CYBERMED: Enhancing Cybersecurity in Wearable Medical Devices using Intra-Body Communication

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

Department of Electronic and Electrical Engineering (EEE), Faculty of Engineering Sciences, University College London

Introduction & Motivation

- **Wearable medical devices** (e.g. ECGs, BPMs, Oximeters, CGMs, insulin pumps) are essential for real-time health monitoring.
- These devices typically communicate via **Bluetooth Low Energy (BLE)**.
- Vulnerabilities in BLE may expose devices to **Sniffing**, **DoS**, and **MITM** attacks.

Medical Devices	Medical Devices			
Stationary	LINAC	Ultrasound Imaging (Sonography)	MRI	X-Ray
Implantable	Cardiac implanted devices: • Pacemakers • Implantable Cardioverter Defibrillator (ICD)	Neurostimulators: • Deep Brain Stimulator (DBS) • Spinal Cord Stimulator	Drug Delivery system	Insulin Pumps
Wearable	Continuous Glucose Monitors (CGM)	Electrocardiogram (ECG) Devices	Blood Pressure Monitors	

- ➢ **Focus:** Identify and demonstrate practical exploitation paths under real-world conditions.
- ➢ **Goal:** Strengthen communication security, resilience, and reliability and promote safer system designs for future devices.

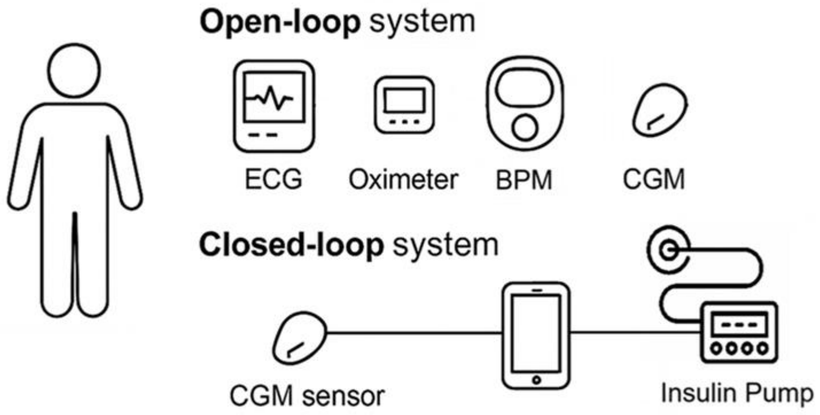
Threat Model

Victim:

- Blood pressure lability
- Heart arrhythmia
- Hypoxemia
- Diabetes

System:

Open-loop system



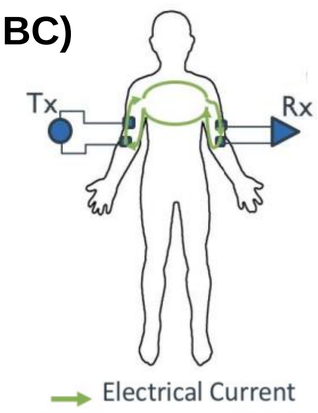
Closed-loop system

Adversary:

