**Step1 Answer:**

* Identify assets:
  + Collected data.
  + Device software.
  + Data collection configuration.
  + Channels for both data collection and admin purposes.
* Threat modeling using STRIDE and suggestions for migrations:
  + Collected data:

|  |  |  |
| --- | --- | --- |
| **STRIDE category** | **Threat** | **Mitigation** |
| **Spoofing** | An unauthorized entity impersonates the server to access data. | Use mutual authentication between devices and the server. |
| **Tampering** | Attacker alters data before it reaches the server. | Secure data transmission with encryption (e.g., TLS). |
| **Information Disclosure** | Data could be exposed during transmission. | Encrypt data in transit and at rest to prevent unauthorized access. |
| **Denial of Service (DoS)** | Attacker floods the device with requests to disrupt data collection. | Implement rate limiting and connection throttling on the device. |
| **Repudiation** | N/A | N/A |
| **Elevation of Privilege** | N/A | N/A |

* Device software:

|  |  |  |
| --- | --- | --- |
| **STRIDE category** | **Threat** | **Mitigation** |
| **Spoofing** | Unauthorized user impersonates the superuser to initiate an update. | Require multi-factor authentication for superuser access to firmware updates. |
| **Tampering** | Attacker modifies the firmware update to introduce malicious code. | Digitally sign firmware and verify signatures before installation. |
| **Information Disclosure** | N/A | N/A |
| **Denial of Service (DoS)** | Malicious superuser could deny initiating unauthorized firmware updates. | Log all firmware update attempts to create an audit trail. |
| **Repudiation** | Attacker repeatedly attempts to install firmware, disrupting service. | Limit update attempts and monitor for abnormal update activity. |
| **Elevation of Privilege** | Regular user gains access to superuser-level firmware updates. | Enforce strict role-based access control, limiting updates to superusers only. |

* Data collection configuration:

|  |  |  |
| --- | --- | --- |
| **STRIDE category** | **Threat** | **Mitigation** |
| **Spoofing** | Unauthorized user pretends to be an admin to change settings. | Use role-based access control and require authentication for admin access. |
| **Tampering** | Attacker modifies device configuration to affect system behavior. | Secure configuration channels with encryption and use secure authentication mechanisms. |
| **Information Disclosure** | Configuration settings may be exposed to unauthorized parties. | Encrypt sensitive configuration data to prevent disclosure. |
| **Denial of Service (DoS)** | Flooding configuration requests to overwhelm the device. | Implement rate limiting for configuration requests. |
| **Repudiation** | N/A | N/A |
| **Elevation of Privilege** | N/A | N/A |

* Channels for both data collection and admin purposes:

|  |  |  |
| --- | --- | --- |
| **STRIDE category** | **Threat** | **Mitigation** |
| **Spoofing** | Unauthorized user impersonates the server to access device data. | Use mutual authentication between server and devices. |
| **Tampering** | Attacker modifies data received from devices. | Use integrity checks (e.g., hashing) and secure communication protocols to verify data integrity. |
| **Information Disclosure** | Sensitive data from devices may be leaked. | Encrypt data storage and enforce strict access controls to limit data exposure. |
| **Denial of Service (DoS)** | Flooding server with requests to disrupt service. | Implement traffic monitoring, rate limiting, and possibly a firewall to mitigate DoS attacks. |
| **Repudiation** | N/A | N/A |
| **Elevation of Privilege** | An attacker gains admin privileges to control server functions. | Enforce multi-factor authentication for administrative access and log all access attempts. |

**Step2 Answer:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Function** | **Device User Role** | **Administrator Role** | **Superuser Role** |
| Collect data | **Yes** | **Yes** | **Yes** |
| Listen to the connection for data collection | **Yes** | **Yes** | **Yes** |
| Send collected data to the server | **Yes** | **Yes** | **Yes** |
| Change data collection configuration | **No** | **Yes** | **Yes** |
| Listen to the connection for admin purposes | **No** | **Yes** | **Yes** |
| Receive collected data | **No** | **Yes** | **Yes** |
| Update device software | **No** | **No** | **Yes** |
| Disable device | **No** | **No** | **Yes** |