Security Design

> **Source File:** generated-documents\technical-design\security-design.md
> **Generated:** 08/07/2025 at 09:44:11
> **Generated by:** Requirements Gathering Agent - PDF Converter

SecurityDesign

Generated by adpa-enterprise-framework-automation v3.1.6
Category: technical-design
Generated: 2025-07-05T17:03:27.951Z
Description:

Security Design Document: Self-Charging Electric Vehicles (SCEV)

1. Introduction

This document outlines the security design for the Self-Charging Electric Vehicle (SCEV) project. The system integrates multiple energy harvesting technologies managed by a central AI-powered Energy Management Unit (EMU). This design prioritizes the security and privacy of user data, vehicle integrity, and the safety of the vehicle and its occupants.

2. Security Overview

The SCEV system presents unique security challenges due to its interconnected nature and reliance on external energy sources. The core security principles guiding this design are:

- **Confidentiality:** Protecting sensitive user data and vehicle operational information from unauthorized access.
- **Integrity:** Ensuring the authenticity and reliability of data and system operations, preventing tampering and malicious modification.
- **Availability:** Maintaining the continuous and reliable operation of the vehicle and its energy harvesting systems.
- **Authentication:** Verifying the identity of users and devices accessing the system.
- **Authorization:** Controlling access to system resources and functionalities based on user roles and privileges.

3. Authentication Design

- **User Authentication:** The vehicle will utilize multi-factor authentication (MFA) for user access. This could include a PIN, biometric authentication (fingerprint or facial recognition), and potentially a smartphone app for secondary verification. The authentication system will be designed to resist brute-force attacks and replay attacks.
- **Device Authentication:** The EMU and other onboard systems will employ secure boot processes and digital signatures to verify their integrity and prevent unauthorized software execution. Communication between components will utilize mutual authentication mechanisms (e.g., TLS with certificate pinning).
- **Cloud Authentication (if applicable):** If cloud connectivity is used for features like remote diagnostics or over-the-air updates, secure authentication protocols like OAuth 2.0 or OpenID Connect will be employed.

4. Authorization Framework

- **Role-Based Access Control (RBAC):** Access control will be implemented using RBAC, defining distinct roles (e.g., Owner, Driver, Mechanic) with specific permissions.
- **Least Privilege Principle:** Each component and user will only have the necessary permissions to perform its assigned tasks.

- **Access Control Lists (ACLs):** ACLs will be used to manage access to sensitive data and system functions.

5. Data Protection

- **Data Encryption:** Sensitive data, including user credentials, vehicle location, and energy harvesting data, will be encrypted both in transit (using TLS) and at rest (using AES-256 encryption).
- **Data Minimization:** The system will only collect and store the minimum necessary data required for its operation and functionality.
- **Data Anonymization/Pseudonymization:** Where possible, data will be anonymized or pseudonymized to protect user privacy.
- **Secure Data Storage:** Data will be stored securely, utilizing encrypted storage solutions and access control mechanisms.

6. Network Security

- **Secure Communication:** All communication between vehicle components and external systems will be secured using TLS 1.3 or later.
- **Firewall:** A robust firewall will be implemented to prevent unauthorized access to the vehicle's internal network.
- **Intrusion Detection/Prevention System (IDS/IPS):** An IDS/IPS will monitor network traffic for malicious activity and take appropriate action.
- **Secure Over-the-Air (OTA) Updates:** OTA updates will be digitally signed and verified to prevent malicious code injection.

7. Security Controls

- **Secure Coding Practices:** Secure coding guidelines will be followed throughout the development lifecycle to minimize vulnerabilities. Regular code reviews and static/dynamic analysis will be performed.
- **Vulnerability Scanning:** Regular vulnerability scans will be conducted to identify and address potential security weaknesses.
- **Penetration Testing:** Penetration testing will be performed to assess the system's resilience against real-world attacks.

- **Regular Security Audits:** Regular security audits will be conducted to verify compliance with security policies and standards.

8. Threat Modeling

A comprehensive threat model will be developed, identifying potential threats and vulnerabilities across all system components and interfaces. This will include:

- **Data breaches:** Unauthorized access to sensitive user data and vehicle information.
- **Denial-of-service (DoS) attacks:** Disrupting the operation of the vehicle or its energy harvesting systems.
- **Software vulnerabilities:** Exploiting software flaws to gain unauthorized access or control.
- **Hardware tampering:** Physically accessing and modifying vehicle components.
- **Supply chain attacks:** Compromising components or software during the manufacturing or development process.

9. Security Testing Strategy

The security testing strategy will encompass:

- **Unit testing:** Testing individual components for security vulnerabilities.
- **Integration testing:** Testing the interaction between components for security flaws.
- **System testing:** Testing the entire system for security vulnerabilities.
- **Penetration testing:** Simulating real-world attacks to identify vulnerabilities.
- **Fuzz testing:** Testing the system's robustness against unexpected inputs.

10. Incident Response Plan

An incident response plan will be developed to handle security incidents effectively and efficiently. This plan will include:

- **Incident detection and reporting procedures.**
- **Incident investigation and analysis.**
- **Containment and eradication of threats.**
- **Recovery and restoration of systems.**
- **Post-incident activity.**

11. Compliance Requirements

The SCEV system will be designed to comply with relevant regulations and standards, including:

- **GDPR (General Data Protection Regulation):** Protecting user data privacy.
- **ISO 27001 (Information Security Management Systems):** Establishing an information security management system.
- **Automotive safety standards (e.g., ISO 26262):** Ensuring the safety and reliability of the vehicle's systems.
- **Other relevant regional and industry-specific standards.**

12. Security Monitoring

Continuous security monitoring will be implemented to detect and respond to security threats in real-time. This will include:

- **Security Information and Event Management (SIEM):** Centralized logging and analysis of security events.
- **Intrusion Detection/Prevention System (IDS/IPS):** Monitoring network traffic for malicious activity.
- **Regular security audits:** Verifying compliance with security policies and standards.

This document provides a high-level overview of the security design for the SCEV project. More detailed specifications will be developed during subsequent design phases. The security design will be iteratively refined throughout the development lifecycle, incorporating feedback from security testing and audits.