Intrusion in IoT Devices

Various Intrusion Techniques

Abir, Aditya, Dhruv, Mihir, Mohak, Rajat

AN ACTIVE MAN-IN-THE-MIDDLE ATTACK ON BLUETOOTH SMART DEVICES

This paper surveys the key security issues in the BLE protocol and discusses a possible architecture for BLE **Man-in-the-Middle (MitM) attacks** together with the related necessary equipment.

- **Security manager** - is in charge of the security capabilities of the protocol: pairing integrity, authentication and encryption.The way the encryption keys are exchanged is insecure and introduces some severe security vulnerabilities.
- **Pairing** - BLE uses the Secure Simple Pairing model in which devices can choose to operate with one of the following methods
    - **Just Works** - Temporary Key (TK) is set to 0, offers no protection at all against MitM attacks. Only possible method that can be employed with devices lacking a display
    - **Passkey** - TK is a six-digit number combination, which the user actively inserts into one of the devices, thus manually exchanging it between the devices.it was proven that also this method can be bypassed.
    - **Out-of-Band** - OOB pairing is the most secure method available in the BLE 4.0/4.1 protocol. Unfortunately, this method is still very uncommon

AN ACTIVE MAN-IN-THE-MIDDLE ATTACK ON BLUETOOTH SMART DEVICES

- **GATT (Generic Attribute Profile)** - The GATT describes the device roles and general behaviors employing hierarchy of services, characteristics, and attributes.

- **BLE connection flow** - In a typical BLE connection flow a smart device continuously broadcasts an advertisement, in order to allow a mobile app to identify and connect to it.This flow enables potential hackers to discover the device services, clone them and re-publish them, in order to lure the victim into their ‘trap’.

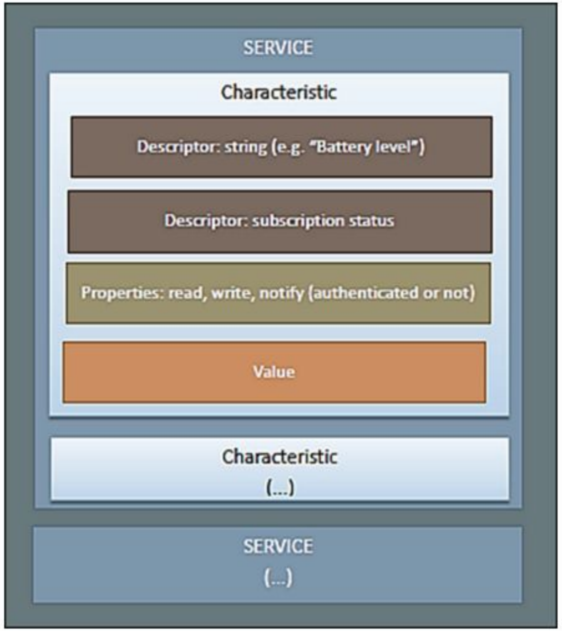

SERVICE
Characteristic
Descriptor: string (e.g. “Battery level”)
Descriptor: subscription status
Properties: read, write, notify (authenticated or not)
Value
Characteristic
(...)
SERVICE
(...)

Figure 2: GATT Profile Hierarchy.

PRACTICAL MITM ATTACK FOR BLE

BLE MitM needs to make use of two BLE components capable of acting together: one connects to the mobile app acting as the smart device, while the other connects to the smart device acting as the mobile app.

It is required that the fake mobile app and the fake smart device exchange the data that each of them received

