Medical Implant Security

Understanding the Need for Secure Implantable Medical Devices

7/04/2025

Anisha Mitra, PhD Scholar, Department of CSE, IIT Kharagpur

Implantable Medical Devices

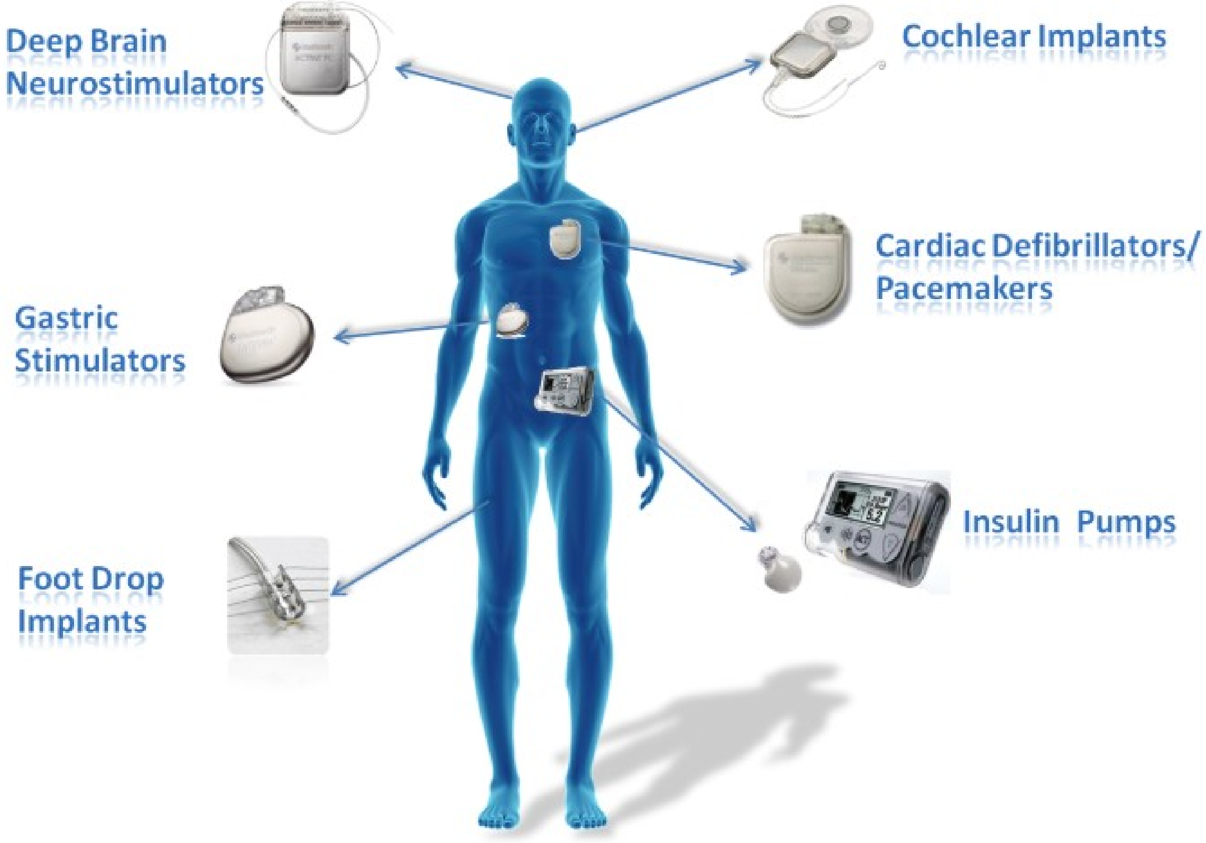
Embedded Technology for Human Health

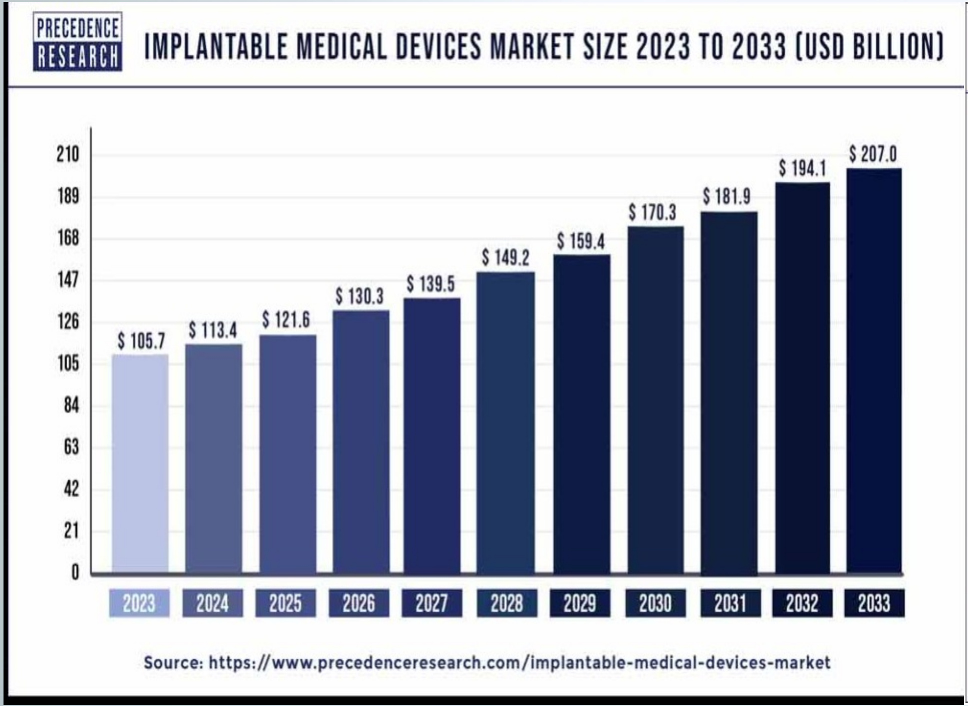
Miniaturized Internal Tech
Implantable medical devices are biocompatible systems inserted into the human body to replace, monitor, or support physiological functions.

