Embedded Security Showcase on PSoC64 (ESSOP)

Requirement Analysis

Author: Aadarsh Kumar Singh, Embedded Systems and Microelectronics

Status: released

Revision	Date	Editor	Reason
1.0	25.08.2020	Aadarsh Kumar Singh	Requirement Analysis for the given use case

Contents

1. Objective 2
1.1 Background 2
1.2 Use-Case 2
1.2.1 Confidentiality: 2
1.2.2 Authenticity: 2
1.2.3 Message Integrity: 2
1.2.4 Non- repudiation: 2
2. Threats based Analysis for Embedded Security Use Case – CIA Model 2
2.1 Protocol Definition 2
2.2 Use case Analysis: secure the communication between remote control and car. 3
2.2.1 Data asset of remote control 3
2.2.2 Data asset of student Car 3
2.2.3 Secure properties associated with data assets 4
2.2.4 Threats on the identified data assets 5
2.3 Security Objectives 6
2.3.1 Access Control 6
2.3.2 Security Storage 6
2.3.3 Firmware Authenticity 6
2.3.4 Communication 7
2.3.5 Secure State 7
2.4 Security Requirements 7
2.4.1 Security Requirements table 7
2.4.2 Avoiding firmware abuse threat 7
2.4.3 Avoiding impersonation threat 8
2.4.4 Avoiding man in middle threat 8
2.4.5 Avoiding tampering data 8
3. References 8

1. Objective

1.1 Background

- During our Embedded Architecture and Application lecture series, a remote-controlled student car with assisted driving was developed. The remote control used PSoC5 MCU for reading the joystick data provided by the driver and transmitted the Joystick data in the form of a protocol to the student car via ZigBee. The student car used the PSoC5 MCU to calculate the control speed of the engine motors based on the protocol values and the ultrasound sensor (obstacle detector).

- The driver controls speed and direction of the car using the joystick in the remote control and additionally, the ultrasound sensor was used a safety mechanism to detect the obstacles.

- The car receives the joystick data via ZigBee. Although car checks the integrity of the received protocol using CRC, but the communication between the remote control and the car is not secure because the received data is neither encrypted nor authenticated.
  - Lack of authentication results in unauthorized remote control taking control over the car or remote controller controlling a car that is not truly their car.
  - Lack of encryption can result in man in middle attack unauthorized actor can eavesdrop the protocol data that is transmitted via unsecure BLE channel. This allows them to tamper/modify the protocol.

1.2 Use-Case

The aim of our project is to secure the communication between the remote control (sender) and the car (receiver). This would enable:

1.2.1 Confidentiality:

Any unauthorized source (e.g. Hacker) will not be able to gain access to the joystick data/car control signals transmitted over unsecure BLE channel.

1.2.2 Authenticity:

The car needs to verify that the remote control going to control it is authorized and the remote control needs to validate if it is the true master of the car.

1.2.3 Message Integrity:

Ensures that the joystick data/car control signals protocol has not been modified /tampered.

1.2.4 Non- repudiation:

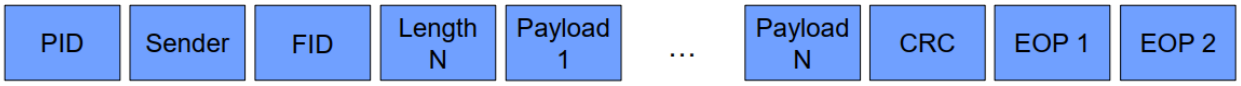
The remote controller (driver) is held credible for the joystick data provided for controlling speed and direction.

2. Threats based Analysis for Embedded Security Use Case – CIA Model

- The CIA Model stands for confidentiality, integrity and authenticity.
- We identify the data and system assets of the product which we want to secure.
- We identify all sources of threats to these data and system assets
- Each threat is assigned a data security objective (confidentiality, integrity and authenticity).

