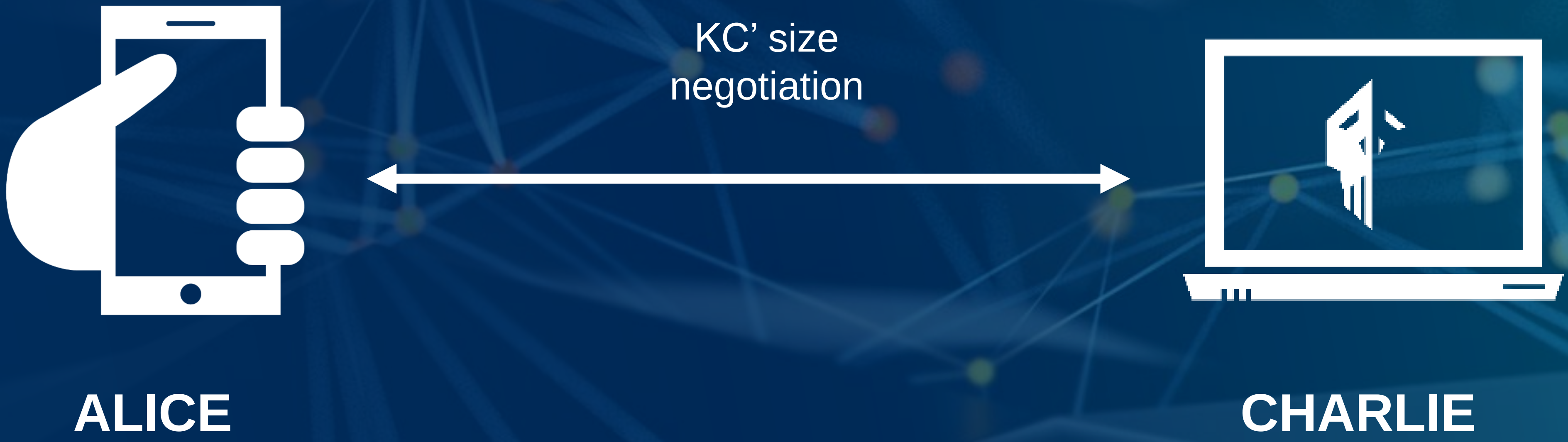
KC´size negotiation

PATCHED “ALICE”

BOB

Knob

# MitM needed



TARLOGIC
CYBERSECURITY EXPERTS

CONCLUSIONS

Conclusions

# Inmense gap between theoretical and practical attacks…

# Papers are really good for theory but often lack implementation details…

# PoCs are useful but designed for specific cases that can be difficult to replicate…

# Bluetooth doc is extremely difficult to read…

# Bluetooth PoCs are… #!&%!”

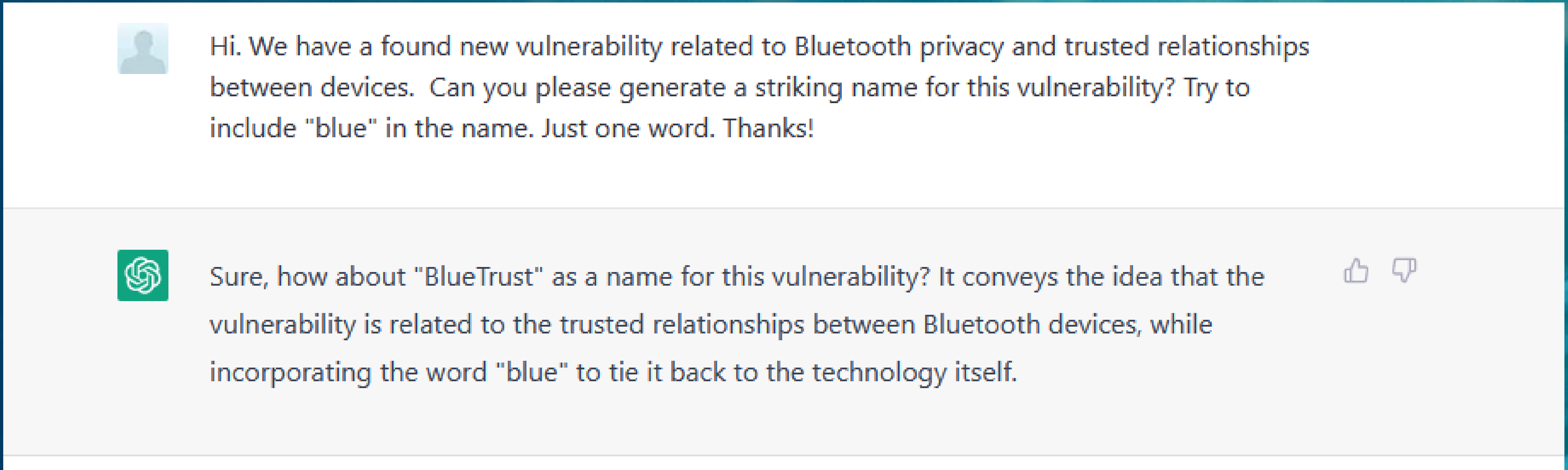
# We have gained a lot of knowledge…

TARLOGIC
CYBERSECURITY EXPERTS

www.tarlogic.com
29.11.23

PLOT TWIST!

