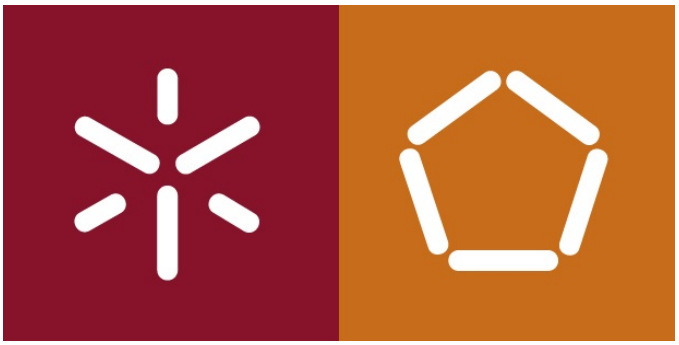
Universidade do Minho

Mestrado Integrado em Engenharia Informática -
Criptografia e Segurança da Informação



Tecnologias de Segurança

Relatório do Trabalho Prático 1- Parte B

Threat modelling

Pedro Freitas	André Gonçalves	Carla Cruz	Adriana Meireles
A80975	A80368	A80564	A82582

October 25, 2019

Contents

1 Introdução

No âmbito da unidade curricular de Tecnologia de Segurança foi-nos proposto uma análise a um sistema de **Precision Agriculture System**. Este trabalho apareceu como complemento ao primeiro onde foram analisadas algumas vulnerabilidades e algumas formas de explorá-las para podermos agora ter uma análise mais consciente e mais fundamentada.

Ao longo deste relatório vamos explicar o sistema, assim como as medidas de segurança que vamos aplicar ao mesmo e ainda propôr soluções ou medidas que evitem vulnerabilidades.

2 Precision Agriculture System

O principal foco deste trabalho é a análise deste sistema sendo por isso necessário, numa primeira fase, um estudo sobre o mesmo.

2.1 O que é?

O **Precision Agriculture System** é , tal como o nome indica, um sistema de agricultura que tem como objetivo utilizar a tecnologia de modo a poder monitorizar mais precisamente todas as áreas de atividades agronômicas. Esta monitorização é baseada nas condições que afetam as colheitas como a temperatura, luz, humidade, entre outros.

2.2 Componentes

O sistema é constituído por:

- Wireless sensor and actuators nodes (WSN)

  Aparelhos com sensores integrados para recolha de dados com ligações sem fios, que comunicam com as Basestations. Os atuadores são aparelhos que podem alterar o estado de operações dos diversos aparelhos agrícolas.

- Basestation/gateway

  Recebe os dados dos sensores e de acordo com a análise destes mesmos dados,segundo os métodos de análise do back-end, envia informações aos atuadores de como devem passar a proceder. Além disso também envia ,periodicamente, resumos dos dados recolhidos para a cloud.

- Cloud-based back-end

  Recebe e agrega dados dos sensores provenientes das Basestation, analisa esses mesmos dados e envia os novos procedimentos aos gateways. Além disso providencia API's para gestão dos dados, quer por experts, quer por agricultores.

- Dashboard/GUI

  Com um web-based front end para dispositivos móveis, é possível usufruí-la de dois modos:

  - *Farmer:* Apresenta o histórico dos dados recolhidos e das análises de negócio para tomar decisões
  - *Expert:* Vai fornecendo dados continuamente de modo a aumentar a inteligência do sistema com base no estado do terreno.

3 Requisitos de Segurança

Para podermos fazer uma análise às possíveis vulnerabilidades do sistema é necessário termos em conta um modelo de ameaças. Para tal vamos basear a nossa análise no modelo STRIDE. Nesta secção vamos explicar este modelo, expondo um pouco o que ele representa.

3.1 STRIDE

STRIDE é um acrónimo que representa todas as ameaças que queremos evitar no nosso sistema pois atacam propriedades de segurança que queremos garantir. Assim temos:

- **S**poofing

  Situação onde um programa ou pessoa consegue fazer-se passar por outra para ter acesso : Impersonating do sistema. Esta ameaça ataca a *Autenticidade*.

- **T**ampering

  Alteração de informação do sistema. Esta ameaça ataca a *integridade*.

- **R**epudiation

  Rejeita a autoria de algo que aconteceu, atacando assim o *Não Repúdio*.

