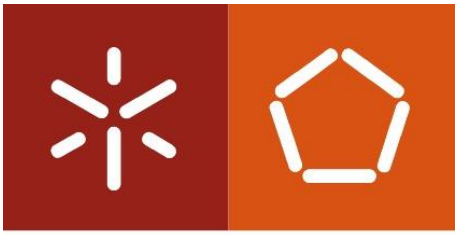

Universidade do Minho

Departamento de Informática

Mestrado em Engenharia Informática

Criptografia e Segurança de Informação

Tecnologias de Segurança
Ficha Prática 2

Grupo Nº11

Ariana Lousada (PG47034) Luís Carneiro (PG46541)
Rui Cardoso (PG42849)

18 de abril de 2022

Resumo

O presente documento descreve um *Threat Model* detalhado feito para o sistema *Precision Agriculture* abordado nas aulas práticas da unidade curricular Tecnologias de Segurança, pertencente ao perfil de Criptografia e Segurança da Informação inserido no Mestrado em Engenharia Informática da Universidade do Minho.

Este relatório encontra-se dividido em duas principais secções: Modelação do Sistema (1), na qual é apresentado um diagrama representante do sistema e Deteção de ameaças/vulnerabilidades de cada componente do sistema (2), na qual são analisadas potenciais ameaças e vulnerabilidades de cada um dos componentes que o constituem.

Capítulo 1

Modelação do Sistema

Uma vez que o objeto de análise se trata de um sistema com arquitetura própria, desenvolveu-se um *Data Flow Diagram*:

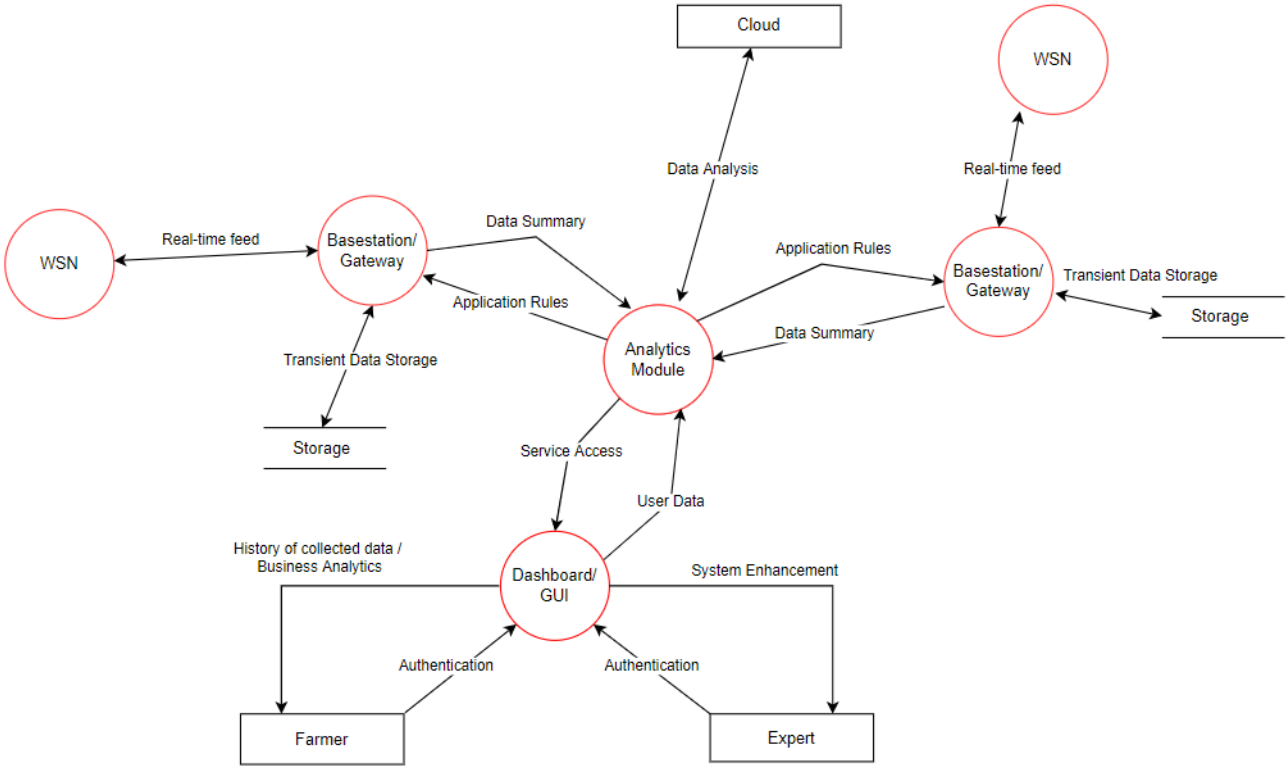

Figura 1.1: *Data Flow Diagram* do sistema *Precision Agriculture*

Capítulo 2

Deteção de ameaças/vulnerabilidades de cada componente do sistema

De modo a ser possível detetar ameaças/vulnerabilidades de cada componente constituinte do sistema utilizou-se o modelo `STRIDE` (*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service* e *Elevation of Privilege*).

