Universidade do Minho
Escola de Engenharia

Universidade do Minho

Trabalho Prático 1 – Parte B

Threat Modelling

Sistema de Agricultura de Precisão

Bruno Rodrigues PG41066

Carlos Alves Pg41840

Índice

Introdução 3
Agricultura de precisão – Modelo de Ameaças 4
Find Threats - Estratégia 5
Front end/Back End 5
Spoofing 6
Tampering 7
Repudiation 7
Information Disclosure 7
Denial of Service DoS (User<->WebS) 8
Elevation of Privilege 8
Cliente web e o servidor(Front end) 8
Gateways 11
Sensores/Atuadores 12
Possíveis ataques (Sensores) (Stride) 13
Tampering 13
Information Disclosure 14
Denial of Service 14
Conclusão 16
Referências 17

Introdução

Este trabalho prático tem como objetivo fornecer um modelo de ameaça detalhado para o Sistema de Agricultura de Precisão descrito no enunciado e por consequência entender as diferentes estratégias e formas de analisar um modelo, além de entender a sua importância entre as diversas atividades relacionadas com segurança de sistemas informáticos.

O sistema de agricultura de precisão visa usar a tecnologia e os princípios científicos para analisar e gerenciar uma cultura com base na variabilidade espacial e temporal do ambiente associada a todos os aspetos da produção agrícola dentro dos campos, quase em tempo real. A plataforma consiste nos seguintes componentes:

Wireless sensor and actuators nodes (WSN) – Constituídos principalmente por sensores e atuadores, são responsáveis pela aquisição dos dados no terreno (Temperatura, Humidade, colheita, vento, radiação entre outros) e pela modificação do estado de operação de diversos dispositivos agrícolas (Rega, Fertilizantes, temperatura da estufa). Os sensores e os atuadores são ativados através de interfaces sem fios e ainda tem como objetivo enviarem os dados recolhidos para um gateway que estará localizado no terreno.

A segunda componente, Basestation/Gateway é responsável por fazer a comunicação via radio entre os sensores/atuadores e a internet, e gere os sensores e os atuadores de acordo com o Back-end.

As últimas componentes são a front-end e o back-end. No modulo front-end é criado baseado na Web para computadores pessoais, tablets e smartphones. Isto para dois tipos de clientes distintos: Agricultores e Especialistas.

Os agricultores apenas poderão ver e analisar o histórico dos dados coletados e também as tomadas de decisão que ocorrem nos terrenos.

Os especialistas terão mais acesso em relação ao cliente agricultor, pois este poderá fazer o mesmo que o agricultor e ainda melhorar, modificar os dados para consequentemente aprimorar continuamente o conhecimento do sistema com base no estado da arte.

E por fim o Cloud basead back-end, responsável pelo armazenamento dos dados na nuvem multilocatario, onde é possível haver vários utilizadores.

Agricultura de precisão – Modelo de Ameaças

Introduzindo ao tema, ameaças à agricultura de precisão abordam as ameaças à segurança relacionadas ao impacto e adoção de novas tecnologias digitais na produção agrícola. Visto que a agricultura de precisão insere uma quantidade variável de tecnologias incorporadas e conectadas que depende de sensores remotos, sistemas de posicionamento global e sistemas de comunicação para realizar o gerenciamento dos dados, analise de dados e até o próprio aprendizado das máquinas. Com estas tecnologias é possível melhorar a precisão dos serviços da gestão agrícola, resultando em custos bem mais reduzidos e em melhores rendimentos, sejam eles colheita; quantidade de água gasta e também fertilizantes. Mas como a tecnologia tem vindo a aumentar demasiado rápido, esta resulta no aumento de exposições/ameaças destes mesmos sistemas. Neste relatório iremos de forma especulativa analisar e perceber que tipos de ameaças podem ocorrem na agricultura de precisão como também alguns cenários hipotéticos.

Geralmente na agricultura de precisão as ameaças mais recorrentes são praticamente as mesmas de qualquer outro sistema informático: roubo de recursos, roubo de dados, perda de reputação, destruição de equipamentos. Dito isto é natural que o uso impróprio de dispositivos moveis de armazenamento tais como pen drivers, phishing e outros ataques maliciosos são vetores de ameaça que podem ser usados para a realização de um ataque. E claro, desastres naturais ou ataques terroristas também podem ser vistos como ameaças que podem afetar os princípios fundamentais da segurança da informação, Confidencialidade, Integridade e Disponibilidade (CIA).

