Universidade do Minho
Mestrado em Engenharia Informática
Tecnologias de Segurança
Ficha 02
Threat modelling

Objective

Provide a detailed threat model for the *Precision Agriculture System* described below. The model consists of a report following any strategies presented in the practical class.

Consider using CWE and EoP cards (https://goo.gl/9WYjcD) as repertoire sources.

Precision agriculture system

The *precision agriculture system* uses technology and scientific principles to analyse and manage a crop based on the spatial and temporal variability of the environment associated with all aspects of agricultural production within fields in near real-time. The platform consists of the following main components:

1 - Wireless sensor and actuators nodes (WSN)

The first type of device is integrated sensors for data acquisition (e.g., temperature, humidity, light) enabled with wireless interfaces for sending the data to a base station/gateway located at the field. It might be ZigBee sensors, TelosB motes, Arduino or Raspberry devices. In a farm installation, the number of nodes could be up to a thousand.

The actuators are also field devices that can modify the operation state of diverse farm devices, such as the amount of water a watering system provides to plants or the temperature of a greenhouse;

2 - Basestation/gateway

They are enabled with diverse radio interfaces for communication with heterogeneous sensors/actuators and cellular radio interfaces with GSM and/or GPRS/LTE for internet connectivity. This type of device is responsible for managing sensors/actuators by adjusting their operation according to analytics in the back end.

In a farm installation, more than one gateway could exist. However, each WSN node is managed by only one gateway. Some of their main tasks include:

- Receive feed from WSN nodes using any protocol available in real-time
- Data aggregation (from sensors in the field);
- Run IoT-enabled applications for real-time control and analytics;
- Provide transient storage;
- Send periodic data summaries to the cloud.

3 - Cloud-based back-end

The back-end system includes:

3.1 - Multi-tenant cloud storage

It might include AWS Cloud, Azure and Google Cloud.

3.2 - Analytics module

Responsible for:
- Receiving and aggregating data summaries from many gateway nodes;
- Performing analysis on the field data;
- Sending new application rules to the gateways;
- Providing open APIs for data handling, service access (from farmers and experts) and development of new applications per farming case

4 - Dashboard/GUI

This is a web-based front-end module for personal computers, tablets, and smartphones. It provides two modes: (i) one for farmers, which presents the history of collected data and business analytics for decision making, and (ii) one for experts, continuously enhancing system knowledge based on the field state of the art.

For such a system, some general security requirements include:

- Integrity: corrupted or manipulated data will affect the provided services;

- Authentication: avoid injecting additional packets and nodes accepting false administrative tasks (e.g. network reprogramming);

- Availability: The users of the sensor network must be capable of accessing its services whenever they need them;

- Auditing: To adjust their behaviour, sensor nodes must be able to know the state of their surroundings;

- Privacy and Anonymity: the location and identities of the base station and the nodes that generated information should be hidden or protected.