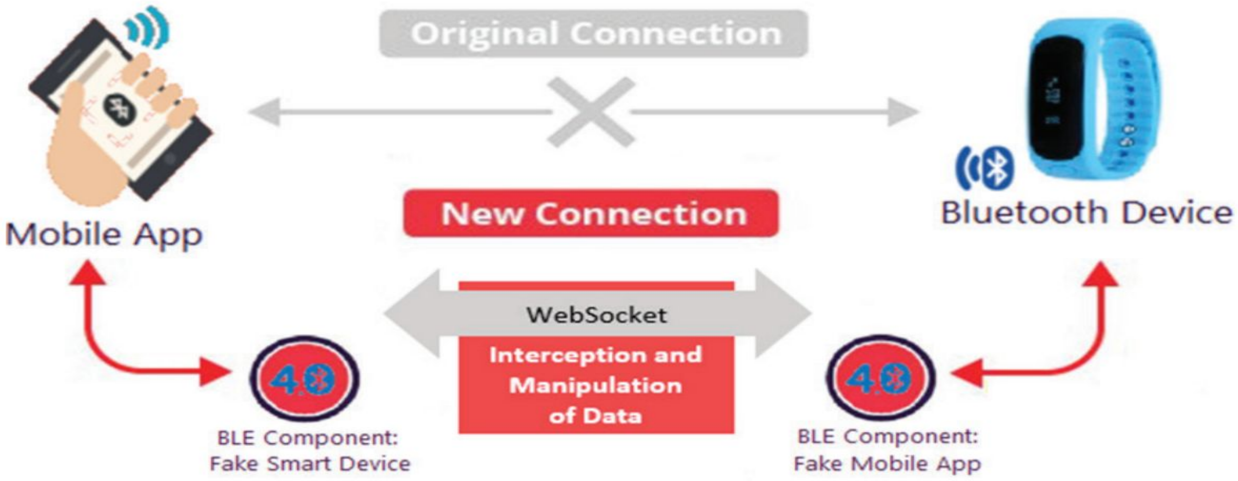

Original Connection
Mobile App
Bluetooth Device
New Connection
WebSocket
Interception and Manipulation of Data
4.0
BLE Component: Fake Smart Device
4.0
BLE Component: Fake Mobile App

Figure 6: Practical man-in-the-middle architecture for BLE.

AVAILABLE TOOLS BASED ON THE BLE MITM ARCHITECTURE

1. **GATTacker** - a Node.js package for BLE MitM
   prerequisite libraries - noble, a NodeJS BLE central module, bleno
   GATTacker can scan and copy BLE advertisements and services which can then be used to run a cloned (fake) version of the smart device. The hacker can intercept and manipulate the transmitted data.

2. **BtleJuice** - a framework to perform MitM attacks on Bluetooth Smart devices
   BtleJuice includes a web interface and – among other useful features – presents Replay GATT operations (Replay attack) and On-the-fly data modification capabilities (Hooking).

CASE-STUDY: HACKING A BLUETOOTH SMART MOBILE APP AND CONCLUSION

- Running GATTacker central (ws-slave) on one VM and running the GATTacker peripheral configured to the ws-slave's IP address.
- Burp ,i.e. a proxy tool that supports WebSocket communication,allowed to intercept and modify the data using Burp Intercept feature.
- If the victim has previously paired the mobile app with the smart device, the mobile app will automatically connect to the fake device, provided that the latter presents the MAC address of the real smart device using MAC spoofing. By advertising the name of the targeted smart device, GATTacker can lure the victim to connect to the fake device.
- It was also possible to take a picture on the victim's mobile device, to play music directly on the victim's mobile.
- With the release of the Bluetooth Core Specification version 4.2, BLE Security has been significantly improved by the new LE Secure Connections pairing model, which includes the Elliptical Curve Diffie-Hellman (ECDH) algorithm for key exchange.

DOS Attacks on devices Paired with Google Home Mini

Denial of Service Attacks: DoS attack is a type of cyber-attack in which a malicious attacker aims to render a computer or IoT device unavailable by interrupting the device's service.

DoS attacks harm by overwhelming a victim machine with requests until normal traffic is unable to be processed, resulting in a denial of service to users.

Materials Required For a DOS attack

1) Google Home Mini

2) **Kali linux**: It is a Linux based Debian operating system. Additional libraries required are:-

   Bluez (bluez.org) is a library that provides the Bluetooth layer and protocol requirements necessary for us to use Bluetooth on our Kali Linux operating system

   Hcitool library, “hcitool scan” command finds those MAC addresses with their device names.

Materials Required for a DOS Attack

We will perform DOS attacks using 3 different softwares:-

1) **L2ping**: L2ping allows us to send packets to Bluetooth devices. During performing l2ping, we need to determine some parameters such as "-i", "-s", "-f". In this study, our Bluetooth adapter was hci0. Mac addresses are scanned by -f command

2) **Blue doser**: Bluedoser is a tool used to perform DoS attacks to disrupt the Bluetooth function. Bluedoser automatically tries to detect the surrounding Bluetooth devices and lists detected devices to the attacker with their MAC address.

