Segurança de Sistemas Informáticos

TPC2
Precision Agriculture System

a85954 Luís Ribeiro

Conteúdo

1 Precision Agriculture System

O objetivo principal deste trabalho é o estudo de um sistema com nome, ***Precision Agriculture System***. Este sistema consiste no uso das tecnologias de modo a explorar técnicas de controlo de atividades que envolvem a Agricultura.

O ***Precision Agriculture System*** é constituída por 4 componentes: *Wireless sensor and actuators nodes (WSN), Basestation/Gateway, Cloud-based back-end e Dashboard/GUI.*

1.1 Wireless sensor and actuators nodes (WSN)

Utilização de sensores para aquisição de *data*, que é enviada para a *Basestation/Gateway.*

Também existem atuadores que servem para modificar o modo de operação dos diversos aparelhos agrícolas.

Esta componente será referida como **Sensor Layer**.

1.2 Basestation/Gateway

É responsável por administrar os sensores e os atuadores, ajustando as suas operações. Usa interfaces de rádio para a comunicação com os sensores/atuadores e para se conectar à Internet.

Junta a informação dos nodos WSN e envia *data* para a ***Cloud***.

Esta componente será referida como **Network Layer**.

1.3 Cloud-based back-end

Esta componente é responsável por receber e juntar toda a informação dos vários *Gateways nodes* e analisa a informação (Performance). Se for preciso, envia regras de aplicação aos *Gateways.*

Esta componente será referida como **Service Layer**.

1.4 Dashboard/GUI

Um modelo *Front-end* baseado em *Web* para todo o tipo de dispositivos (computadores, *tablets* e *smartphones*). Providencia 2 tipo de modelos:

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

Esta componente será referida como **Application Layer**.

2 STRIDE

Nesta secção vou apresentar o conceito de STRIDE, um acrónimo que representa, de modo geral, as possíveis ameaças do nosso sistema. O objetivo desta identificação de ameaças serve para tentar garantir a segurança.

- **S**poofing:

  O ato de fazer-se passar por alguém ou por algo, que não o próprio. *Impersionating* de um sistema ou pessoa. A propriedade violada é a Autenticação.

- **T**ampering:

  O ato de modificar dados num disco, memória ou numa *network*. A propriedade violada é a Integridade.

- **R**epudiation:

  Rejeita a autoria de algo que aconteceu, violando o Não-Repúdio.

- **I**nformation Disclosure:

  Divulgação de informação privada a uma entidade não autorizada a aceder a esses dados, quebrando assim a confidencialidade da informação.

- **D**enial of Service:

  Atacar um sistema, de modo a absrover os seus recursos necessários para providenciar um serviço. A disponibilidade do sistema é comprometida.

- **Elevation** of Privilege - EoP:

  Permitir uma entidade a fazer algo que não deveria poder fazer. Compromete a autorização do sistema.

3 Modelação do Sistema

Nesta secção é apresentado uma modelação do sistema para facilitar a compreensão e análise das possíveis vulnerabilidades que podem surgir em cada componente do Sistema.

3.1 Threat Model

Threat modeling é um processo onde ameaças potenciais, tais como vulnerabilidades estruturais ou a ausência de segurança, podem ser identificadas e enumeradas. O objetivo da modelação é fornecer defesas que precisam de ser implementadas, dado a natureza do sistema, o tipo de possíveis invasores e os que mais os motiva a atacar o sistema.

