Smart Security System Security Blueprint

This is a security Blueprint for the Smart Security System. The purpose of this document is to enable implementation of controls and/or measures to ensure any risks identified or foreseen are mitigated.

**Access Management**

Access to the application (embedded system) and the underlying OS Raspberry pi was restricted using a username and password. Also access to the internet was done through a secure WiFi network that employs WPA2/WPA3 encryption.

The website also allows users to authenticate using a username and password to view the access logs.

**MQTT Broker Security**

Ensured broker connection security through configuration of secure communication (TLS) to the MQTT broker. In addition to this, a username and password was used to allow publishing of the MQTT messages.

**Logging Security**

Restrict access to the log file generated when a PIN is input.

**Rate Limiting**

Implement a rate-limiting mechanism to prevent brute-force attacks and also ensure PINs are securely handled.

**Display Security**

Avoided displaying sensitive information on the screen. Asterisks were used when user inputs a PIN.

**Secure Dependencies**

Regularly update dependencies and libraries.

Ensure dependencies are obtained securely through trusted sources.

**Summary**

These measures outlined here ensure that access management to secure communication and user interface confidentiality. Regular updates and a focus on secure practices contribute to an overall robust security posture for the system.