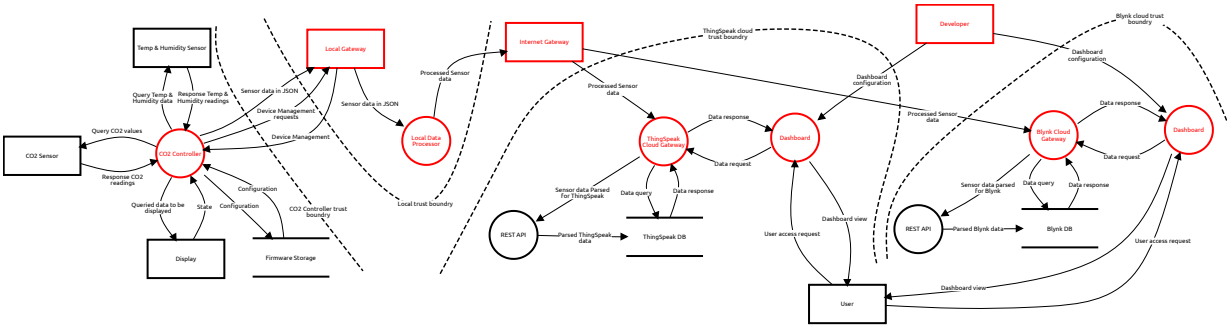
Threat model report for IOT Prototype Threat Model

Owner:
Hamza Shabir
Reviewer:
Contributors:

High level system description

Threat modelling diagram for an IOT prototype which monitors CO2 concentrations in the Air.

IOT Prototype Threat Model



CO2 Controller (Process)

Description:
The brains of the prototype and is an electronic hardware development/prototyping board. This is used to power the sensors and get appropriate values with the use of software and any other processing required like in our case calculating AQI.

Impersonating the device for illicit purposes

Spoofing, Open, Medium Priority

Description:

Mitigation:

Modification or destruction of the device or it's sensors

Tampering, Open, Medium Priority

Description:

Mitigation:

Temp & Humidity Sensor (External Actor)

Description:
DHT 22 - This is a Humidity and Temperature sensor.

No threats listed.

CO2 Sensor (External Actor)

Description:
MQ 135 - This is a Gas sensor which offers a low-cost solution for detecting the concertation of gases in the Air (especially CO2) in PPM (parts per million).

No threats listed.

Display (External Actor)

Description:

No threats listed.

Query Temp & Humidity data (Data Flow)

Description:

No threats listed.

Response Temp & Humidity readings (Data Flow)

Description:

No threats listed.

Query CO2 values (Data Flow)

Description:

No threats listed.

Response CO2 readings (Data Flow)

Description:

No threats listed.

Queried data to be displayed (Data Flow)

Description:

No threats listed.

State (Data Flow)

Description:

No threats listed.

Firmware Storage (Data Store)

Description:

No threats listed.

Configuration (Data Flow)

Description:

No threats listed.

Configuration (Data Flow)

Description:

No threats listed.

Internet Gateway (External Actor)

Description:

Man in the Middle attack

Tampering, Open, Medium Priority

Description:

Mitigation:

Impersonating to inject false data

Spoofing, Open, Medium Priority

Description:

Mitigation:

Overload attack

Denial of service, Open, Medium Priority

Description:

Mitigation:

Local Data Processor (Process)

Description:
This is an app that retrieves the data sent by the controller through serial.

Modification of data being processed

Repudiation, Open, Medium Priority

Description:

Mitigation:

Unauthorised access to data or Software which stores API keys

Information disclosure, Open, Medium Priority

Description:

Mitigation:

Local Gateway (External Actor)

Description:
This is a computer the controller is connected to.

Impersonating the device for illicit purposes

Spoofing, Open, Medium Priority

Description:

Mitigation:

Restrict access by overloading resources

Denial of service, Open, Medium Priority

Description:

Mitigation:

Sensor data in JSON (Data Flow)

Description:

No threats listed.

Device Management (Data Flow)

Description:
Flashes the controller with new firmware

No threats listed.

Device Management requests (Data Flow)

Description:
Request for firmware upgrade

No threats listed.

Sensor data in JSON (Data Flow)

Description:

No threats listed.

Processed Sensor data (Data Flow)

Description:

No threats listed.

ThingSpeak Cloud Gateway (Process)

Description:

Injecting false data

Spoofing, Open, Medium Priority

Description:

Mitigation:

Man in the Middle attack

Tampering, Open, Medium Priority

Description:

Mitigation:

User (External Actor)

Description:

No threats listed.

ThingSpeak DB (Data Store)

Description:

No threats listed.

Data query (Data Flow)

Description:

No threats listed.

Data response (Data Flow)

Description:

No threats listed.

REST API (Process)

Description:

No threats listed.

Parsed ThingSpeak data (Data Flow)

Description:

No threats listed.

Processed Sensor data (Data Flow)

Description:

No threats listed.

Sensor data Parsed for ThingSpeak (Data Flow)

Description:

No threats listed.

Dashboard (Process)

Description:

Spoofing data

Spoofing, Open, Medium Priority

Description:

Mitigation:

Eavesdropping attack or Unauthorised data access

Information disclosure, Open, Medium Priority

Description:

Mitigation:

Overload server

Denial of service, Open, Medium Priority

Description:

Mitigation:

Data request (Data Flow)

Description:

No threats listed.

Data response (Data Flow)

Description:

No threats listed.

Developer (External Actor)

Description:

Impersonate Developer

Spoofing, Open, Medium Priority

Description:

Mitigation:

Dashboard configuration (Data Flow)

Description:

No threats listed.

Dashboard view (Data Flow)

Description:

No threats listed.

User access request (Data Flow)

Description:

No threats listed.

Blynk Cloud Gateway (Process)

Description:

Injection of false data

Spoofing, Open, Medium Priority

Description:

Mitigation:

Man in the Middle attack

Tampering, Open, Medium Priority

Description:

Mitigation:

Processed Sensor data (Data Flow)

Description:

No threats listed.

REST API (Process)

Description:

No threats listed.

Sensor data parsed for Blynk (Data Flow)

Description:

No threats listed.

Blynk DB (Data Store)

Description:

No threats listed.

Data query (Data Flow)

Description:

No threats listed.

Data response (Data Flow)

Description:

No threats listed.

Parsed Blynk data (Data Flow)

Description:

No threats listed.

Dashboard (Process)

Description:

Spoofing data

Spoofing, Open, Medium Priority

Description:

Mitigation:

Eavesdropping attack or Unauthorised data access

Information disclosure, Open, Medium Priority

Description:

Mitigation:

Overload server

Denial of service, Open, Medium Priority

Description:

Mitigation:

Data request (Data Flow)

Description:

No threats listed.

Data response (Data Flow)

Description:

No threats listed.

User access request (Data Flow)

Description:

No threats listed.

Dashboard view (Data Flow)

Description:

No threats listed.

Dashboard configuration (Data Flow)

Description:

No threats listed.