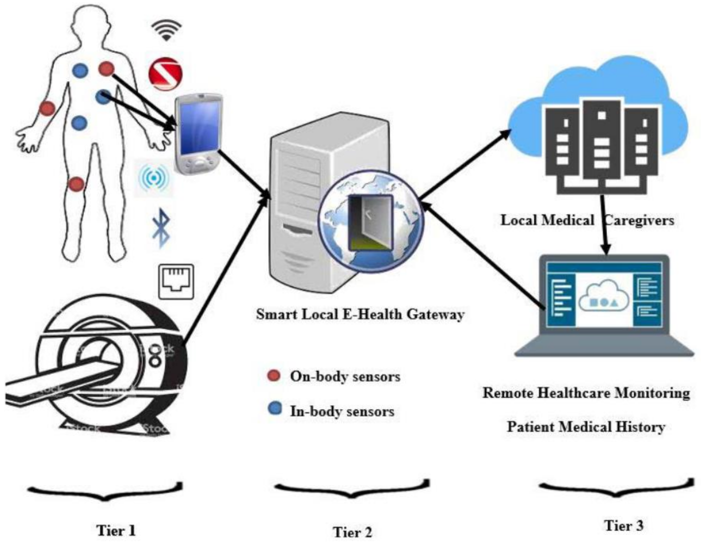
Attacks, Vulnerabilities and Countermeasures in Implantable Medical Devices

Paoletti Riccardo

Introduction

- Medical devices are different from others in terms of design, implementation, and application.
- **Reducing energy consumption** is still one of the top priorities in **Implantable Medical Devices (IMD)** design.
- Complicated cryptographic computations and long-range wireless transmissions are considered **unaffordable**.
- **Wireless communication** and **networking capabilities** in IMD are the major source of security risks.
- Healthcare have a **huge attack surface**, something like 10-15 different MDs per bed in hospital.

Overview of Networked Medical Devices



- These devices incorporate intelligent and small sensors to be used on human body → **WBAN** (Wireless Body Area Network).
- **Medical Devices communication architecture**: three-tier level
  - **Tier 1**: sensors on human body that gather information and transmit them to a gateway (BCU). Also, medical equipment connected to internet.
  - **Tier 2**: transmission of data from tier 1 to a smart local gateway. It performs operations on data and provides data access to health providers.
  - **Tier 3**: cloud computing used to store information gathered. Performs several analysis and delivers a GUI for feedback and visualization.

Demonstrated Cyber Attacks on Medical Devices

- **Firmware modification attack**: attacker tries to modify programs stored in non-volatile memory that controls hardware of devices.
- **Eavesdropping**: interception of user information by an unauthorized entity.
- **Sniffing**: sniff traffics and perform analysis.
- **Information disclosure**: information exposure by unauthorized entity due to weakness in device communication medium.
- **MITM**: interception between two legitimate parties.

Demonstrated Cyber Attacks on Medical Devices – cont.ed

- **Replay attack**: obtaining valid packet data transmitted by medical devices with intention to use it in a new protocol run.
- **Tampering and Modification attack**: alteration in data without proper authorization.
- **DOS, Resource depletion and Jamming attack**: disabling the devices by exhausting their energy.
- **Side channel attack**: consists in analysing power consumption and electromagnetic radiations multiple times to extract secret information.
- **Other attacks**: hardware Trojan, buffer overflow attack, brute force attack, grey hole, sybil attack, masquerading attack, remote code execution…

Security Policies in Medical Devices

- **Need to define security policies** in order to face the attacks.
- **Food and Drug Administration (FDA)** categorizes medical devices in **three categories** according to the risk
  - **Class I**: simple devices, free from controls;
  - **Class II**: more security issues, more concerned about effectiveness and safety;
  - **Class III**: highest danger and most stringent controls.
- **Medical Device Directive (MDD)** regulates marketing and safety for medical devices in Europe since 1990s.

Countermeasure

- Definition: any change to a system that decrease the success probability of an attacker.
- Classification
  - **Prevent** – deception, honeypot.
  - **Resist** – resiliency, robustness.
  - **Detect** – intrusion detection, consistency check.
  - **Recovery** – hetereogeneity, cold/hot redundancy.
  - **React** – change to architecture/configuration/application.
- No action is taken on the attacking system because of steppingstones and high number of attackers.

Countermeasures for securing MDs

- **Low power sensor-based devices** are ill-prepared in security challenges and exposed to attacks.
- Similarly, **on-site medical equipment** lacks security features due to age.
- For **internet connected devices** is very important to secure both hardware and software layers.
- Due to the different nature of these devices, common security mechanisms cannot be used.
- Some **state-of-art countermeasures** are listed in the following.