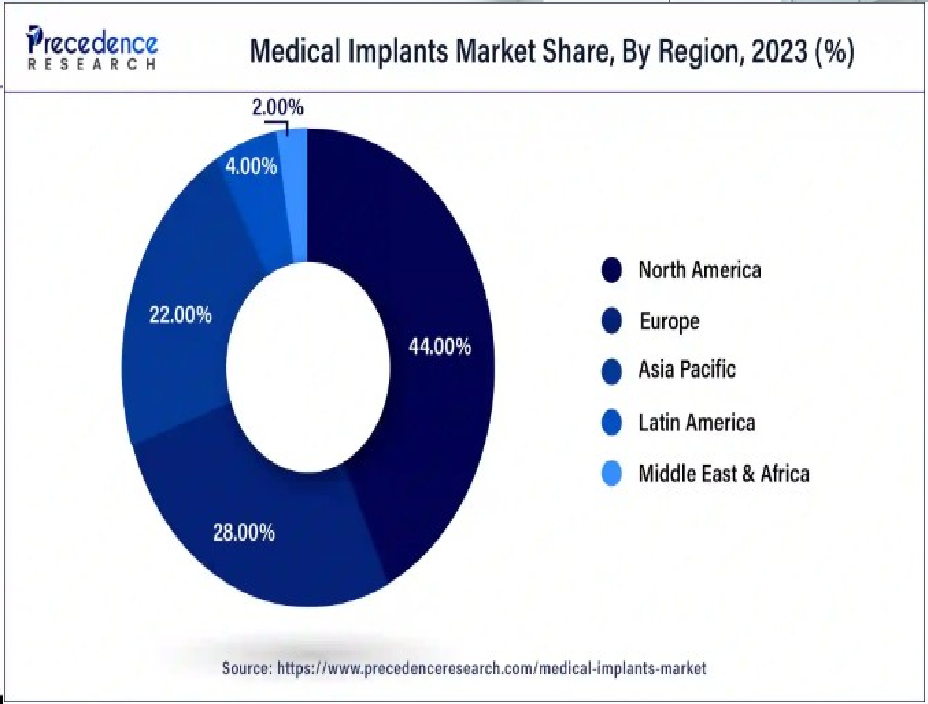
Autonomous Life Management
These devices are designed to operate continuously inside the body, enhancing health outcomes through automated therapeutic intervention.

Why Important?

WIRELESS IMPLANTABLE MEDICAL DEVICES




PRECEDENCE RESEARCH
IMPLANTABLE MEDICAL DEVICES MARKET SIZE 2023 TO 2033 (USD BILLION)
210
189
168
147
126
105
84
63
42
21
0
$ 105.7
$ 113.4
$ 121.6
$ 130.3
$ 139.5
$ 149.2
$ 159.4
$ 170.3
$ 181.9
$ 194.1
$ 207.0
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
Source: https://www.precedenceresearch.com/implantable-medical-devices-market


Precedence RESEARCH
Medical Implants Market Share, By Region, 2023 (%)
2.00%
4.00%
22.00%
44.00%
28.00%
North America
Europe
Asia Pacific
Latin America
Middle East & Africa
Source: https://www.precedenceresearch.com/medical-implants-market

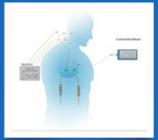
Medical Implant: Vulnerable?

Evaluation of Implant Communication Interface

1958

First Pacemaker

The first implantable pacemaker was developed, operating independently to regulate heart rhythms.



1970s

Telemetry Added

Basic telemetry systems were incorporated into implants, enabling one-way communication to external monitoring equipment.

FOOD AND DRUG ADMINISTRATION FDA

1999

MICS Established

The FCC allocated a specific frequency band for MICS, facilitating reliable, short-range wireless communication for implantable devices.

2006

MedRadio Expansion

MICS was expanded to MedRadio, incorporating additional frequency bands to support a broader range of medical devices with enhanced communication.

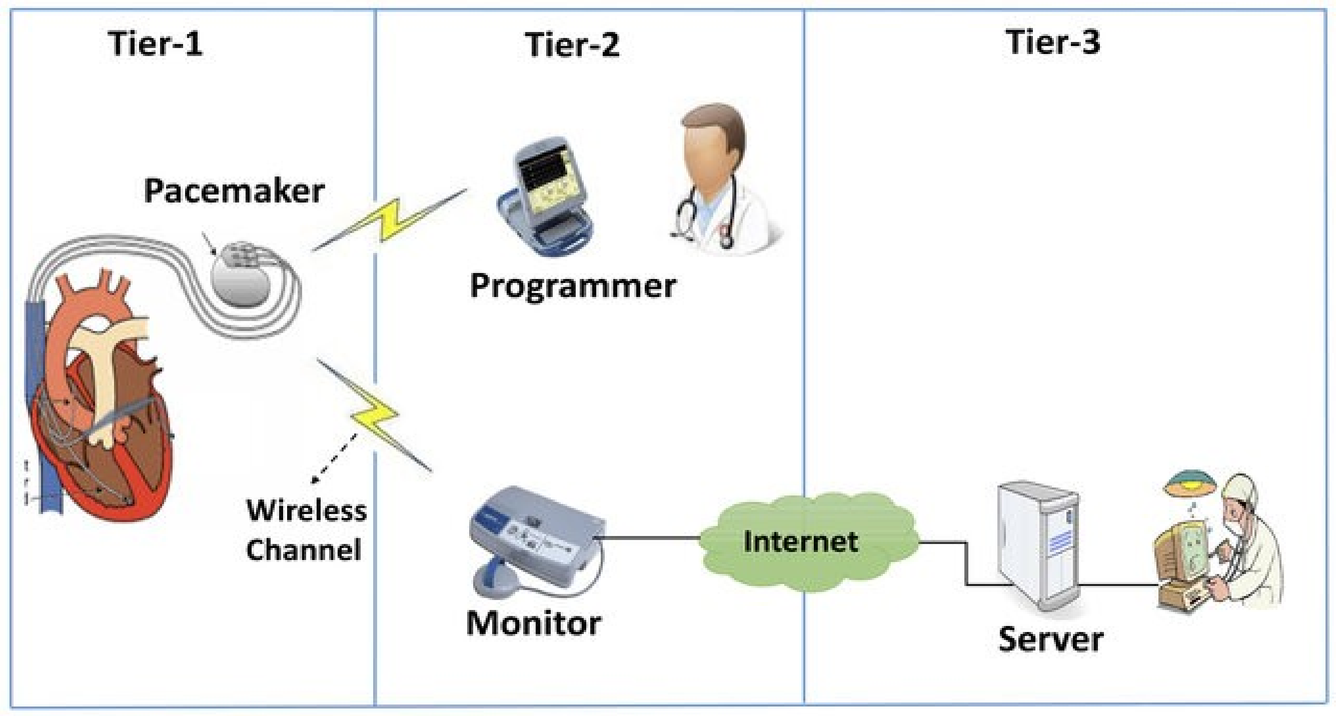
2010s

Bluetooth Integration

Implantable devices began integrating Bluetooth technology, enabling secure, low-power wireless communication with external devices like smartphones and tablets.