2.1 Wireless sensor and actuators nodes (WSN)

Spoofing

Um atacante pode utilizar algum tipo de dispositivo/equipamento que o permita disfarçar-se no sistema como um sensor ou atuador. Isto pode afetar negativamente o sistema caso o atacante decida enviar informação errada ou alterada, comprometendo o *data flow*.

Uma solução possível para este problema seria inserir uma espécie de identificação para cada nodo do sistema, de modo a ser possível verificar a entidade e a autenticidade deste tipo de aparelhos.

Tampering

Um atacante pode intercetar os pacotes de informação enviados pelos WSN para o resto do sistema, adicionando informação falsa ou alterando a que já está inserida no pacote.

Para evitar ataques desta natureza, poderia-se aplicar uma estratégia de cifra para a informação enviada. Deste modo, o atacante não iria conseguir extrair dados dos pacotes mesmo tendo acesso a estes.

Information Disclosure

Como já abordado na secção anterior, o atacante pode ser capaz de intercetar a conexão e extrair dados e informação enviada aos restantes componentes do sistema.

Uma estratégia de cifra da informação também iria reduzir este tipo de risco.

2.2 Basestation/gateway

Spoofing

Um atacante pode ser capaz de fazer *IP-Spoofing*, substituindo um IP pertencente a um *gateway* do sistema pelo seu próprio. Isto daria-lhe acesso parcial aos dados, visto que estes componentes fazem *Transient Data Storage*, além de ter comunicação direta com o *backend* do sistema. O atacante pode alterar, por exemplo, os sumários de data enviados ao *backend* de forma a conterem informação falsa.

Uma solução para reduzir este tipo de risco seria fazer uma espécie de filtragem de pacotes provenientes de IP's não pertencentes ao sistema.

Tampering

Como já referido anteriormente, o atacante pode conseguir alterar dados referentes aos sumários de dados enviados ao *backend* do sistema.

Uma possível solução de redução deste risco seria por exemplo uma realização periódica de *backups* da informação contida na Cloud do sistema. Também se poderia converter a cloud num *WORM system* (*Write Once Read Many*), no qual os dados apenas seriam acedidos para escrita uma vez, não permitindo posteriores modificações.

Information Disclore

Como já foi referido anteriormente, o atacante pode ter acesso a dados referentes aos sumários de dados enviados ao *backend* do sistema e pode partilhá-los com outras fontes.

De modo a reduzir este risco devia ser utilizada uma boa estratégia de cifragem dos dados contidos nos sumários enviados ao backend do sistema.

Denial of Service

Um atacante pode fazer um ataque de negação de serviço enviando pacotes "lixo"para o gateway (comprometendo a disponibilidade dos gateways para receção e envio de informação) ou bloqueando diretamente as comunicações entre os *gateways* com os restantes nodos do sistema.

Para a primeira estratégia de ataque, poderiam apenas ser aceites pacotes com uma determinada estrutura definida, de modo a que o *gateway* descarte os pacotes "lixo".

Para a segunda estratégia de ataque, cada nodo poderia ter redundância de uma certa porção de dados, o suficiente para permitir o seu funcionamento mesmo com as comunicações temporariamente indisponíveis.

Elevation of Priviliege

Um utilizador com más intenções poderá intercetar o tráfego de dados, disfarçando-se como administrador do sistema. Isto pode permitir que aumente os privilégios a ele próprio, dando-lhe acesso a partes do sistema que não é suposto e permissões para executar ações prejudiciais ao sistema.

De modo a reduzir este risco é necessário aplicar mecanismos de autenticação de confiança.

2.3 Cloud-based back-end

Spoofing

Este sistema está vulnerável a spoofing. O sistema utiliza *Multi-tenant cloud storage* para tratar de um conjunto de informações, por isso, várias entidades têm acesso ao *back-end*.

Isto possivelmente permite que um atacante consiga fazer alguns ataques de *spoofing*, como por exemplo *Man-in-the-middle* e roubar as credenciais de acesso ao back-end.

Visto que várias pessoas tem acesso ao *back-end*, a probabilidade de alguém ser vítima de um ataque e o sistema ser comprometido aumenta significativamente.