3) **Bluetooth Dos Script**: Working same as Blu Doser, but allows thread count to be a parameter as well.

Results

1) **L2ping**: L2ping attack was failed even though the Bluetooth headphone accepted the packets. The packages sent couldn’t be received because the speakers already had a bluetooth connection to the GHM.
2) **Bluedoser**: In the attack on the connected speakers expected success was not achieved and the Bluetooth connection could not be disconnected. When the attack is performed on unpaired Bluetooth headphones and then tried to connect to the GHM which was not possible.
3) **BDS**: The attack on the connection between the GHM and bluetooth speakers was a success and the bluetooth connection was disabled. Experimentally the ideal thread count was found to be 7.

Conclusion

In conclusion, attacks that were performed using l2ping, Bluedoser, and Bluetooth DoS script (BDS) were observed. No success was achieved using Bluedoser and l2ping against Bluetooth headphones and other Bluetooth speakers. Attack, which was performed using BDS against Bluetooth headphones, was able to disconnect Bluetooth service and victim headphone was denied of service.

Successful DoS attack was performed on the device which supports more than one Bluetooth connection. Other devices didn't support more than one Bluetooth connection, so they didn't accept packets while the DoS attack was performed.

IDS Architecture and Phases

Architecture: Entire Process logic is performed by an internal node, the watchdog which classifies all the traffic that passes through and detects threats. Operations of the watchdog can be divided into two phases:-

1) **Learning Phase**: Classifier Machine learning model created by training a shallow neural network to identify traffic flow patterns. Consists of preprocessing and training

    a) **Preprocessing**: Data extracted from available datasets is properly filtered and manipulated to avoid biased configuration
    b) **Training**: ML model trained using the processed data

2) **Detection Phase**: After the training, the model is saved and uploaded on the watchdog, making the IDS to be fully active in the network.

Conducting the Attacks

1. **Targeted Grey Hole attack network setup**
   Targets only one of the servers, the others elements connected to the malicious relay are not affected at all, having their messages correctly forwarded for the whole duration of the experiment. The attack follows a binomial distribution with a success probability of 0.5, thus fulfilling the partial loss of victim’s packets and so the partial denial of service.

2. **Black Hole attack network setup**
   While some of the devices could eventually keep communicating with the rest of the network, the remaining affected devices are completely excluded from any form of service, ending up in a shadow zone .

IDS Evaluation

Two main tools for evaluation confusion matrix and Receiver Operating Characteristic (ROC) curve:-

1) **Confusion matrix**: First few columns show some false negatives, that is IDS has good accuracy but has a serious issue making a distinction between grey and black hole attacks.

2) **ROC Curve**: This metric is used to evaluate classifier output for different time windows.