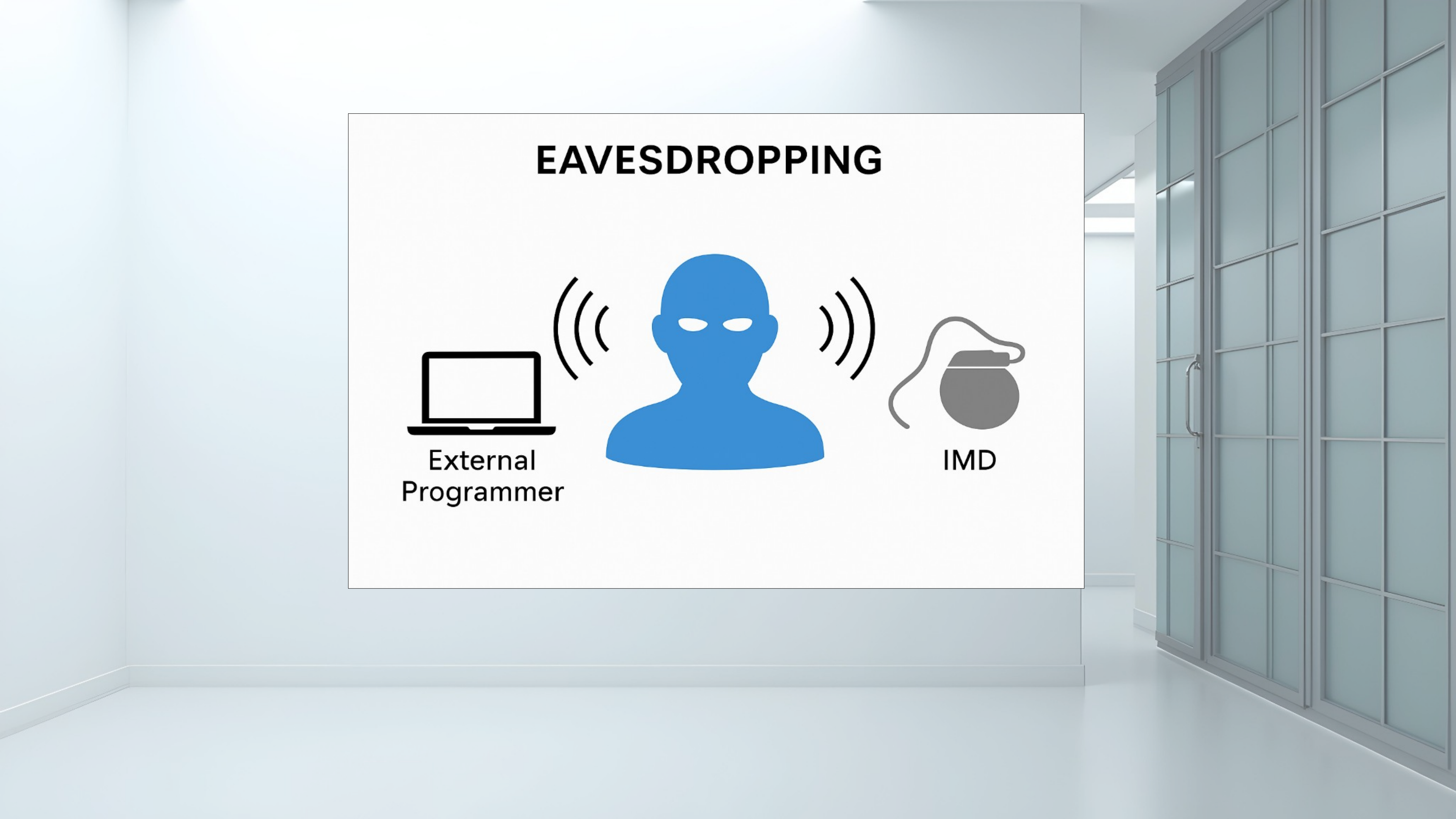
Type 1

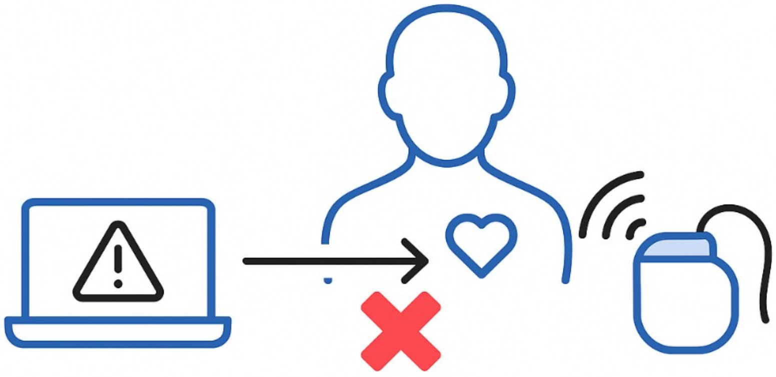
A Typical IMD Communication System- Unauthorized Access



Security Attacks

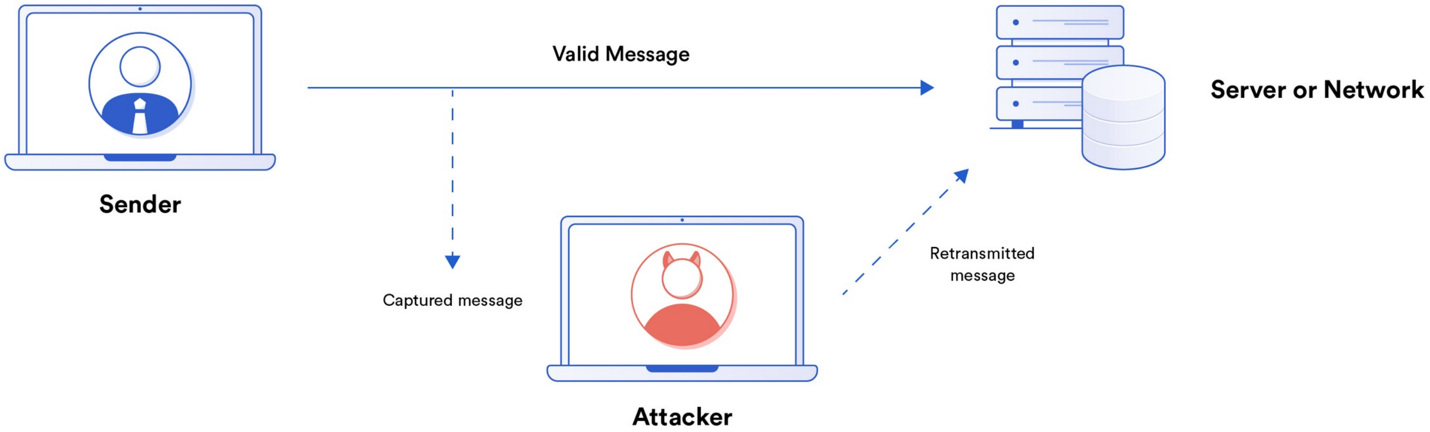
- Eavesdropping Attack
- Denial of Service(DoS) Attack
- Replay Attack
- Man-in-the-Middle Attack
- Software Injection Attack