Bad Memory Management and Buffer Overflows

- In order to detect those attacks, two approaches are proposed.
- **First approach**: based on **path signatures**. A **hash** is calculated based on execution path. Every time the execution flow changes, a **comulative hash is computed**. A **Verifier** (remote) uses this hash to **validate the execution flow** of the program. Still vulnerable to control flow hijacking.
- **Second approach**: identify each vertex of the **execution flow graph** with a **label**, then each label is verified during the execution. Here **control flow hijacking is easily detected**, but it’s still vulnerable to data attacks.

Isolation-Based Mechanisms

- These techniques are used to **reduce attack surface** and to **isolate resources** of particular applications in distinct spaces.
- Resources in **trusted areas** are inaccessible from untrusted ones.
- **CPU provides APIs** to use special memory areas, called **enclaves**, separated from other processes and reachable from **distintc entry points**.
- In other cases, segregation is made with **hardware primitives** and uses **Memory Protection Unit (MPU)**.

Data Flow Integrity

- Three programming techniques are proposed in order to **increase the robustness** of the implementation.
- **Storing pointers' base and limit** in an **unaccessible area** in the hardware, and marking each pointer at compilation time. **Validity is checked on access**, and unauthorized modification is detected **checking the stored pointers values**. (Dynamic)
- **Encrypting pointers** in memory and **before data is retrieved, decrypt them**. If modified, decryption fails. **No protection from direct modification of pointer value**. (Dynamic)
- **Keep track of the write instructions** performed being able to **distinguish data corruption**. (Reactive)

Bio-Cryptographic Key Generation Schemes

- Cryptography can be helpful in order to **secure communication and data stored**, so key generation schemes are needed.
- **Physiological features**, being random, work well for keys.
- Frequent approaches include
  - **time-domain** physiological parameter generation (IPI).
  - **frequency-domain** physiological parameter generation (CPSD).
  - **heathbeat-based Random Binary Sequences (RBSs)** to secure communications
- **128-bit RBSs** are generated from ECG signals in order to **authenticate users**.

Fuzzy Vault Physiological Scheme

- Being classic cryptographic schemes not always possible to implement, other mechanisms have to be tried, like **Fuzzy Vault**.
- The schema improves security by **minimizing the rate of data exchange** during the key management process and thus increasing **network lifetime** and **energy efficiency**.
- However, security of such schema is **totally dependent on the size of the vault** and it’s **weak because of the small size of the attributes**, infact it’s demonstrated that an adversary can estimate appropriate points in the vault.

Lightweight Encryption and Key Management Protocol

- **Vibration-Based lightweight** and **ultra low-battery key exchange protocol** can be used between **external** and **wearable** devices.
- In order to **exchange key**, the external device produces a key and turns it into a **vibration signal**. On the other side, the wearable device receives signals and, using **two-feature On-Off Keying (OOK) demodulation mechanism**, transforms the signal into bit strings and encrypts further communications.
- Anyway, the **key could be extracted** by an adversary since it’s just electromagnetic waves.

Proximity-Based Scheme

- Based on **plaintext authentication scheme** to prevent **replay**, **resource depletion**, **DOS** and **MITM** attacks. Packets travel not encrypted.
- Uses **Diffie-Hellman modified (DHM)** approach, with **packet expiration time** and **time constraint mechanisms** to authenticate users.
- Since **it does not use encryption techniques**, it puts the privacy of users in danger.

BLE Security Mechanisms

- **Four secure pairing approaches** are proposed. When someone near turns itself on, device starts transmitting packets to pair.
- **Simplest approach**: just working and does not involve the user. Suitable for wearables (MITM, identity tracking, sniffing).
- **Second approach**: needs a UI. Pairing for the first time, both pheriferal and central devices will exhibit a 4/6-digit code to connect (sniffing, identity tracking).
- **Third approach**: based on passkey entry. Both devices need interface. More secure (but still identity tracking).
- **Fourth approach**: ECC Diffie-Hellman (ECDH). Prevent also identity tracking with Resolvable Private Address (RPA) scheme to randomize the MAC address.

Access Control

- Every access to every object must be checked for authority. Each not controlled operation is a potential vulnerability.
- IMDs support remote access by the doctors of the hospital, so cyber attacks directed to the hospital network/server may steal private patient’s data or credentials.
- For this reason, a **lightweight but effective access control scheme** for IMDs is higly desiderable.

Three general categories for existing IMD access control schemes

- **Direct** access control with **preloaded keys**
- **Direct** access control with **temporary keys**
- **Indirect** Access Control **via Proxy**

Let’s see them one by one.

