ISCAS 2025
IEEE INTERNATIONAL SYMPOSIUM ON CIRCUITS AND SYSTEMS
LONDON, UK | May 25-28, 2025

Hacking Health: Unveiling Vulnerabilities in BLE-Enabled Wearable Sensor Nodes

Mohammad Alhussan, Francesca Boem,
Sara Ghoreishizadeh, Anna Maria Mandalari

University College London

Background

- Global Market for **Wearable Sensor Nodes → $33.85 billion** in 2023
- **537 million adults living with diabetes** globally in 2021
- **10% are living with type 1 diabetes**
- Year **2045**, **1 out of every 8 adults** → around **783 million** individuals, will be diagnosed with diabetes

https://www.grandviewresearch.com/industry-analysis/wearable-medical-devices-market

https://idf.org/about-diabetes/what-is-diabetes/

ISCAS 2025

Background

- Global Market for **Wearable Sensor Nodes → $33.85 billion** in 2023
- **537 million adults living with diabetes** globally in 2021
- **10% are living with type 1 diabetes**
- Year **2045**, **1 out of every 8 adults** → around **783 million** individuals, will be diagnosed with diabetes

https://www.grandviewresearch.com/industry-analysis/wearable-medical-devices-market

https://idf.org/about-diabetes/what-is-diabetes/

ISCAS 2025

Background

- Global Market for **Wearable Sensor Nodes → $33.85 billion** in 2023
- **537 million adults living with diabetes** globally in 2021
- **10% are living with type 1 diabetes**
- Year **2045**, **1 out of every 8 adults** → around **783 million** individuals, will be diagnosed with diabetes

https://www.grandviewresearch.com/industry-analysis/wearable-medical-devices-market

https://idf.org/about-diabetes/what-is-diabetes/

ISCAS 2025

Background

- Global Market for **Wearable Sensor Nodes → $33.85 billion** in 2023
- **537 million adults living with diabetes** globally in 2021
- **10% are living with type 1 diabetes**
- Year **2045**, **1 out of every 8 adults** → around **783 million** individuals, will be diagnosed with diabetes

https://www.grandviewresearch.com/industry-analysis/wearable-medical-devices-market

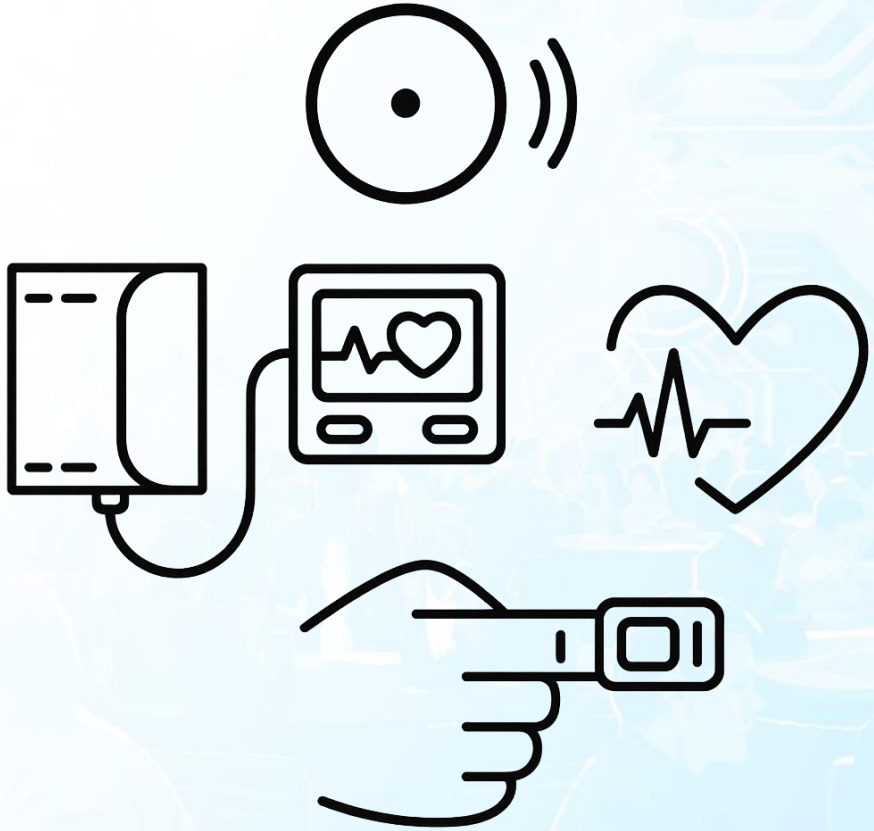
https://idf.org/about-diabetes/what-is-diabetes/

ISCAS 2025

Wearable Sensor Nodes

Continious Glocuse Monitors (CGM)

Blood Pressure Monitors (BPM)

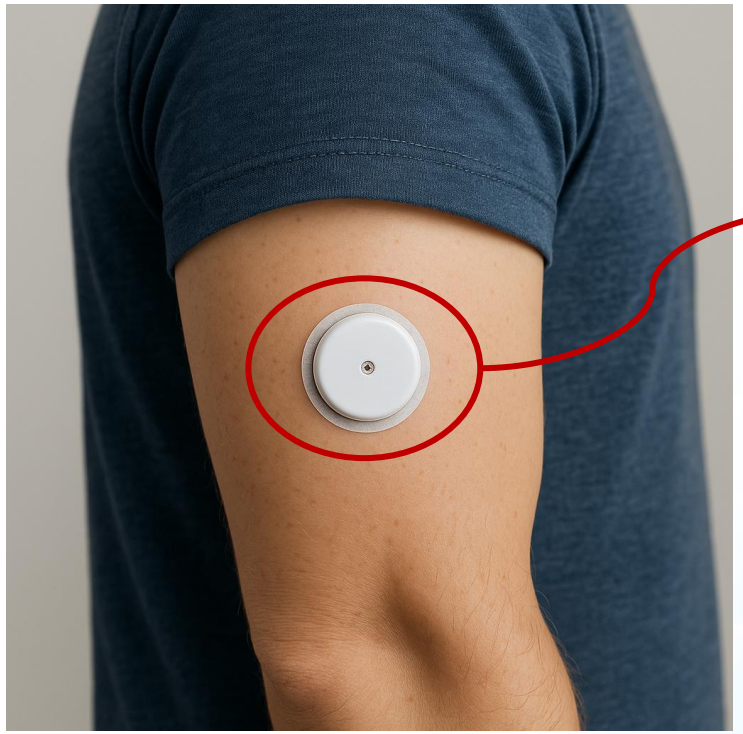


Electrocardiograms (ECG)

Oximeters

Continuous Glucose Monitors

Continuous Glucose Monitors



Artificial Pancreas
Closed Loop Control

Problem Statement

- **Wearable sensor nodes** connected via wireless protocols
  → **Bluetooth Low Energy (BLE) → Cybersecurity risks.**
- **Patient safety, data integrity**, and the **reliability** of essential healthcare systems
  → **Artificial Pancreas technology.**
- **Single-protocol** wireless communication systems, like **BLE**
  → **Insufficient** to protect against sophisticated **cyber threats.**
- **Uncover** these **vulnerabilities → Healthcare manufacturers**, **policymakers**, and **security researchers → Enhance** the **security** and **resilience** of wearable sensor nodes.

ISCAS 2025

Problem Statement

- **Wearable sensor nodes** connected via wireless protocols
  → **Bluetooth Low Energy (BLE) → Cybersecurity risks.**
- **Patient safety, data integrity**, and the **reliability** of essential healthcare systems
  → **Artificial Pancreas technology.**
- **Single-protocol** wireless communication systems, like **BLE**
  → **Insufficient** to protect against sophisticated **cyber threats.**
- **Uncover** these **vulnerabilities → Healthcare manufacturers**, **policymakers**, and **security researchers → Enhance** the **security** and **resilience** of wearable sensor nodes.

Problem Statement

- **Wearable sensor nodes** connected via wireless protocols
  → **Bluetooth Low Energy (BLE) → Cybersecurity risks.**
- **Patient safety, data integrity**, and the **reliability** of essential healthcare systems
  → **Artificial Pancreas technology.**
- **Single-protocol** wireless communication systems, like **BLE**
  → **Insufficient** to protect against sophisticated **cyber threats.**
- **Uncover** these **vulnerabilities → Healthcare manufacturers**, **policymakers**, and **security researchers → Enhance** the **security** and **resilience** of wearable sensor nodes.

ISCAS 2025

Problem Statement

- **Wearable sensor nodes** connected via wireless protocols
  → **Bluetooth Low Energy (BLE) → Cybersecurity risks.**
- **Patient safety, data integrity**, and the **reliability** of essential healthcare systems
  → **Artificial Pancreas technology.**
- **Single-protocol** wireless communication systems, like **BLE**
  → **Insufficient** to protect against sophisticated **cyber threats.**
- **Uncover** these **vulnerabilities → Healthcare manufacturers**, **policymakers**, and **security researchers → Enhance** the **security** and **resilience** of wearable sensor nodes.

ISCAS 2025

Common Wireless Attacks in BLE

- Man in the Middle (MITM) → Manipulation of Data

Man in the Middle

Common Wireless Attacks in BLE

- Man in the Middle (MITM) → Manipulation of Data

Man in the Middle

- Denial of Service (DoS) → Loss of View

Denial of Service

Common Wireless Attacks in BLE

- Man in the Middle (MITM) → Manipulation of Data

Man in the Middle

- Denial of Service (DoS) → Loss of View

Denial of Service

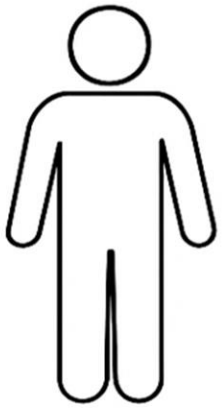
- Sniffing → Eavesdropping

Sniffing

Threat Model

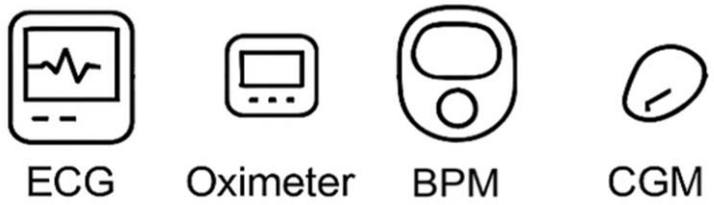
Victim:

- Blood pressure lability
- Heart arrhythmia
- Hypoxemia
- Diabetes

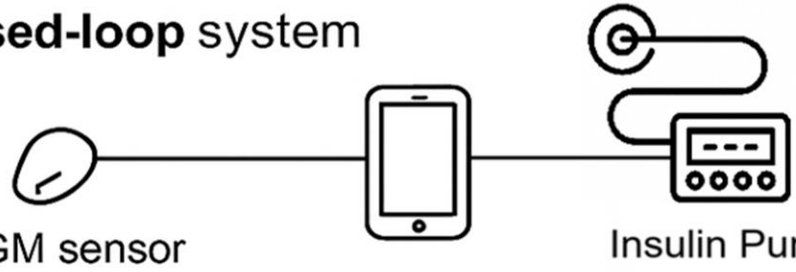


System:

