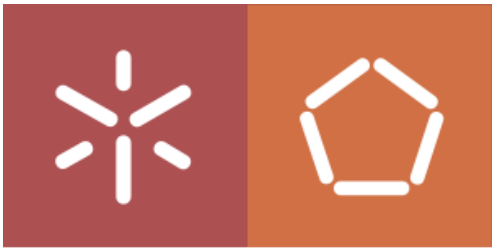


Universidade do Minho
Escola de Engenharia

Segurança de Sistemas Informáticos

Ficha de Exercicios 2 – Threat Modelling

Grupo 04

2022/2023

A91697 - Luís Filipe Fernandes Vilas

A91671 - João Manuel Novais da Silva

Prazo de submissão: 23:59 de 18/04/2023

Wireless sensor and actuators nodes (WSN)

. Integrated sensors for data acquasition (temperature, humidity, light)

. Data is sent to a base station/gateway located at the field (#ZigBee sensors, TelosB motes, Arduino or Raspberry <1000)

. Actuators can change some operation states

. Organized in nodes

Basestation/gateway

. They communicate through diverse radio interfaces with sensors and actuators, and they use cellular radio interfaces with GSM and/or GPRS/LTE for

internet connectivity (se nao ha segurança na rede, implementamos isso na aplicaçao)

. They are responsible to manage sensors and actuators's operations according to the analytics from the back end

. There can be more than one gateway but each WSN node is managed by only one gateway

. Their job:

-> receive feed from WSN nodes

-> data aggregation

-> run IoT-enabled applications for real-time control and analytics

-> provide transient storage

-> send data summaries to the cloud

Cloud-bases back-end

3.1 - Milti-tenant cloud storage

: it can include AWS cloud, Azure and Google cloud

3.2 - Analytics module

: Receiving and aggregating data summaries from gateway nodes

: Performing analysis on the field data

: Sending new application rules to gateways

: Providing open APIs for data handling, service access (for farmers or experts (READ-ONLY)) and development

Dashboard/GUI

. Web bases, front-end module for personal computers, tablets and smartphones with 2 modes:

-> For the farmers

- Presents history of collected data and business analytics

-> For experts

- Provide a platform for the users to enhance the system knowledge

Threat modelling

- Analysis of what can be wrong with what you are creating

- A set of idealised attackers

- tempering, spoofing

    - Strategies for modelling:

        -> Unstructured (brainstorming, literal review)

        -> Structured (focusing on assets, attacker and on software)

    - Focus on attackers

        -> Use Barnard's list

        -> Use Verizon's list

        -> Understand the reasons of attack

    - Take into a count the types of attacks and their impact on the system

. Model System

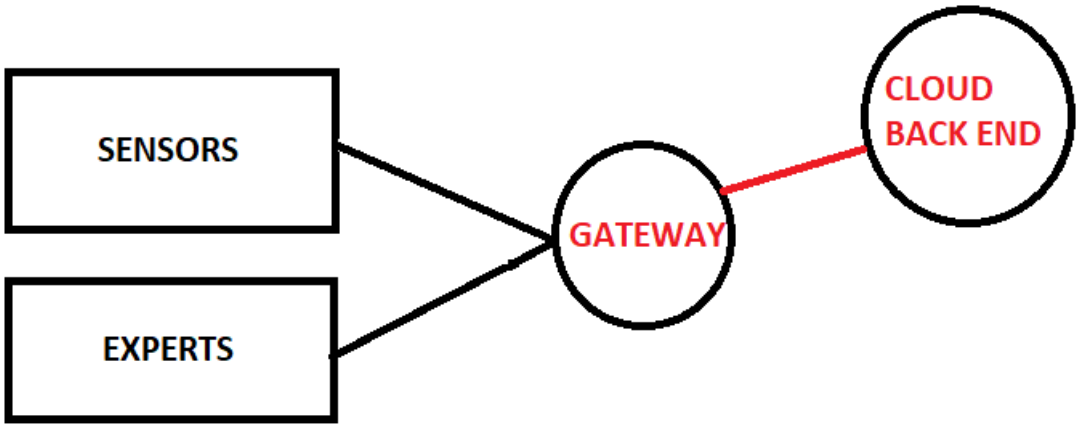
    - Diagrams are a natural way to model software

        -> Data flow Diagrams (table with collumns: Elemente, Appearance, Meaning, Examples)

        -> UML

        -> Swim Lane Diagrams (diagrams from SCR and CC)

-> State Diagrams



. Find threats