Kai Tindall

k.tindall-2018@hull.ac.uk

Abstract

This document will define the requirements for the security in internet of things devices project software.

Software requirements specification

Security in Internet of Things Devices

Table of Contents

[1.1 Revision History 2](#_Toc57201636)

[1.2 Document References 2](#_Toc57201637)

[1.3 Acronyms 2](#_Toc57201638)

[1.4 Glossary 2](#_Toc57201639)

[2 Specific Language Definitions 3](#_Toc57201640)

[3 Requirements 3](#_Toc57201641)

[3.1 IoT Device Requirements 3](#_Toc57201642)

[3.2 Command and Control Server Requirements 3](#_Toc57201643)

[3.3 Client Requirements 4](#_Toc57201644)

[3.4 Security Requirements 4](#_Toc57201645)

## Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Date** | **Author** | **Comment** |
| 1.0 | 25/11/2020 | Kai Tindall | Initial draft of the document. |

## Document References

|  |  |  |  |
| --- | --- | --- | --- |
| **Identification Number** | **Description** | **Version** | **Reference Number** |
|  |  |  |  |
|  |  |  |  |

## Acronyms

|  |  |
| --- | --- |
| **Acronym** | **Definition** |
| IoT | Internet of Things |
| C&C | Command and Control |
| API | Application Programming Interface |
| GUI | Graphical User Interface |

## Glossary

|  |  |
| --- | --- |
| **Word** | **Definition** |
| Traffic | The encrypted messages being passed between the IoT devices, C&C server, and the client. |
|  |  |

# Specific Language Definitions

The use of "shall", "should", "must", "will", and "may" within this document observe the following rules:

The word "shall" in the text expresses a mandatory requirement of this document. Departure from such a requirement is not permissible without formal agreement of the project manager.

The word "should" in the text expresses a recommendation or advice on implementing such a requirement of the specification. The project manager expects such recommendations or advice to be followed unless good reasons are stated for not doing so.

The word "must" in the text is used for legislative or regulatory requirement (e.g. Health and Safety) with which the project is to comply with. It is not used to express a requirement of this document.

The word "will" in the text expresses a provision or service external to the project or an intention external to the project in connection with a requirement of this document. The project is implicitly authorised to rely on such service or intention.

The word "may" in the text expresses a permissible practice or action. It does not express a requirement of this document.

# Requirements

## IoT Device Requirements

|  |  |
| --- | --- |
| **Requirement ID** | **Description** |
| SITD-DD-001 | The IoT device shall run the driver software on start-up. |
| SITD-DD-002 | The IoT device shall be able to transmit messages to the C&C server. |
| SITD-DD-003 | The IoT device shall be able to receive message from the C&C server. |
| SITD-DD-004 | The IoT device shall be able to decode encrypted messages. |
| SITD-DD-005 | The IoT device shall be able to encode messages. |
| SITD-DD-006 | The IoT device shall be able to sign messages. |
| SITD-DD-017 | The IoT device shall be able to check the authenticity of messages. |
| SITD-DD-007 | The IoT device shall be able to perform a key exchange with the C&C server. |
| SITD-DD-008 | The IoT device shall reject unauthorised communication. |
| SITD-DD-009 | The IoT device shall not crash if it encounters erroneous traffic. |
| SITD-DD-010 | The IoT device shall reply with a standard error report when it encounters erroneous traffic. |
| SITD-DD-011 | The IoT device shall reply to any authorised traffic with an acknowledgement message. |
| SITD-DD-012 | The IoT device shall wait for an acknowledgement message before sending repeat messages. |
| SITD-DD-013 | The IoT device should wait for 100 milliseconds before attempting repeat messages. |
| SITD-DD-014 | The IoT device shall be able to receive a workload to be deployed. |
| SITD-DD-015 | The IoT device shall be able to receive data to pass through to the running workload. |
| SITD-DD-016 | The IoT device shall be able to transmit data from the running workload back to the command and control server. |
| SITD-DD-017 | The IoT device shall receive the encryption method being used by the C&C server. |

## Command and Control Server Requirements

|  |  |
| --- | --- |
| **Requirement ID** | **Description** |
| SITD-CC-001 | The C&C server shall run on start-up. |
| SITD-CC-002 | The C&C server shall poll the network to discover new devices to connect to. |
| SITD-CC-003 | The C&C server should poll the network every 10 seconds. |
| SITD-CC-004 | The C&C server shall attempt to connect to a device when it receives the command to from the client. |
| SITD-CC-005 | The C&C server shall expose an API that the client can connect to. |
| SITD-CC-006 | The C&C server shall be able to encrypt traffic. |
| SITD-CC-007 | The C&C server shall be able to unencrypt traffic |
| SITD-CC-008 | The C&C server shall be able to perform a key exchange. |
| SITD-CC-009 | The C&C server shall be able to sign messages. |
| SITD-CC-010 | The C&C server shall be able to check the authenticity of messages. |
| SITD-CC-011 | The C&C server shall be able to transmit encrypted traffic. |
| SITD-CC-012 | The C&C server shall be able to receive encrypted traffic. |
| SITD-CC-013 | The C&C server shall reject unauthorised communication. |
| SITD-CC-014 | The C&C server shall not crash if it encounters erroneous traffic. |
| SITD-CC-015 | The C&C server shall serve API requests it receives from clients. |
| SITD-CC-016 | The C&C server may have the option to change the encryption method. |
| SITD-CC-017 | The C&C server shall act as a central authority for public keys. |

## Client Requirements

|  |  |
| --- | --- |
| **Requirement ID** | **Description** |
| SITD-CL-001 | The Client shall be able to perform a key exchange with the C&C server. |
| SITD-CL-002 | The Client shall be able to display information received from the C&C server. |
| SITD-CL-003 | The Client shall allow the user to input data to send to an IoT device. |
| SITD-CL-004 | The Client shall allow the user to send a workload to an IoT device. |
| SITD-CL-005 | The Client shall have a GUI. |
| SITD-CL-006 | The Client shall be able to sign encrypted traffic. |
| SITD-CL-007 | The Client shall be able to encrypt traffic. |
| SITD-CL-008 | The Client shall be able to decrypt traffic. |
| SITD-CL-009 | The Client shall be able to send encrypted traffic over an API. |
| SITD-CL-010 | The Client shall be able to receive encrypted traffic over an API. |
| SITD-CL-011 | The Client shall request data from the C&C server. |
| SITD-CL-012 | The Client should request data from the C&C server every five seconds. |
| SITD-CL-013 | The Client should give the user an option to change the amount of time the client waits to request data from the C&C server. |
| SITD-CL-014 | The Client shall reject unauthorised communication. |
| SITD-CL-015 | The Client shall not crash if it encounters erroneous traffic. |
|  |  |

## Security Requirements

|  |  |
| --- | --- |
| **Requirement ID** | **Description** |
| SITD-SEC-001 | All traffic shall be encrypted using a reputable method. |
| SITD-SEC-002 | All encryption methods shall be written by qualified reputable external authors. |
| SITD-SEC-003 | Each message shall be signed by the author. |
| SITD-SEC-004 | Encryption functionality shall be written as a library to enable reuse. |