- **I**nformation Disclosure

  É caracterizado por haver leaks ou brechas de informação privada, podendo assim ser acedida por outros. Esta ameaça ataca a *Confidencialidade*.

- **D**enial of Service

  Sobrecarga dos recursos necessários para providenciar um serviço, tornando-o indisponível. Ataca a *Disponibilidade* do sistema.

- **E**levation of Privilege

  Permitir uma entidade a fazer algo que não deveria poder fazer. Ataca as propriedades de *Autorização* do sistema.

4 Modelação do sistema

Sabendo os requisitos de segurança a serem considerados, também é necessário fazer uma modelação de sistema para podermos compreender onde cada vulnerabilidade se pode encaixar. Assim vamos apresentar alguns diagramas que nos ajudaram a tomar consciência de problemas que esta *PAS* poderiam ter.

4.1 Threat Model

Os diagramas de *Threat Model* são diagramas de fkuxo de dados (**DFD's**). Estes diagramas são usados para arquiteturas de sistemas e encaixam nos problemas de fluxo de dados. De forma a obtermos uma abordagem fidedigna vamos usar como nomenclatura do diagrama:

Figure 1: Nomenclatura DFD's

Sabendo isto começamos por identificar as entidadas externas, os processos do sistema e a entidade responsável pelo armazenamento de dados:

- Entidades externas: Farmers e Experts
- Processos: WSN, Basestation, Back-end e GUI.
- Base de dados: Cloud

Assim, juntamente com os fluxos de dados, podemos prosseguir para a construção do diagrama propriamente dito:

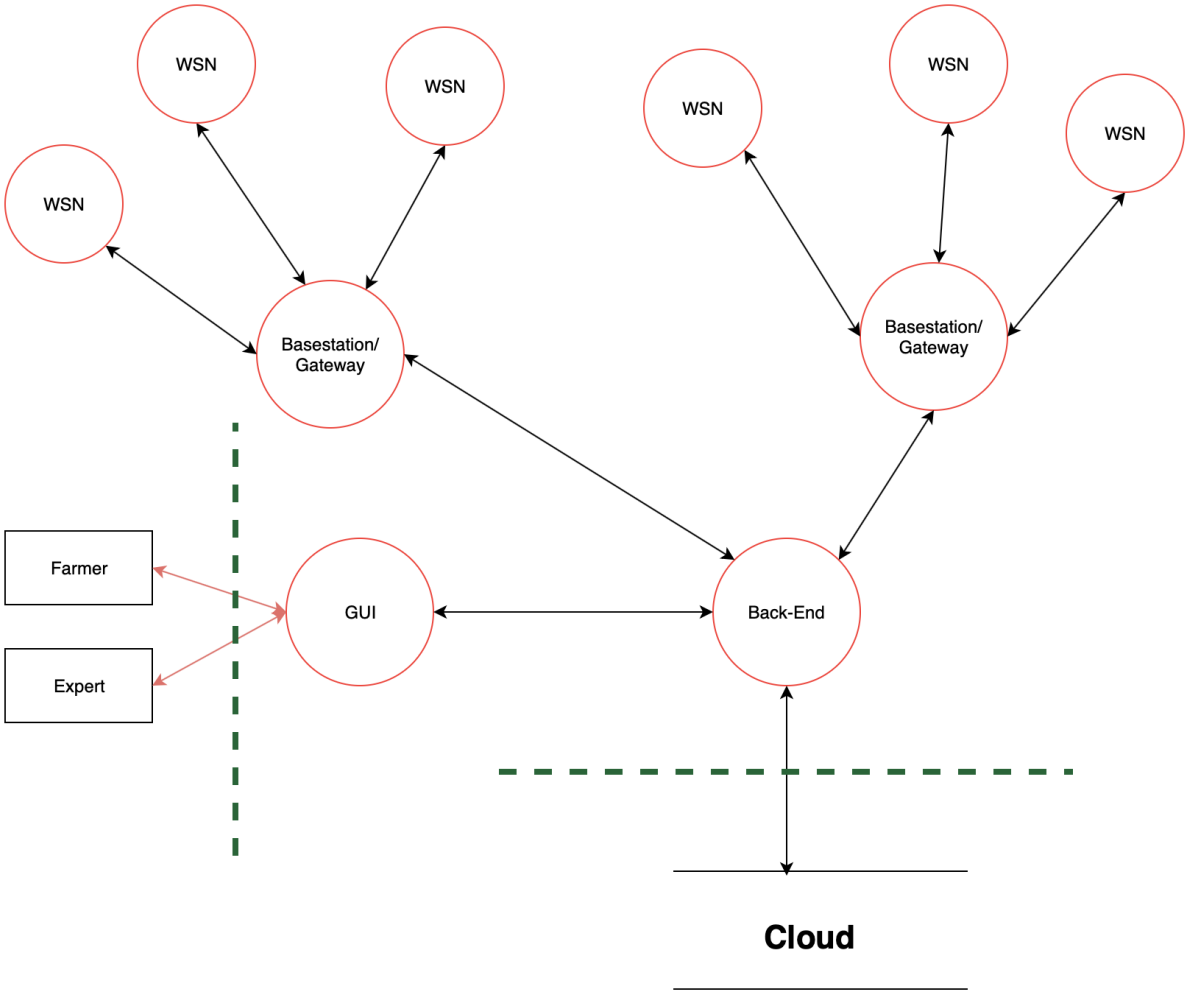


Figure 2: Diagrama DFD

5 Ameaças ao sistema

5.1 Basestation

A basestation é a componente do sistema que controla a rede de sensores e, de modo a salvaguardar os dados, envia-os para uma Cloud. Também recebe dados de controlo dos sensores resultantes da Cloud de backend.

Este constituinte comunica com a WSN através da tecnologia GSM e estabelece ligação à Internet através do uso de GPRS/LTE. Com as tecnologias referidas anteriormente os utilizadores podem autenticar-se e ter a sua privacidade devido à utilização de algoritmos de encriptação dos dados.

5.1.1 GPRS/LTE

As operadoras móveis, como é o caso de GPRS, são responsáveis pela proteção dos dados pois utilizam IP's privados, tradutores de endereços de rede e firewalls, de maneira a restringir o acesso aos dados privados. Pelo facto de as firewalls não garantirem privacidade e confidencialidade, torna-se fundamental juntar as medidas referidas anteriormente com VPN. O mesmo garante autenticação dos utilizadores, estabelece canais seguros entre componentes que comunicam entre si e garante o encapsulamento e proteção dos dados da rede. No entanto, apesar de todos os mecanismos de segurança, algumas falhas podem ser detetadas como, por exemplo, das categorias *Denial of Service* e *Information Disclosure*

⇒ **Denial of Service**

- **Descrição:** É possível identificar uma interface,Gp, que é o ponto de ligação entre diferentes redes GPRS e que possui algumas ameaças. As mais relevantes são integridade e confidencialidade dos dados, autenticação e autorização dos utilizadores bem como disponibilidade de recursos. Esta interface possui poucas ou nenhumas medidas de segurança no que toca ao protocolo GTP (grupo de protocolos que atuam sobre as comunicações IP dentro da GPRS). Deste modo, é possıvel a um atacante gerar uma quantidade de tráfego, quer IP, quer GTP, suficiente para inundar os nodos com tráfego inútil que consome a maior parte dos recursos de comunicação, indisponibilizando-os ao utilizador. Em simultâneo,ainda através do GTP, um utilizador malicioso consegue apagar ou atualizar contextos PDP, que podem remover ou modificar canais usados para a transferência de dados o que indisponibiliza os recursos aos utilizadores.
- **Mitigação:** Dada pela introdução de medidas de segurança nos protocolos como a cifragem dos dados.

⇒ **Information Disclosure**

- **Descrição:** Esta tecnologia utiliza o protocolo de sinalização SS7. O mesmo para além de não providenciar nenhuma medida de proteção capaz de garantir confidencialidade ou integridade dos dados também não fornece nenhum sistema de autenticação para os nodos da rede e para as mensagens da mesma.

  Nos dias de hoje, por estar disponível para um maior número de instituições, a falta de medidas de segurança permite a um atacante ter acesso a informação privada. Para isso, basta realizar um pedido de autenticação ao componente responsável.

- **Mitigação:** A solução passa por cifrar as mensagens e também pelo uso de sistemas de autenticação dos utilizadores como,por exemplo, o IMSI (International Mobile Subscriber Identity)

5.1.2 GSM

O GMS é responsável por garantir integridade, confidencialidade dos dados e autenticação do cliente. Deste modo, recorre a três algoritmos, A3 para autenticação do cliente com uma chave de 128 bits, A5 para encriptar e desencriptar a informação e A8 para a geração de chaves aleatórias.