3.2 Modelo do Sistema

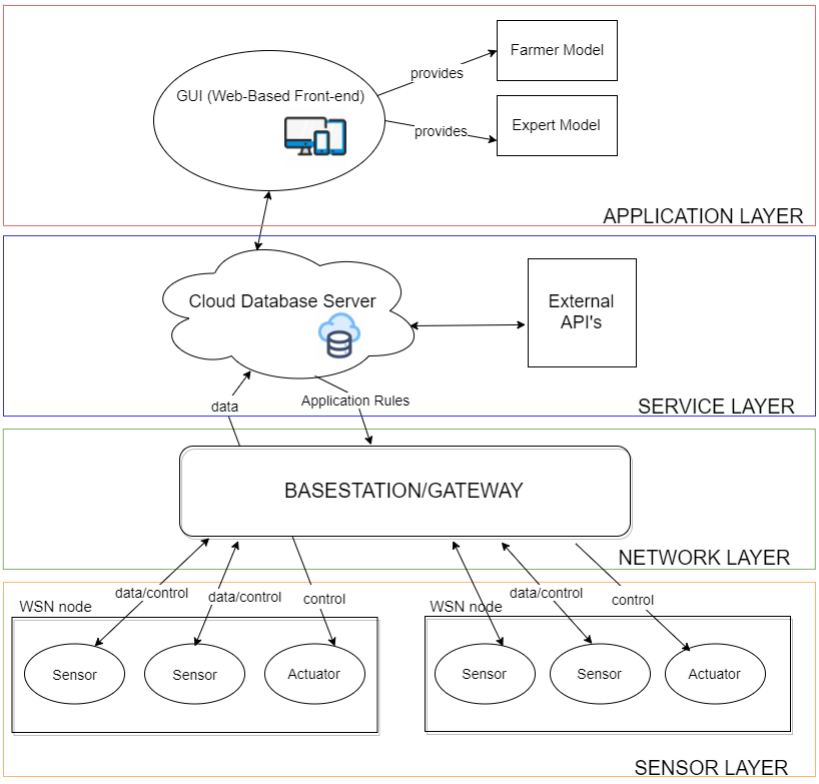

Figura 1: Modelação

4 Ameaças ao Sistema

4.1 Sensor Layer

Os sensores *Wireless* são responsáveis pela recolha de informação, e os nodos atuadores são responsáveis por alterar o estado dos aparelhos agrícolas. Sendo esta a fase de recolha de informação, isto é, a componente inicial, qualquer vulnerabilidade irá afetar o resto do Sistema.

- **Spoofing**

  Um invasor/atacante pode tentar personificar um nodo da rede WSN privilegiado. Esta personificação pode resultar num encaminhamentos dos dados de outros nodos para ele, comprometendo assim o Sistema.

- **Denial of Service**

  O atacante pode saturar o sistema enviando pacotes de modo a que o nodo em que ele esteja ligado deixe de estar disponível.

- **Tampering**

  Inserção de informações falsas nos sensores que o invasor tem acesso. Isto resulta no envio de informação corrompida ao *Gateway*, e ao resto do Sistema indiretamente, afetando a análise dos dados.

4.2 Network Layer

A Basestation é a componente responsável por administrar os sensores e os atuadores, ajustando as suas operações, e salvaguarda os seus dados e envia-os para a Cloud/Back-end. Também recebe *rules* da Cloud/Back-end.

Esta usa interfaces de rádio para a comunicação com os sensores/atuadores (GSM) e para estabelecer ligação à Internet (GPRS/LTE).

4.2.1 GPRS/LTE e GSM

As operadoras móveis, como é o caso da 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.

Este garante autenticação dos utilizadores, estabelece canais seguros entre componentes que comunicam entre si e garante o encapsulamento e proteção dos dados da rede.

O GSM garante segurança *ent-to-end*, mantendo a confidencialidade das chamadas e o anonimato do subscritor GSM. O GSM verifica a autenticação da identidade do subscritor através do uso de um mecanismo *challenge-response*. Deste modo, recorre a três algoritmos:

1. A3 para autenticação do cliente com uma chave de 128 bits
2. A5 para encriptar e desencriptar a informação

3. A8 para a geração de chaves aleatórias.

- **Spoofing**

  Os ***Base transceiver station (BTS)*** são equipamentos que facilitam a comunicação *wireless* entre o utilizador e a *network*.

  O ataque de *Spoofing* usa este conceito de BTS no sentido em que, o invasor pode se fazer passar por uma BTS, com o mesmo código da *network* do utilizador, explorando assim uma falha na autenticação da GSM que permita que a BTS seja um *Man in the middle* e receba todo o tráfico que passa na rede.

- **Tampering**

  O atacante usa a mesma técnica referida em cima, age como um *Man in the middle*, recebendo todo a informação na rede. Com esta informação, o invasor pode alterar ou criar informação que passa por ele.

- **Information Disclosure**

  O ***International mobile subscriber identity (IMSI)*** é o número que identifica exclusivamente todos os utilizadores/subscritores de uma *network*.

