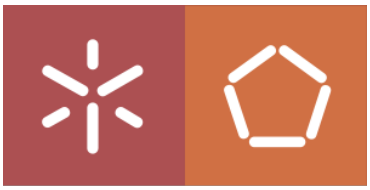

Universidade do Minho
Escola de Engenharia

Universidade do Minho
Mestrado Integrado em Engenharia Informática

SSI

Segurança de Sistemas Informáticos
Ficha 2

Outubro 2020

Tânia Filipa Amorim Rocha
A85176

Maria Miguel Albuquerque Regueiras
A85242

Conteúdo

Lista de Figuras

1 Introdução

No âmbito da segunda ficha prática da UC de Segurança de Sistemas Informáticos, foi atribuída a tarefa da construção de um modelo de ameaças para um sistema denominado por *Precision Agriculture System* e as respetivas estratégias para o desenvolvimento do respetivo modelo de ameaças.

Para isso, realizou-se o seguinte relatório que passa pelas várias etapas do processo. Primeiramente fala-se do sistema com a sua análise e modelo para melhor compreensão de onde possíveis falhas poderiam existir assim como perceber melhor o movimento dos dados no sistema.

É então apresentado o Modelo de Ameaças com uma breve explicação da abordagem escolhida. Por fim é feito o resumo das ameaças encontradas.

2 Análise do Sistema

O sistema *Precision Agriculture System* é um sistema que utiliza tecnologia e factos científicos para analisar e gerir plantações baseando-se na variação temporal e espacial do ambiente em tempo real.

Esta plataforma é constituída por quatro elementos principais a serem analisados no modelo de ameaças. Estes são:

- **Wireless sensor and actuators nodes (WSN)**

  WSN é um conjunto de sensores e atuadores que se encontram diretamente no campo representando a fonte de dados que se movimentam no sistema. Estes podem ser compostos por sensores ZigBee, motes TelosB e dispositivos Arduino/Raspeberry sendo que podem existir até 1000 nodos no campo.

  Os sensores adquirem os dados (como temperatura, luz...) e enviam para a basestation responsável via Wireless. Os atuadores são responsáveis por alterar os estados das operações no campo dado as novas regras recebidas do *backend*.

- **Basestation/gateway**

  A basestation é responsável por gerir os sensores e atuadores no campo ajustando as suas operações de acordo com as regras do *backend*. Possui interfaces rádio para comunicar com estes e interfaces celulares rádio para conectar com GMS e/ou GPRS/LTE para Internet. Pode existir mais do que uma basestation mas 1 WSN apenas pode ser gerido por uma única basestation. Entre todas as suas funcionalidades, este pode:

  - Receber feed dos WSN em real time através de qualquer protocolo.
  - Agrega os feed recebidos.
  - Corre IoT-enabled apps para controlo e análise em real time.
  - Fornece armazenamento transiente.
  - Envia sumários periódicos à Cloud.

- **Cloud-based back-end**

  O *backend* deste sistema incluí duas componentes principais, uma de armazenamento através de um sistema *cloud multi-tenant*, isto é que permite vários utilizadores simultaneamente. Para esta componente pode ter sido utilizado sistemas já conhecidos como *Microsoft Azure* e *Google cloud.*

  A outra componente é conhecido como modulo analítico que tem como principais funções receber e agregar informação de todos os nodos *gateway*, analisar estes dados e posteriormente enviar novas regras de volta aos nodos. Tem ainda como função fornecer uma API para manipulação de dados e desenvolvimento de novas aplicações neste contexto.

- **Dashboard/GUI**

  Este sistema conta com um modelo de *frontend* baseado em *web* para computadores, tablets e *smartphones* pessoais.

  Este modelo fornece dois nodos distintos: um para os agricultores que permite-lhes ter acesso a dados e analise dos mesmos e auxilia na tomada de decisões, e um para os profissionais que poderem continuamente melhorar a base de conhecimento do sistema conforme a experiência dos mesmos.