Para mitigar isto, é importante que todos os clientes com acesso ao *back-end* tenham conhecimento de métodos de segurança, como por exemplo garantir que se estão a ligar directamente ao *cloud provider* através de HTTPS.

Tampering

A partir do momento que um cliente seja vitima de um ataque de *spoofing*, torna possível que o atacante tenha acesso à *cloud-based back-end* e altere valores críticos das base de dados, crie novas regras de aplicações para os *gateways* e altere as APIs do sistema.

De modo a contornar este risco poderia-se adotar uma política de *backups* periódicas dos dados presentes na cloud, de modo a que a totalidade destes não seja comprometida nem irreparável.

Repudiation

Um atacante pode utilizar roubar uma conta de um *farmer/expert* para causar danos; os logs vão apontar para a entidade a quem a conta pertence, dificultando a descoberta do indivíduo que realmente fez o ataque.

No entanto, alguns fornecedores de cloud como a google cloud possuem técnicas avançadas de logs que podem ser activadas para mitigar isto, como por exemplo activar *'Data access logs for IAM APIs'*.

Information Disclosure

Como dito anteriormente, caso um atacante consiga efectuar um ataque de man-in-the-middle a um dos clientes com acesso à cloud, este pode ter acesso a informação sensível.

Uma boa estratégia de cifra de dados pertencentes à Cloud iria reduzir este risco significativamente.

Denial of Service

Os fornecedores de cloud AWS Cloud, Azure e Google Cloud possuem muitas técnicas de protecção contra negação de serviço.

Para um atacante conseguir com sucesso efetuar um ataque de negação de serviço sem ter acesso à cloud, seria necessário utilizar uma quantidade gigante de bots a fazer pedidos constantes para o sistema.

Contudo, é possível que um atacante tente fazer um *Syn Flood Attack*, no qual ele inicie uma conexão sem a finalizar. Isto pode levar a que o servidor da Cloud aguarde infinitamente pela finalização de várias conexões, levando à indisponibilidade dos seus serviços para receber informações do *Data Analyser*.

Uma maneira de mitigar este risco seria aplicar uma estratégia de *4-way-handshake* de modo a que conexões semi-abertas não afetem os servidores da cloud.

2.4 Dashboard/GUI

À partida, uma solução *web-based* apresenta todas as vulnerabilidades típicas presentes na *stack* da Internet, quer na camada de aplicação, que inclui diversos protocolos, tais como o BGP, OSPF, RIP, DNS, HTTP e HTTPS, quer na camada de transporte, com protocolos como o TCP e UDP.

A segurança do sistema está altamente dependente de práticas e metodologias seguras, tais como o uso de HTTPS, a cifra de dados sensíveis (por exemplo, a password do utilizador na autenticação), definição de políticas de acesso adequadas, entre outras.

Spoofing

O *spoofing* pode ocorrer se os atacantes construirem um website que seja parecido o suficiente ao original, de modo a atraír os utilizadores legítimos e ter acesso a informações confidenciais.

Tampering

O *tampering* é, sem dúvida, também possível, visto que um atacante pode não só ler os dados, mas também modificá-los e/ou apagá-los. Um exemplo mais concreto seria, de acordo com as políticas de segurança implementadas, injetar valores falsos na rede ou até mesmo desativar os sensores presentes na rede.

Information Disclosure

Este sistema está vulnerável a *information disclosure*, pois permite que os administradores do sistema melhorem o desempenho do sistema através desta interface web. Um atacante malicioso pode-se fazer passar por um administrador e ter acesso a informação privilegiada, quer dos sistemas implementados, quer dos seus utilizadores.

Para mitigar estes riscos é possível implementar mecanismos de autenticação mais rígidos já discutidos anteriormente.

Repudiation e Denial of Service

O repúdio permite que um atacante possa dizer que não fez determinada ação, o que permite ataques tais como fazer pedidos repetidos de *login* para estourar com a capacidade do servidor de responder a pedidos (ataque DDoS), ou mesmo alterar os logs e privilégios de outros utilizadores. O repúdio torna muito mais difícil detetar um intruso no sistema, pois este pode apenas "negar"os estragos causados, sem grande consequência.

2.5 Resumo de ameaças do sistema

Ameaças	WSN	Gateway	Cloud-based back-end	Dashboard/GUI
Spoofing	✗	✗	✗	✗
Tampering	✗	✗	✗	✗
Repudiation	-	-	✗	✗
Information Disclosure	✗	✗	✗	✗
Denial of Service	-	✗	✗	✗
Elevation of Privilege	-	✗	-	-

Tabela 2.1: Resumo de ameaças do sistema *Precision Agriculture*

Capítulo 3

Referências

- https://en.wikipedia.org/wiki/Internet_protocol_suite