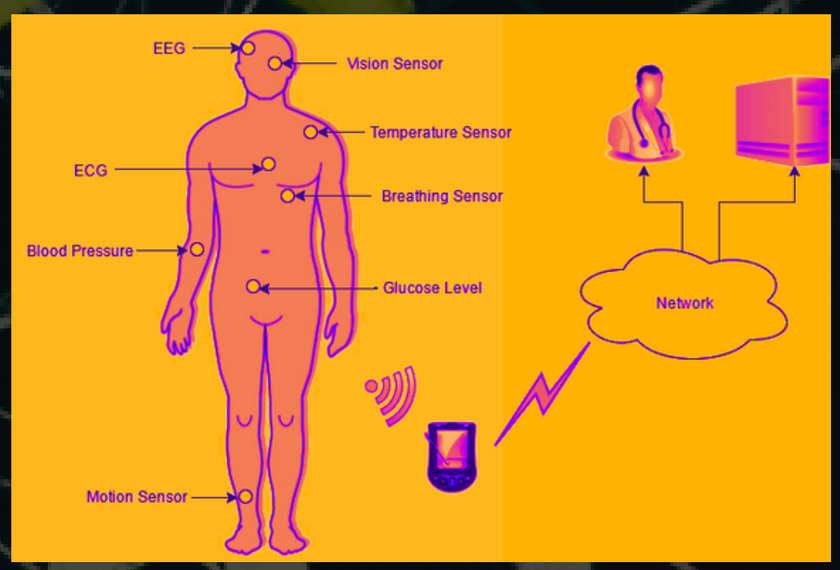
The Security of Wireless Body Area Network Communications (WBANs)

COM6017 - Security of Control and Embedded Systems
Jagpreet Jakhar

Introduction

A Wireless Body Area Network (WBAN) connects independent nodes (e.g. sensors and actuators) that are situated in the clothes, on the body or under the skin of a person. The network typically expands over the whole human body and the nodes are connected through a wireless communication channel.[2]
The IEEE 802.15 Standard governs the standard for implementation of WBANs.



Major Threats:

As WBANs mainly communicate over Radio Frequency or over Wireless Networks, they are susceptible to same threats these technologies face, but because of the role they play , for example an Cardiac implant or Insulin Pump, the repercussions can be deadly, as was evident when doctors deactivated US Vice-President's heart implant fearing hacking.[3]

Major threats to WBANs on different levels include:

A) **Hardware**:
- Hardware Trojans inserted during production manipulating the device's intended functionality.

B) **Software**:
- Outdated Operating systems allowing privilege escalation or data leak, for example WannaCry Ransomware.
- Malware or Ransomware attack, fo example Kwampirs malware can trigger equipment malfunction.
- Counterfeit firmware Update, for example Fitbit and Garmin fitness watch makers lack integrity check for firmware updates.
- Electroencephalography (EEG) attacks:An attacker developed a malicious software called brain spyware that was integrated into a Brain-Computer-Inteface device to detect private information of the user[5]

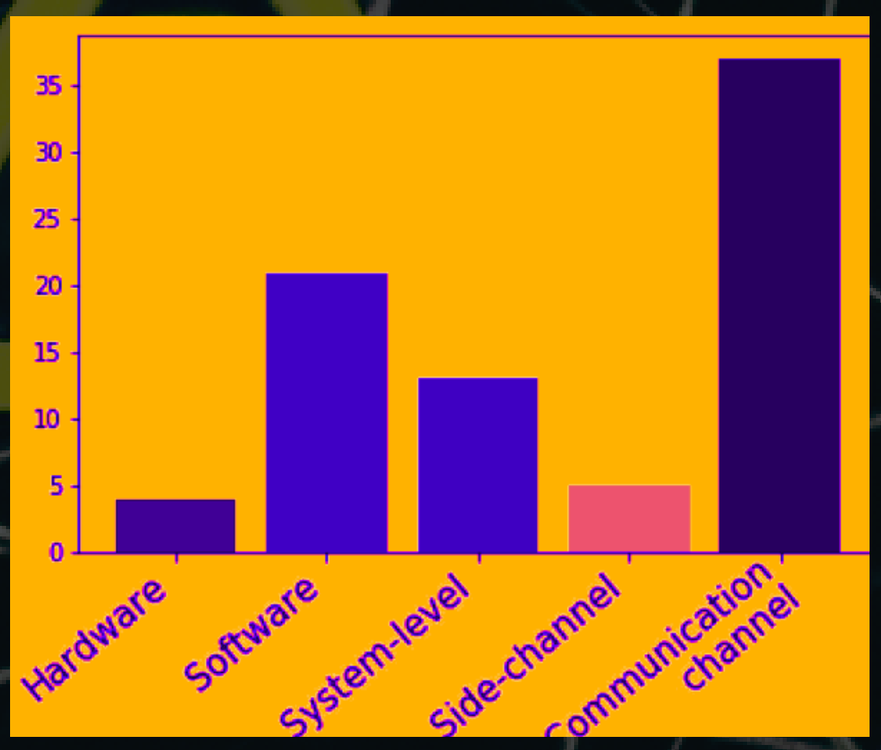
C) **System Level**:
- Breaking weak authentication systems to allow illegal access of data or privilege escalation.