3 Modelo do Sistema

Ao realizar o modelo do sistema escolheu-se fazer um DFD (Data Flow Diagram) para representar o movimento de dados entre as várias entidades. Isto pois assim tornava-se mais simples a identificação de barreiras de confiança e onde possíveis problemas podiam existir.

É de realçar a existência de três fatores principais: as entidades do sistema (representados por retângulos azuis), os processos que motivam o movimento dos dados (representados pelas caixas azuis e brancas) e o movimento de dados em si (representado pelas setas uni e bi direcionais).

Dividiu-se o sistema em três partes fundamentais, no topo do diagrama tudo o que é diretamente relacionado com o campo e a recolha de dados, no fundo à esquerda o backend que lida com toda a análise e processamento dos dados com posteriores decisões e, por fim, no fundo à direita o frontend que liga os utilizadores ao sistema.

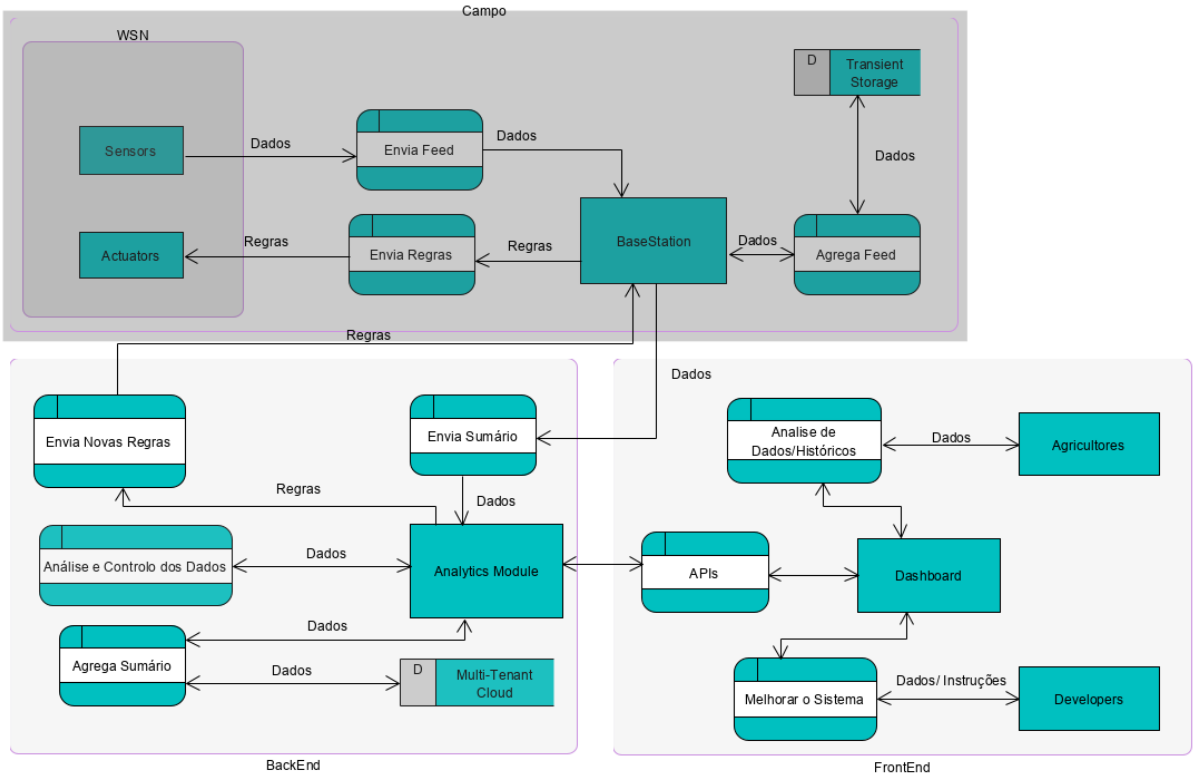

Figura 1: Modelo do Sistema - DFD

4 Modelo de Ameaças / Threat Model

O modelo de ameaças ou mais conhecido por *Threat Model* é um processo que reconhece ameaças potencias tais como vulnerabilidades de estrutura ou de segurança e enumera-as. O objectivo desta modelação é fornecer aos defensores os possíveis atacantes e ataques ideais ao sistema através da análise às vulnerabilidades e fraquezas do mesmo. Este tipo de modelação visa encontrar os problemas de segurança antecipadamente para os analisar, corrigir e posteriormente elevar a qualidade e segurança do produto.