Open-loop system

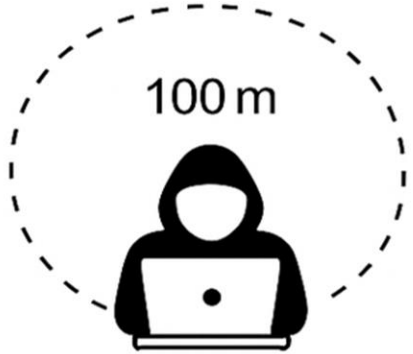


Closed-loop system



Adversary:

BLE 4.0 / BLE 5.0

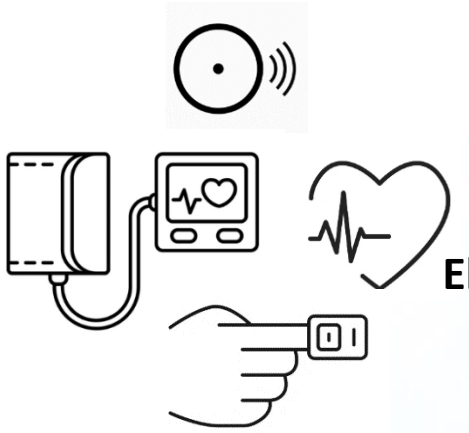


Passive (Sniffing/Eavesdropping) and
Active (MITM, DoS)

Testbed & Experimental Setup

Dexcom ONE and
FreeStlye Libre2
Continious Glocuse Monitors (CGM)

Wellue Blood Pressure Monitors (BPM)

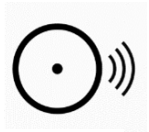


SnapECG and
DuoEK Wellue
Electrocardiograms (ECG)

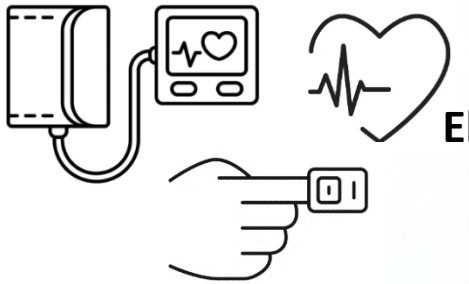
Oxylink and
SleepO2 1400
Oximeters

Testbed & Experimental Setup

Dexcom ONE and
FreeStlye Libre2
Continious Glocuse Monitors (CGM)



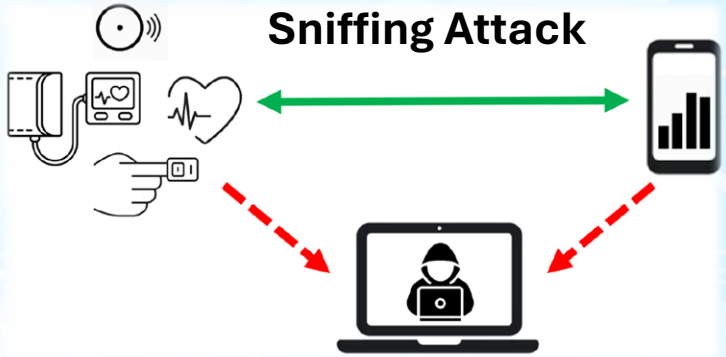
Wellue Blood Pressure Monitors (BPM)



Oxylink and
SleepO2 1400
Oximeters

nRF52840 Nordic
Sniffer Dongle

SnapECG and
DuoEK Wellue
Electrocardiograms (ECG)



iPhone 13 Pro/Google Pixel 3

Wireshark Tool

Testbed & Experimental Setup

Dexcom ONE and
FreeStlye Libre2
Continious Glocuse Monitors (CGM)

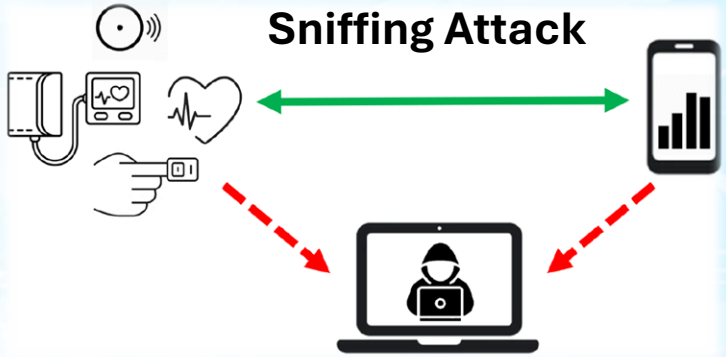
Wellue Blood Pressure Monitors (BPM)

Oxylink and
SleepO2 1400
Oximeters

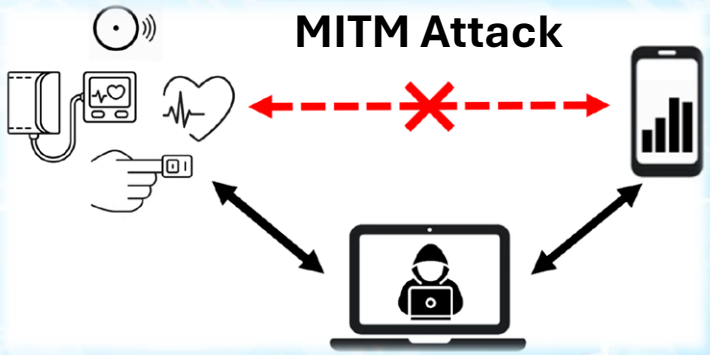
nRF52840 Nordic
Sniffer Dongle

SnapECG and
DuoEK Wellue
Electrocardiograms (ECG)