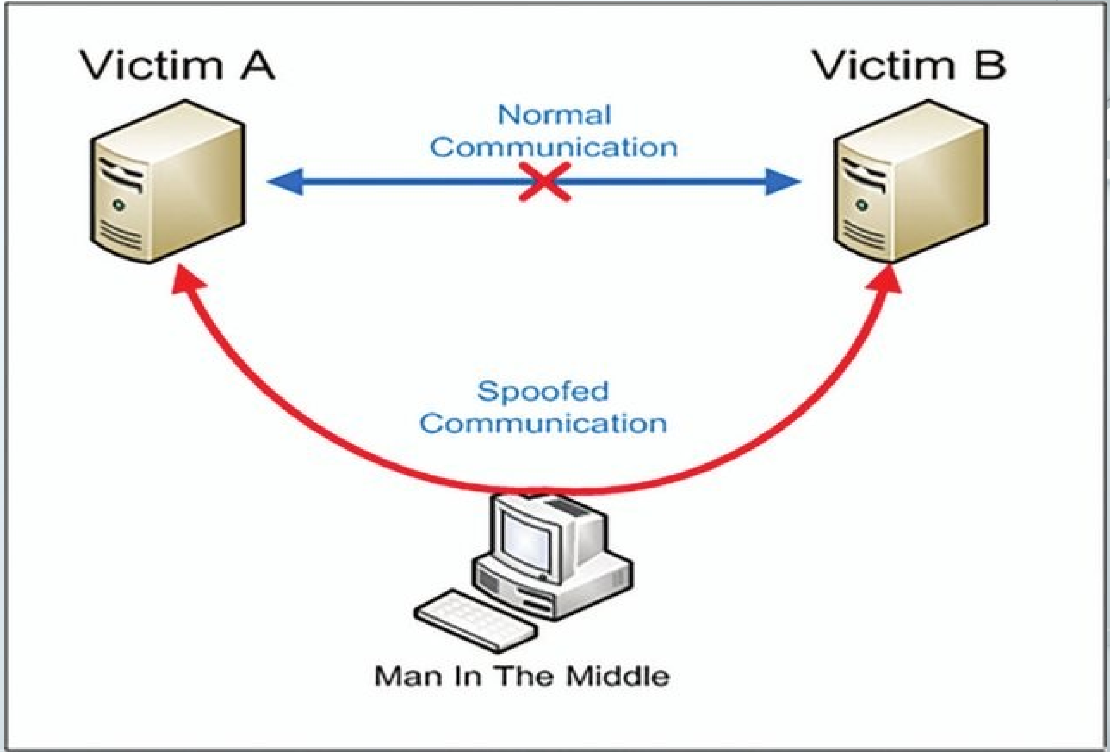

EAVESDROPPING
External
Programmer
IMD



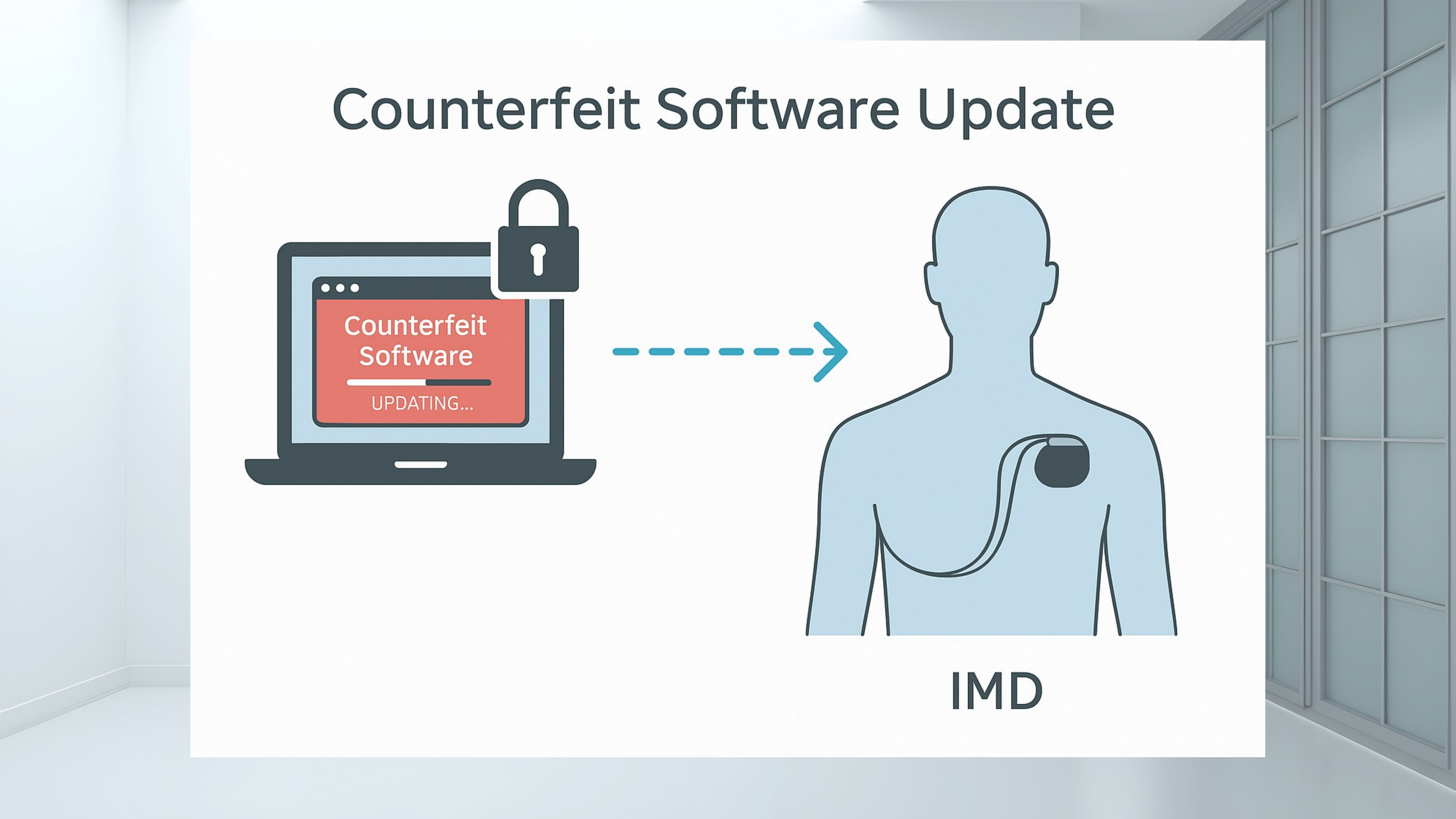
Denial of service

Replay Attack





Victim A
Victim B
Normal
Communication
Spoofed
Communication
Man In The Middle


Counterfeit Software Update
Counterfeit Software
UPDATING...
IMD

Type 2: Medical data Safety

Key Stages & Threat Vectors:

1. Data Collection

Varies by device type (e.g., neural signals require noise filtering).
Trusted sources (hospital firewall) vs. untrusted sources (internet).
Threat: Data manipulation from non-trust zones.