Existem várias estratégias para a modelação de ameaças mas a que será implementada neste trabalho será uma análise estruturada que se foca nos ataques e atacantes possíveis do sistema. Este tipo estratégia adopta uma visão no sentido de "o que é que um atacante quererá do meu sistema?", o que nos permite enumerar vários tópicos com dados a manter seguros.

Através da abstracção das ameaças é possível organiza-las através de um sistema de classes nomeado de *STRIDE* o que permite uma melhor análise de riscos e *exploits* comuns usados por atacantes.

STRIDE é um acrónimo de várias situações:

- *Spoofing*: utilizar a identidade de algo ou alguém, ou seja, personificar um sistema ou uma pessoa, violando a autenticação correta.
- *Tampering*: modificar dados num disco, rede ou memoria violando a integridade de dados.
- *Repudiation*: o acto de recusar a confirmação de que algo ocorre, por exemplo, eliminar *logs* do sistema.
- *Information Disclosure*: fornecer informação a uma entidade que não está autorizada a ter acesso à mesma comprometendo confidencialidade.
- *Denial of Service*: esgotar os recursos necessários ao funcionamento do sistema, violando assim a disponibilidade do sistema.
- *Elevation of Privilege*: permitir que uma entidade tenha acesso a funcionalidades ou recursos aos quais não devia estar autorzado violando autorização no sistema.

4.1 Ameaças de Segurança do Sistema

4.1.1 WSN

Como mencionado anteriormente, existe uma componente constituída por sensores e atuadores no campo responsáveis pela recolha de dados e pela realizações de alterações de estados em operações no campo em si. Nesta podem ser possíveis ameaças as seguintes:

- **Spoofing**, nesta componente do sistema não conseguimos encontrar alguma situação em que tal acontecesse.
- **Tampering** poderia ocorrer a nível dos sensores e do envio dos dados. Como referido anteriormente, os sensores são ZigBee, norma que contém várias vulnerabilidades segundo o NVD e é um possível ponto onde a informação obtida e enviada pode ser alterada. Outra forma seria através do dispositivo Arduino ou Raspberry, visto que são dispositivos que correm um sistema operativo à escolha do responsável, dando assim a oportunidade a alguém (talvez mesmo da própria organização) de correr código malicioso que altere os dados.
- **Repudiation** não é relevante nesta componente.
- **Information Disclosure** poderia ser uma consequência do ponto de tampering mencionado anteriormente, onde pode haver nos atuadores revelação de segredos do negócio quando há alterações de estado. Em termos de sensores, não se torna tão grave nem tão importante.
- **Denial of Service** tanto nos sensores como nos atuadores, ambos podem ser impossibilitados de fazerem as suas funções, quebrando assim a circulação de informações e regras para alteração de estados.
- **Elevation of Privilege** não parece ser relevante nesta componente.

4.1.2 Basestation/Gateway

Nas basestations há oportunidades de alguém obter o seu controlo e assim correr código malicioso e prejudicar o funcionamento do sistema. Isto visto as conexões serem wireless entre este e os WSN assim como com o backend. Com isto em mente, analisemos O STRIDE:

- **Spoofing** - neste contexto não é relevante ter em conta este tipo de ameaça.
- **Tampering** pode ocorrer pela razão mencionada anteriormente: as próprias conexões entre componentes serem wireless introduz uma gama de oportunidades para atacantes intervirem e tentarem alterar os dados que estão a ser enviados. Também pode acontecer de tentarem adulterar os próprios sumários que a basestation realiza antes de os enviar para a cloud. Para além disso, como a basestation oferece armazenamento transiente, esse pode ser objetivo de ataques também.