REPURPOSING BIAS WITH BLUETRUST



Hi. We have a found new vulnerability related to Bluetooth privacy and trusted relationships between devices. Can you please generate a striking name for this vulnerability? Try to include "blue" in the name. Just one word. Thanks!

Sure, how about "BlueTrust" as a name for this vulnerability? It conveys the idea that the vulnerability is related to the trusted relationships between Bluetooth devices, while incorporating the word "blue" to tie it back to the technology itself.

PATENT PENDING

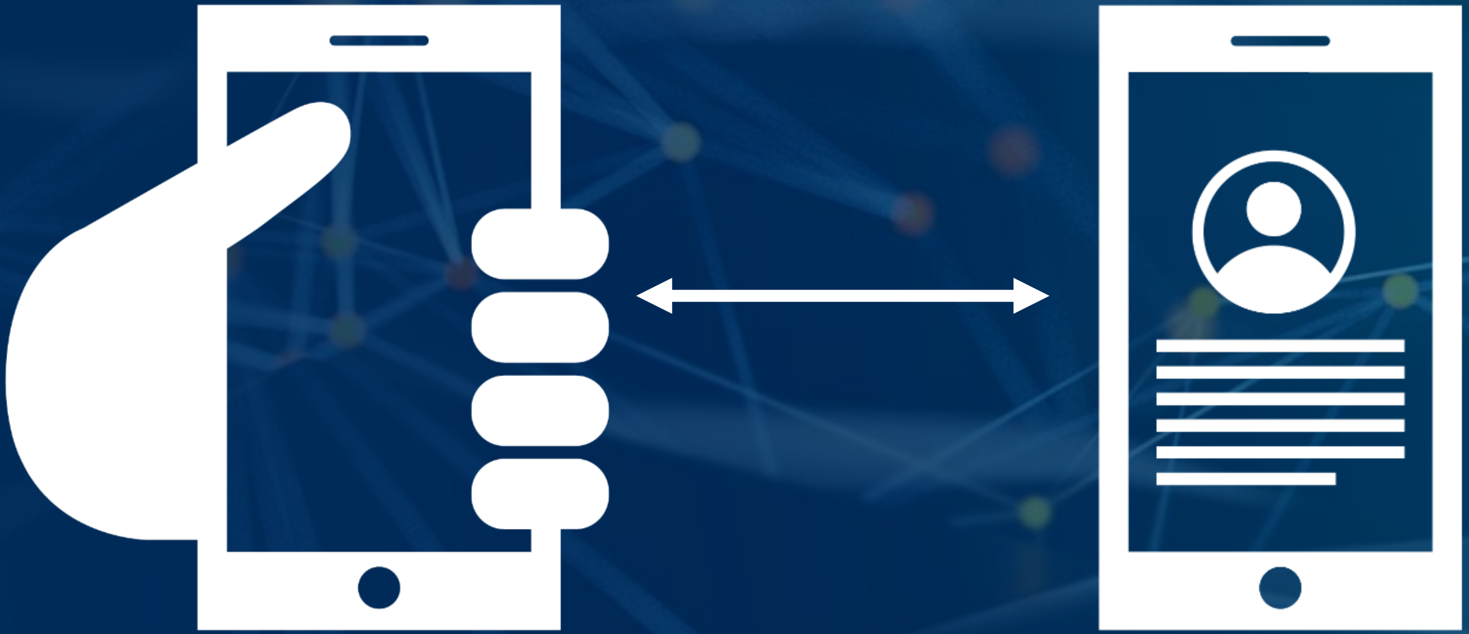
BlueTrust

# Scanning

DISCOVERABLE DEVICES

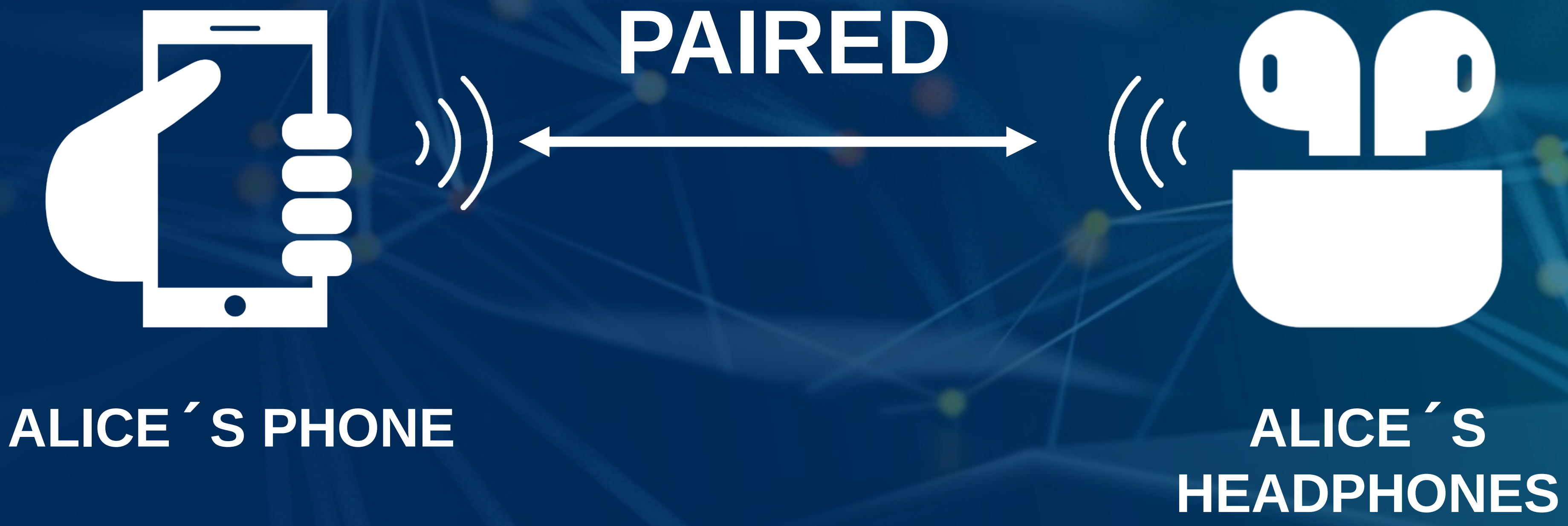
PATENT PENDING

# Profile creation

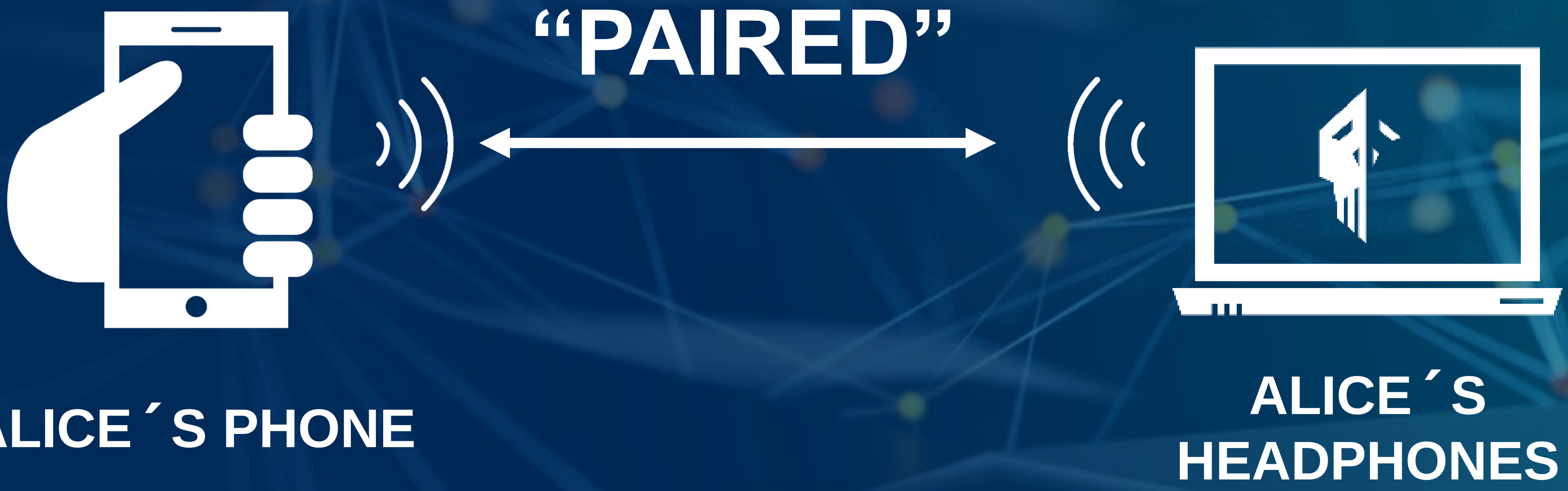


PATENT PENDING

# Device impersonation



# Device impersonation



“PAIRED”