D) **Communication Channels**:
- Eavesdropping using sniffing tools or man in the middle attacks to leak sensitive data- TISmartRF-Wireshark.
- Using Man in the Middle attacks to Impersonate and alter functioning of devices through commands.
- Denial of Service through flooding of network using SYN packet flood or other
- Depleting Battery by sending and receiving useless data or denial of sleep attack

E) **Side Channel Attacks**:
- Electromagnetic interference to deny proper functioning.
- Spoofing Sensors by manipulating sensor data.

Solutions:

Several solutions have been developed to address the security challenges in WBANs by maintaining confidentiality, integrity, and availability of these devices.
These include:
- **Electric Current Analysis** to detect Hardware level anomalies.
- **Encryption**: PRESENT and KATAN lightweight hardware-oriented block ciphers can be useful as these devices are generally low power.
- **Machine Learning** approaches like decision trees or support vector machines to detect atacks.
- **Blockchain** Based record keeping for securing data, for example GHOSTDAG, a novel and unique blockchain protocol for remote patient monitoring
- **Shielding and filtering** to protect against electromagnetic attacks for example Faraday Cages.
- Using Near Field Communication Protocols or RFID protocols to secure the network, forcing the attacker to be proximate to conduct an attack.
- **Access Control Mechanisms**: They can be proximity based, identity based or role based to secure the access and control of device and data, for example using physical obfuscated key (POK)-based access control mechanism where researchers leveraged Integrated Circuit cards of POKs for secure credential storage.
- External Devices to secure the network, for example Medmon uses different physical characteristics (i.e., received signal strength indicator (RSSI), time of arrival, differential time of arrival) to detect signal anomalies in transmission and alerts users regarding the attack.



Threats by Components

Future Challenges:

"Connecting everything to each other via the internet will expose new vulnerabilities"-Bruce Schneier[6]
Despite the existing solutions, there are several challenges that need to be addressed to ensure the security of WBANs in the future.
These include:

1. **Resource Constraints**: WBANs have limited resources in terms of processing power, memory, and energy. Security solutions that are too resource-intensive may not be feasible.
2. **Interoperability**: WBANs often consist of devices from different vendors with different protocols and security mechanisms. Ensuring interoperability and compatibility between these devices can be challenging.
3. **Current software verification** tools are written in a high-level programming language, which are not suitable for platform-specific and low-level applications of these devices.
4. Use of different communication protocols like Zigbee, make it harder to agree on a common set of security practices and standards.
5. **Lack of awareness** in consumers using these devices about their security vulnerabilities
6. **Optimization** Of Network Resources: To develop ultra low radio power levels for transmission and reception that are safe for human use.

References :

1) Image:https://www.everythingrf.com/community/what-is-wban-or-ieee-802-15-6
2) https://www.waves.intec.ugent.be/research/wireless-body-area-networks
3) https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/
4) A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses-AKM Iqridar Newaz, Amit Kumar Sikder, Mohammad Ashiqur Rahman, A. Selcuk Uluagac
5) I. Martinovic, D. Davies, M. Frank, D. Perito, T. Ros, and D. Song, "On the feasibility of side-channel attacks with brain-computer interfaces." in USENIX security symposium, 2012, pp. 143–158.
6) https://www.schneier.com/blog/archives/2017/02/security_and_th.html
7) C. A. Chin, G. V. Crosby, T. Ghosh and R. Murimi, "Advances and challenges of wireless body area networks for healthcare applications," 2012 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 2012, pp. 99-103, doi: 10.1109/ICCNC.2012.6167576.