WHITEPAPER

Threat Model and Security Objectives

SensorTile.box (ST Microelectronics)

Author – Yashodhan Vivek Mandke

About The Author

Yashodhan is an IoT Product Security Researcher. He has Research and Development experience in the IoT and AI domain of more than 11 years. Currently, he is pursuing a doctoral degree in Astrophotonics. His academic qualification involves M. Tech Satellite Communication, M. Tech Signal Processing, B.E (E&TC). He has developed and delivered Industrial IoT products with AI capabilities. He also has research experience in Signal Processing, RF and Electromagnetics, and cubesatellite. He is experienced with security assessment, creating threat models and security architecture for IoT products, and is working on research focusing on Side-channel attacks and Fault injection.

Contents

1. Executive Summary

This document discusses Threat Model and Security Objectives for the STEVAL-SensorTileBox (IoT Sensor Node) product from ST Microelectronics. The manufacturer can refer to this document as a system level threat model and can develop the rest of the security objectives on top of it. it. Based on the description of the system, the document lists the assets that need protection and the threats that are considered in the scope. The threats have been considered based on major security features in the system. The security problem has been defined with respect to Confidentiality, Integrity, and Availability, i.e., CIA Triad. The necessary security objectives have been discussed to mitigate the threats that have been identified.

2. Introduction

This section provides an overview of the Target of Evaluation (TOE) The threat model and security objectives for the mentioned TOE have been evaluated based on Common Criteria (CC) and Platform Security Architecture (PSA). CC is an ISO/IEC 15408 standard for computer security certification.

Common Criteria is a framework in which computer system users can specify their security functional and assurance requirements (SFRs and SARs respectively) in a Security Target (ST) and may be taken from Protection Profiles (PPs). Common Criteria maintains a list of certified products, including operating systems, access control systems, databases, and key management systems.

Platform Security Architecture (PSA) is an initiative from Arm that aims to address some of the shortcomings with IoT security. It has the goal to demystify implementation choices and bring coherence to the IoT ecosystem.

The basic and minimalistic data logger architecture includes following components

1. BareMetal MCU with ARM Cortex-M4 architecture
2. Sensors include temperature, pressure, temperature-humidity, two different accelerometers, magnetometer, 3D Accelerometer & Gyroscope and audio sensor
3. Micro-SD card for storage of data locally
4. The wireless communication being executed via Bluetooth Low Energy 4.2 (BLE 4.2)
5. The Sensortile BLE mobile application for scanning the device and interacting with device with various apps such as Barometer app, Compass and level app, Step Counter app, Baby crying app, Vibration monitoring app, Data recorder and vehicle/goods tracking app, Compensated magnetometer app
6. For control and indication 3 buttons and 3 LED respectively
7. Li-ion battery and battery charger
8. Firmware runs as BareMetal code over MCU