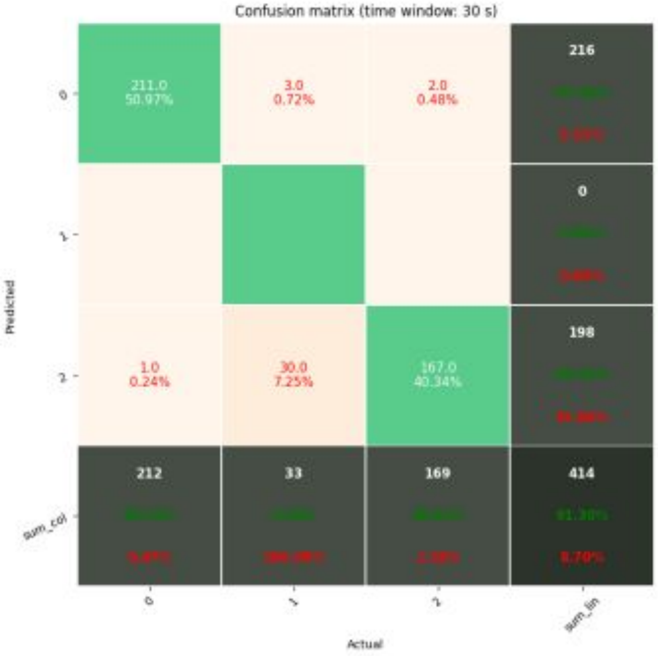
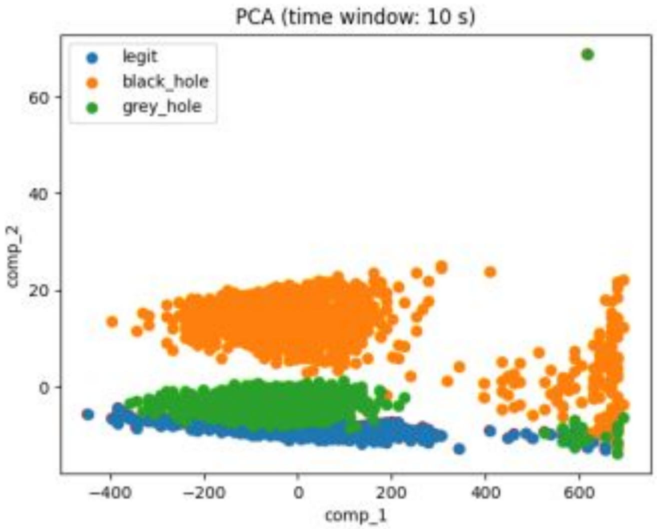


Fig. 4. Confusion matrix ($t = 30$).

RESULT AND CONCLUSION

- IDS allows the detecting of the ongoing anomalies with a strong accuracy, but its performances strongly degrades when it comes the time to understand what exactly the aforementioned anomalies are.

- Therefore, while the IDS has proved to have excellent potentialities and while this approach can be successful even in large implementations, the experiments done so far have been insufficient to give a more precise accuracy range.



Bluetooth Speakers

Attack Methodology :- No extra connection needs to be established.

- Directly injecting voice command signals into analog circuit of microphone.

- Frequency of intruding voice signals will not be in 20Hz - 20KHz. Hence, the attack is hidden from human ear. Usually, it is lower than audible frequency.

- The injected signal exploits the *non-linearity* of microphone circuits to manifest as an attack.

- Non-linearity :- S(out) = x . S(in) + y . S(in)^2....

- The (inaudible) attack signal is multiplied with high-freq carrier signal, and the squared term S(in)^2 propels the low-frequency attack signal into audible range, by doubling it's frequency.

- The math is pretty straightforward. Low-pass filter in the circuitry eliminates all high freq (carrier wave) components, leaving behind only the attack signal with twice the freq.

- Hence, rather than directly multiplying carrier wave with the attack signal, the square rooted wave (with an added DC signal) is used, to accentuate the original attack freq.

Bluetooth Speakers - The KNOB Attack

- Type of MITM attack. Allows 2 paired BLE devices to connect without authentication.

- When 2 devices negotiate, they agree upon a particular encryption. The *Key Negotiation of Bluetooth (KNOB) Attack* exploits a vulnerability in the bluetooth specification that affects the encryption process. **KNOB forces the devices to use a weaker encryption.**

- It lowers the entropy of the link to 1-byte. The level of entropy indicates how much encryption changes over time, and is the most significant determinant of Bluetooth security.

- Hijacker must be physically close to the 2 Bluetooth devices. Also, only a concise time window to interrupt the handshake and force a different encryption.

- Once the link is decrypted using KNOB, it can be passed onto a controlled hijacking Bluetooth session. The MITM framework can be setup with all the previously discussed tools, like BtleJuice, Kali Linux, BlueZ, Metasploit, etc.

Personal Medical Devices

- An attacker capable of exploiting well-known vulnerabilities in communication protocols like BLE or Wi-Fi could gain access to sensitive healthcare data from PMDs devices.

- An external attacker can gain access to PMD traffic simply using publicly available tools and software to eavesdrop sensitive patient information, while also disrupting the PMD’s communication via Denial of-Service (DoS), Man-in-the-Middle (MITM), replay, and false data injection attacks.