⇒ **Spoofing**

- **Descrição:** A Base Statio(BS) é o hardware responsável pelo tráfico da rede, encaminhamento e decisão de encriptação dos sinais para o GSM core-network.

  Este ataque envolve a componente referida anteriormente e faz com que um atacante se comporte como uma BS e explore uma falha na autenticação da GSM que permite que a BS aja como o man in the middle e receba todo o tráfico que passa na rede. A decisão do uso de encriptação é incumbida à BS e, portanto, o atacante pode baixar a segurança da mesma desligando a encriptação dos dados. Deste modo, passa a ter acesso a toda a informação que passar na BS.

  No caso de estudo, o sistema de agricultura, este ataque pode ser usado para o roubo de informação sobre as plantações em questão.
- **Mitigação:** A solução seria eliminar a tecnologia 2G (GSM) e a passagem para 3G (GPSR), que providencia canais mais seguros e outras formas de segurança como protocolos SSL/TLS.

⇒ **Tampering**

- **Descrição:** Um ataque spoofing desencadeia outros ataques como é o caso de *Man in the middle* no qual são guardados dados falsificados devido à comunicação entre a basestation e a Cloud onde são gerados dados adulterados.
- **Mitigação:** A solução seria eliminar a tecnologia 2G (GSM) e a passagem para 3G (GPSR), que providencia canais mais seguros e outras formas de segurança como protocolos SSL/TLS.

5.2 Base de dados em Cloud

⇒ **Information Disclousure**

- **Descrição:**

  Acesso não autorizado - O sistema fica sensível dado que um utilizador atacante poderá aceder a informação contida na base de dados.

  Roubo de informção sensível - O atacante poderá obter informações sensíveis ao sistema ao realizar um ataque, pois o sistema fica vulnerável permitindo que o atacante tenha acesso às credenciais que lhe permite obter essas informações.
- **Mitigação: Acesso não autorizado** - Toda a informação que se pretende obter da base de dados será autenticada.

  Roubo de informção sensível - De forma a restringir a base de dados, é utilizada uma *Firewall* que limita o acesso dos ips existentes na rede do servidor.

⇒ **Tampering**

- **Descrição:**

  A base de dados utilizada foi fornecida por outrem, deste modo não temos garantias de que a nossa informação lá guardada não foi alterada.

- **Mitigação:**

  Ficheiros de Log - Registar todas as operações efectuadas na base de dados em ficheiros de log.

  Hash de Informação - Quando é realizado o armazenamento de informação na base de dados é necessário calcular uma hash da informação guardada ,em MD5 ou Sha-1/Sha-3 por exemplo, num local diferente e depois, ao realizar a consulta na base de dados, deveremos por sua vez, calcular a Hash da informação obtida e comparar esta com a que foi previamente armazenada.

⇒ **Denial of Service**

- **Descrição:**

  Para que a base de dados perca a capacidade de resposta de pedidos esta é atacada de forma a que os recursos disponíveis sejam consumidos em demasiada, perdendo essa capacidade.

- **Mitigação:**

  Redundância de Dados - De forma a precaver que o sistema sofra um ataque e que percamos todo o acesso à nossa informação, deveremos ter os nossos dados guardados em diferentes bases de dados.

⇒ **Elevation of Privileges**

- **Descrição:**

  A base de dados tem diferentes tipo de permissões conforme o tipo de utilizador que está a ir buscar informação. Assim, o atacante pode utilizar diferentes vetores de ataque e conseguir os privilégios do administrador, alterando a informação armazenada.

- **Mitigação:**

  A implementação de um sistema de permissões bem elaborado

⇒ **Repudition**

- **Descrição:**

  Ficheiros de logs - O atacante pode tentar ler, alterar ou apagar ficheiros de logs sobre as operações efectuadas na base de dados.

- **Mitigação:**

  Ficheiros de logs - Utilizar um sistema de controlo de integridade seguro.

5.3 Dashboard/GUI

A dashboard é a componente do sistema que permite o monitoramento dos dados do sistema. Possui dois modos: um para os agricultores analisarem as produções de forma a tomar decisões e outro para especialistas conseguirem melhorar o sistema com base no estado de arte.Dashboards são painéis que

mostram métricas e indicadores importantes para alcançar objetivos e metas traçadas de forma visual, facilitando a compreensão das informações geradas. As falhas que podem ser apontadas a este componete são todas aquelas representadas pelo acrónimo STRIDE: *Spoofing*, *Tampering*, *Repudition*, *Information Disclosure*, *Denial of Service* e *Elevation of Privileges*.