The high-level architectural diagram is shown next

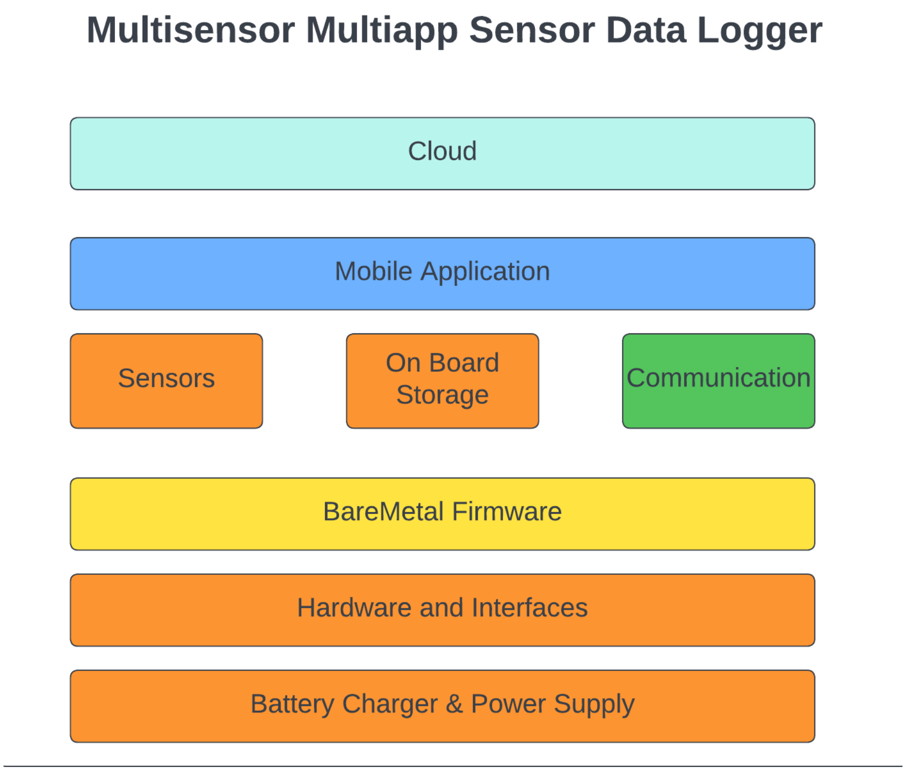

Fig 1. Fundamenatal Blocks of Sensor Data Logger

2.1 TARGET OF EVALUATION (TOE) OVERVIEW

2.1.1 TOE TYPE

1. The TOE of this protection profile (PP) is the Multisensor and Multiapp Sensor Data logger product.
2. The TOE is a platform composed of a hardware device and firmware implementing sensing, data logging, data processing, signal processing, Edge AI, BLE 4.2 communication and Cloud connectivity functionalities such as sensor data logging, signal filtering, Fast Fourier Transform (FFT), BLE communication, Mobile app data integration etc. The firmware will BareMetal for ARM-Cortex M4 architecture. Additionally on device data storage and battery.

2.1.2 TOE USAGE AND MAJOR SECURITY FEATURES

1. The TOE may include sensors such as temperature sensor, humidity sensor, temperature & humidity integrated sensor, pressure sensor, triaxial accelerometer, magnetometer, vibration sensor, 3D accelerometer & gyroscope integrated sensor and audio sensor.
2. The TOE includes indicator LED and buttons
3. PP includes Mobile application, microSD card and MCU as part of data logger

2.2 TARGET OF EVALUATION (TOE) DESCRIPTION

The below figure shows hardware blocks for the product and illustrates the Hardware and connectivity components for the sensor data logger i.e., TOE for this is PP.

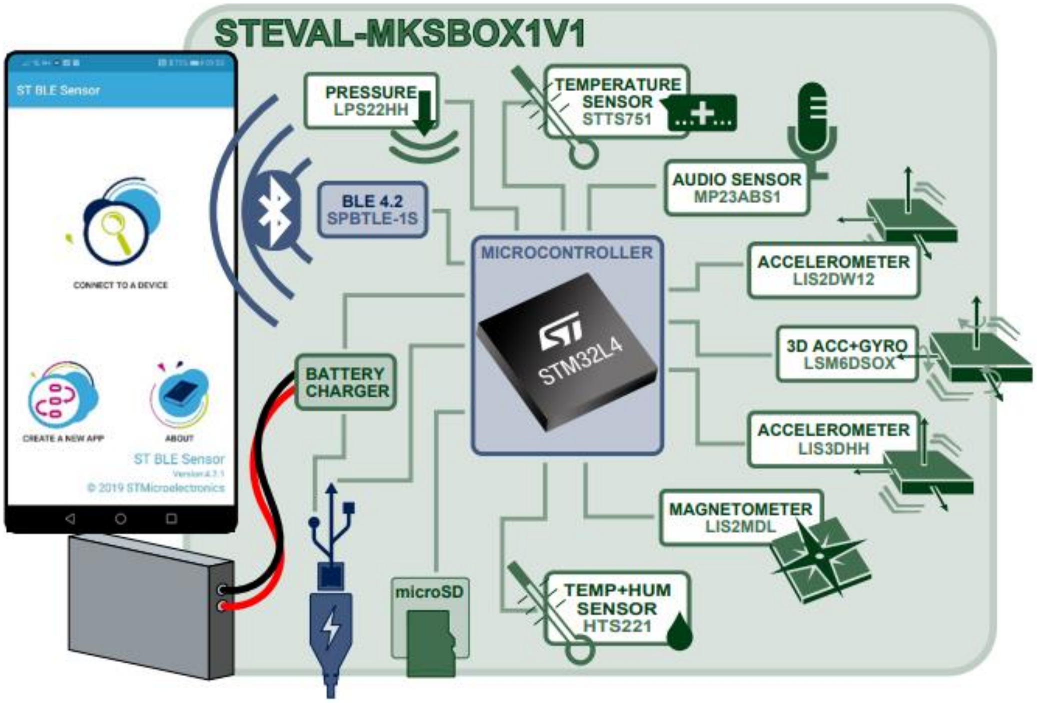

Fig. 2. Hardware Components and Connectivity Block Diagram for Sensor Data Logger