Bluetooth 4.0
Adapter USB
Dongles



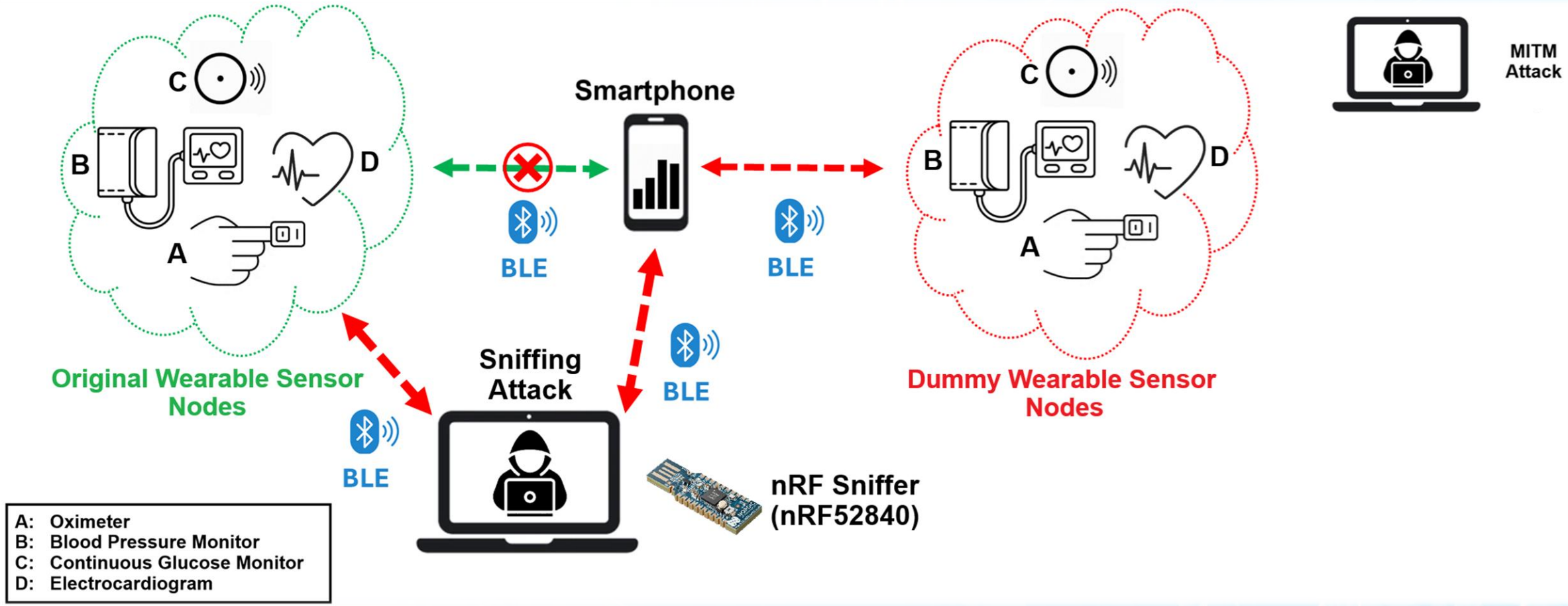
Wireshark Tool



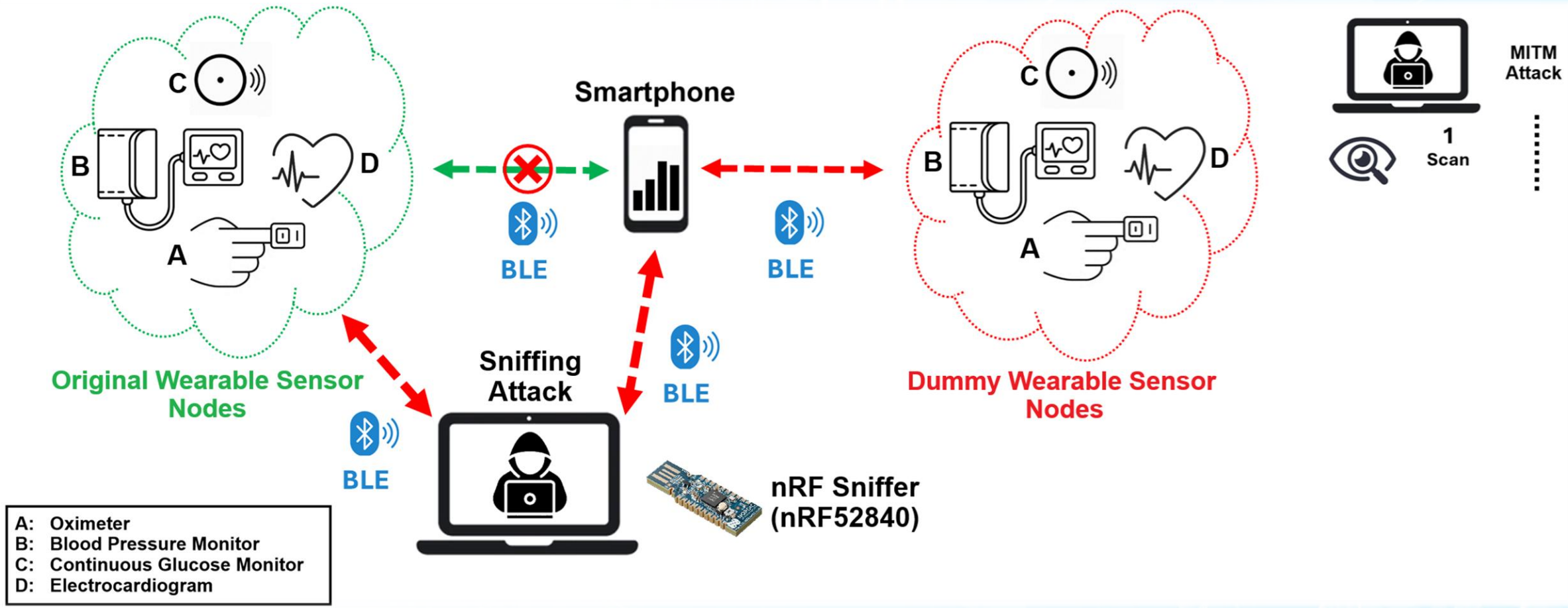
Kali Linux
Mirage Tool

ISCAS 2025

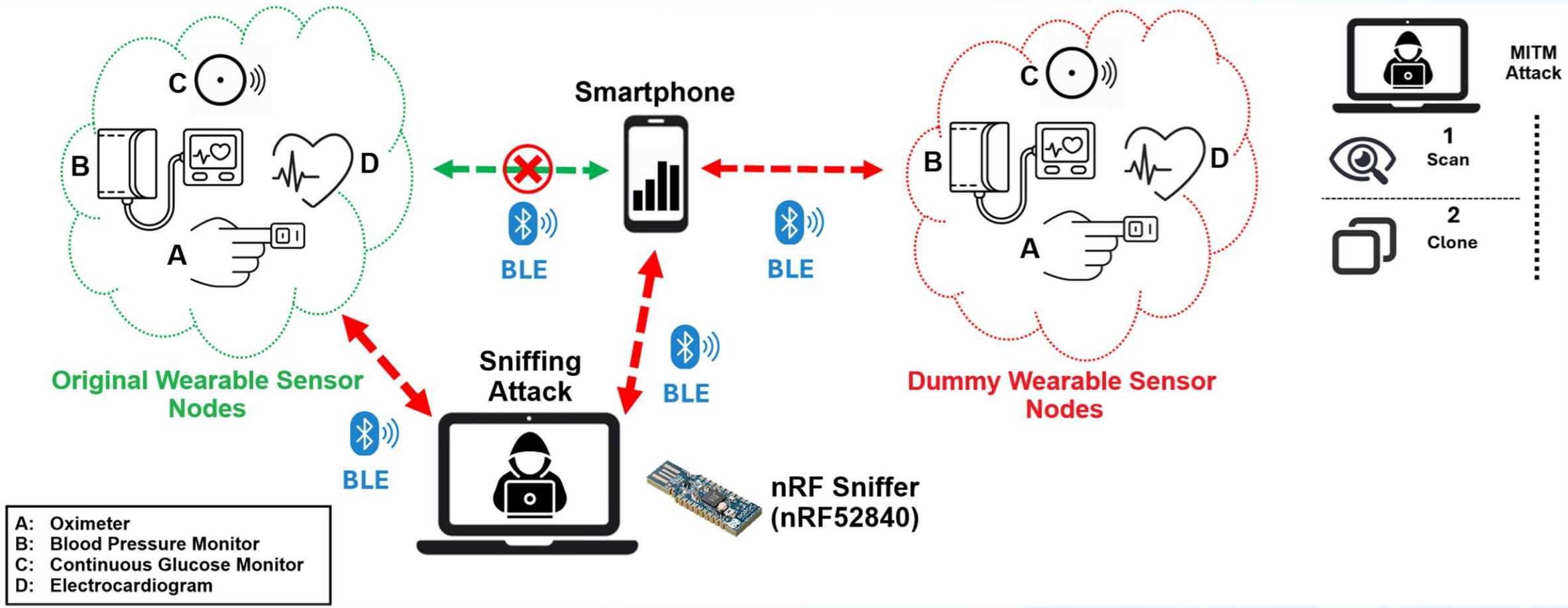
MITM & Sniffing Auditing Methodology



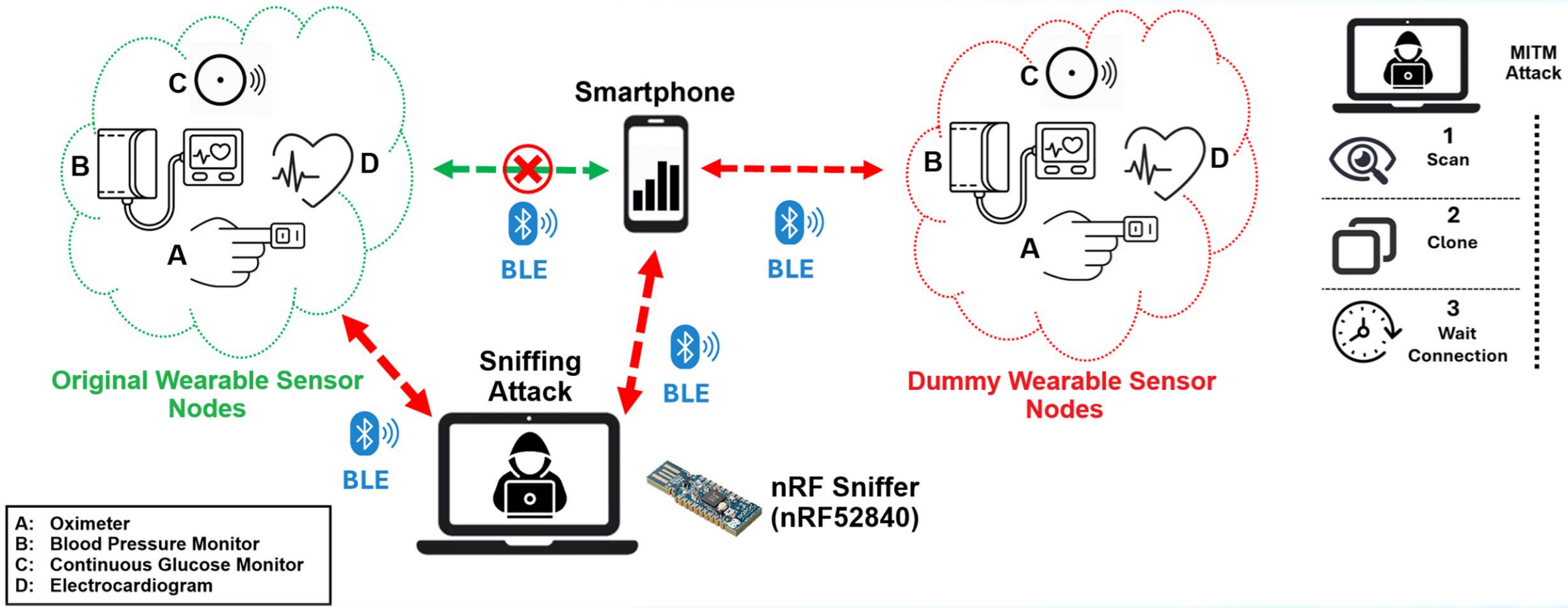
MITM & Sniffing Auditing Methodology



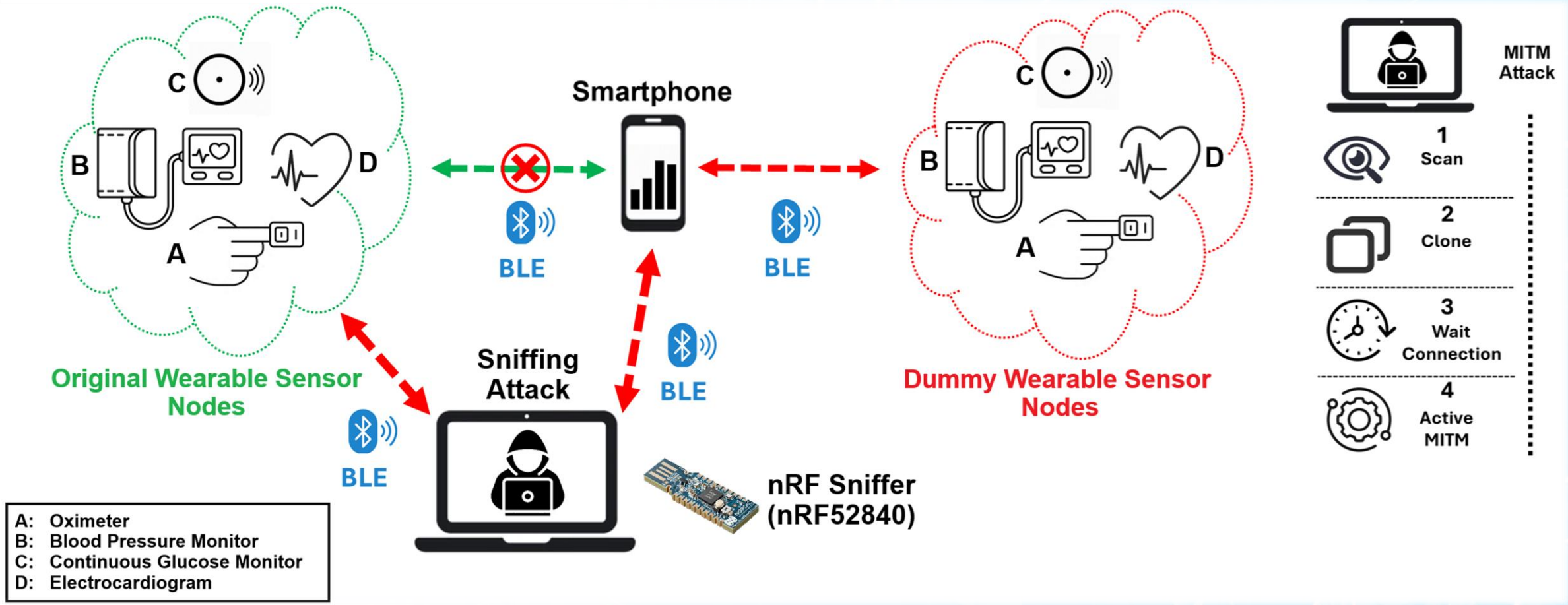
MITM & Sniffing Auditing Methodology



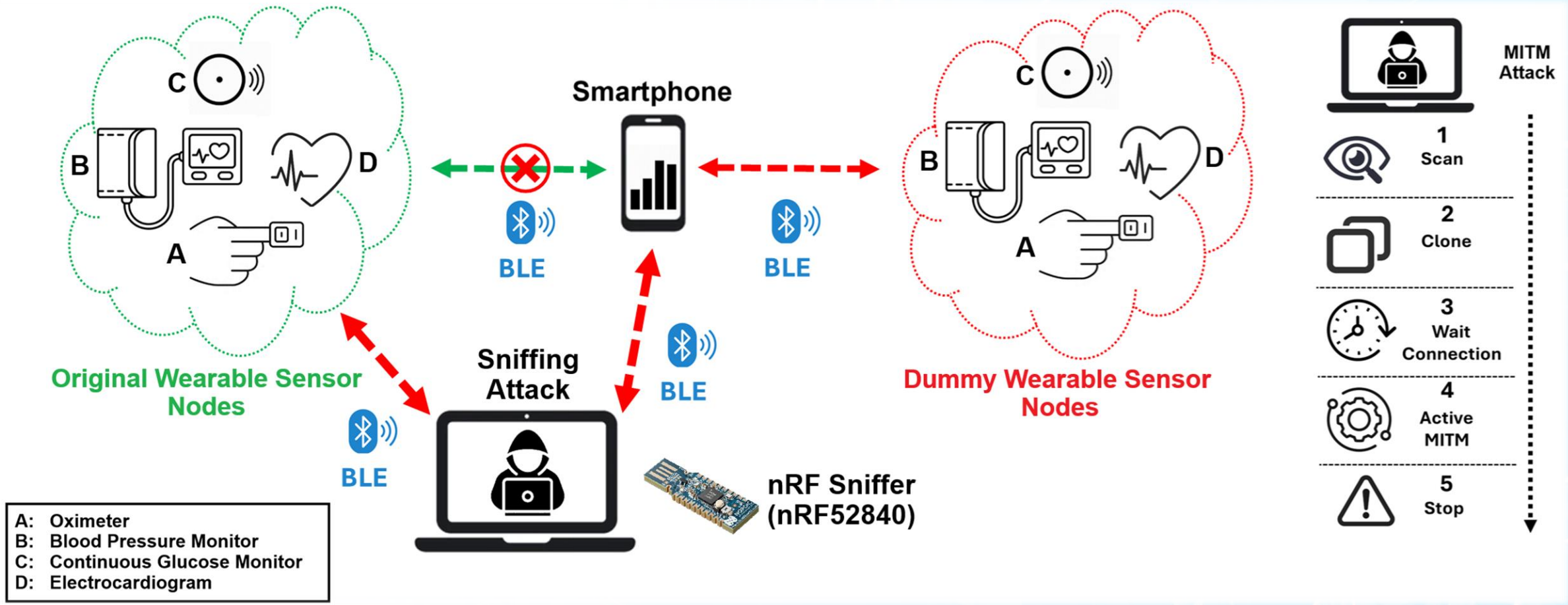
MITM & Sniffing Auditing Methodology



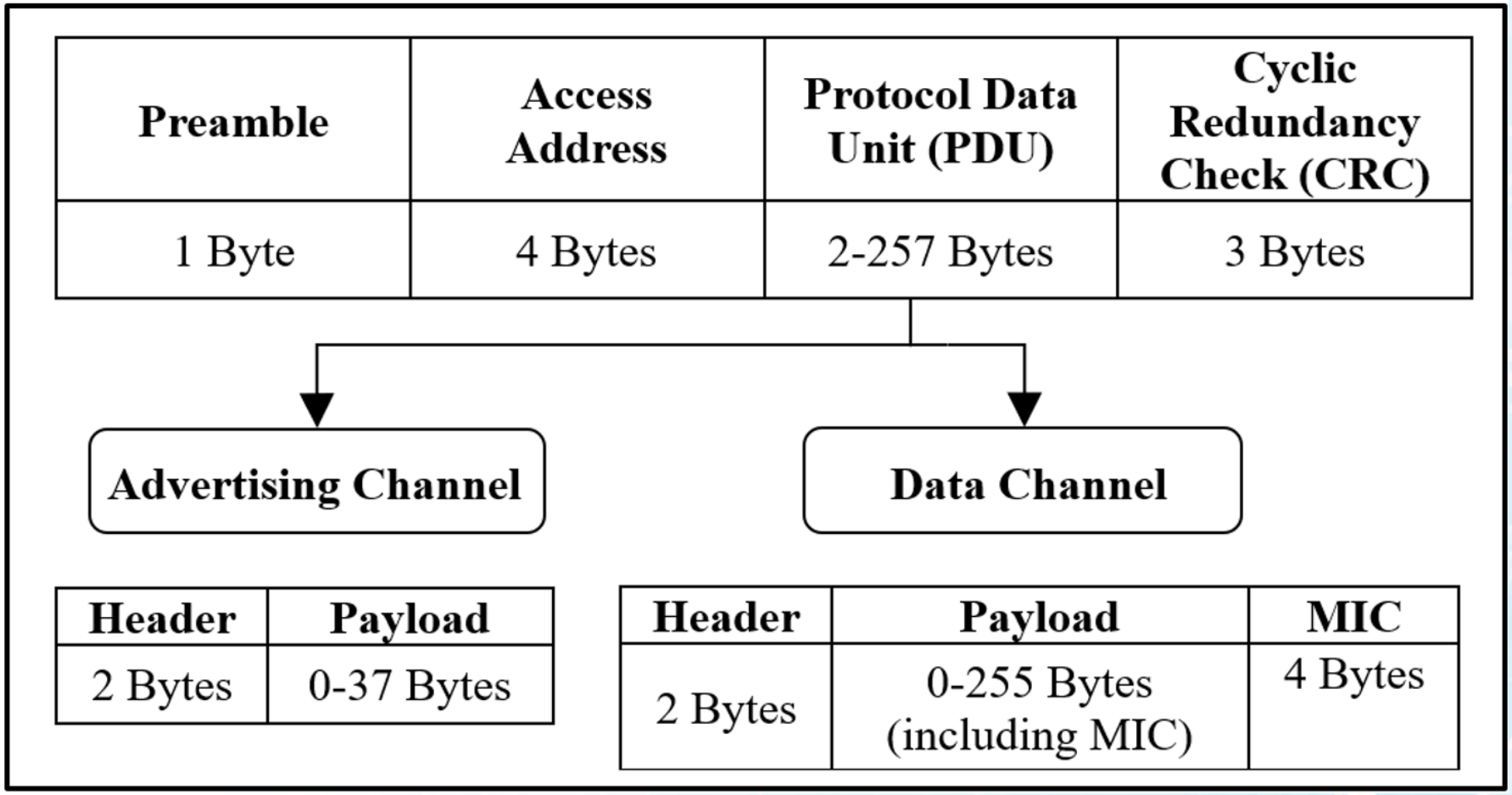
MITM & Sniffing Auditing Methodology