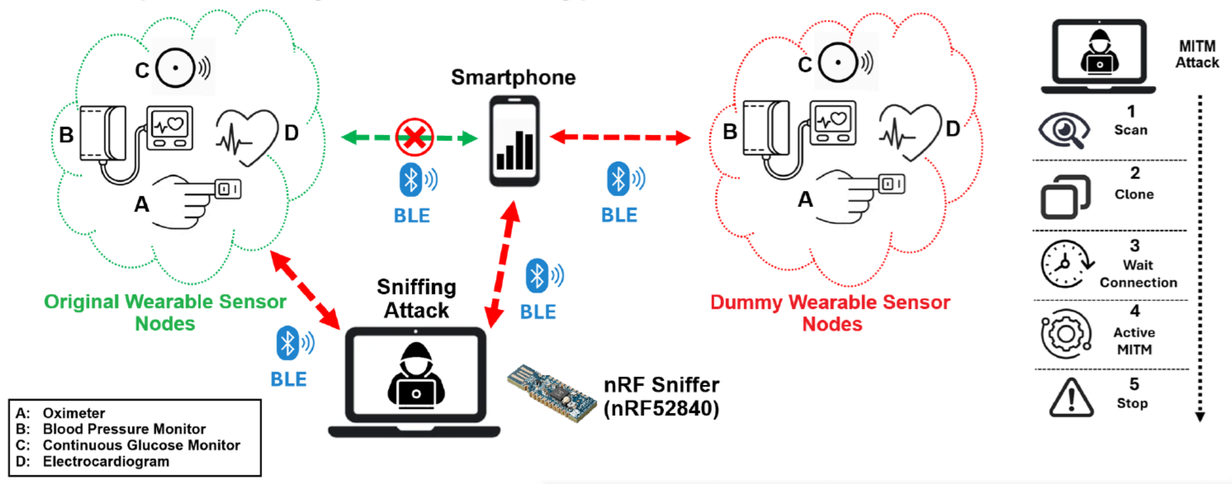
Intra-Body Communication (IBC)

Galvanic Coupling (GC) method is chosen for its performance in the areas of:

- Power consumption
- Tissue safety
- Security
- Transceiver complexity



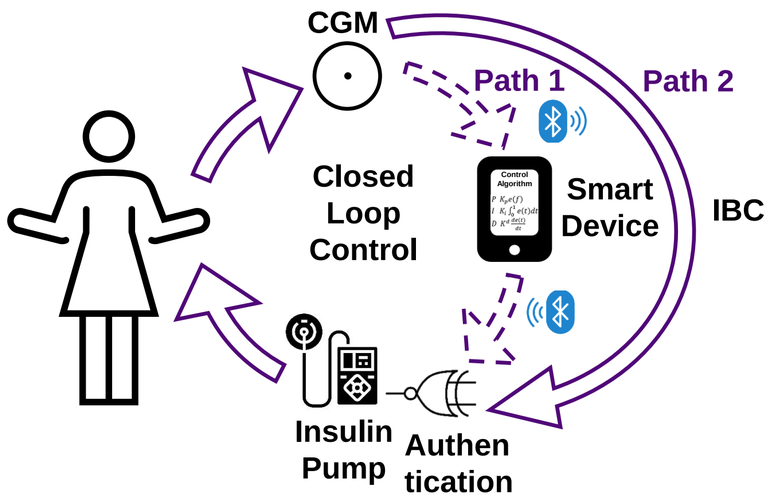
Vulnerability Auditing Methodology



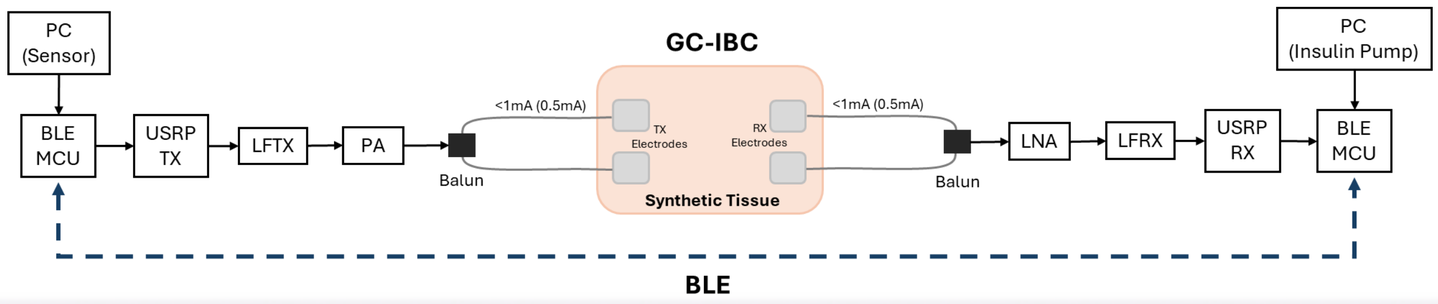
Key Results

Devices	Types of Attacks			
	Sniffing (nRF52840 Nordic Dongle)	Passive MITM (Mirage)	Active MITM (Mirage)	DoS (Mirage)
ECG#1	✓	✓	✓	✓
ECG#2	✓	✗	✗	✓
OXI#1	✓	✓	✓	✓
OXI#2	✓	✓	✓	✓
BPM#1	✓	✓	✓	✓
CGM#1	✓	✗	✗	✓
CGM#2	✓	✗	✗	✓

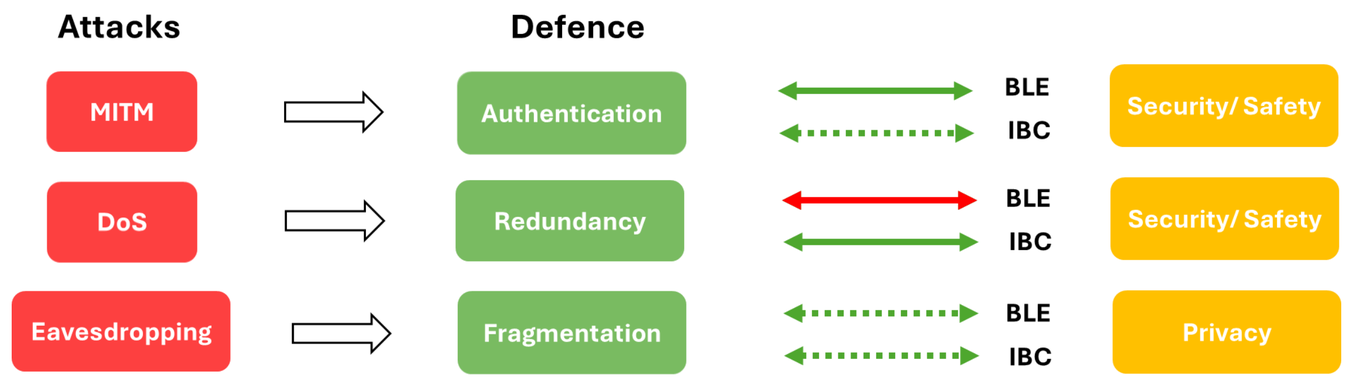
Proposed System Design



GC IBC – BLE Block Diagram



Proposed Defence Mechanism



Publications & Recognition

- **BioSensors 2024 –** Cambridge, UK **– Demo Presentation**
- **RITICS 2024 –** London, UK **– Presentation**
- **EWSN 2024 –** Abu Dhabi, UAE **– Demo Presentation** → **Best Demo Award**
- **EWSN 2024 –** Abu Dhani, UAE **– PhD School Poster Presentation**
- **KFAS 2024-2027 –** Kuwait → **PhD Students Supplementary Fund Grant (£25,000)**
- **ISCAS 2025 –** London, UK **– Conference Paper Presentation**

Conclusion & Future Direction

- Systematic auditing of wearable medical devices:
  → **BLE communication vulnerabilities: sniffing, MITM,** and **DoS** risks.
- Resilient cybernetic safeguarding:
  → **Independent**, **Reliable** and **Redundant** layer of protection.
- **Future works: I**ntegration of **IBC technology** with the **BLE communication** protocol for signal authentication.

E: mohammad.Alhussan.23@ucl.ac.uk T: +44 (0) 73 6580 6677
E: f.boem@ucl.ac.uk T: +44 (0) 20 7679 3966 (int. 33966)
E: s.ghoreishizadeh@ucl.ac.uk T: +44 (0) 20 7679 2000
E: a.mandalari@ucl.ac.uk T: +44 (0) 20 7679 7303 (int. 37303)
University College London, Roberts Building - Department of Electronic & Electrical Engineering, 1108 Torrington Place, London, WC1E 7JE, United Kingdom