Reference : STEVAL-MKSBOX1V1 Databrief - Sensortile Box Product Brief Manual

2.2.1 TOE FEATURES

1. Authentication: User must be authenticated prior to modifying configuration or updating system functionality
2. Authorizations: Some of the features such as BLE pairing, SD card data access should be limited to limited users
3. Secure communication: Generally, any communication over the network is performed using a protocol that includes integrity and confidentiality protections. Also, the communication between peripherals and the main processor should be secure, e.g., communication between external storage and processor, communication module and MCU, sensors and MCU.

4. Log of security events: Security events are logged locally on the device to be made available in the forensic analysis of an attack or after another suspicious event.
5. Firmware update: The firmware running on the TOE can be updated to fix vulnerabilities identified after the device's deployment. Also, it needs to verify that the device cannot be downgraded to known vulnerable versions i.e., anti-rollback for a firmware update.
6. Tampering detection: The device is likely to include a combination of hardware and software measures to detect attempts to tamper with the device.

2.2.1.1 HARDWARE

1. Basic hardware of the sensor data logger embedded system typically consists of a processor with internal/external flash memory, sensors, communication module and optionally external storage such as SD card or NAND/NOR Flash memory.
2. Sensor data stored in SD card
3. Access to USB port and BLE communication
4. Battery charging system and power supply

2.2.1.2 FIRMWARE

1. The sensor data logger ideally has BareMetal Firmware or RTOS based firmware running over the microcontroller
2. The firmware is responsible for implementing TOE functionalities.
3. The sensor interfacing firmware section consists of firmware for individual protocol interface with MCU and sensor configuration and SD card interface for logging of data
4. Firmware for communication component such as BLE that advertises data from sensors over MQTT protocol
5. Firmware usually stored in internal flash memory which also support upgrades
6. Bootloader for Firmware Over the Air (FOTA), secure boot during booting

2.2.1.3 APPLICATION SOFTWARE

1. The mobile application that scans BLE device, identifies Sensortile box device ID
2. Updates the firmware over the air for use case such as vibration monitoring, sensor data logging, quaternion
3. Acts as a gateway between device and cloud to integrate data with public cloud
4. Firmware upgrade over the air for the sensor data logger based on the specific firmware used for the use cases mentioned in point 2 above

3. SECURITY PROBLEM DEFINITION

This section uses abbreviations for the following terms:

Threat = T.

Assumptions = A

Organizational Security Policy = P

Objective for the Target of Evaluation (TOE) = OT

Objective for the Environment = OE

3.1 USERS AND EXTERNAL ENTITIES

1. The external entities that are considered in this PP are:
    a. Remote Admin: The remote admin here refers to sensor data logger manufacturers. This entity operates from backend servers and can configure the data logger embedded system platform remotely.
    b. Local Admin: Local admin here refers to the user. This entity operates locally and can configure the sensor data logger embedded system platform and perform firmware updates.
    c. Attacker: This user can target the sensor data logger embedded system for financial or malevolent reasons. Attackers can operate remotely or locally.
2. Remote and Local Admin entities are not necessarily users but can be devices or systems controlled by trusted users

3.2 ASSETS

3.2.1 TARGET OF EVALUATION SECURITY FUNCTIONALITY (TSF) DATA

The following assets contain data that belongs to TSF.

3.2.1.1 Sensor Data Logger PLATFORM ID

1. A unique ID to identify the device on a network, which may be the Media Access Control (MAC) address of the i.e., BLE MAC address/ BT address.
2. Unique ID for physically accessible ports such as USB
3. Properties: Integrity

3.2.1.2 FIRMWARE

1. BareMetal Firmware /RTOS Firmware for sensor data logger
2. Sensor firmware
3. Storage firmware
4. BLE communication firmware
5. Bootloader and secure boot
6. Properties: Integrity, Authenticity

3.2.1.3 FIRMWARE CERTIFICATE

1. The cryptographic certificate is used to authenticate firmware and firmware updates
2. Properties: Integrity

3.2.1.4 LOGS

1. The sensor data logs in SD cards
2. The event logs that can be used to detect suspicious activities
3. Properties: Integrity, Confidentiality