2.1 Protocol Definition

The data that has to be transmitted is composed into a protocol, the protocol looks like this:



where,

- PID stands for protocol Identifier: (Joystick data / Control Signal)
- Sender represents Identifier of the sender (CAR/Remote controller)
- FID stands for feature Identifier: (Connect, Disconnect, Feature, Stop)
- Length : Number of bytes (N)to be transmitted
- Payload : N bytes to be transmitted
- CRC : cyclic redundancy check to ensure integrity of message
- EOP stands for End of payload

2.2 Use case Analysis: secure the communication between remote control and car.

2.2.1 Data asset of remote control

Data Asset	**Description**
Remote Control Identifier	Unique Identifier for the remote control
Remote Control Firmware	Defines the behavior/functionality of the remote control
Cryptographic Credentials	Keys used for Cryptographic procedures
Feature Data	Joystick Data/ Car Control (connect, disconnect, stop) Signals

2.2.2 Data asset of student Car

Data Asset	**Description**
Car Identifier	Unique Identifier for the student car
Car Firmware	Defines the behavior/functionality of the student car
Cryptographic Credentials	Keys used for Cryptographic procedures
Feature Data	Acknowledgement and feature available data

2.2.3 Secure properties associated with data assets

Data Asset	Security Properties	Description
Identifier(ID)	Integrity	ID is a unique proof of identity for the device hence, one should not be able to tamper/modify the ID associated with the device.
Firmware	Confidentiality	Any unauthorized source should not be able to gain access to the firmware, otherwise they can copy it and use in duplicate products.
	Integrity	Any unauthorized actor should not be able to gain access otherwise, they can modify and affect the quality of software leading to uncontrolled behavior.
	Authenticity	The firmware running on the remote control/car should be authentic and the remote control/car on which the firmware is running should be genuine.
Cryptographic Credentials	Confidentiality	Unauthorized source should not be able to access the keys that is used for cryptographic operations like encryption, signature.
	Integrity	Unauthorized actors should not be able to modify/tamper the keys used for Cryptographic services Like Encryption, Signature
Feature Data	Confidentiality	Unauthorized source should not be able to gain access to the Joystick data / car control data otherwise, they can tamper the Joystick data and provide wrong values instead.
	Integrity	Unauthorized actors should not be able to modify/tamper the joystick data and car control signal.

2.2.4 Threats on the identified data assets

Threats	Target data assets	Description
Impersonation	Cryptographic credentials (Keys)	Keys form the cryptographic basis to secure the communication between the remote control and car via BLE. If the confidentiality of keys is compromised, then they can be used by unauthorized actors can gain access to the data that is being communicated via BLE.
Man in the Middle	Cryptographic credentials (Keys)	Secret keys used for cryptographic services like encryption should not be exposed via the unsecure channel, there is chance that unauthorized sources can eavesdrop and tamper/modify the Joystick data or control signals that is being transmitted.
	Feature Data	If the Joystick data/ control signals is not encrypted and authenticated than it can be easily replayed by an unauthorized actor, leading to unapproved sources driving the car.
Firmware Abuse	Firmware	The firmware flashed into MCU of the car and remote control should be genuine, one provided by authorized OEM. If unauthorized firmware is flashed and remote control/car starts, it can lead to undefined/uncontrollable behavior.
Tamper	Cryptographic credentials (keys)	Keys should be unique to the user and it should be stored in a secure environment. Any form of key exchange should be confidential and have a cryptographic basis.
	Firmware	The remote control and the car should always run authorized firmware. Modification of firmware by the unauthorized sources, it must be prohibited.

	Feature Data	The Joystick data or the control signals communicated via the BLE should be secure, any unauthorized sources should not be able to read and tamper these data.
	Unique Identifier	The identifier associated with the remote control and the car are unique. It should not be possible by unauthorized sources to tamper the identifier associated with the device.

2.3 Security Objectives

- To secure the communication between the remote control and the car, we have identified the data assets and its associated security properties.
- Based on this information we have enumerated all possible threats linked with each of the data assets.
- We need to define the security objectives based on the enumerated threats. The table below

Threats →

Security Objectives ↓

	Impersonation	**Man in the middle**	**Firmware Abuse**	**Tamper**
Access Control	X		X	
Secure Storage				x
Firmware Authenticity			X	
Communication		X		
Secure State			X	X

2.3.1 Access Control

- The remote control and the car must allow only the authentic firmware to be flashed.
- The cryptographic keys must be unique for the car and the remote control and must be confidentially inserted/generated in them.
- Before communication is established between the remote control and the car, the remote control should verify if it is communicating with the genuine car and the car needs to verify if it is being controlled by authentic remote control.