2. Data Transfer

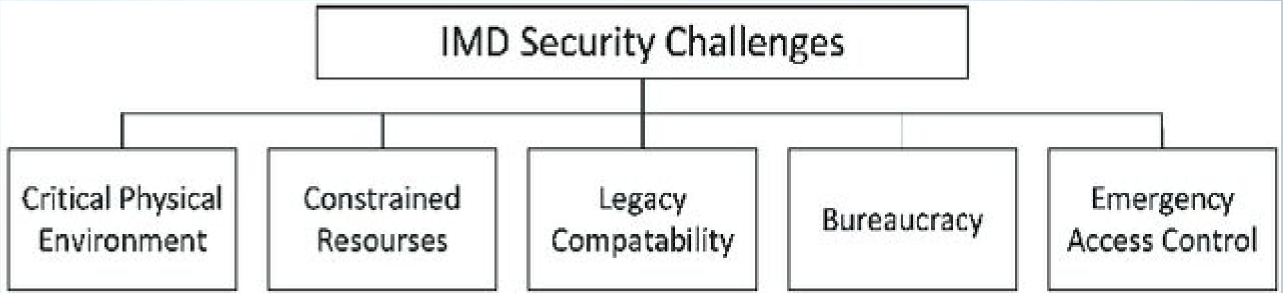
Uses wireless protocols to transmit data to external systems.
Security Concerns: Integrity, confidentiality, and authenticity can be compromised.
Threat: Man-in-the-middle attacks or packet injection.

3. Data at Rest

Stored in hospital servers, cloud platforms, or databases.
Threat: Unauthorized access, tampering, or ransomware attacks.

Attack Type	Implications
Eavesdropping	Unauthorized access to sensitive patient data, violating privacy
Denial of Service (DoS)	Depletes device battery, prevents normal operation
Replay Attack	Reuses previously captured valid commands to manipulate device behavior
Man-in-the-Middle (MITM)	Intercepts/modifies communication between IMD and external devices
Software Injection Attack	Malicious commands alter device functionality or compromise its operation
Medical Data Manipulation	Leads to incorrect diagnosis or therapy due to altered or falsified patient data

CHALLENGES AND SECURITY TRADE-OFFS IN IMDs


IMD Security Challenges
Critical Physical Environment
Constrained Resourses
Legacy Compatability
Bureaucracy
Emergency Access Control

Critical Physical Environment

- **Biocompatibility:**
 Made from non-reactive materials like titanium/silicone,
 but may still trigger rejection or inflammation in some patients.

- **Form Factor:**
Must be compact and lightweight to avoid disrupting daily activities.

- **Thermal & RF Limits:**
Security mechanisms must respect limits on **heat dissipation** and **RF radiation** to prevent tissue damage or allergic responses.

Resource Constraints

- **Non-rechargeable batteries** with a lifespan of **8–10 years**.
- **Efficient power management** is critical for both processing and communication tasks.
- **Traditional cryptographic methods** (e.g., symmetric encryption, PKI, hashing) are **resource-intensive**.
- Frequent cryptographic operations can **drain the battery prematurely**.
- **Battery depletion** requires **surgical replacement**, posing health risks.

Legacy Compatibility

- **Updating cryptographic protocols** often requires **modifying the IMD hardware**.

- **Millions of legacy IMDs** are already implanted and remain **vulnerable**.

- **~700,000 new cardiac implants** are added **each year**.

- Ideal security solutions should also **protect already-implanted devices** without needing surgical updates.

Bureaucracy

- **Security updates** require **regulatory approval** due to impact on
- IMD functionality.

- In the **U.S., FDA approval** is mandatory and may take up to **7 years**.

- **Bureaucratic delays** make it difficult to quickly adopt new solutions.

- By the time approval is granted, the solution may be **outdated** due
- to **technological advances**.

Security Trade-Offs

Security
vs
Accessibility

Normal
vs
Emergency

🛡️ *Medical Device Recalls Due to Cybersecurity Vulnerabilities*

Year	Device Model	Reason for Recall
2017	*St. Jude Medical Cardiac Devices*	Vulnerabilities enabled unauthorized control—risk of battery depletion or pacing hacks
2019	*Medtronic MiniMed 508 & Paradigm Pumps*	Unencrypted wireless communication could be exploited to deliver incorrect insulin
2020	*BD Alaris System Infusion Pumps*	Cyber flaws in software could allow remote tampering with infusion settings
2021	*Medtronic MyCareLink Patient Monitors*	Vulnerabilities in third-party communication stack (URGENT/11) posed risk

Case Study:
Implantable Cardioverter Defibrillator(ICD) Security

Emerging IMD: Implantable Cardioverter Defibrillator

Figure: INOGENTM EL ICD by Boston Scientific [3]

Parts of an ICD

- Pulse Generator
- Electrodes

ICD Therapies

- Anti-tachycardia pacing(ATP)
- Cardioversion
- Defibrillation
- Bradycardia pacing

- Apart from the conventional ICDs, implanted under the skin, there is now a **Subcutaneous** version.

Primary Security Breach: ICD Communication environment

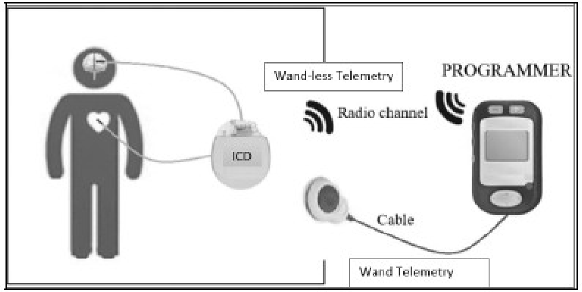


Figure: ICD Telemetry Service [5]

Telemetry Service

- Inductive coil telemetry using inductive Radio Frequency (RF) field(0-300 kHz) for proximity based communication.
- RF link telemetry using Medical Implant Communication System(MICS) [402-405 MHz] frequency band.
- This communication interfaces though beneficial for treatment delivery can turn into a significant attack surface.