3.2.2 USER DATA

3.2.2.1 SENSOR DATA

1. The data collected by any/all the sensors on data logger viz. temperature sensor, humidity sensor, temperature & humidity integrated sensor, pressure sensor, triaxial accelerometer, magnetometer, vibration sensor, 3D accelerometer & gyroscope integrated sensor and audio sensor at regular intervals. The data either stored locally on the SD card or pushed on the cloud server
2. Properties: Integrity, Confidentiality

3.2.2.2 CONFIGURATION

1. The sensor data logger's configuration is split into three major components
    a. The BLE profile configuration of the device
    b. Sensor configuration based on the use case (e.g., Vibration monitoring, Vehicle / goods tracking, Sensor data logger, Barometer / environmental monitoring, Pedometer optimized for belt positioning etc.)
2. Properties: Integrity, Availability

3.2.2.3 CREDENTIALS

1. Authentication credentials, used for local and remote authentication, and for data protection during communication
2. The secret keys such as Short-Term Key (STK), Long Term Key (LTK) shared during BLE communication pairing
3. Cloud credentials for logging data over public cloud
4. Properties: Integrity, Confidentiality

3.3 THREATS (T.)

An attacker is a threat agent (a person or a process acting on his/her behalf) trying to undermine the TOE security policy defined by the current Security Target (ST) and, hence, the Target of Evaluation Security Functionality (TSF). The attacker especially tries to change the properties of the assets defined in Section 3.2.

3.3.1 T. IMPERSONATION

1. An attacker impersonates a maintenance device on the local interface.
2. The credentials may be obtained through insecure communication protocols or exposed through data disclosure.
3. The attacker may then modify configuration, firmware, or logs.
4. Assets threatened directly: Credentials.
5. Assets threatened indirectly: Firmware, Configuration, Logs, Communication.

3.3.2 T. MITM

1. An attacker performs a Man-In-The-Middle (MITM) attack on BLE and Mobile application communication.
2. An attacker can perform MITM over MQTT protocol while data being shared
3. The attacker may alter or modify messages exchanged with the device.

4. The attacker may then disclose and modify Location Records, Logs, Credentials, Configuration data
5. Assets threatened directly: Credentials (Server/BLE), Logs, Configuration

3.3.3 T. FIRMWARE_ABUSE

1. An attacker installs a flawed version of the firmware and obtains partial or total control of the Sensortile box. The firmware may have been modified prior to the attack to include malware or consist of an outdated version of the original firmware may be due to vulnerable libraries used.
2. The attacker may, for instance, modify on the device the value of the firmware certificate used to authenticate the installed firmware or firmware updates
3. The attacker may also exploit functionalities of the TOE that are available as functional requirements of the device
4. Such an attack can allow for disclosing or modifying Configuration Data, Credentials, Firmware, or Logs
5. Assets threatened directly: Firmware, Firmware Certificate
6. Assets threatened indirectly: All

3.3.4 T. HARDWARE_ABUSE

1. An attacker performs sensor sniffing over protocols such as UART, SPI, I2C and get access to data
2. An attacker does the reverse engineering of PCB and gets access to debugging headers of JTAG, SWD, and UART
3. An attacker can bypass the secure boot stage or even erase SRAM by performing Electromagnetic Fault Injection (EMFI) attack
4. An attacker can get access to cryptographic keys by performing side channel analysis during operation
5. An attacker can perform Direct Memory Access (DMA) attacks that can compromise firmware locally or remotely on peripheral hardware
6. Assets threatened directly and indirectly: All

3.3.5 T. REPUDIATION

1. A User of the device denies action performed on the TOE on its behalf
2. This can be the local or remote administrator for configuration or firmware update
3. Assets threatened directly: Logs, Location Records, Firmware

3.3.6 T. TAMPER

1. An attacker tampers with the Sensortile box and tries to access or modify assets in persistent or volatile memory. The main targeted assets are Location Record, Logs, Credentials, Cryptographic keys, Configuration data
2. To perform this attack, the attacker may use debug functionalities or direct memory access or even reverse engineer the PCB
3. Such an attack can, for instance, allow for cloning the device, modifying the actual records or logs of the device, getting access to non-authorized features of the device, getting unauthorized access to the BLE, and performing a denial-of-service
4. Assets threatened directly and indirectly: All

3.4 ORGANIZATIONAL SECURITY POLICIES (P.)

The TOE and its environment shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operation.