MITM & Sniffing Auditing Methodology



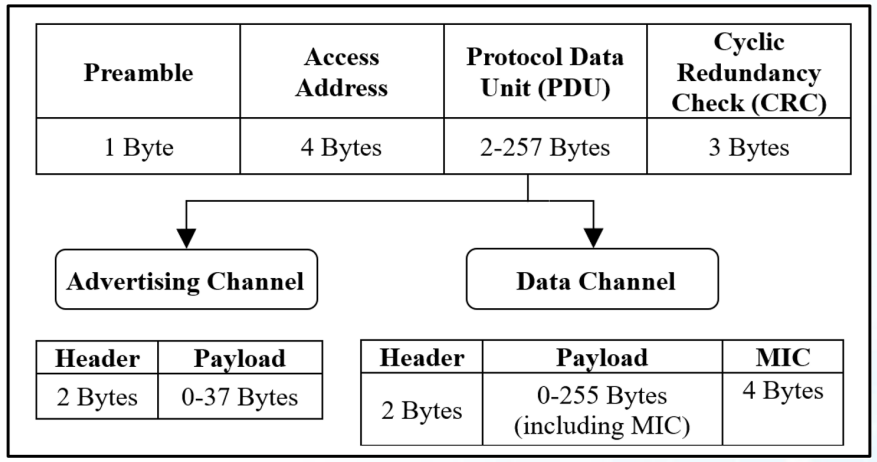
Bluetooth Low Energy – Packet Format



Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

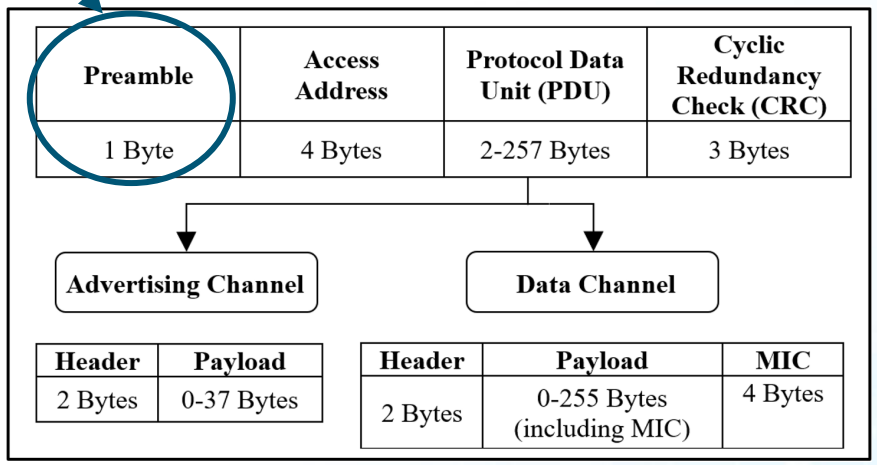
Handle “0x19”: 5500ff00000d00615e00000000004200070e0100



Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

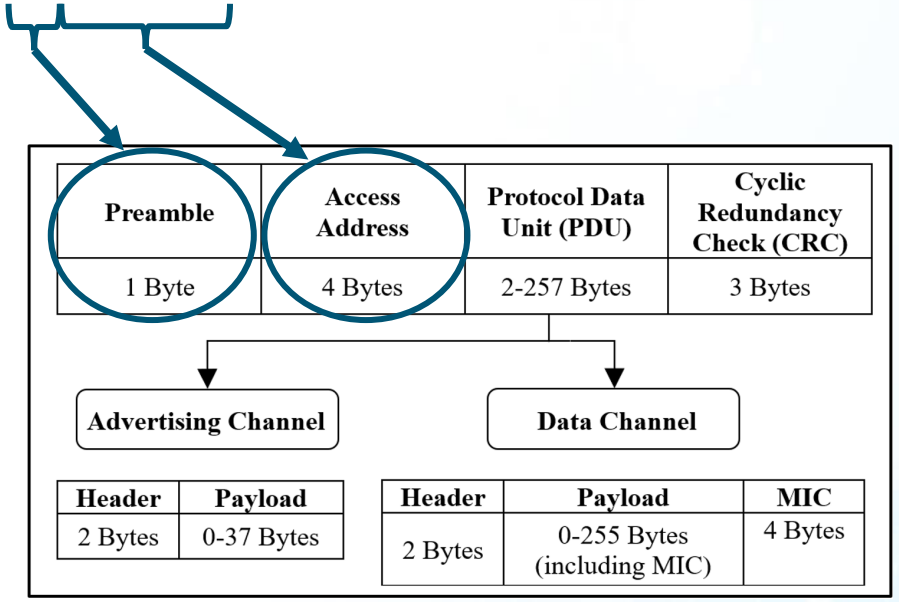
Handle “0x19”: 5500ff00000d00615e00000000004200070e0100



Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

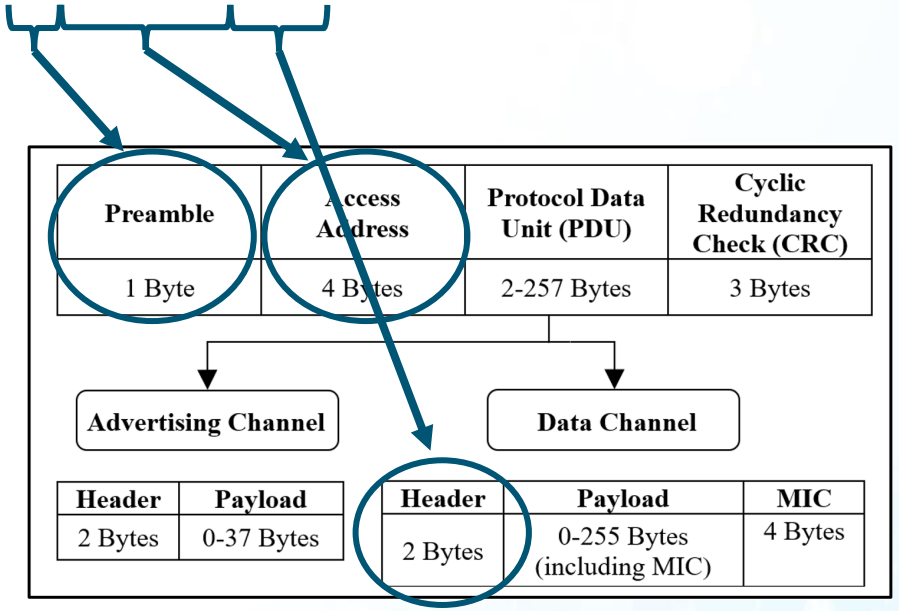
Handle “0x19”: 5500ff00000d00615e00000000004200070e0100



Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

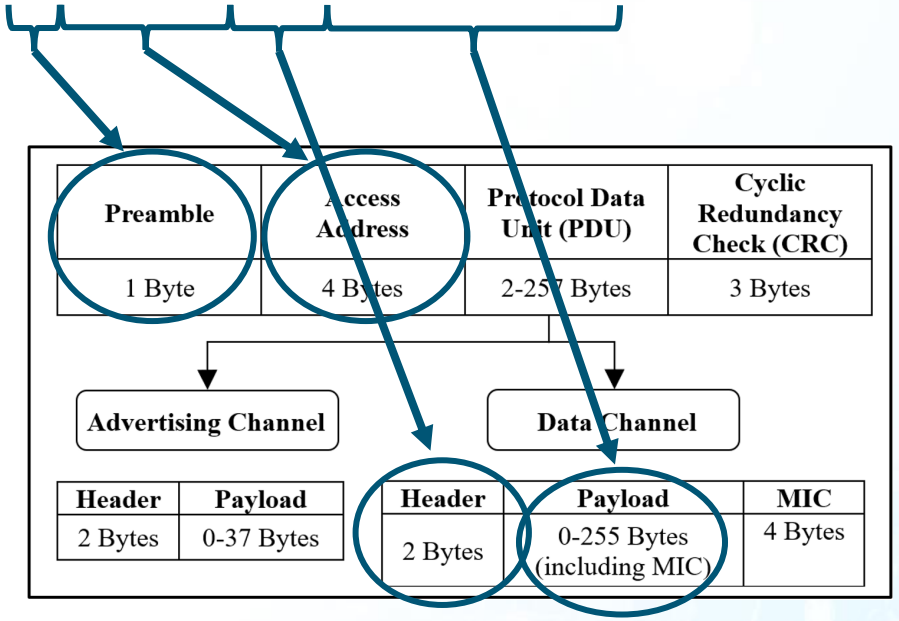
Handle “0x19”: 5500ff00000d00615e00000000004200070e0100



Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

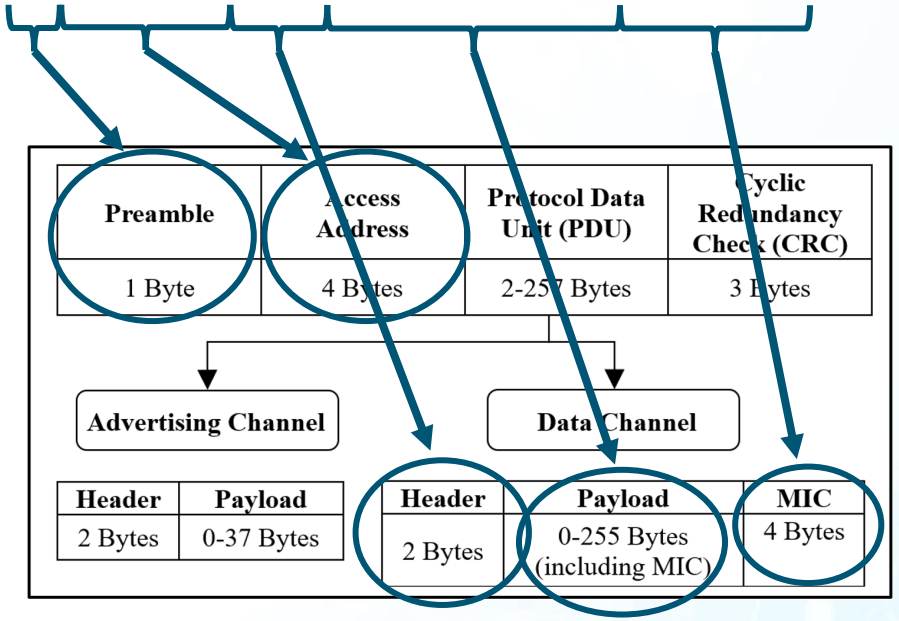
Handle “0x19”: 5500ff00000d00615e00000000004200070e0100



Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

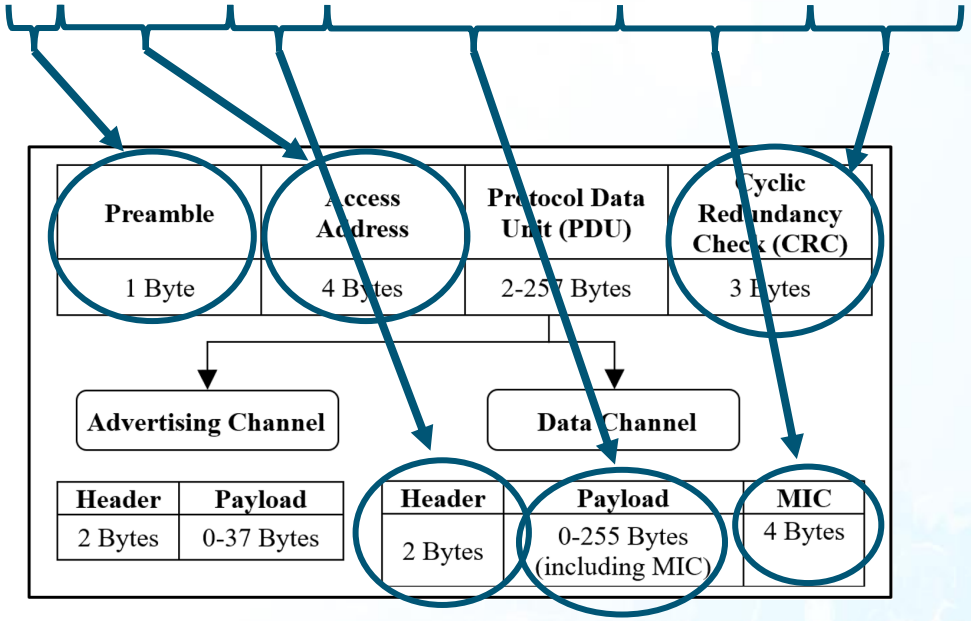
Handle “0x19”: 5500ff00000d00615e00000000004200070e0100



Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

Handle “0x19”: 5500ff00000d00615e00000000004200070e0100

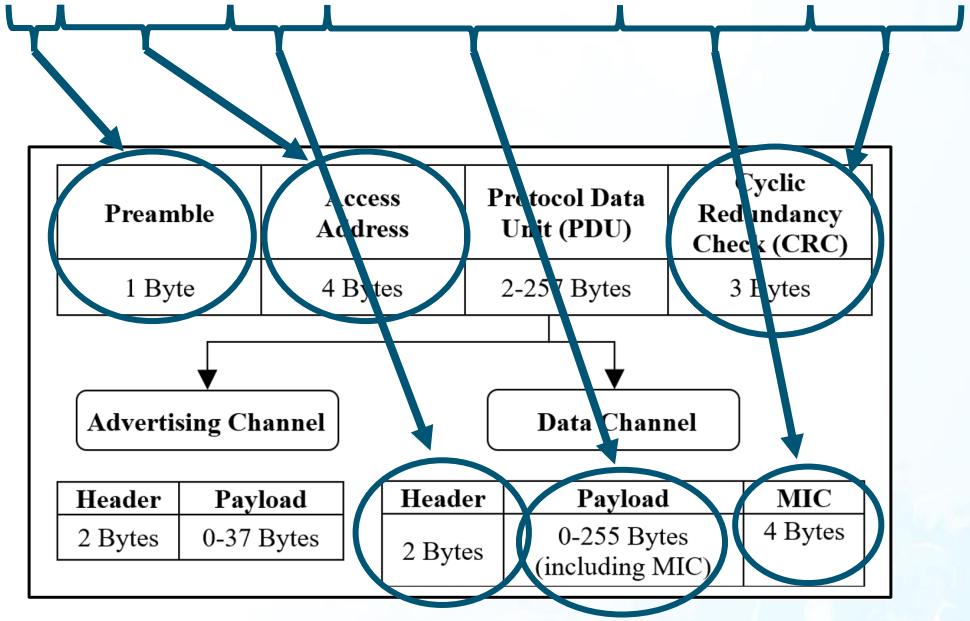


Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

Handle “0x19”: 5500ff00000d00615e0000000004200070e0100

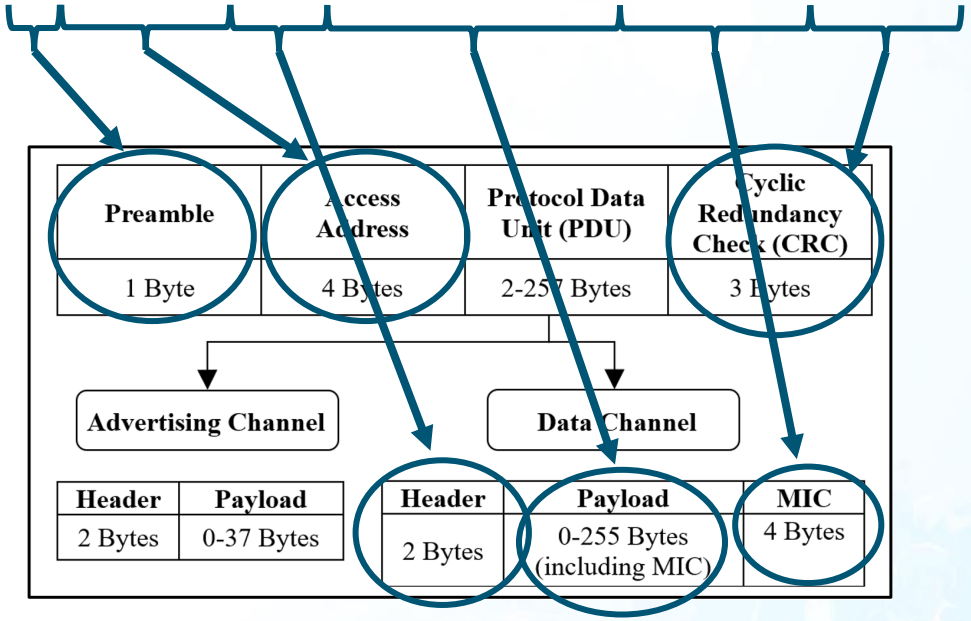
615e00000000



Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

Handle “0x19”: 5500ff00000d00615e0000000004200070e0100



615e00000000

61 (hex) = 97 (dec)

