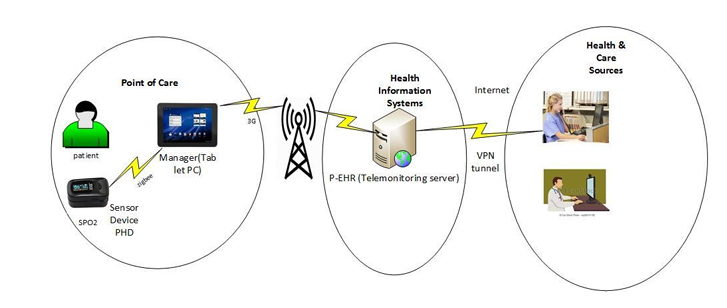
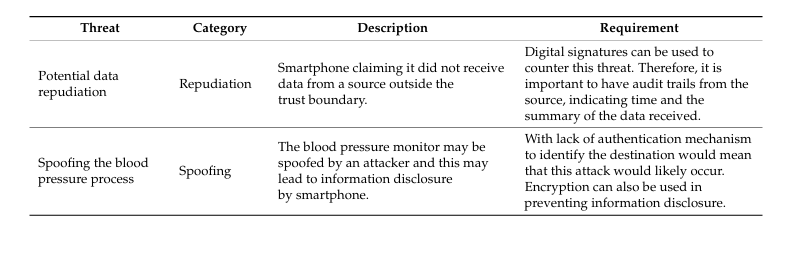
**SECURE HEALTHCARE ARCHITECTURE**

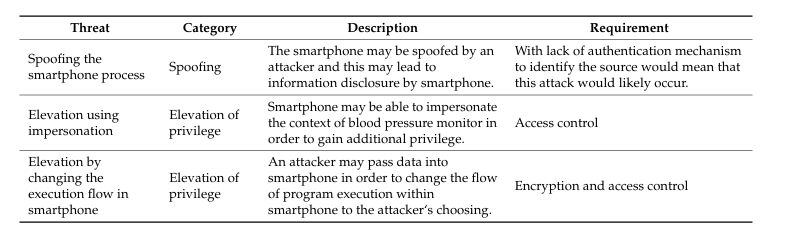
****

**Components:**

* Patient devices: These devices collect data from the patient, such as heart rate, blood pressure, and blood oxygen levels.
* Telemonitoring server: This server receives and stores the data from the patient devices.
* Manager's tablet PC: The manager uses this tablet to view the patient data and manage the system.
* VPN tunnel: This tunnel encrypts the data transmitted between the patient devices and the telemonitoring server.

**Threats and Security:**

****

****

**SECURITY GUIDELINES:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Sub Category** | **Guideline** | **Standard** | **ID** |
| System and Information Integrity | Firmware Updates | Regularly update device firmware to patch bugs, fix vulnerabilities, and add new functionalities. Ensures devices are protected against known vulnerabilities and potential cyber threats. | NIST - SI-02 |  |
| System and Information Integrity | Monitoring the Network | Implement tools to monitor IoT device connections during message transfer. Enables the detection of unusual activities or potential security breaches, enhancing overall network security. | NIST - SC-05(03) D |  |
| Authentication | Multi-Factor Authentication | Utilize multi-factor authentication (MFA) and device-based authentication. Identify the type of MFA used by the application. Determine whether the MFA implementation is robust and secure. Attempt to bypass the MFA. | OWASP - 4.4.11 | WSTG-ATHN-11 |
| Authentication | Roles and Responsibilities | Identify and document roles used by the application. Attempt to switch, change, or access another role. Review the granularity of the roles and the needs behind the permissions given. | OWASP - 4.3.1 | WSTG-IDNT-01 |
| Data Encryption | Sensitive Information | Implement data encryption measures to protect sensitive information. Utilize strong encryption algorithms (e.g., AES, RSA). Apply encryption at rest and segment encryption based on data nature and criticality. | OWASP - 4.4.1 | WSTG-CRYP-03 |
| Network Infrastructure Configuration | Security and Configuration | Review the applications’ configurations set across the network and validate that they are not vulnerable. Validate that used frameworks and systems are secure and not susceptible to known vulnerabilities due to unmaintained software or default settings and credentials. | OWASP - 4.2.1 | WSTG-CONF-01 |
| Cloud Storage | Access control | Assess that the access control configuration for the storage services is properly in place. First, identify the URL to access the data in the storage service, and then consider the following tests: read unauthorized data upload a new arbitrary file Determine if OAuth2 implementation is vulnerable or using a deprecated or custom implementation. | OWASP - 4.2.11 & OWASP - 4.5.5 | WSTG-INPV-15 & WSTG-ATHZ-05 |
| HTTPS methods |  | Enumerate supported HTTP methods. Test for access control bypass. Test HTTP method overriding techniques. | OWASP - 4.2.6 | WSTG-CONF-06 |
| Threat Modelling | Threat | Optimise Network/Application/Internet security through identifying objectives, threats, and defining countermeasures to mitigate the effects of the threat | OWASP | WSTG - 2.2 |
| Wireless Communication | Encryption and Monitoring | Utilize strong encryption for wireless communication. Implement frequency hopping or spread spectrum techniques. Deploy Wireless Intrusion Detection Systems (WIDS) to detect and respond to unauthorized activities. Implement physical security measures and network segmentation. | NIST - AC-18 W |  |
| Permissions | CI/CD and Secure Logging | Permissions for CI/CD:  Specify permissions for the Continuous Integration/Continuous Deployment (CI/CD) system. Secure Logging:  Ensure secure logging practices for hardware tags, IoT gateways, and the central hub. Logging Policy: Logs from hardware tags, IoT gateways, and the central hub are copied to a separate server using a secure protocol (e.g., syslog). Only authorized personnel have access to modify logging configurations. Application logs containing security events are retained securely for audit purposes. | NIST - 800 - 53 |  |