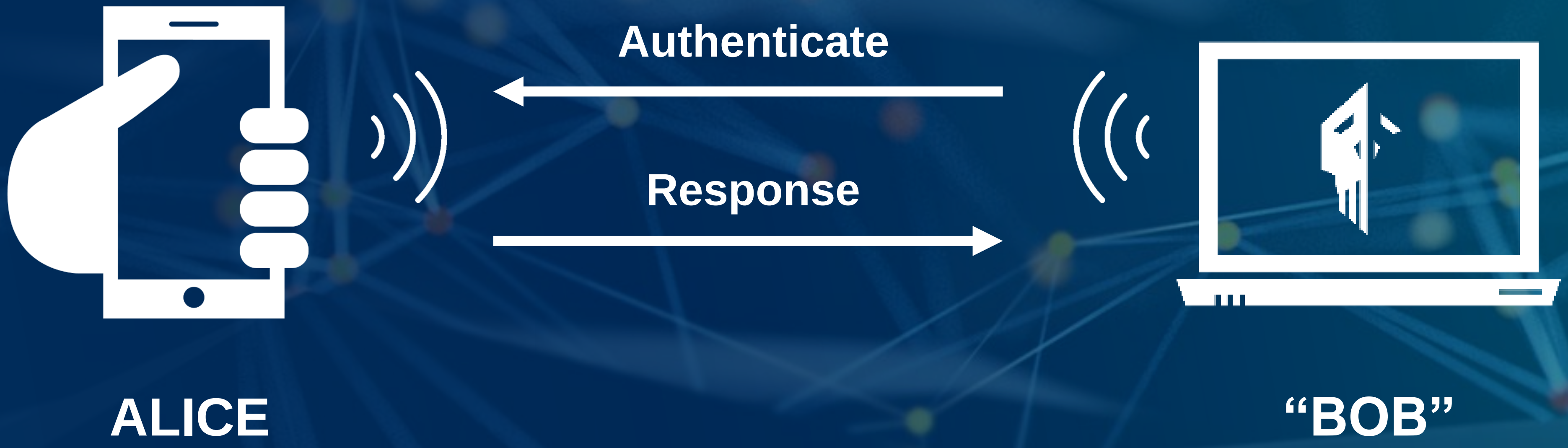
ALICE´S PHONE

ALICE´S HEADPHONES

BlueTrust

# Pairing detection

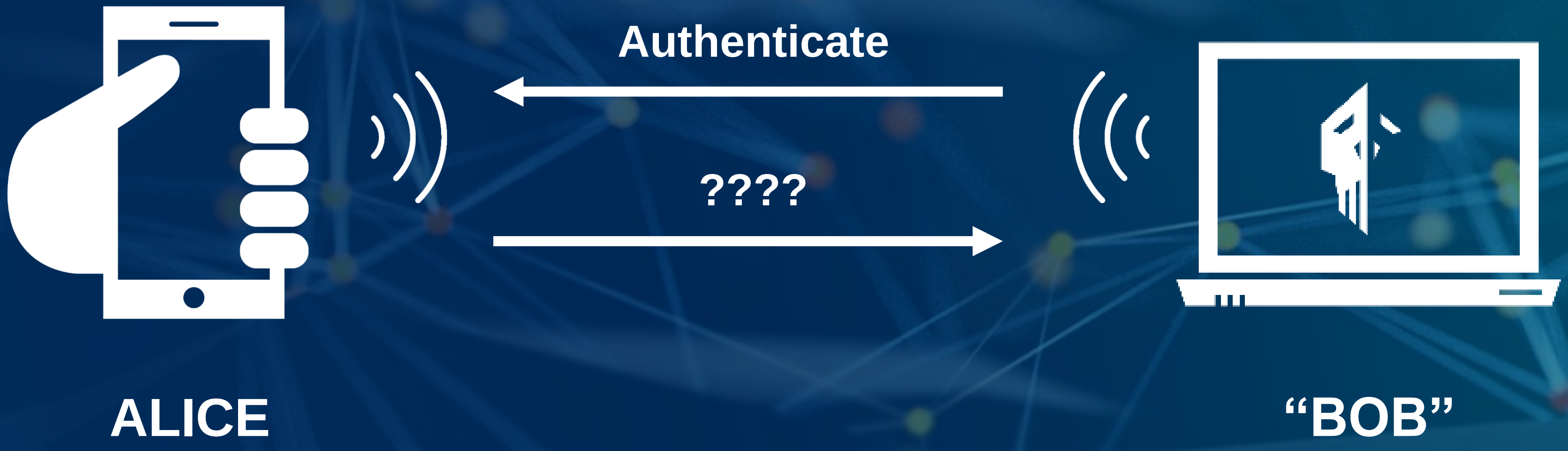
SUCCESS!