- All of the PMDs included in this research use the ”just works” pairing method, which is a very simple authentication mechanism that has been proven to be vulnerable to brute force attacks and eavesdrop on the connection.

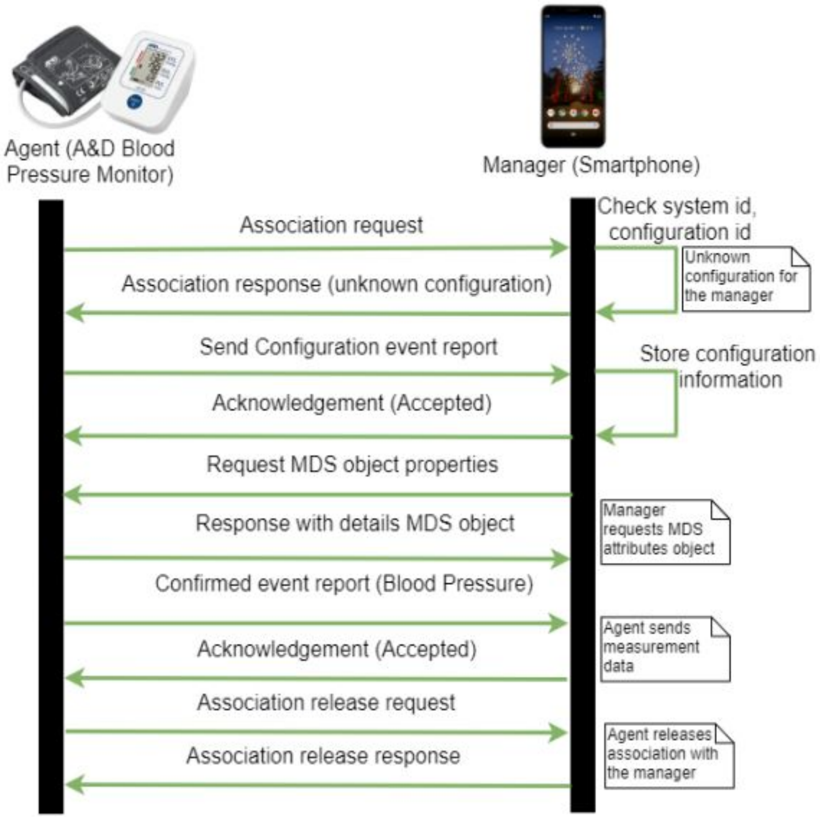

Agent (A&D Blood Pressure Monitor)
Manager (Smartphone)
Association request
Check system id, configuration id
Unknown configuration for the manager
Association response (unknown configuration)
Send Configuration event report
Store configuration information
Acknowledgement (Accepted)
Request MDS object properties
Manager requests MDS attributes object
Response with details MDS object
Confirmed event report (Blood Pressure)
Agent sends measurement data
Acknowledgement (Accepted)
Association release request
Agent releases association with the manager
Association release response

Fig. 1: An example of data exchange diagram between a PMD and its manager.

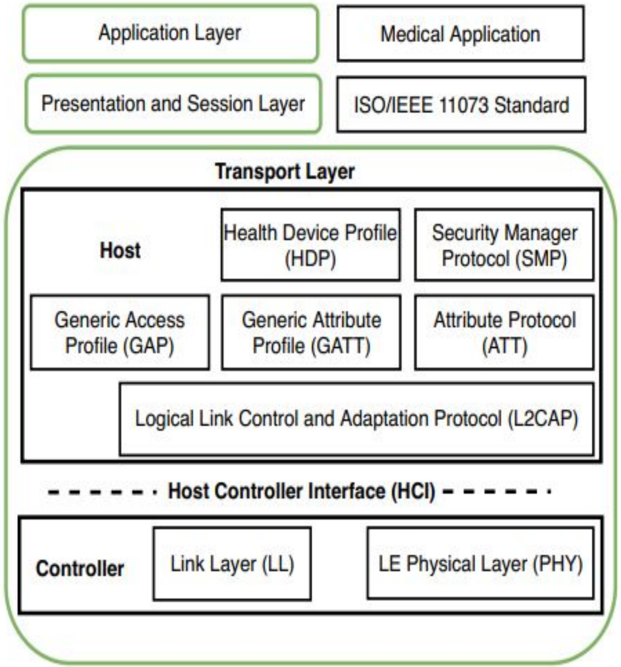

Application Layer
Medical Application
Presentation and Session Layer
ISO/IEEE 11073 Standard
Transport Layer
Host
Health Device Profile (HDP)
Security Manager Protocol (SMP)
Generic Access Profile (GAP)
Generic Attribute Profile (GATT)
Attribute Protocol (ATT)
Logical Link Control and Adaptation Protocol (L2CAP)
Host Controller Interface (HCI)
Controller
Link Layer (LL)
LE Physical Layer (PHY)