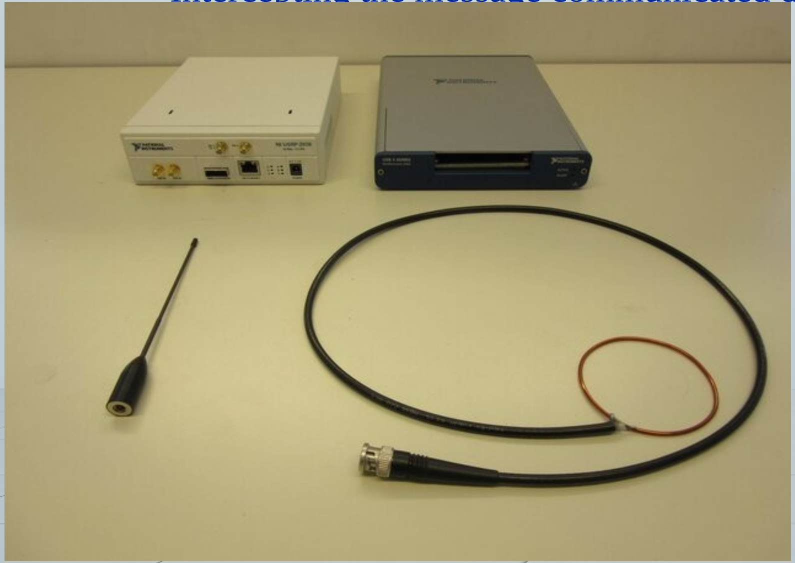
Attack Approach

- Employing a **Black box** approach to analyse the underlying proprietary protocol
- between ICD-Device programmer.

- Reverse engineering the underlying long-range communication protocol by

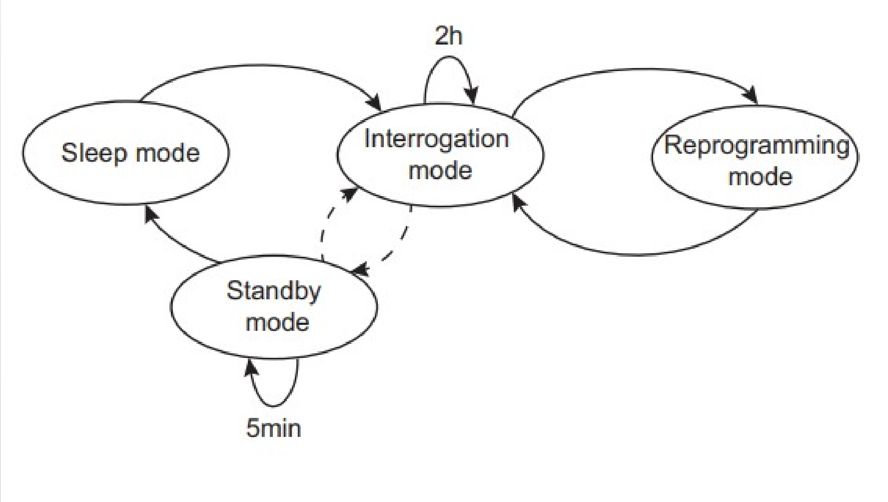
  - Identifying the wireless transmission parameter
  - Intercepting the message communicated during ICD-device programmer

- **Equipment used**



Hardware	**Software**
Universal Software Radio Peripheral(USRP)	Transmitter & Receiver Program
A data acquisition System (DAQ)	
A few Antennas	
A base station	
A few ICD models	

ICD Activation



- **Exploit an Active Session**
- **Standby Mode usage**
- **Wake up ICD from ‘Sleep’ mode**
- **Using a legitimate external device**

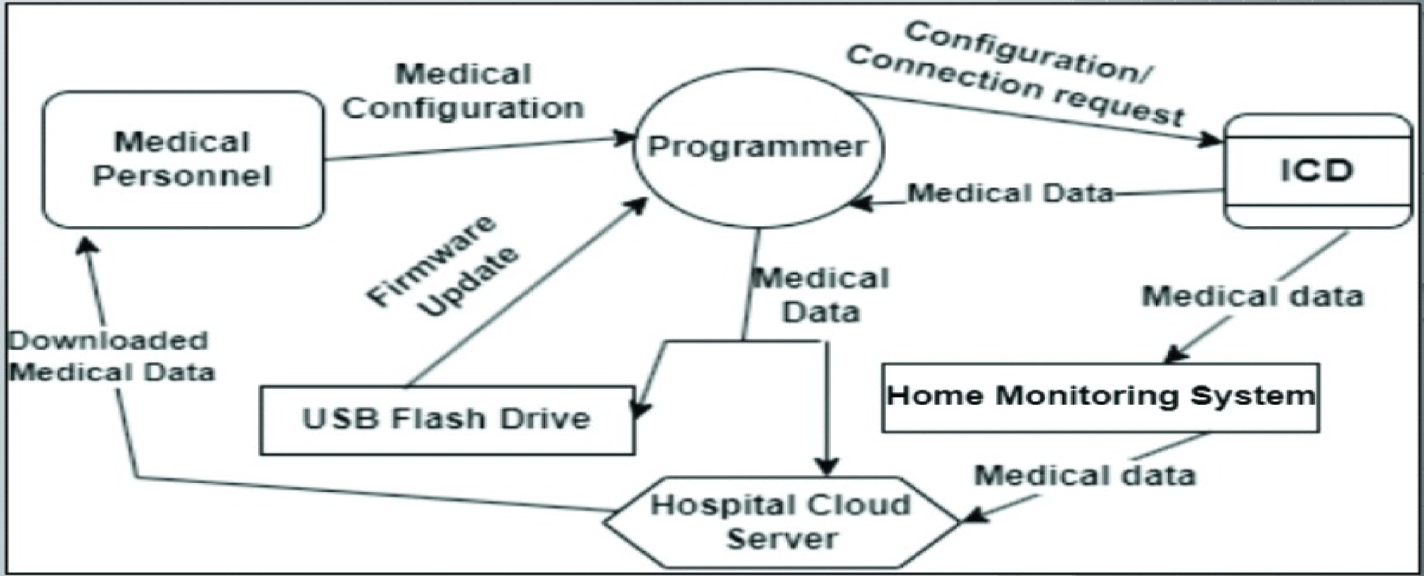
Marin et al., ACSAC 2016: On the (In)Security of Modern Implantable Cardiac Defibrillators – https://doi.org/10.1145/2991079.2991094

Data Manipulation Attack

Data Manipulation attacks on ICD environment

- An ICD delivers therapy based on some pre-programmed configurations which can be modified by a programmer.
- Various external communication paths existing in the ICD environment become vulnerable in the presence of an adversary.
- An unintended programming error or malfunctioning programmer can launch most threatening **Data Manipulation (DM) attack**.