- **Repudiation** - neste contexto não é relevante ter em conta este tipo de ameaça.
- **Information Disclosure** ocorre se tentarem desviar os dados, mais uma vez pelas mesmas razões do ponto de tampering, isto é, através de um ataque é possível originar automaticamente a divulgação de informações privadas.
- **Denial of Service** é possível acontecer pois podem tentar sobrecarregar as basestations com pedidos e pacotes impedindo o funcionamento correto do sistema e o movimento de dados é fragilizando, senão completamente destruído.
- **Elevation of Privilege** não é relevante nesta componente.

4.1.3 Backend Baseado em Cloud

No contexto do sistema em si, é utilizado uma *cloud* para o armazenamento de dados para vários tipos utilizadores. Utilizando os exemplos fornecidos nomeadamente *Amazon AWS* e *Azure*, haverá também um modulo para os dados recebidos dos *gateways* sobre as plantações dos quais serão posteriormente desenvolvidas regras e comandos a serem executados pelos *WSNs*. Estes softwares fornecem também *APIs* abertas para o controlo, modificações e acessos ao serviço, tanto pelos agricultores como pelos especialistas anteriormente apresentados.

A este nível do sistema, as falhas de segurança são muito restritas devido à escala da segurança e ao anonimato fornecido pela *Microsoft* e *Amazon*, sendo por isso necessário que haja uma quebra logo ao nível de autenticação para que haja um ataque ou quebra na *cloud*.

Aplicando esta análise ao sistema de classes *STRIDE* temos então os seguintes possíveis ataques:

- **Spoofing** que pode ocorrer se a página de *login* de acesso ao *backend* por acesso de administrador for falsificada de modo a obter as informações inseridas através dos formulários incluindo credenciais de acesso. Neste caso o atacante poderá ter acesso total ao sistema o que poderá gerar todo o tipo de falhas.

  É possível evitar este problema através de métodos de autenticação que requeiram a identificação sem falha de uma entidade como, por exemplo, impressão digital.
- **Tampering** que poderia ocorrer com facilidade, visto que todos os dados, tarefas, etc vão para a *cloud* por um mesmo caminho o que, abre a possibilidade de alteração de ficheiros no sistema.
- **Repudiation** que, neste seria necessário que ocorresse uma situação de *Spoofing* para poderem ser, por exemplo, eliminados ou alterados os *logs*.
- **Information Disclosure**, visto que no momento que um atacante entra num sistema através de *Spoofing* este passa a ter acesso a uma quantidade de informação à qual não estaria autorizado a ter acesso.
- **Denial of Service** que, da mesma maneira que as ameaças anteriores, no momento em que um atacante tem acesso administrador ao sistema este pode roubar e utilizar os recursos e dados de utilizadores o que deterá o sistema de funcionar posteriormente devido à falta de elementos essenciais ao seu funcionamento.
- **Elevation of Privilege** que ocorre desde o inicio quando um atacante tem acesso ao sistema por *Spoofing* visto que passa a ter privilégios que não devia ter para manipular informações e dados.

4.1.4 DashBoard/GUI

No sentido deste sistema, a *Dashboard/GUI* trata-se de uma interface para que os utilizadores possam interagir com os diversos recursos digitais. Como descrito anteriormente, esta *GUI* apresenta dois modos diferentes - um para os agricultores no qual apenas terão acesso a históricos de dados colectado e processados no seu próprio domínio, e outro para os especialistas que para além de receberam todas as informações disponíveis, podem também interagir e alterar com objectivo a melhorar o sistema.

Neste sentido, sendo então este modulo *frontend* é compreensível que haja vulnerabilidades que permitam falhas de segurança que estejam visíveis para os utilizadores ou outras entidades. Esta situação não ocorre por ser de facto *frontend*, mas sim devido a ser a parte do sistema mais exposto ao "exterior". Algumas das falhas possíveis de ser usadas por atacantes enquadram-se nas classes *STRIDE*, sendo estas:

- **Spoofing** - Tal como descrito anteriormente a nível de *backend*, uma das ameaças desta classe pode ser a falsificação da página *Web* de *login* que permite a um atacante obter as credencias e dados de acessos por exemplo, de um profissional do sistema, o que permite posteriormente a acesso não autorizado ao sistema por parte dos atacantes. Esta situação permitira acesso à totalidade do sistema visto que um profissional tem direito quase que administrativo para poder alterar o sistema pondo em risco todos os componentes do mesmo. Visto que a nível de *frontend* é quase impossível proteger destes tipos de ataques porque qualquer pagina web pode ser replicada, é necessário que a nível de *backend* exista níveis de protecção adicionais para não colocar em risco toda a estrutura.
- **Tampering** - A nível de *frontend* é praticamente impossível a qualquer tipo de dados para que ocorra a sua adulteração, daí esta ameaça não ser considerada.
- **Repudiation** - Da mesma forma que *Tampering*, não tendo qualquer acesso a dados também se torna impossível este tipo de ameaça visto que, não há acesso a qualquer tipo de registo ou históricos.
- **Information Disclosure** - Tendo em conta que é possível falsificar uma pagina *web* de, por exemplo, login, é possível o roubo de credenciais. Para além disto, muitas páginas *web* por si só já apresentam várias informações sobre o sistemas como por exemplo *paths* para ficheiros e dados existentes no sistema, esta situação é conhecida como *path disclosure*.
- **Denial of Service** - Este tipo de ameaça acontece quando um atacante tem como objetivo fazer com que os recursos do sistema fiquem indisponíveis para os utilizadores. Este ataque é feito através da sobrecarga do sistema de um número enorme de pedidos num período de tempo reduzido o que previne que estes pedidos sejam atendidos. O tráfego gerado nesta situação geralmente efetuado de várias zonas ou ips torna praticamente impossível de defender ou travar devido à impossibilidade de bloquear apenas um conjunto de ips.

  Um método de prevenção para esta situação é através de *Captchas* nas páginas comuns de acesso como por exemplo pagina de *login, registo*, etc, permitindo assim se é um utilizador real ou *bots*, visto que geralmente este tipo de ataques são efectuados através de *bots*.
- **Elevation of Privilege** - Não é comum este tipo de ameaça a este nível do sistema.

4.2 Resumo de Ameaças

Finalmente, como forma de resumo e para melhor visualização da análise feita anteriormente, desenhou-se a tabela seguinte que apresenta que componentes são afetadas por que tipo de ameaça.

	WSN	Basestation/ Gateway	Backend	Dashboard/GUI
Spoofing			X	X
Tampering	X	X	X	
Repudiation			X	
Information Disclosure	X	X	X	X
Denial of Service	X	X	X	X
Elevation of Privilege			X	

Figura 2: Tabela resumo das ameaças

As ameaças referidas podem não ser as únicas, mas foram as que , a ver do grupo, teriam mais impacto no funcionamento do sistema e assim as mais prioritárias caso uma equipa de desenvolvimento que fosse ler este relatório soubesse o que corrigir primeiro clara e objetivamente.

5 Conclusões

O processo de modelação de ameaças tem como foco um processo para descobrir possíveis erros e falhas num sistema a nível de segurança para futura correcção e melhorias do mesmo.

No contexto deste projecto, o sistema *Precision Agriculture System* teve esta modelação de ameaças baseada numa descrição detalhada das tecnologias e componentes envolvidas e posteriormente foi então possível desenvolver um *Data Flow Diagram* DFD baseado no funcionamento do sistema para permitir uma boa observação sobre o mesmo.

Quando à analise das ameaças foi seguido o modelo *STRIDE* com objectivo a analisar todas as falhas de segurança por classe em cada componente.

Fica assim concluído o relatório de analise e desenvolvimento do modelo de ameaças do sistema *Precision Agriculture System*.

Referências

[1] https://medium.com/@manojsingh047/understanding-frontend-security-ff6585395534

[2] https://owasp.org/www-community/attacks/Form$_{a}ction_{h}ijacking$

[3] https://owasp.org/www-community/attacks/Credential$_{s}tuffing$

[4] https://owasp.org/www-community/attacks/Full$_{P}ath_{D}isclosure$

[5] https://www.toptal.com/security/10-most-common-web-security-vulnerabilities

[6] https://owasp.org/www-community/attacks/Denial$_{o}f_{S}ervice$