97% Oxygen Level

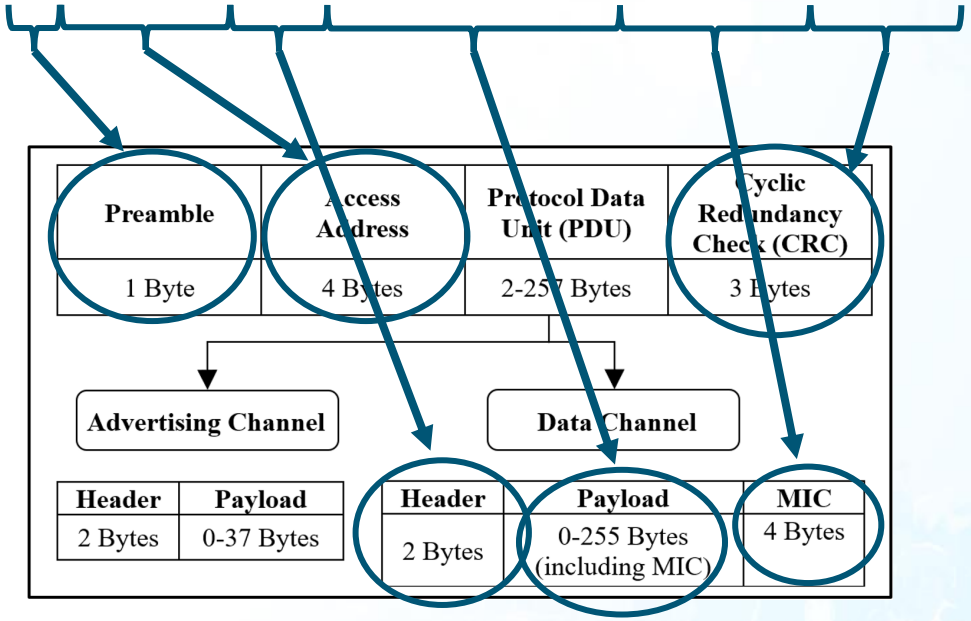
5e (hex) = 94 (dec)

94/min Heart Rate

Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

Handle “0x19”: 5500ff00000d00615e0000000004200070e0100



615e00000000

61 (hex) = 97 (dec)

97% Oxygen Level

5e (hex) = 94 (dec)

94/min Heart Rate

Original: Handle “0x19”: 5500ff00000d00615e0000000004200070e0100

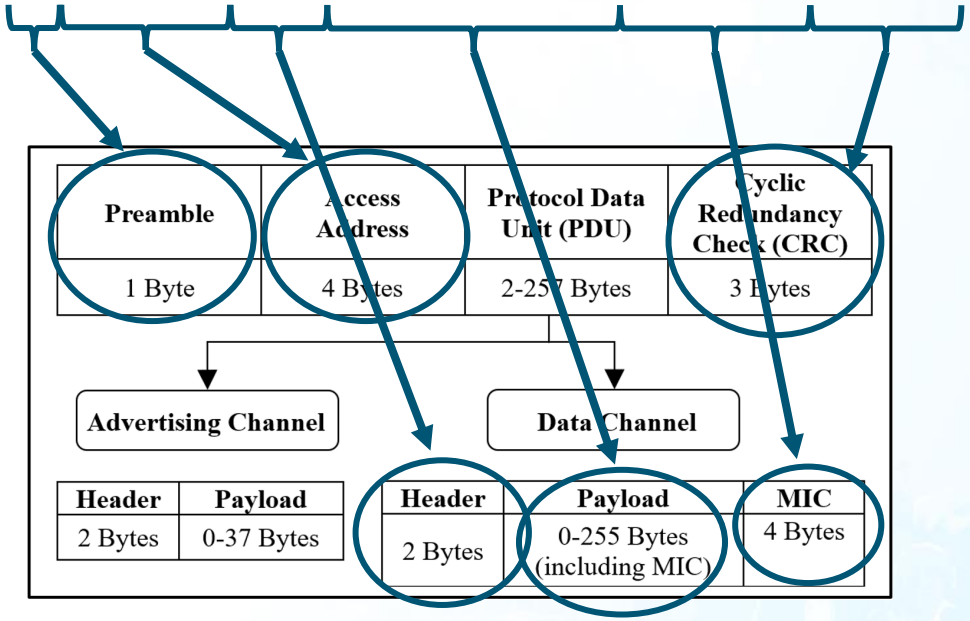
???

Key: “39”

Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

Handle “0x19”: 5500ff00000d00615e0000000004200070e0100



615e00000000

61 (hex) = 97 (dec)

97% Oxygen Level

5e (hex) = 94 (dec)

94/min Heart Rate

Original: Handle “0x19”: 5500ff00000d00615e0000000004200070e0100

Replay: Handle “0x19”: 5500ff00000d006041000000000550000050100

???

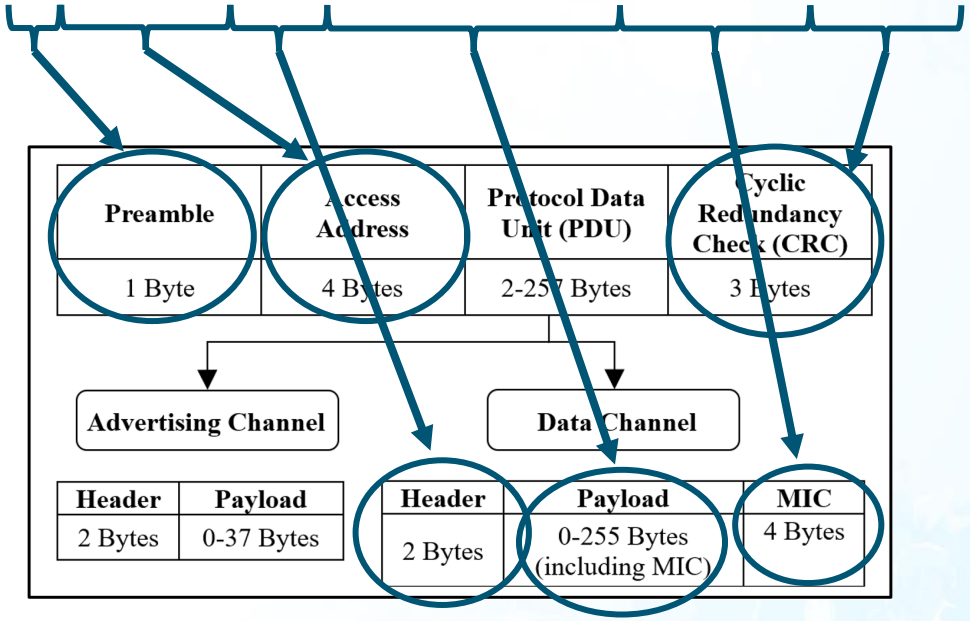
Key: “39”

Key: “db”

Bluetooth Low Energy – Packet Format

Oxylink Oximeter Encrypted Payload Content:

Handle “0x19”: 5500ff00000d00615e0000000004200070e0100



615e00000000

61 (hex) = 97 (dec)

97% Oxygen Level

5e (hex) = 94 (dec)

94/min Heart Rate

???

Key: “39”

Key: “db”

Original: Handle “0x19”: 5500ff00000d00615e0000000004200070e0100

Replay: Handle “0x19”: 5500ff00000d006041000000000550000050100

60 (hex) = 96 (dec)

96% Oxygen Level

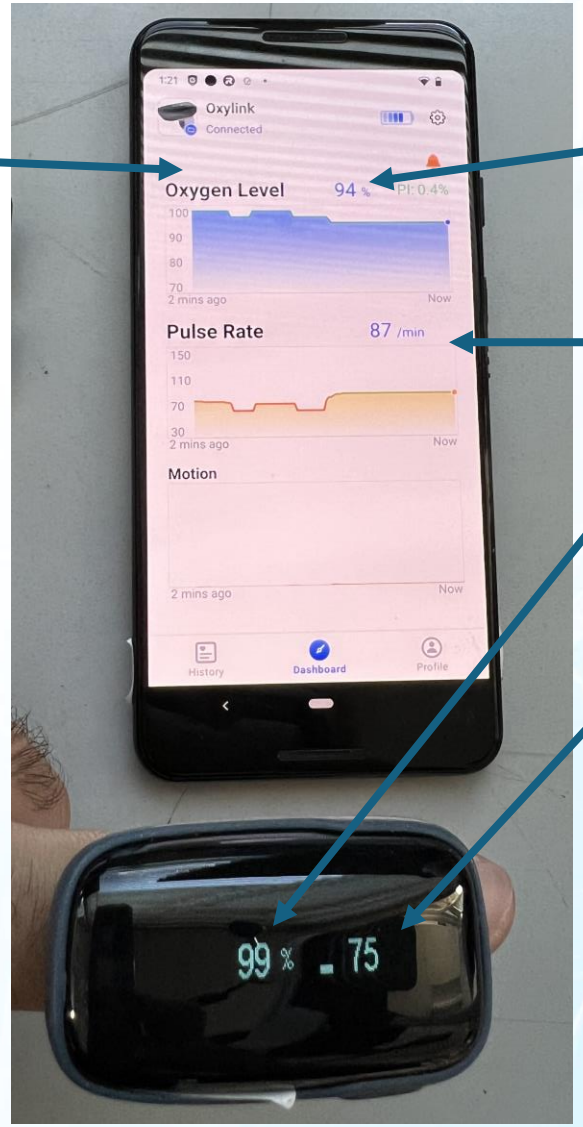
41 (hex) = 65 (dec)

65/min Heart Rate

ISCAS 2025

Oximeter Experimental Results (MITM Attacks)

