**LAB 5**

**SMART HOME SYSTEM**

**1. Identify Assets**

Smart Home Hub: The central device that controls all smart devices.

Smart Devices: Smart lights, smart locks, smart thermostats, smart appliances, security cameras, etc.

User Credentials: Usernames and passwords used to access the system.

User Personal Data: User preferences, schedules, location data, usage patterns.

Home Network: The network that connects all smart devices.

Mobile App: The mobile application used to control the smart home system.

Firmware of Devices: Software running on the devices themselves.

**2. Identify Threats using STRIDE**

|  |  |  |
| --- | --- | --- |
| **STRIDE**  **Category** | **Threat Description** | **Affected Asset(s)** |
| Spoofing | Attackers gain unauthorized access by pretending to be legitimate users or devices. | Smart Home Hub, Smart Devices, User Credentials |
| Tampering | Unauthorized modification of device settings, firmware, or user data. | Smart Devices, Firmware of Devices, User Personal Data |
| Repudiation | Users deny actions performed by the system, leading to accountability issues. | Smart Locks, Smart Thermostats, Smart Appliances |
| Information Disclosure | Exposure of sensitive user data, device settings, or system configuration information. | User Personal Data, Device Settings, Smart Home Hub, Security Cameras |
| Denial Of Service (DoS) | Rendering smart devices or the entire system unavailable to legitimate users. | Smart Home Hub, Smart Devices, Home Network |
| Elevation  of Privilege | Gaining unauthorized administrative access to the smart home hub or individual devices. | Smart Home Hub, Smart Devices, Firmware of Devices |

**3. Attack Vectors & Mitigation Strategies**

|  |  |  |
| --- | --- | --- |
| **Attack Vector** | **Possible Threat**  **(STRIDE)** | **Mitigation** |
| Weak Passwords | Spoofing | Enforce strong password policies, multi-factor authentication (MFA) |
| Unsecured Network | Spoofing, Information Disclosure, Tampering | Use WPA3 encryption, segment the home network, guest network for untrusted devices |
| Vulnerable Firmware | Spoofing, Tampering, Information Disclosure, Elevation of Privilege | Regular firmware updates, secure boot mechanisms, code signing |
| Man-in-the-Middle (MITM) Attacks | Spoofing, Tampering, Information Disclosure | Use HTTPS, TLS encryption, certificate pinning |
| Cloud Service Exploits | Information Disclosure, Tampering, Denial of Service | Secure cloud storage, access controls, data encryption |
| Phishing Attacks | Spoofing, Information Disclosure | User education, MFA |
| Physical Access | Tampering, Elevation of Privilege | Physical security measures (e.g., secure enclosures), tamper detection |
| IoT Botnets | Denial of Service, Spoofing | Regular security scans, intrusion detection systems, firmware updates |
| Mobile App Vulnerabilities | All STRIDE categories | Secure coding practices, code reviews, penetration testing, data protection |
| Supply Chain Attacks | Tampering, Information Disclosure, Denial of Service | Vendor risk management, security audits, third-party security assessments |

**4. Threat Model Diagram (Basic Structure)**

Device Status Updates

User Commands

System Logs

Firmware Updates

Personal Data

Device Configuration

User Account Database

Authentication Process

Device Database

Device Control

Cloud Services

(Data Storage)

Homeowner

(External User)