⇒ **Spoofing**

- **Descrição:** Muitos dos protocolos no TCP/IP não disponibilizam mecanismos adequados de autenticação da origem e destino da mensagem e ficam assim vulneráveis a ataques de spoofing quando as aplicações não tomam precauções relativamente à verificação da identidade do host que envia ou recebe.
- **Mitigação:** Ataques de spoofing que tiram partido disto podem ser mitigados com o uso de *firewalls* capazas de inspecionar os pacotes ou de verificar a identidade do host que envia ou recebe as mensagens.

⇒ **Tampering**

- **Descrição:** Um ataque spoofing desencadeia outros ataques como é o caso de *Man in the middle* o que permite remover ou adicionar pacotes na comunicação.
- **Mitigação:** Ataques de MITM podem ser prevenidos ou detetados de duas formas: autenticação e "tamper detection". Autenticação permite garantir algum grau de segurança através do conhecimento de que a mensagem provém de uma origem legítima. Tamper detection permite saber se a mensagem foi ou não alterada.

⇒ **Repudition**

- **Descrição:**
  Ficheiros de Log -Um atacante poderá tentar ler, alterar ou apagar ficheiros de logs.
  Negação -Um atacante poderá enviar diversa informação para o servidor e negar a sua autoria.
- **Mitigação:**
  Ficheiros de Log -Utilizar um sistema de controlo de integridade seguro.
  Negação -Utilizar um sistema de autenticação e guardar todas as operações efetuadas num ficheiro de log seguro.

⇒ **Information Disclosure**

- **Descrição:** Information Disclosure diz respeito a uma entidade aceder a informação à qual não é autorizado. Neste caso corresponderia a farmers acederem à informação dos experts e vice-versa.
- **Mitigação:** Garantir a confidencialidade através de uma devida encriptação ou de usar Certificate Authority (CA).

⇒ **Denial of Service**

- **Descrição:** Dos é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Os ataques de negação de serviço procuram tornar as páginas hospedadas indisponíveis na rede. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

- **Mitigação:** Para prevenir estes ataques é necessário identificar e bloquear este "mau" tráfego enquanto, ao mesmo tempo, permitir a receção de mensagens legítimas. No entanto, estas defesas devem se localizar antes ou dentro do web server (não fazem mesmo parte da web application).

⇒ **Elevation of Privileges**

- **Descrição:** Um atacante poderá atacar o servidor de maneira a alojar um código JavaScript malicioso que será executado no browser do cliente (Reflected XSS)
- **Mitigação:** Para combater este ataque é necessário efetuar uma validação rigorosa do input recebido.

5.4 Back-end

O back-end é a entidade/processo que gere todo o sistema, sendo ele o motor de todo o bom funcionamento do PAS. Como qualquer outro componente este também apresenta vulnerabilidades que são importantes ter em conta.

⇒ **Spoofing**

- **Descrição:** Um atacante poderia configurar um servidor falso e, deste modo, abster-se de qualquer comunicação com os restantes elementos ou comunicaria de forma errada. Esta vulnerabilidade poderia abrir um caminho para atacarmos todas as outras propriedades de segurança.
- **Mitigação:** A comunicação entre o *back-end* e as diferentes *basestations* deverá ser sempre autenticada. Se quisermos assegurar um maior nível de segurança poderá ser utilizada autenticação multi-fatores, baseada em parâmetros pré-definidos e num historial de comunicação, e/ou implementar um sistema de assinaturas digitais.

⇒ **Tampering**

- **Descrição:** Para esta ameaça podemos ter dois comportamentos diferentes. O atacante poderá modificar a informação que flui no sistema. Por outro lado o atacante poderá tentar alterar a informação guardada no servidor.
- **Mitigação:** De forma a protegermo-nos contra a modificação de informação a fluir no sistema deveremos usar uma conexão cifrada e/ou assinaturas digitais para garantir a integridade dos dados. Quanto à alteração de dados, deverá ser usado um *Access Control List* restrito e complexo.