PATENT PENDING

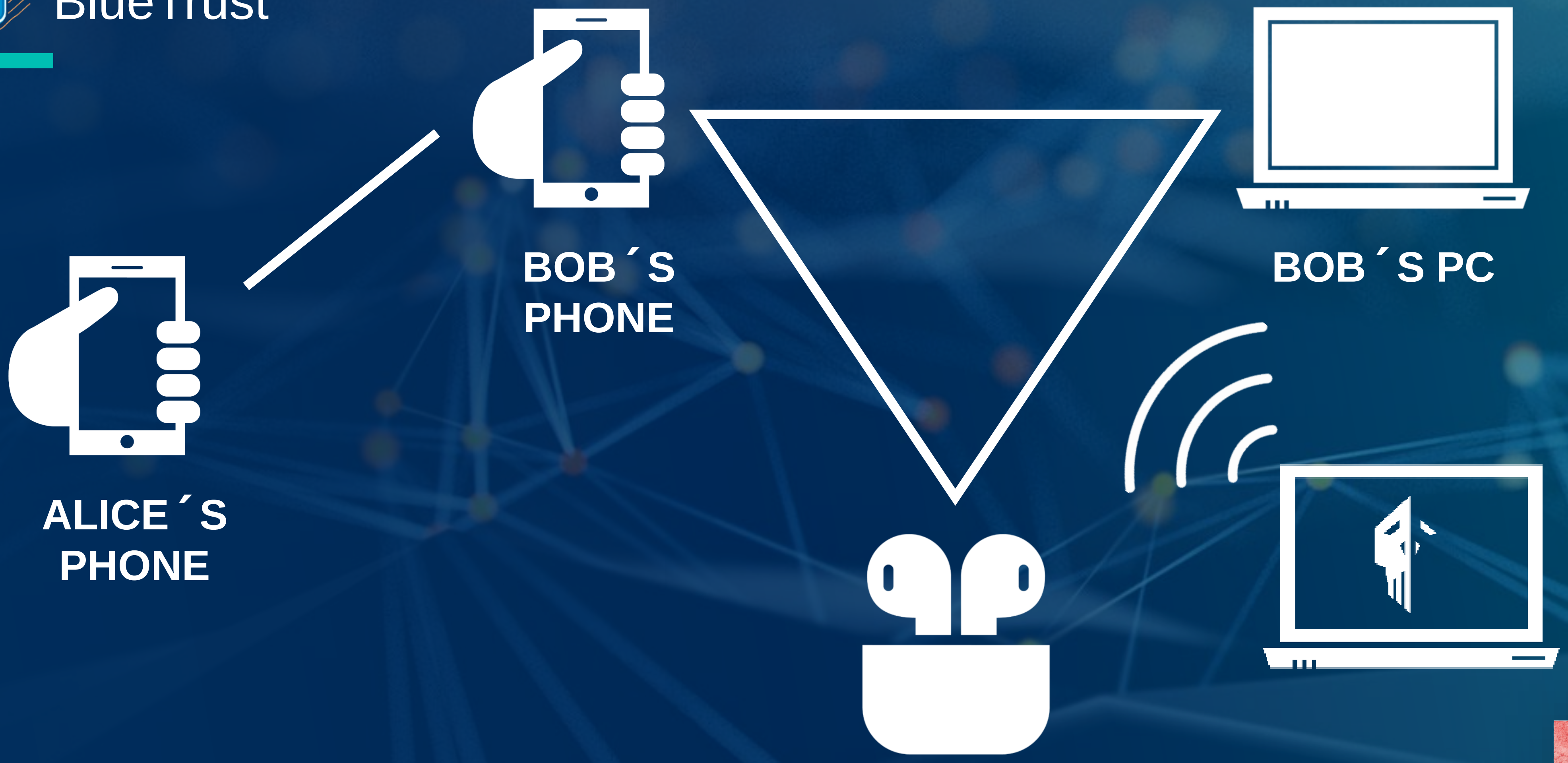
# Pairing detection

FAILURE



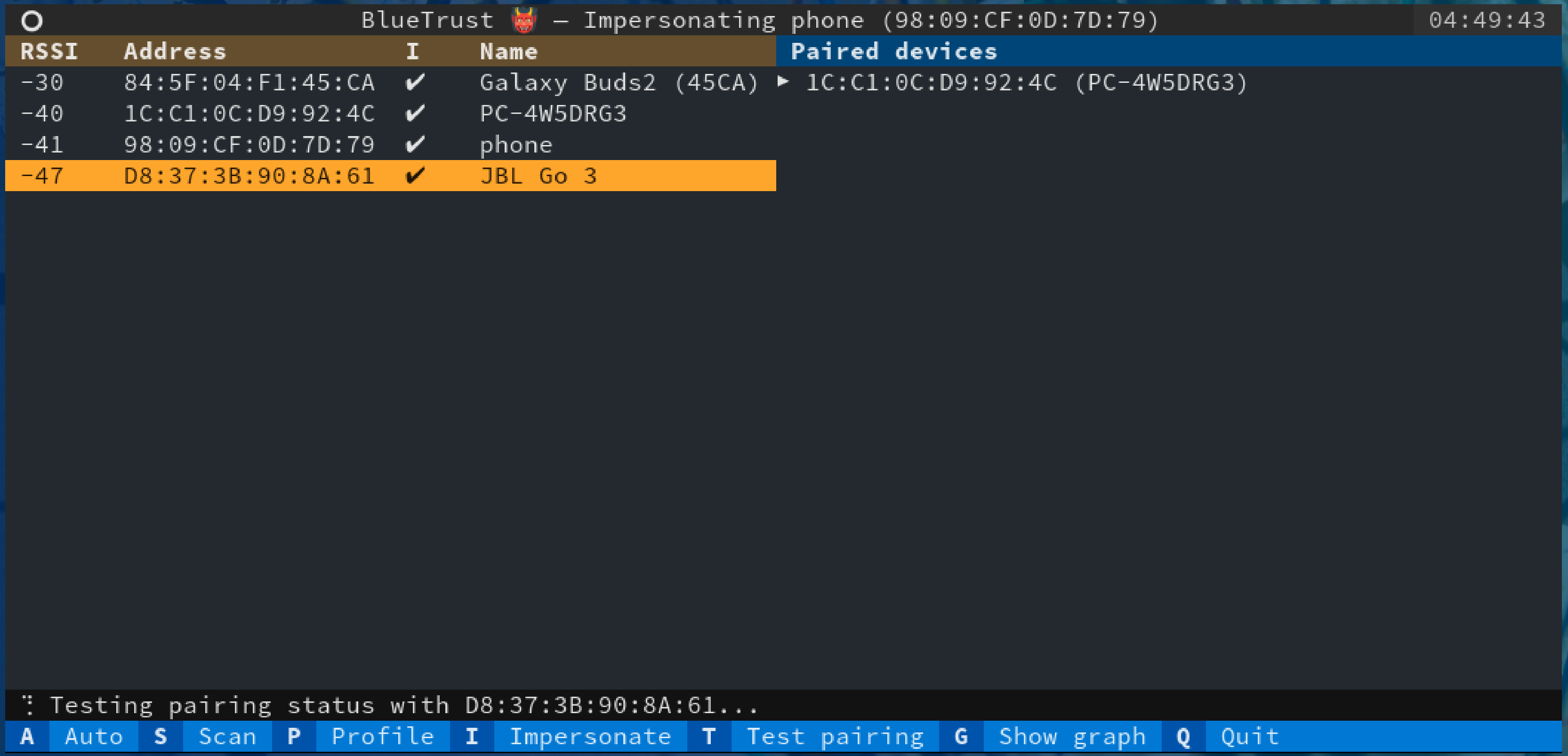
PATENT PENDING

BlueTrust



PATENT PENDING

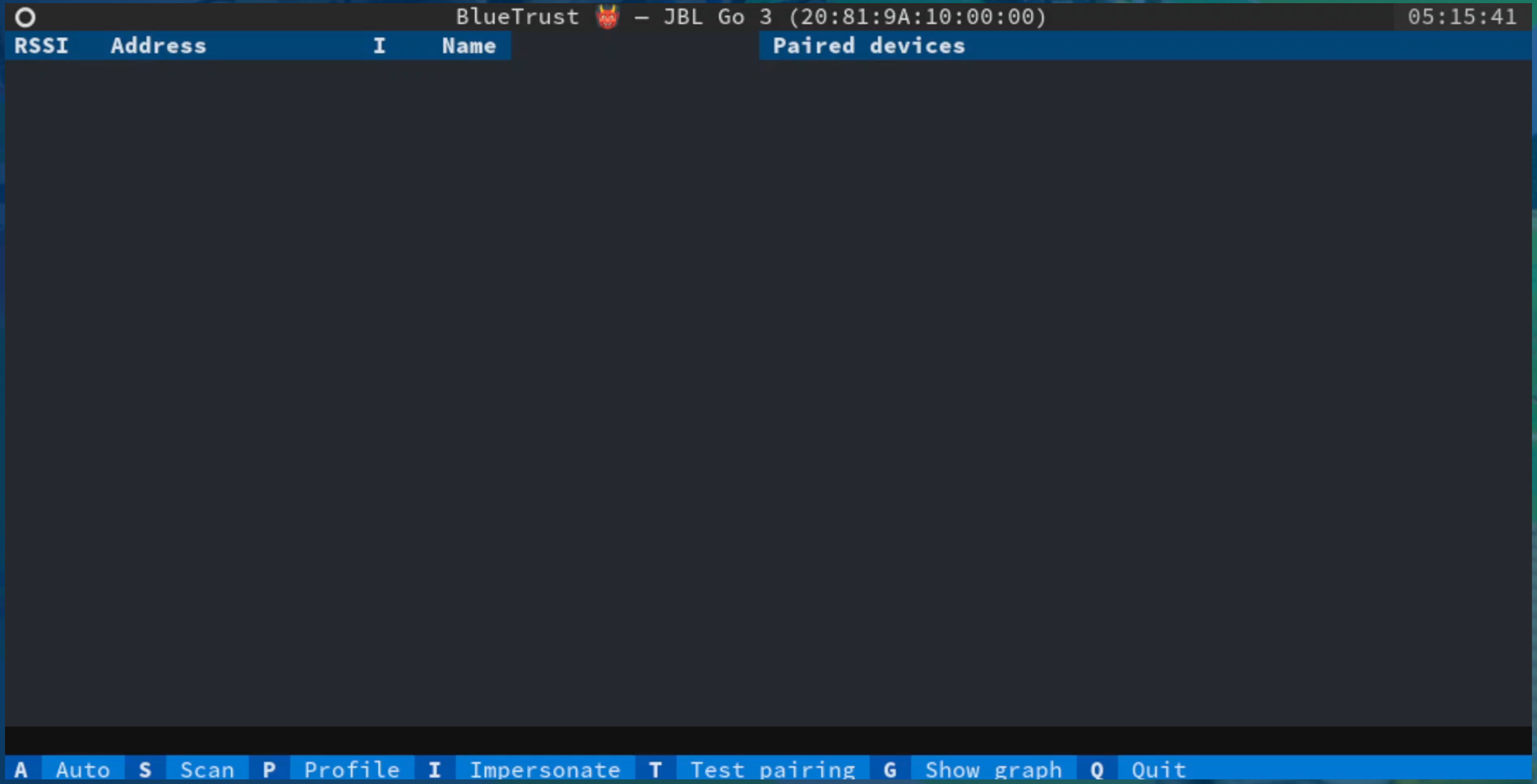
THE PoC



```
○                     BlueTrust 👹 — Impersonating phone (98:09:CF:0D:7D:79)                04:49:43
RSSI   Address             I    Name                   Paired devices
-30    84:5F:04:F1:45:CA   ✔    Galaxy Buds2 (45CA)   ▸ 1C:C1:0C:D9:92:4C (PC-4W5DRG3)
-40    1C:C1:0C:D9:92:4C   ✔    PC-4W5DRG3
-41    98:09:CF:0D:7D:79   ✔    phone
-47    D8:37:3B:90:8A:61   ✔    JBL Go 3

⠅ Testing pairing status with D8:37:3B:90:8A:61...
 A  Auto  S  Scan  P  Profile  I  Impersonate  T  Test pairing  G  Show graph  Q  Quit
```