3.4.1 P. KEYS_MANAGEMENT

The cryptographic keys, credentials, and certificates used in the TOE shall be securely generated, provisioned on the TOE.

3.5 ASSUMPTION (A.)

This section describes the assumptions about the operational environment of the TOE.

3.5.1 P. KEYS_MANAGEMENT

Admin of the TOE is assumed to follow and apply administrative guidance in a trusted manner.

4. SECURITY OBJECTIVES

This section uses abbreviations for the following terms:

Threat = T.

Assumptions = A

Organizational Security Policy = P

Objective for the Target of Evaluation (TOE) = OT.

Objective for the Environment = OE.

4.1 SECURITY OBJECTIVES FOR THE TARGET OF EVALUATION (OT.)

4.1.1 OT. ACCESS_CONTROL

The TOE shall authenticate Remote and Local Admin entities before granting access to the configuration and logs and before performing firmware updates.

4.1.2 OT. SECURE_STORAGE

The TOE shall protect the integrity and confidentiality of the Sensor data, Credentials when stored, and protect integrity of Firmware Certificate, Configuration, and Logs when stored.

4.1.3 OT. FIRMWARE_AUTHENTICITY

1. The TOE shall authenticate and verify the integrity of the firmware image during boot and of new firmware versions prior to the upgrade
2. The TOE shall also reject attempts of firmware downgrade, especially with vulnerable versions or vulnerable libraries

4.1.4 OT. DATA_INTEGRITY

1. The TOE shall authenticate and verify data before reading from the SD card or from cloud storage
2. Based on the use case, the data may be classified as Public, Internal, Confidential and Restricted
3. Based on the level of the sensitivity of data the appropriate data encryption techniques shall be applied

4. Also, the data integrity can be applied with the help of Triple Modular Redundancy (TMR) Check

4.1.5 OT. HARDWARE_AUTHENTICITY

1. The TOE shall protect the hardware from Side-channel attacks (SCA) by selecting MCU and other chips which are protected against SCA
2. The TOE shall protect the hardware from fault injection, and glitching with tamper-proof casing
3. For critical use cases the MCU and other peripherals such as memory / sensors can be combined to design SOM
4. The TOE shall disable debug ports during operation

4.1.6 OT. COMMUNICATION

1. The TOE shall only accept remote connections from configured back-end servers and be able to authenticate these servers
2. The TOE shall only accept Bluetooth pairing with the authenticated device
3. The TOE shall also provide authenticity, confidentiality, and replay protection for export outside of the TOE

4.1.7 OT. AUDIT

The TOE shall maintain log of all significant events and allow access and analysis of these logs to authorized users only. Accessing the logged data shall ensure the log events of authenticated user has accessed the data either from local storage or from cloud server

4.1.8 OT. SECURE_STATE

1. The TOE shall maintain a secure state even in case of failures, for instance failure of verification of firmware integrity
2. The TOE shall maintain a secure state in case of failures, such as firmware integrity error, firmware upgrade error, Random Number Generation (RNG) error, failure to establish a trusted communication channel.
3. The TOE shall ensure residual information protection for credentials and session keys after they are being used

4.1.9 OT. TAMPER

The TOE shall react to physical tampering attempts. The tampering event detection can be achieved by various means such as crypto chip protection, sensors outside TOE that senses the opening and closing of the device case, PCB track connected to processor pin to detect event, etc.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT (OE.)

4.2.1 OE. CREDENTIALS_MANAGEMENT

Like point discussed 3.4.1 P. KEYS_MANAGEMENT

4.2.2 OE. TRUSTED_ADMIN

The Admin of the TOE is not careless, willfully negligent, or hostile

4.3 SECURITY OBJECTIVES RATIONALE

The following table provides an overview of security objectives coverage (TOE and its environment) and gives evidence for the sufficiency and necessity of the defined objectives. It shows that all threats and Organizational Security Policies (OSPs) are addressed by the security objectives, and it also shows that all assumptions are addressed by the security objectives for the TOE operational environment. The table below shows the Security Objective Rationale Matrix.