Fig. 2: Health device profile for BLE-based communications between medical agents and managers as defined by the ISO/IEEE 11073 standard.

Attacker Model

- **Connection delay** : An attacker tries to connect with the PMD using a malicious app installed in the manager (smartphone/laptop), and make the device unavailable for an authorized app.
- **Data Interception** : An attacker sniffs the PMDs' communications to eavesdrop and collect sensitive information such as the patient's vitals and device information.
- **Data Modification**: An attacker attempts to modify the patient's vitals measured by a PMD to perform malicious activities such as triggering false alerts, altering treatments, etc.

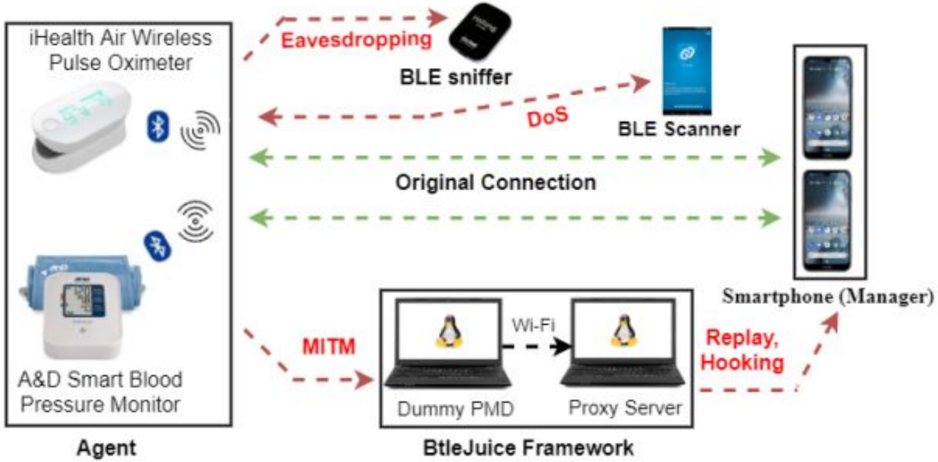


Fig. 3: Our attack environment for PMDs.

Attack Methodology

- **Eavesdropping**: Passively capture the network traffic between the PMD (i.e., pulse oximeter) and the smartphone without interrupting normal communication.

- **DoS (Denial of Service) attack**: The majority of the PMDs use the ”Just Work” pairing method, which does not require any authentication process to connect with the associated manager. In a DoS attack, we target this feature to pair an unauthorized app with a targeted PMD.

- **Man-in-the-Middle (MITM) attack**: BtleJuice framework used to establish a proxy connection between the PMD and the manager.

- **Replay attack**: Attacker aims to send a specific packet in a recurring manner to interrupt normal communication between a PMD and the manager. To implement this attack, a particular packet from the PMD traffic was repeatedly sent in a loop.

- **False data injection**: Payload of a particular packet is altered. Here, we captured the communication packets from the PMD using the BtleJuice framework and determined the GATT operation, including service and characteristic values.