PATENT PENDING

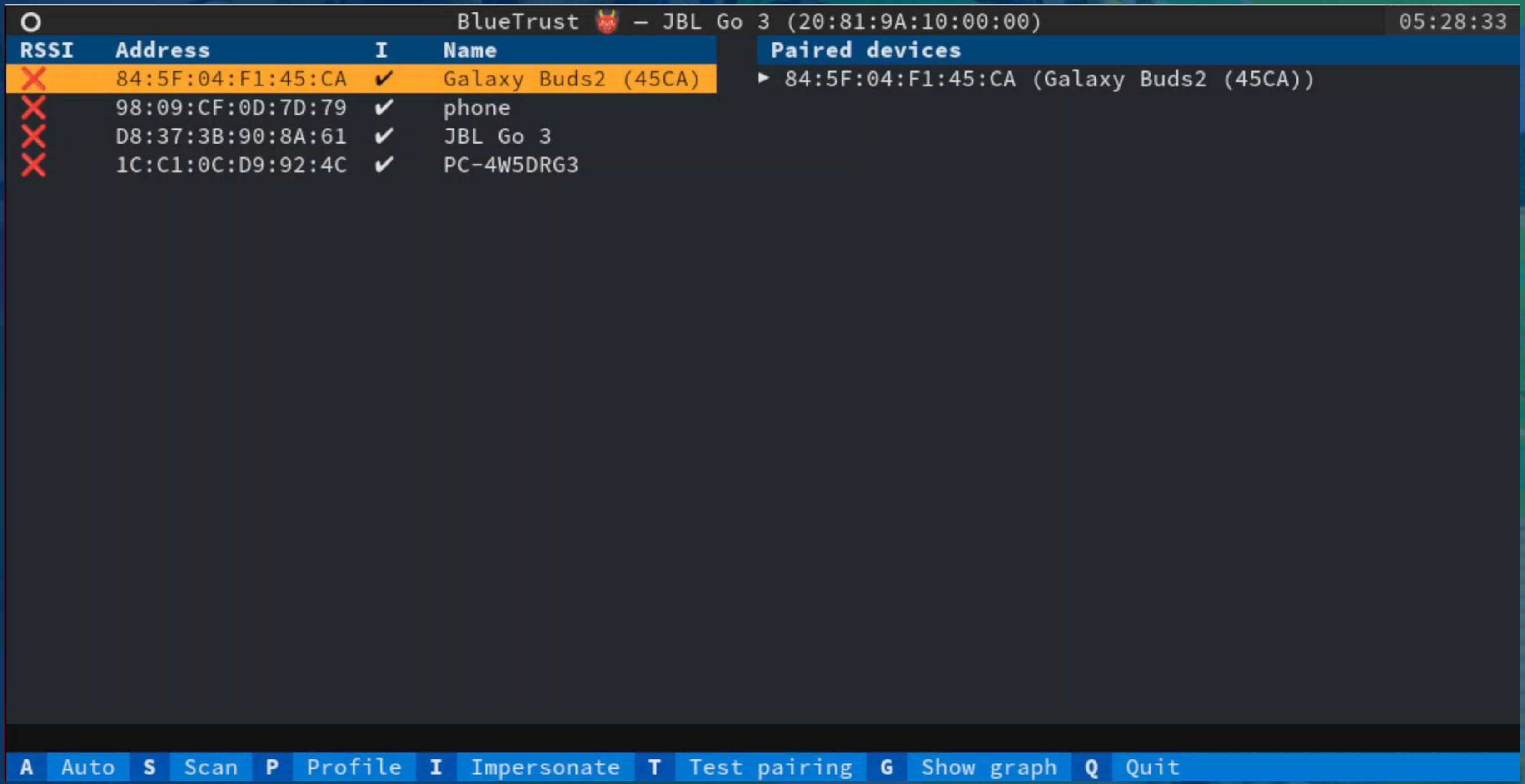
DEMO: MANUAL MODE



```
○                BlueTrust 👹 – JBL Go 3 (20:81:9A:10:00:00)               05:15:41
RSSI   Address            I    Name                   Paired devices









A  Auto  S  Scan  P  Profile  I  Impersonate  T  Test pairing  G  Show graph  Q  Quit
```

PATENT PENDING

DEMO: AUTO MODE



```
○                  BlueTrust 👹 — JBL Go 3 (20:81:9A:10:00:00)                 05:28:33
RSSI  Address            I   Name                    Paired devices
❌    84:5F:04:F1:45:CA  ✔   Galaxy Buds2 (45CA)     ► 84:5F:04:F1:45:CA (Galaxy Buds2 (45CA))
❌    98:09:CF:0D:7D:79  ✔   phone
❌    D8:37:3B:90:8A:61  ✔   JBL Go 3
❌    1C:C1:0C:D9:92:4C  ✔   PC-4W5DRG3




A  Auto  S  Scan  P  Profile  I  Impersonate  T  Test pairing  G  Show graph  Q  Quit
```

PATENT PENDING

TARLOGIC
CYBERSECURITY EXPERTS

AGRADECIMIENTOS

/Rootəd CON

Resto del equipo:

- Francisco Manuel Álvarez Wic
- David Sandoval Rodríguez-Bermejo
- Miguel Tarascó Acuña

TARLOGIC
CYBERSECURITY EXPERTS

AGRADECIMIENTOS

/Rootəd CON

Resto del equipo:

- Francisco Manuel Álvarez Wic
- David Sandoval Rodríguez-Bermejo
- Miguel Tarascó Acuña