2.3.2 Security Storage

- The cryptographic keys must be stored in a secure area inside memory.
- The MCU must not allow overwriting the unique keys, which is already present in the key storage area.
- The secret keys must never be exposed to non-secure environment.

2.3.3 Firmware Authenticity

- The MCU must verify the firmware authenticity before booting and before upgrading based on digital signatures.
- It should also check if the authentic firmware is modified/tampered by using mechanisms like CRC checks.

2.3.4 Communication

- The communication between the remote control and the receiver must be encrypted, so that unauthorized sources are not able to read or modify the protocol that is being transmitted.

2.3.5 Secure State

- The car and the remote control firmware should be able to maintain a secure state in case verification of firmware integrity and authenticity fails during boot up / upgrading.

2.4 Security Requirements

2.4.1 Security Requirements table

Security Objectives	Threats	Methods to avoid threats
Firmware authenticity	Firmware Abuse	Digital Signature (Flashing digitally signed firmware and verifying the authenticity of the signed firmware prior to boot or upgrade) using asymmetric cryptographic algorithm.
Access Control	Impersonation	Digital Signature (Signing the unique credentials exclusive to the car/remote control and verifying the signed credentials of the partner before starting communication with it) using asymmetric cryptographic algorithm.
Secure key Storage and key exchange	Tamper	Once the cryptographic keys are written in key storage area, the firmware must not allow it to be over-written. This can be implemented using e-fuses present in MCU Cryptographic algorithms such as diffie-hellman Algorithm must be used for key exchange between car and remote control.
Communication	Man in middle	Encryption (Encoding the protocol before transmitting in such a way that only authorized person can decode it) using symmetric cryptographic algorithm.

2.4.2 Avoiding firmware abuse threat

- The authenticity of the firmware has to be verified prior to boot/upgrade. This can be done by signing the firmware using digital signature. The MCU must boot only if the digital signature of the flashed firmware is authentic also known as secure boot.

- The firmware can be signed digitally using keys generated by cryptographic algorithms. The cryptographic algorithm used for generating signature must be asymmetric to ensure non-repudiation, i.e. the actors (OEMs) signing the firmware (or a message) are held credible for the firmware that is flashed.

- The authorized source signs the firmware using a key. This key must be exclusively associated with the source and it must be kept confidential.

- The cryptographic key used to verify the authenticity of the flashed firmware must be injected in the MCU of remote control/car in a secure and confidential manner.

2.4.3 Avoiding impersonation threat

- The car and remote control will have a unique identification number (credentials) associated with them.
- Before starting communication between car and remote control, the car needs to verify that the remote control going to control it is authorized and the remote control needs to validate if it is the true master of the car.
- This can be achieved using Digital signatures. Both car and remote control should sign the credentials that are uniquely linked with them. This digitally signed credentials acts as an exclusive proof of identity.
- Remote control sends its signed credentials and car should be able to verify it and then the car sends its signed credentials and remote control should be able to verify it.
- The keys used for verifying the signed credentials should be exchanged between the car and the remote control in a confidential and a secure manner.

2.4.4 Avoiding man in middle threat

- We need to encrypt the protocol that is being transmitted via unsecure BLE channel so that if the unauthorized actors eavesdrop they are not able to read/tamper the original protocol data.
- Encryption can be done using symmetric cryptographic algorithm, since the credibility of the actor/source is verified during authentication. It is only required to encode the original protocol such that only the authorized device is able to decode it.
- We need to exchange a secret key between the car and remote control so that using this key encryption can be performed. This key exchange should be done in a secure and confidential manner.

2.4.5 Avoiding tampering data

- The cryptographic keys are linked exclusively to the device (remote control/car). Hence, it must be stored in a secure and confidential manner. It is vital for the MCU to have hardware-based isolation between secure and unsecure execution environments.
- Once the cryptographic keys are written in key storage area, the firmware must not allow it to be over-written. This can be implemented using e-fuses present in MCU.
- The key used for signing the firmware (secure boot to avoid firmware abuse), the keys used for the signing the credentials (to avoid impersonation) and keys used for encryption must be different. This is necessary because if same key is used to avoid the threats, compromising the confidentiality of the keys can lead to multiple/all security threats.
- The key exchange between the car and remote control via unsecure BLE channel should be performed using cryptographic algorithms such as diffie-hellman so that the confidentiality of the keys are not compromised.

3 References

- https://www.cypress.com/file/447056/download