Different DM attack flows on ICD environment



Countermeasures

A pseudo Command Set for ICD Functionalities

- ICDs' working depends on the detection of Ventricular Arrhythmias based on mainly two characteristics: **Heart Rate** and **Arrhythmias duration** [3].
- A pseudo command set is proposed based on identified primary functionalities of market-available ICDs.

Functionalities	**Purpose**	**Pseudo Command**
Tachycardia Zone Detection	VT1 rate/interval	SET VT1 GT value1
	VT2 rate/interval	SET VT2 GT value2
	VF rate/interval	SET VF GT valueF
Tachycardia detection counter or interval	VT1 detection counter	SET VT1 time1
	VT2 detection counter	SET VT2 time2
	VF detection counter	SET VF timeF
Shock dose releases after VF detections	VF first shock	VF1 REL dose-v1
	VF second shock	VF2 REL dose-v2
	VF 3-n^{th} shock	VF3n REL dose-vn
Tachycardia detection enable/disable	To decide whether to enable or disable tachycardia detection	ENL DET ON/OFF
Beeper control	Alerts about inappropriate ICD conditions	DISABLE BEEP

Figure: A Glimpse of the proposed Pseudo Command Set

Data manipulation attack (DMA) scenarios in ICD environment

SI. NO.	Pseudo Command	Identified modification	Possible outcome
1.	SET VT1 GT value1	value1 = 100(bpm)	May provide electric shock when not required
2.	SET VT2 GT value2	value2 = 120(bpm)	
3.	SET VT1 time1	time1 $<$ 10	May cause unnecessary ICD intervention
4.	SET VT2 time2	time2 $<$ 10	
5.	VF1 REL dose-v1 VF2 REL dose-v2	(i) dose-v1 $<$ 10 or dose-v1 $>$ 80 Joule (ii) dose-v2 $<$ 10 or dose-v2 $>$ 80 Joule	May not terminate VF, can lead to death
		(iii) dose-v1 $>$ dose-v2	When 1st shock dose value is greater than 2nd shock dose value it fails to terminate VF, can lead to death
6.	DISABLE BEEP	Execute this command unnecessarily	Removes beeper functionality
7.	VF1 REL dose-v1 VF2 REL dose-v2 VF3n REL dose-vn	dose-v1 = 1(Joule), dose-v2 = 2(Joule), dose-vn = 0[OFF]	In case of VF, the ICD will provide only two shocks of very low energy which will not stop arrhythmias and can lead to death

Figure: Some DMA scenarios in ICD environment

Pseudo Command	Legitimate Shock delivery
• **VF1 REL dose-v1** • **VF2 REL dose-v2**	**'dose-v1' and 'dose-v2' should range between 10 to 80 Joule**

Adversarial modification

- **Case 1:** Attacker changes and sets either **dose-v1** or **dose-v2** to be less than 10 Joule or both.
  Low energy shock cannot halt detected Ventricular Fibrillation (VF).
- **Case 2:** Attacker changes and sets either **dose-v1** or **dose-v2** to be greater than 80 Joule or both.
  Unnecessary high-energy shock can lead to a patient's death.
- **Case 3:** Attacker sets a moderate value for **dose-v1** (10 to 80 Joule) but for **dose-v2**, a value less than **dose-v1**.
  Do not terminate VF.

Security Goals

ICD's resource-contained, vulnerable environment necessitates two security goals: **Confidentiality, Integrity**

Confidentiality	Integrity
• Security Primitives: Encryption and Authentication • Functional instructions consisting of parameter values • Parameter values consist of information about patient-specific health conditions.	• Security Primitive: Authentication • Functional instructions consisting of generic information • Instructions to change ICD operating modes, abort or start specific therapies, etc.

Data Transmission Protocol for ICD-Programmer Communication

- A comprehensive, secure protocol for ICD-programmer communication emphasises authenticated, unmodified message delivery.
- This security protocol consists of certain security primitives:
  - **Key Management**
  - **Lightweight Encryption Scheme**
  - **Lightweight Authentication scheme**

Key Management and Lightweight Encryption Scheme

Key Management

- Two secret keys are considered for Encryption and Authentication schemes respectively
- We plan to utilise the dynamic key concept to provide a higher level of security
- Key revocation for various emergency conditions involving patients, medical practitioners must be taken into consideration

Lightweight Encryption Scheme

- Resource-constrained ICD environment cannot support resource-consuming traditional encryption ciphers
- We prefer to propose a lightweight ARX based cipher design for the secure protocol

A Lightweight Authentication Scheme

- Authentication of the secret message prevents revelation, deception, and modification of message content.
- During ICD-Programmer communication, at the programmer's end, an authentication **Tag** is computed on the transmitting data, which gets recomputed and verified at the ICD's end.
- Any adversarial modification to the transmitted data leads to incorrect tag generation.

Resource Depletion Attack

Resource Depletion Attacks on ICD Environment

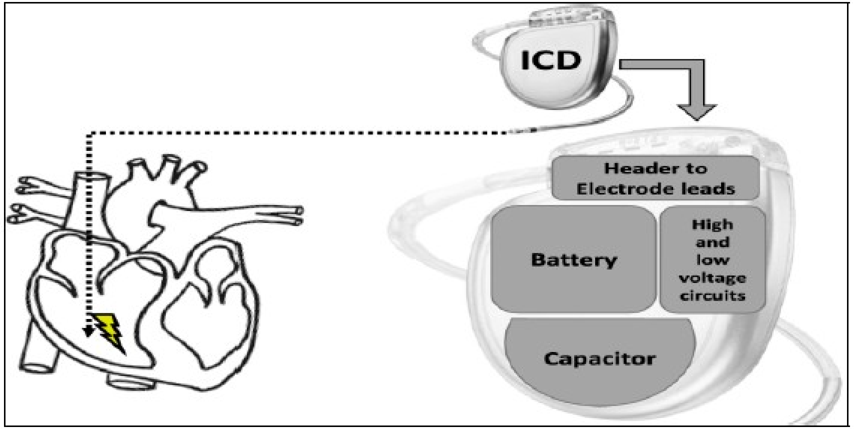


Figure: ICD Components [4]

- Battery-powered ICD environment is vulnerable to rapid battery depletion attack.
- Resource Depletion can lead to Denial of Service (DoS).
- ICD's telemetry service is exploited to launch Resource Depletion attacks.