ViHealth App
Real-time Data
Manipulation

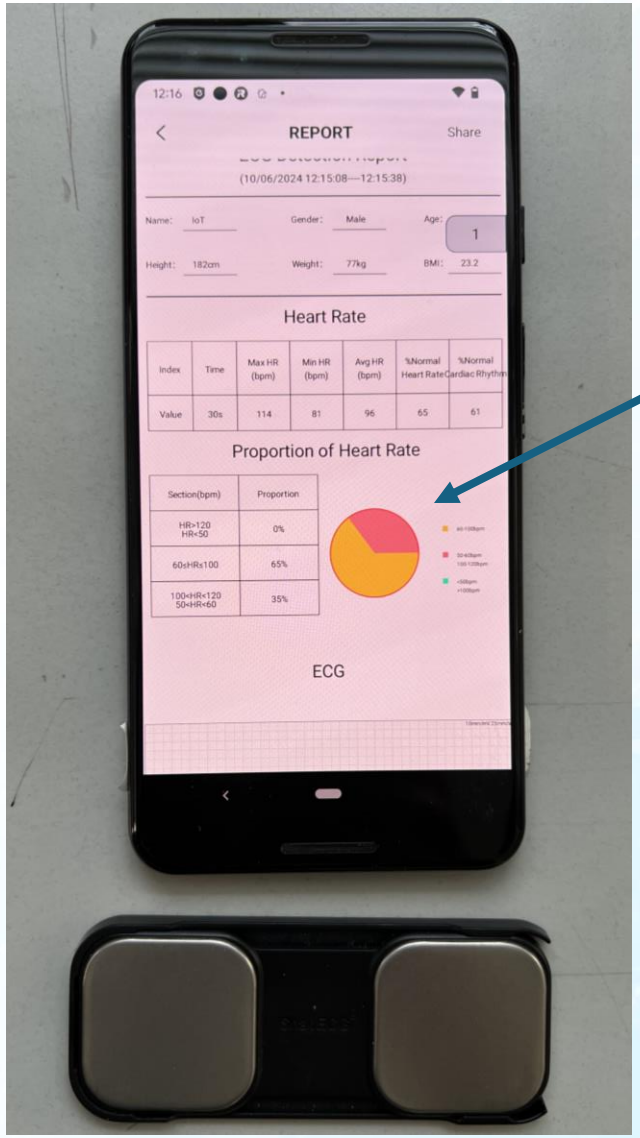


Oxygen Level
Manipulation

Pulse Rate
Manipulation

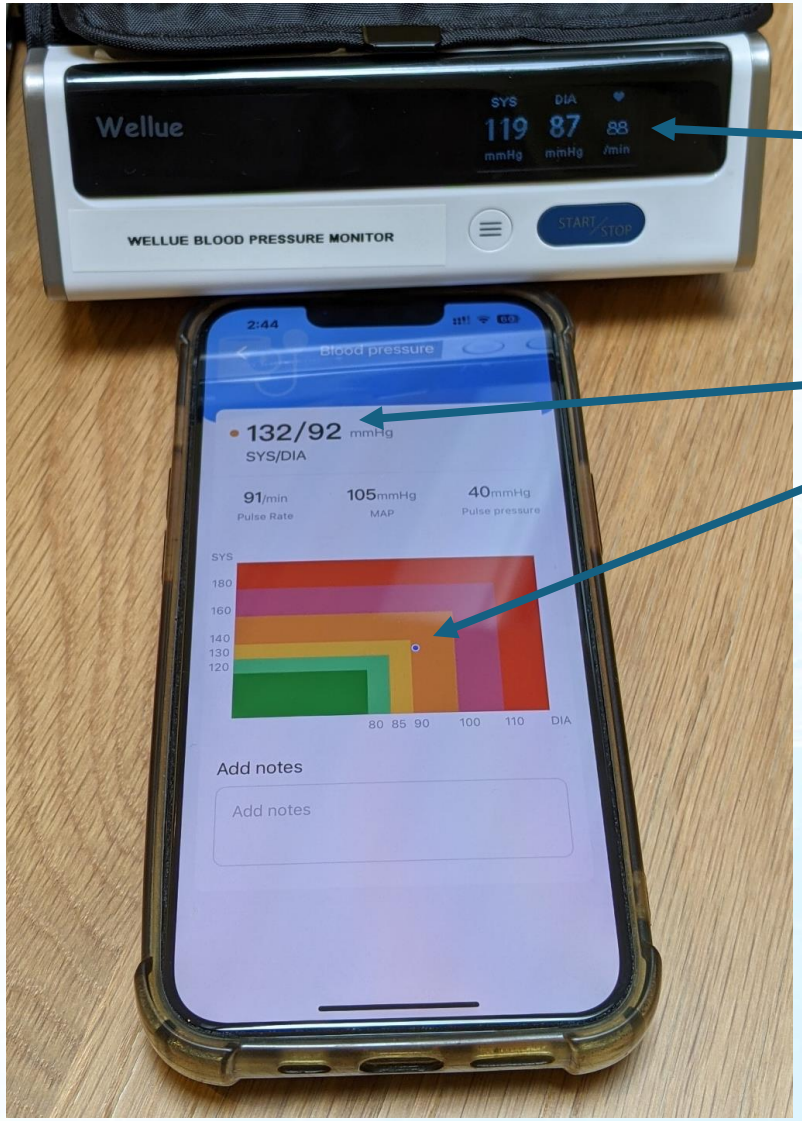
ISCAS 2025

ECG Experimental Results (MITM Attacks)



Unhealthy Report

BPM Experimental Results (MITM Attacks)



Typical Normal Reading

Hypertension Stage 1

CGMs Improved Security Mechanisms

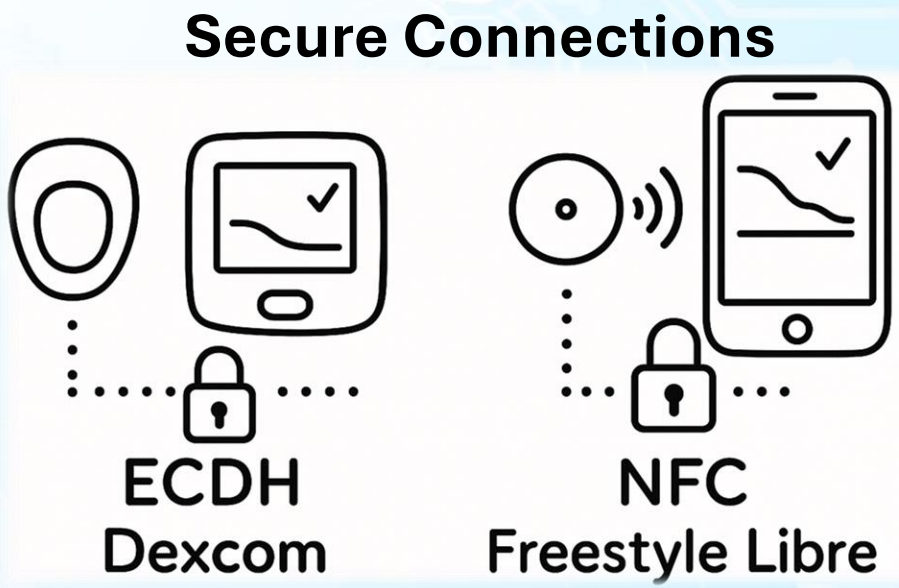
Secure Connections (for initial pairing and keys exchange):

- **Elliptic Curve Diffie-Hellman (ECDH).**

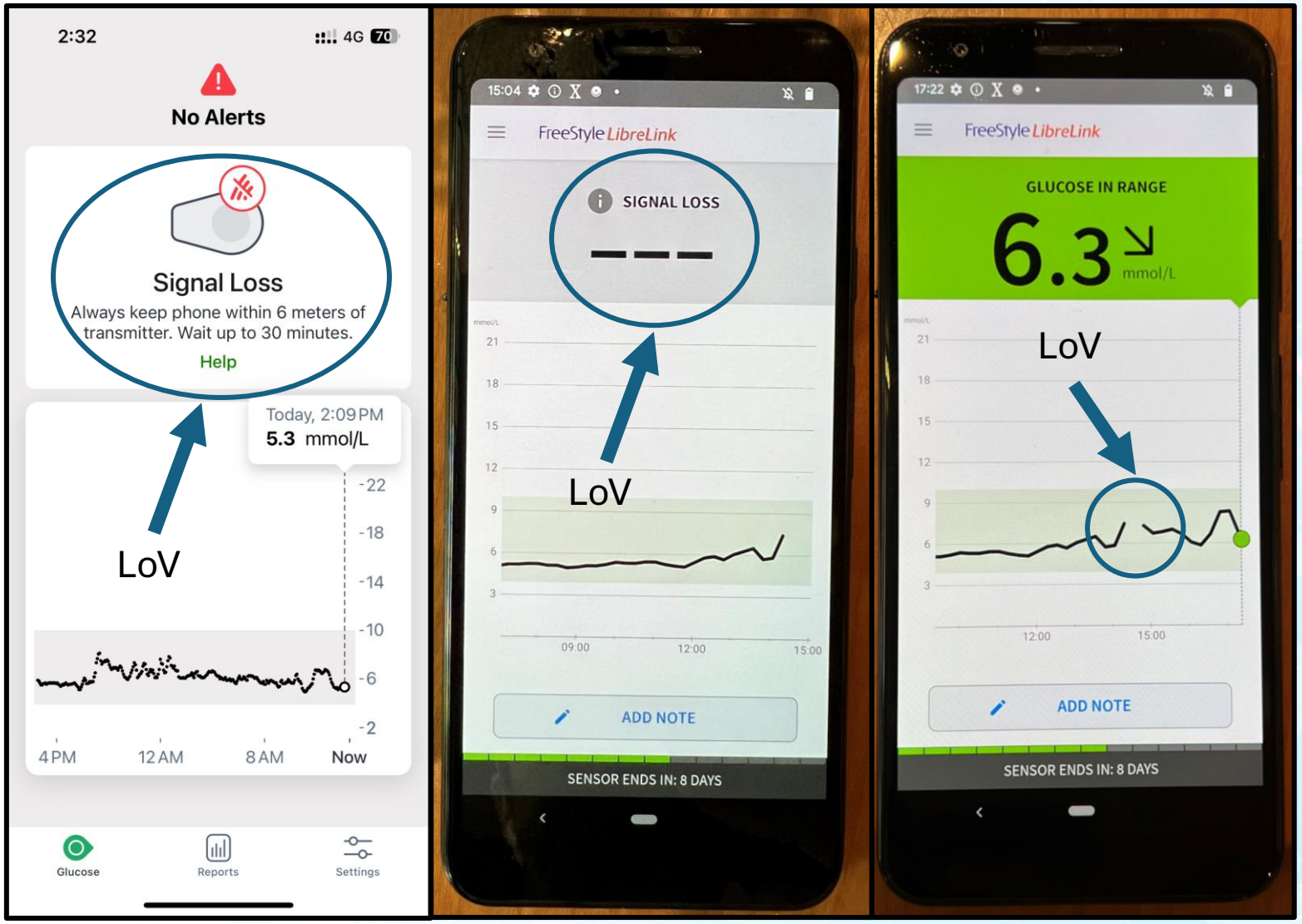
  → Private keys → Public keys → ECDH → Shared secret →
  KDFs → rand → EDIV → IVs →

Session key

- **Near Field Communication (NFC).**

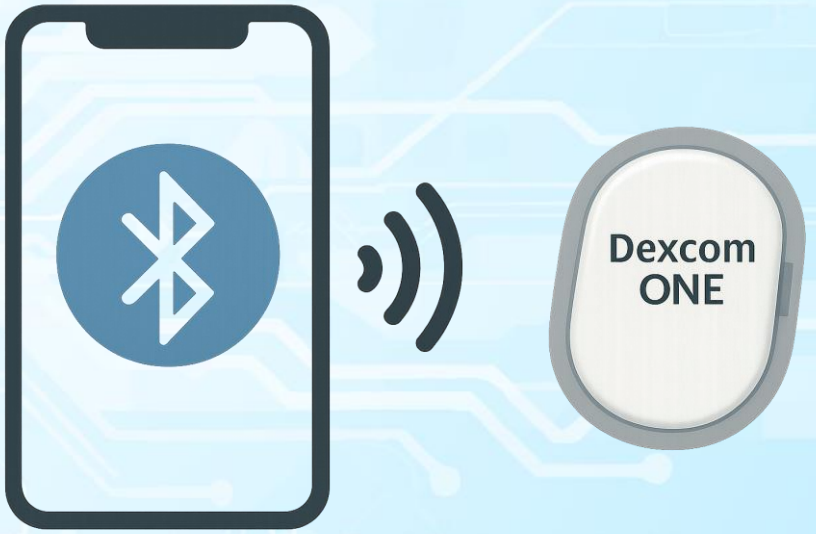


CGM Experimental Results (DoS Attacks)