⇒ **Repudition**

- **Descrição:** O atacante poderá tentar aceder aos ficheiros de log. Sendo estes os ficheiros que guardam as operações efetuadas o atacante poderá tentar ler,apagar ou alterar todos os ficheiros que contém operações entre o *back-end* e os restantes elementos do sistema.
- **Mitigação:** Para tal é necessário utilizar um sistema de controlo de integridade seguro, ou ainda um sistema de backups deste tipo de ficheiros.

⇒ **Information Disclosure**

- **Descrição:** O atacante poderá ter acesso a informação sensível se conseguir intercetar a comunicação entre o *back-end* e os restantes elementos do sistema. Esta interceção leva à exposição dessa mesma informação.
- **Mitigação:** Para tal é necessário um canal de comunicação cifrado entre os elementos do sistema para garantir a confidencialidade dos dados.

⇒ **Denial of Service**

- **Descrição:** Um atacante pode sobrecarregar a rede onde se encontra o servidor de back-end e torná-lo inacessível pela falta de capacidade da rede, pois esta encontra-se saturada de pedidos por responder.
- **Mitigação:** Uma solução seria usar uma *firewall* que reconheça e filtre pedidos possívelmente nocivos para o sistema.

5.5 Sensores Wireless e Actuators nodes

Os sensores wireless e os actuators nodes são responsáveis por recolher dados e alterar o estado de operações dos aparelhos agrícolas, respetivamente. Assim qualquer vulnerabilidade encontrada nestes dispositivos irão afetar todo o sistema, visto que irão comprometer os dados logo desde um estado muito primário.

⇒ **Spoofing**

- **Descrição:** Um atacante pode usar um nodo que se apresenta à rede com múltiplas entidades falsas, tentando personificar um dos sensores do sistema com certos privilégios. Se ele conseguir personificar-se como um sensor vizinho ele pode fazer com que os dados sejam encaminhados para si,corrompendo assim toda a rede.
- **Mitigação:** Podemos assegurar uma comunicação segura entre os nodos de rede através de chaves como Radio Resource Testing (RST), Random Key Predistribution (RKP), Random Password Algorithm (RPA) e Grid Based Transitory Master Key (GBTMK).

⇒ **Tampering**

- **Descrição:** O atacante pode inserir informações falsas em alguns sensores. Esta injeção pode levar a obstruções dos sinais de rádio ou falsificação de dados recolhidos. Isto levará ao envio de informação não fidedigna que resultará em novos procedimentos incorretos ao sistema. Esta injeção poderá ser efetuada presencialmente. Se um atacante tiver acesso físico aos sensores poderá simular(embora de forma não tão fidedigna) propriedades ambientais que poderão levar a recolhas falsas.
- **Mitigação:** Mais uma vez , a solução deste ataque será encriptação de dados. Para o acesso físico toda a área explorada deverá ser restrita.

⇒ **Denial of Service**

- **Descrição:** Se o atacante ganhar acesso a um dos nodos, ele pode saturar o sistema enviando um número suficientemente grande de pacotes de modo a haver tantas colisões quanto necessárias para ser cortada a potência desse mesmo nodo. Também poderá haver esta ameaça através de uma obstrução do sinal.
- **Mitigação:** Podemos resolver as colisões através de ECC (error correcting code). Para o caso da obstrução do sinal basta aumentarmos a largura de banda em relação à mensagem.

5.6 Resumo

Posto isto, podemos resumir todas as vulnerabilidades de cada elemento do sistema com a seguinte tabela:

Threat	**BaseStation**	**Cloud**	**GUI**	**Back-end**	**WSN**
Spoofing	✓	✗	✓	✓	✓
Data Tampering	✓	✓	✓	✓	✓
Repudiation	✗	✓	✓	✓	✗
Information Disclosure	✓	✓	✓	✓	✗
Denial of Service	✓	✓	✓	✓	✓
Elevation of privilege	✗	✓	✓	✗	✗

6 Conclusão

A realização deste trabalho permitiu aprender a elaborar um Threat Model. A sua concretização é muito importante para o sistema mesmo antes de o criar pois permite traçar um mapa das ameaças por componente da plantação (GUI, Backend, BaseStations,WSN) que dessem resposta aos requisitos mínimos de segurança, maioritariamente, a preservação da integridade e disponibilidade dos dados, assim como a privacidade e o anonimato dos mesmos.

Em suma, apesar das dificuldades encontradas ao longo do trabalho, após a realização do mesmo, estamos motivados para os próximos projetos desta Unidade Curricular.