Resource Depletion Attack Models

1. Attacks on Low Power Modes of ICD

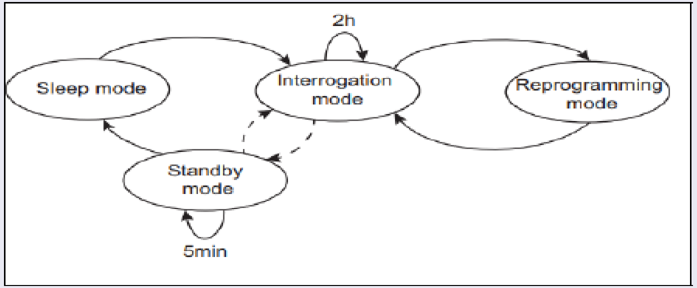


Figure: ICD modes of operation[6]

- Attacker's target ICDs power-conserving **'Sleep'** and **'Standby'** mode.
- **Barrage Attack:** Attackers prevent ICD from entering 'Sleep mode' by bombarding it with genuine access requests.
- **Sleep Deprivation Attack:** Attackers do not let ICD leave 'Standby mode'.

A. Mitra and D. Roy Chowdhury, ICMC 2024 – *Guarding the Beats: Defending Resource Depletion Attacks on ICDs*, LNNS, Springer.
doi: 10.1007/978-981-97-2069-9_17

Algorithm 1 Barrage Attack

$i \leftarrow 1$; $n \leftarrow N$; ▷ Consider 'N' to be a large value
while TRUE **do**
L1:
  if 'ICD' is in 'SM' **then** ▷ Sleep Mode: 'SM'
    Attacker $\xrightarrow[\text{with 'M'}]{\text{Access Request}}$ 'ICD' ▷ 'M' defines Attacker's identification
    for $i = 1, \ldots, n$ **do** ▷ Checks 'M' for Authentication
      if Authorised **then**
        Release Access Grant
        Attacker $\xrightarrow[\text{with 'M'}]{\text{Access Request}}$ 'ICD'
      else
        delay(5) ▷ Wait for '5 minutes' for 'standby' mode to end
        goto L1
      end if
    end for
  end if
end while

Algorithm 2 Sleep Deprivation Attack

$i \leftarrow 1$; $n \leftarrow N$; ▷ Consider 'N' to be a large value
for $i = 1, \ldots, n$ **do**
L2:
    if 'ICD' is in 'SB' **then** ▷ Standby Mode: 'SB'
        Attacker $\xrightarrow[\text{message}]{\text{A Specific}}$ 'ICD'
        delay(4) ▷ Wait for '4 minutes' to keep the ICD in 'Standby' mode
        goto L2
    end if
end for

2.Prolonged Telemetry Communication

- Attackers target ICDs magnet based short-range communication.
- Using a strong magnet, the ICD is kept in telemetry interrogation mode.

Algorithm 3 Prolonged Telemetry Communication

```
i ← 1; n ← N;                                          ▷ Consider 'N' to be a large value
for i = 1, . . . , n do
    if 'Wand-telemetry' is established then
        L3: Replay 'Wand-less telemetry' initiation Command
        if 'Wand-less Telemetry' is enabled then
            wait(60)                                   ▷ Wait for 'one hour'
            goto L3
        end if
    end if
end for
```

3.Electromagnetic Interference on the Wireless Channel(Jamming)

- **Step 1:** Attacker checks if any active session is going on between ICD and programmer.
- **Step 2:** If no ongoing active session exists, go to **Step 1**.
- **Step 3:** If there is an active session, then the attacker sends high power noise signal at ICD's reception frequency.
- **Step 4:** Disrupts ICD's ongoing session.
- **Step 5:** ICD raises signal power to receive legitimate telemetry data.

4. Device Functional Parameter Modification

- Functional Model-based ICDs working depends on certain programmable parameters.
- **Pulse Amplitude** and **Pulse Width** may control battery longevity and potential battery drain.
- The number of high-energy shocks delivered in a single session may affect battery performance.

Attacker's approach

- Record RF signal involving target parameter change.
- Replay recorded RF signal with attacker specified values.

Table: Malicious Device Parameter Modification

Sl. NO.	Parameters	Identified modification
1.	Atrium pulse amplitude (P.A.)	P.A. = 7.5
	Left Ventricular pulse amplitude (L.V.A.)	L.V.A. = 7.5
	Right Ventricular pulse amplitude (R.V.A.)	R.V.A. = 7.5
2.	Atrium pulse width (P.W.)	P.W. = 1.5
	Left Ventricular pulse width (L.V.W.)	L.V.W. = 0.4
	Right Ventricular pulse width (R.V.W.)	R.V.W. = 0.4
3.	Maximum shock delivery (maxsh)	maxsh » 5

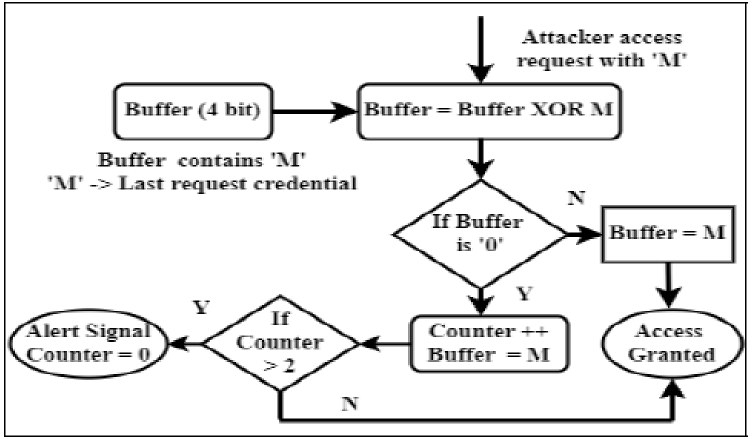
Countermeasures

Possible Countermeasures

- **Attacks on Low Power Modes of ICD**

Assumptions

- ICD uses a 4-bit buffer and a 2-bit counter.
- Counter is initialized to zero, a threshold of 3 is set.
- Buffer stores the ID of the user sending an access request in the most recent past.
- The counter keeps track of the consecutive requests sent by the same user.



- **Resource depletion attack involving a strong magnet can be stopped by using a timer.**
- **Jamming attacks requires anti-jamming techniques.**
- **Secure Programmer-ICD communication using lightweight authenticated encryption to prevent malicious parameter modification.**

Future Scope

- Complete Software Simulation and real-time simulation of the proposed scheme in an ICD environment
- Future emphasis is placed on the necessity of collaboration with device manufacturers, healthcare institutions, and regulatory boards
- The future objective is to establish a standardized, real-time legal framework for medical implant security assessments that extends beyond national boundaries

Thank you!

Do you have any questions?