	OT. ACCESS_CONTROL	OT. SECURE_STORAGE	OT. FIRMWARE_AUTHENTICITY	OT. DATA_INTEGRITY	OT. HARDWARE_AUTHENTICITY	OT. COMMUNICATION	OT. AUDIT	OT. TAMPER	OT. SECURE_STATE	OE. CREDENTIAL_MANAGEMENT	OE. TRUSTED_ADMIN
T. IMPERSONATION	×						×			×	
T. MITM						×					
T. FIRMWARE_ABUSE	×		×						×		
T. HARDWARE_ABUSE	×	×			×			×			
T. REPUDIATION											
T. TAMPER		×	×	×				×			
P. KEYS_MANAGEMENT	×									×	

TABLE 1: Security Objective Rationale Matrix

4.3.1 SECURITY OBJECTIVE RATIONALES: THREATS

4.3.1.1 THREAT: T. IMPERSONATION

This threat assumes that the TOE can be attacked by impersonating a legitimate user. This threat is countered by the security objectives OT. ACCESS_CONTROL that ensures authentication of users to access TOE functionalities and OT. AUDIT allows for an audit of TOE users' activities and by the security objective on the operational environment OE. CREDENTIALS_MANAGEMENT ensures that no default password can be used on operational usage

4.3.1.2 THREAT: T. MITM

This threat assumes that the TOE can be attacked by intercepting or spying communications with remote servers and local Bluetooth devices. This threat is countered by the security objective OT. COMMUNICATION that ensures authentication of remote servers, local, low-power, low-range communication, and protection in confidentiality and integrity of exchanged data.

4.3.1.3 THREAT: T. FIRMWARE_ABUSE

This threat assumes that the TOE can be attacked by modifying the firmware or installing an outdated, vulnerable version. This threat is countered by the security objectives OT. ACCESS_CONTROL that ensures only Admin can initiate firmware upgrade, OT. FIRMWARE_AUTHENTICITY that ensures verification of firmware authenticity prior use and prior upgrade, and OT. SECURE_STATE that ensures that the TOE maintains a secure state even in case of failure of verification of firmware integrity.

4.3.1.4 THREAT: T. HARDWARE_ABUSE

1. This threat assumes that the TOE can be attacked via open debug ports, extraction of firmware from external flash. These can be encountered by OT. ACCESS_CONTROL and OT. HARDWARE_INTEGRITY that ensures the TOE has protection against physical attacks. Also T. HARDWARE_INTEGRITY ensures that the debug ports of hardware are disabled.
2. This threat also assumes that TOE can be attacked with Fault Injection mechanisms such as EMFI, Voltage Glitching. To mitigate this attack, the device needs tamper protection that has been addressed in OT. TAMPER

4.3.1.5 THREAT: T. REPUDIATION

This threat assumes that TOE users can deny their actions on the TOE. This threat is countered by the security objectives OT. ACCESS_CONTROL that ensures authentication of users to access TOE functionalities, OT. COMMUNICATION that ensures protection in the authenticity of exported TOE data and OT. AUDIT that allows for an audit of the TOE users' activities

4.3.1.6 THREAT: T. TAMPER

This threat assumes that the TOE can be attacked by physical tampering. This threat is countered by the security objectives OT. SECURE_STORAGE that ensures a secure storage for TOE assets, by OT. SECURE_STATE that ensures that the TOE maintains a secure state in case of failure, by OT. DATA_INTEGRITY for data protection and by OT. TAMPER that ensures reaction to physical tampering attempts

4.3.2 SECURITY OBJECTIVE RATIONALES: SECURITY POLICIES

Each identified security policy in this Security Target is addressed by at least one security objective for the TOE or security objective for the operational environment. This section provides a mapping from each security policy to the security objectives and provides a rationale for how the security policy is fulfilled.

4.3.2.1 POLICY: P. KEYS_MANAGEMENT

This security policy is directly upheld by the security objective on the operational environment OE. CREDENTIALS_MANAGEMENT.

4.3.3 SECURITY OBJECTIVE RATIONALES: ASSUMPTIONS

Each security assumption in this Security Target is addressed by at least one security objective for the operational environment. This section maps assumptions to environmental security objectives and provides a rationale for how the assumption is fulfilled

4.3.3.1 ASSUMPTION: A. TRUSTED_ADMIN

This security policy is directly upheld by the security objective on the operational environment OE. TRUSTED_ADMIN.

5. CONCLUSION

The Threat model and security objectives discussed in the document considers different components of the system architecture as an asset and evaluates the possible threat for each of them. To counter the threats, we have also discussed about the security objectives. The security rationale matrix mapped for security objectives against the listed threats in the document addresses security efficiently.

6. REFERENCES

1. ARM-PSA, Link
2. ST Sensortile Box Wireless Multisensor Development Kit, Link