HEKA: A Novel IDS for attacks to PMDs

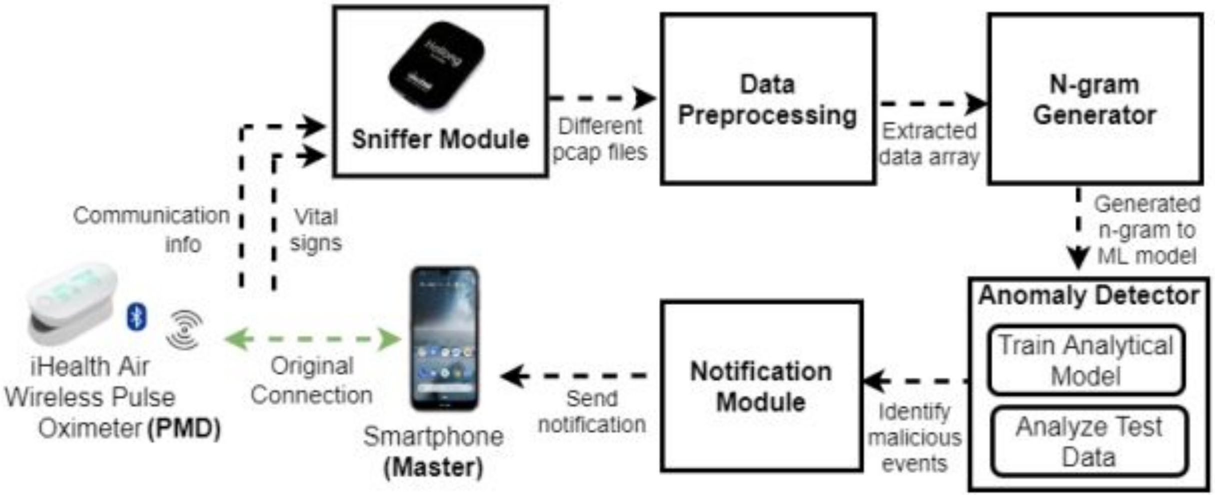


Fig. 9: Our proposed HEKA framework.

- Sniffer Module : Passively captures PMD traffic from different PMDs without interrupting normal communication.

- **Data Pre-Processing** : Collects the PMD traffic captured in the sniffer module and removes the irrelevant packets / noise from the dataset.

- **N-gram Generator** : N-gram generator considers the captured traffic as a contiguous sequence of n items. Sliding windows are used to extract features from the traffic.

- **Anomaly Detector Module** : Uses the generated n-grams from the captured traffic to train different ML algorithms and detect malicious events in the PMD traffic. The models used are **Multi-class Support Vector Machine (SVM), Decision Tree (DT), Random Forest** and **K-Nearest Neighbor (KNN)**

- HEKA was tested using each of the aforementioned models and accuracy of each model was tested. It was found that HEKA is highly effective and efficient in detecting different attacks (and also combination of number of attacks) with around 97% accuracy. The least effective model was the KNN, in every type of attack.

BlueBorne

- BlueBorne attack does not require the targeted device to be paired to the attacker’s device, or even to be set on discoverable mode. The BlueBorne attack vector can be used to conduct a large range of offenses, including remote code execution as well as Man-in-The-Middle attacks.

- Several stages of attack :- First, attacker locates active Bluetooth connections around him or her. Devices can be identified even if they are not set to “discoverable” mode.

- Next, the attacker obtains the device’s MAC address, which is a unique identifier of that specific device. By probing the device, the attacker can determine which operating system his victim is using, and adjust his exploit accordingly.

- The attacker will then exploit a vulnerability in the implementation of the Bluetooth protocol in the relevant platform and gain the access. At this stage the attacker can choose to create a Man-in-The-Middle attack and control the device’s communication, or take full control over the device.

Vulnerabilities that BlueBorne attacks

- **Information Leak Vulnerability :** The major vulnerability in the Android operating system reveals valuable information which helps the attacker leverage one of the remote code execution vulnerabilities. The vulnerability was found in the SDP (Service Discovery Protocol) server.

- **Remote Code Execution Vulnerability :** resides in the Bluetooth Network Encapsulation Protocol (BNEP) service, which enables internet sharing over a Bluetooth connection (tethering). Due to a flaw in the BNEP service, a hacker can trigger a surgical memory corruption, which is easy to exploit and enables him to run code on the device. This does not require any authentication from the device.

- **A stack overflow :** This vulnerability was found in the Bluetooth stack of the Linux Kernel, which is the very core of the operating system. An internal flaw in the L2CAP (Logical Link Control and Adaptation Protocol) that is used to connect between two devices causes a memory corruption. An attacker can use this memory corruption to gain full control of the device.