Direct access control with preloaded keys

1. Common master key **Km** for all commercial programmers. Each IMD **i** has a device-specific key **K = f(Km, i)**, with **f** cryptographic function. To access IMD **i**, programmer first request its identity **i**, and a nonce **N**, and then it computes **K = f(Km, i)** and **R = RC5(K, N)**. IMD verifies **R** and grants access.
2. IMD and programmer **share a key** used to **encrypt a sequence number**. Access is granted if the difference of the sequence numbers is **within a set range**. Also a **wake up code** is given to the programmer, that is checked by the IMD before waking up, in order to **prevent resource depletion attacks**.
3. IMD programmer obtains the key **right before** he attempts to access the IMD, either using physical characteristics of the human body, or an item possessed by the patient. **Danger**: adversary could obtain bio-features stealthy, and permanent access.

Direct access control with temporary keys

- **IMD** and **programmer extract features** from the same source at the same time, and **generate temporary keys based on them**. **Proximity-based methods** can be used:
  - **Biometrics** – ECG signals are random and to gather them you have to be close.
  - **Body-Coupled Communication** – human body as medium, range very short, less power consumption.
  - **Vibration** – Short range, requires contact. Need to mask sound to avoid eavesdropping.
  - **Audio and Ultrasound** – audio channel-based key exchange method. IMD generates random value as session key and broadcasts it as a modulated soundwave. Vulnerable to eavesdropping.
  - **Near Field Communication (NFC)** – Short range. Round trip time to delete replay attack.

Indirect Access Control via Proxy

- **External device (proxy)** usually is a **wearable/smartphone** which has **more computational resources** than IMD.
- Communication between IMD and proxy are protected with **lightweight symmetric encryption** and access control is **delegated to the proxy**. More sofisticated access control schemes, but also **increse vulnerability surface**.
- In case of emergency can be disabled.
- Several types:
  - **Friendly Jamming** – Cloaker, IMDGuard, base station shield (weak).
  - **Gateway** – non-key scheme, external proxy embedded in gateway.
  - **Mobile Device** – motion-based key generation methods.

Machine Learning Approaches

- **Anomaly-Based Intrusion Detection**
  Decision tree algorithm to **detect data injection attacks** on MD.
  Normal behaviour is tracked, **if deviation then an attack is detected**.
- **Authentication**
  Makes use of **physiological parameters** like calorie burn, average step count, minute hearth rate and metabolic activity, **with help of machine learning classifiers** like SVM, trees, and ensemble **to authenticate users**.
  WARNING: Consumes a lot of energy so that **can influence medical processes**.

Hybrid Mechanisms

- Use two cryptosystems (**symmetic** and **asymmetric**) to ensure **authentication** and **confidentiality**.
- To secure wearables with authorized apps, **OS level access control mechanisms** can be used. **They produce/apply security policies automatically**. Once a device pairs with another, the model checks bonding policy and its compliance. In case the app is in connecting policy, the connection will be established, otherwise refused. Also **biometrics are used for authentication**.
- **FitLock**: bind and upload procedure to **connect devices to social network accounts**. Takes **<ID,shared key>** and returns **6-digits random monotonically increasing code** to connect for one session (**Prevent replay attacks**).

External Mechanisms

- **IMD Shield**: full-duplex **radio device:** a **receiver** and a **jamming antenna**. The receiver obtains a signal and deciphers it. Jamming antenna, meanwhile, transfers an arbitrary flag to **prevent eavesdropping**.
- **IMDGuard**: uses **ECG signals** for key exchange. A **challenge-response technique** is used to enter an **emergency mode**: device sends two challenges at different time intervals. It authenticates the programmer verifying the signature of the device (Prone to MITM).
- **Cloaker**: important device to **provide security to IMD**. While turned on, **implantable devices simply ignore all requests**. Otherwise, IMD accept all requests. Prone to jamming.

Future Directions

- **Technical Countermeasures**
  - **On-site** MDs – upgrade software, self-authentication, access control.
  - **Implantable/Wearable** MDs – boost accuracy, trust, security, communication and firmware integrity check.
  - **Communication Technologies** – BLE security, drop radio interference.
- **Regulatory Countermeasures**
  - **FDA** – insert **security section in regulations**, unify security approach
  - **MDD** – **harmonize security standards** across EU members.
- **Online Authentication** – medical treatment over **long-range**, **high bandwidth secure wireless links.**
- **Low-Power and Zero-Power Authentication** – harvest energy from an external source without drawing energy from primary battery.

Thank You