  Quando um subscritor está numa nova localização pela primeira vez ou quando a tabela de mapeamento (*Mapping Table*) entre o TMSI(*Temporarily Mobile Subscriber Identity*) e IMSI do subscritor é perdida, a *network* pede ao subscritor para declarar, de novo, o IMSI. Este pedido para ser enviado o IMSI pode ser usado de forma a mandar um *Indetity Request* de um BTS não identificado.

- **Denial of Service**

  A ***Base Station Subsystem (BSS)*** é a secção da *network* os telefones tradicionais que é responsável pelo tratamento do tráfico. O ***Base Station Controller (BSC)*** é o controlador principal da BSS, onde a informação é tratada e onde são alocadas canais de rádio (*Radio Channels*).

  O atacante/invasor pode enviar várias mensagens de *Channel Request* para o BSC, em que o protocolo do request não é feito por causa da seguinte *Channel Request*. Visto que existe um limite de requests, isto compromete a disponibilidade do BSC.

4.3 Service Layer

Esta componente é responsável por receber e juntar toda a informação dos vários *Gateways nodes* e analisa a informação (Performance). O *Back-end* é a entidade "cérebro"de todo o sistema, onde o código e base de dados implementado.

- **Spoofing**

  Um atacante poderia configurar um servidor falso e tentar comunicar com o resto das componentes do sistema, assim conseguiria também explorar as vulnerabilidades do resto do sistema.

- **Tampering**

  O atacante ao configurar o servidor falso e ao aceder à informação que lhe é recebida do resto do sistema, poderá modificar essa informação.

  O ataque *SQL injection* permite o atacante interferir com as *queries* feitas à base de dados, conseguindo aceder e até modificar informação lá dentro.

- **Information Disclosure**

  O atacante poderá ter acesso à informação que é recebida pelo *Back-end*, podendo expor essa informação.

  Relativamente à base de dados, o atacante poderá tentar aceder diretamente aos dados que estão dentro da BD, através por exemplo, de *SQL injections*.

- **Repudiation**

  Os ficheiros logs permitem reconhecer quem acedeu e alterou tudo dentro da BD, e o atacante poderá alterar/remover esses ficheiros logs, permitindo o repúdio das suas ações.

- **Denial of Service**

  A *Back-end* de um sistema normalmente está alojada num servidor de rede. Se o atacante conhecer essa rede, poderá sobrecarregar e torná la indisponível e inacessível, por se encontrar saturada de *requests*, ao nosso sistema.

  É muito comum também o atacante tentar comprometer a disponibilidade da BD, podendo levar à impossibilidade de acesso a essa BD.

4.4 Application Layer

Esta componente representa a parte frontal do sistema, isto é, o nível de aplicação, nomeado também como *Front-end* do sistema, que tem como objetivo facilitar a compreensão das informações geradas. Por isso, é a componente que permite também a monitorização dos dados. Como dito em cima, possui 2 modos, um para os agricultores e outro para o especialistas.

- **Spoofing**

  Como a camada de aplicação trabalha sobre a camada da Internet, tem que usar os seus protocolos, como o TCP/IP. Muitos dos protocolos dentro do TCP/IP não disponibilizam mecanismos de autenticação, tanto de origem como destino. Assim, os ataques de spoofing são mais frenquentes neste tipo de protocolos.

- **Tampering**

  Ataques de *Spoofing* pode desencadear outros ataques, como o ataque *Man in the middle*, referido em cima, que permite o atacante fazer-se passar por outro, acedendo aos seus dados, podendo modifica-los se quiser, comprometendo a sua integridade.

- **Denial of Service**

  O atacante pode querer tornar os recursos do sistema indisponíveis, como por exemplo, não permitir que os agricultores ou especialistas tenham acesso aos seus dados, por causa da indisponibilidade do serviço.

- **Elevation of Privileges**

  Um invasor poderá inserir um código JavaScript malicioso que será executado no lado do cliente, comprometendo também o sistema.

4.5 Resumo

Threat	Sensor Layer	Network Layer	Service Layer	Application Layer
Spoofing	**X**	**X**	**X**	**X**
Tampering	**X**	**X**	**X**	**X**
Repudiation			**X**	
Information Disclosure			**X**	
Denial of Service	**X**	**X**	**X**	**X**
Elevation of Privilege				**X**