Sniffing Experimental Results – Example (Dexcom ONE CGM)

- **Initial Pairing Process (ECDH Key Exchange):**
  - **Public Key (Master and Slave)**
  - **Random Key (Master)**
  - **Pairing Confirmation (Slave)**
  - **DHKey checks (Master and Slave)**

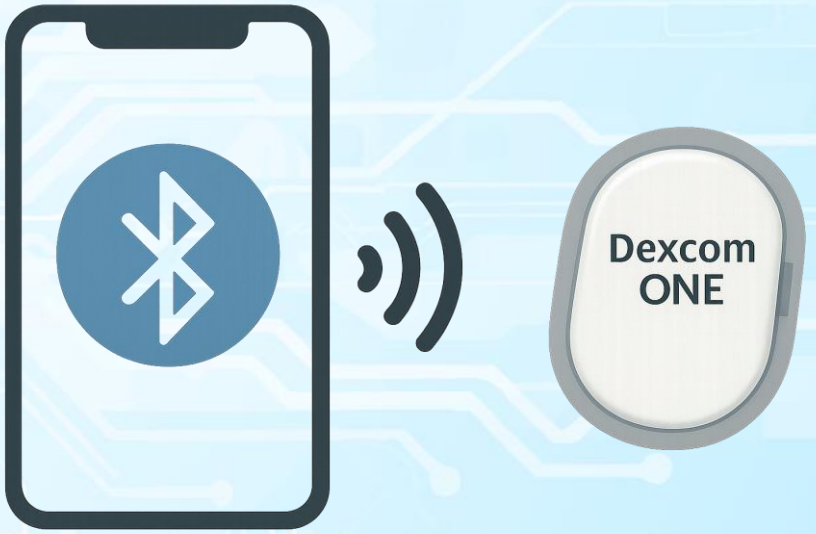


- **Established Session (Post-Pairing Communication):**
  - **Random Number (rand):** All zeros.
  - **Encrypted Diversifier (EDIV):** Non-random or default value.
  - **Session Key Diversifiers (SKDm, SKDs):** Secure, randomized session key generation.
  - **Session Initialization Vectors (IVm, IVs):** Sufficiently randomized.

ISCAS 2025

Sniffing Experimental Results – Example (Dexcom ONE CGM)

- **Initial Pairing Process (ECDH Key Exchange):**
  - **Public Key (Master and Slave)**
  - **Random Key (Master)**
  - **Pairing Confirmation (Slave)**
  - **DHKey checks (Master and Slave)**



- **Established Session (Post-Pairing Communication):**
  - **Random Number (rand):** All zeros.
  - **Encrypted Diversifier (EDIV):** Non-random or default value.
  - **Session Key Diversifiers (SKDm, SKDs):** Secure, randomized session key generation.
  - **Session Initialization Vectors (IVm, IVs):** Sufficiently randomized.

ISCAS 2025

Key Findings

Devices	Types of Attacks			
	Sniffing (Eavesdropping)	**Passive MITM (Eavesdropping)**	**Active MITM (Data Manipulation)**	**DoS (Loss of View)**
SnapECG **(ECG)**	✓	✓	✓	✓
DuoEK Wellue **(ECG)**	✓	✗	✗	✓
OXYLINK **(Oximeter)**	✓	✓	✓	✓
SleepO2 1400 **(Oximeter)**	✓	✓	✓	✓
Wellue BP2A 2031 **(BPM)**	✓	✓	✓	✓
Dexcom ONE **(CGM)**	✓	✗	✗	✓
FreeStyle Libre 2 **(CGM)**	✓	✗	✗	✓

ISCAS 2025

Responsible Disclosure

- **DexCom Inc.** responded and addressed the findings → D1+ includes improved security.
- Other **manufacturers** (i.e. Abbott Laboratories, Nanjing Xijian, and Shenzhen Viatom) were contacted, but **did not respond.**
- All **experiments** were conducted in a **controlled lab environment.**
- No sensitive **health data** was **exposed** in our testing.

Responsible Disclosure

- **DexCom Inc.** responded and addressed the findings → D1+ includes improved security.
- Other **manufacturers** (i.e. Abbott Laboratories, Nanjing Xijian, and Shenzhen Viatom) were contacted, but **did not respond.**
- All **experiments** were conducted in a **controlled lab environment.**
- No sensitive **health data** was **exposed** in our testing.

Responsible Disclosure

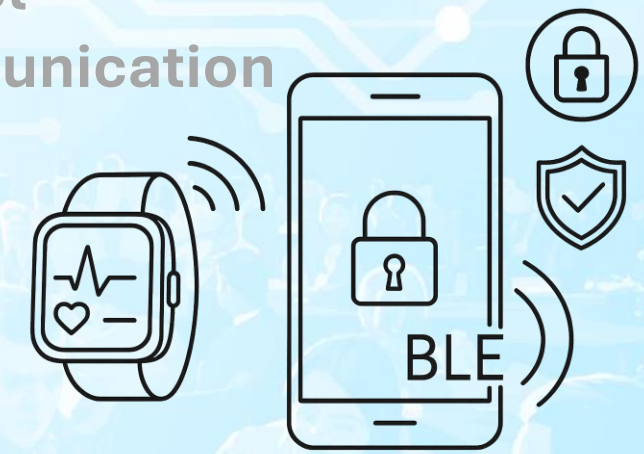
- **DexCom Inc.** responded and addressed the findings → D1+ includes improved security.
- Other **manufacturers** (i.e. Abbott Laboratories, Nanjing Xijian, and Shenzhen Viatom) were contacted, but **did not respond.**
- All **experiments** were conducted in a **controlled lab environment.**
- No sensitive **health data** was **exposed** in our testing.

Responsible Disclosure

- **DexCom Inc.** responded and addressed the findings → D1+ includes improved security.
- Other **manufacturers** (i.e. Abbott Laboratories, Nanjing Xijian, and Shenzhen Viatom) were contacted, but **did not respond.**
- All **experiments** were conducted in a **controlled lab environment.**
- No sensitive **health data** was **exposed** in our testing.

Conclusion

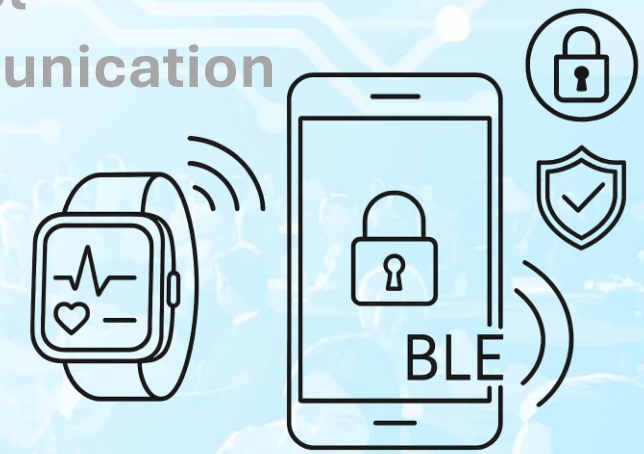
- Significant **vulnerabilities** in BLE-enabled **Wearable Sensor Nodes** → **legacy pairing** and **secure connections** protocols.
- **Impacts and implications** → potential application of pioneering **hacking techniques** on sensitive **Wearable Sensor Nodes**.
- Importance of not relying solely on a **single wireless protocol** → instead depending on a **multilayered cybersecure communication system** for improved **security** and **reliability**.
- Call to action for **manufacturers & stakeholders** to address these issues.



ISCAS 2025

Conclusion

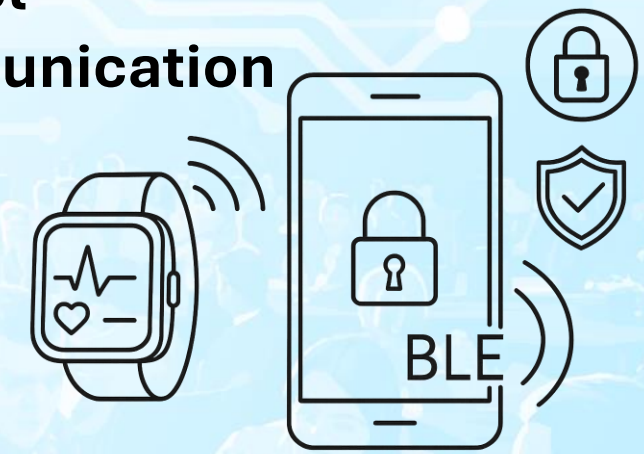
- Significant **vulnerabilities** in BLE-enabled **Wearable Sensor Nodes** → **legacy pairing** and **secure connections** protocols.
- **Impacts and implications** → potential application of pioneering **hacking techniques** on sensitive **Wearable Sensor Nodes**.
- Importance of not relying solely on a **single wireless protocol** → instead depending on a **multilayered cybersecure communication system** for improved **security** and **reliability**.
- Call to action for **manufacturers & stakeholders** to address these issues.



ISCAS 2025

Conclusion

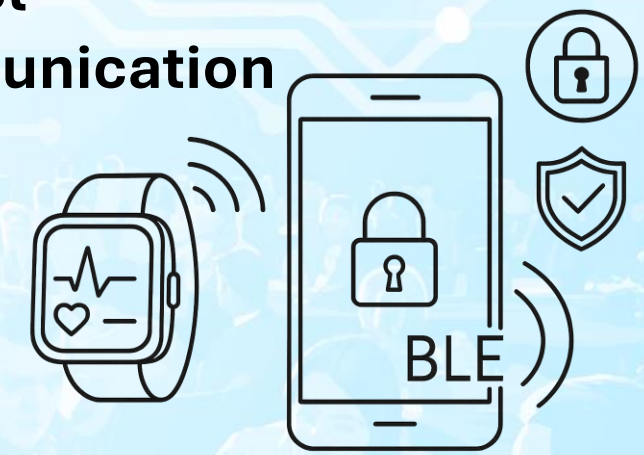
- Significant **vulnerabilities** in BLE-enabled **Wearable Sensor Nodes** → **legacy pairing** and **secure connections** protocols.
- **Impacts and implications** → potential application of pioneering **hacking techniques** on sensitive **Wearable Sensor Nodes**.
- Importance of not relying solely on a **single wireless protocol** → instead depending on a **multilayered cybersecure communication system** for improved **security** and **reliability**.
- Call to action for **manufacturers & stakeholders** to address these issues.



ISCAS 2025

Conclusion

- Significant **vulnerabilities** in BLE-enabled **Wearable Sensor Nodes** → **legacy pairing** and **secure connections** protocols.
- **Impacts and implications** → potential application of pioneering **hacking techniques** on sensitive **Wearable Sensor Nodes**.
- Importance of not relying solely on a **single wireless protocol** → instead depending on a **multilayered cybersecure communication system** for improved **security** and **reliability**.
- Call to action for **manufacturers & stakeholders** to address these issues.



ISCAS 2025

Thanks

KFAS
مؤسسة الكويت للتقدم العلمي
Kuwait Foundation for the Advancement of Sciences

SafeNetIoT
SECURING THE IOT

SafeNetIoT Lab
University College London

Find Us!

https://safenetiot.github.io/

ISCAS 2025