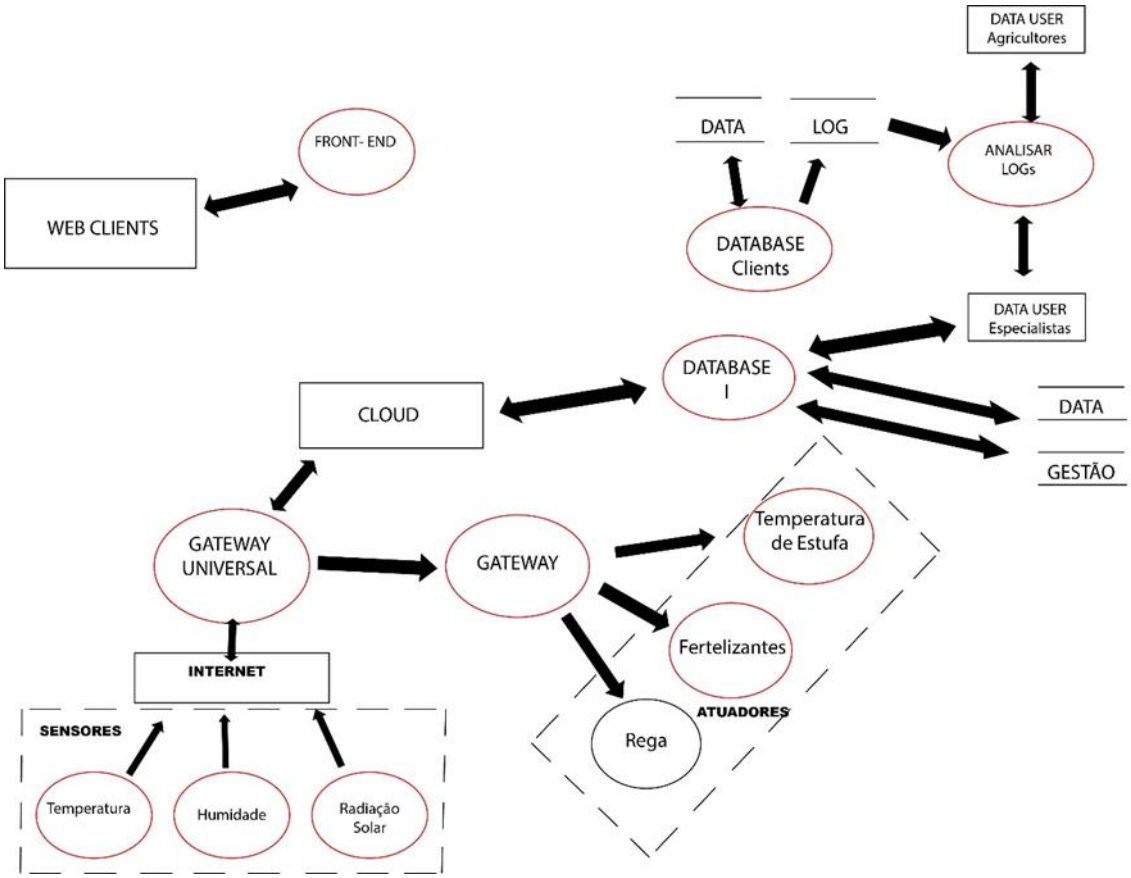


Figura 1- DFD (esboço) do sistema de agricultura de precisão.

Find Threats - Estratégia

Inicialmente, ao construir os diagramas e a projetar o sistema, iriamos apenas abordar uma estratégia das 3 dadas em aula, mas achamos por bem fazer uma mistura, principalmente entre foco sobre os assets e foco sobre o atacante. Deste modo, será possível observar abordagens das duas estratégias neste relatório – modelo de ameaças.

As ameaças/falhas e ataques aqui descritos são meramente especulativos relativamente ao sistema que foi criado, deste modo foi possível criar muitíssimos cenários de ataques, e diversas ameaças que se encontrariam neste sistema de agricultura de precisão descrito no enunciado do trabalho prático.

Front end/Back End

O front-end é a interface entre o banco de dados e os vários clientes, agricultores e especialistas. Variando de sites a programas complexos que fazem consultas SQL. O front-end destina-se a

lidar com autenticação, balanceamento de carga e funções relacionadas, para que o banco de dados central possa ser o mais rápido possível. Dito isto, neste nosso modelo:

Somente usuários autenticados como especialistas terão permissões de criação, leitura, modificação, atualização e exclusão de acordo com as políticas implementadas pelos administradores do banco de dados.

Os usuários autenticados como agricultores apenas terão permissões de leitura dos históricos dos dados coletados e das análises de tomada decisão. Para ambos os clientes, a autenticação de fator único é suficiente. Além disso os dados podem estar sujeitos a modificações, tanto agricultores como especialista, apenas por usuários autorizados. Com apenas esta implementação, da autenticação, combinamos dois requisitos importantes num sistema (Autenticação e Confidencialidade).

No esboço que fizemos, os detalhes relativos a uma falha de validação de entrada serão registados no ficheiro de log do servidor. Permitindo que os users com maioríssimos privilégios consigam ver e analisar a causa da falha na validação e claro, verificar se foi realmente uma falha de autenticação.

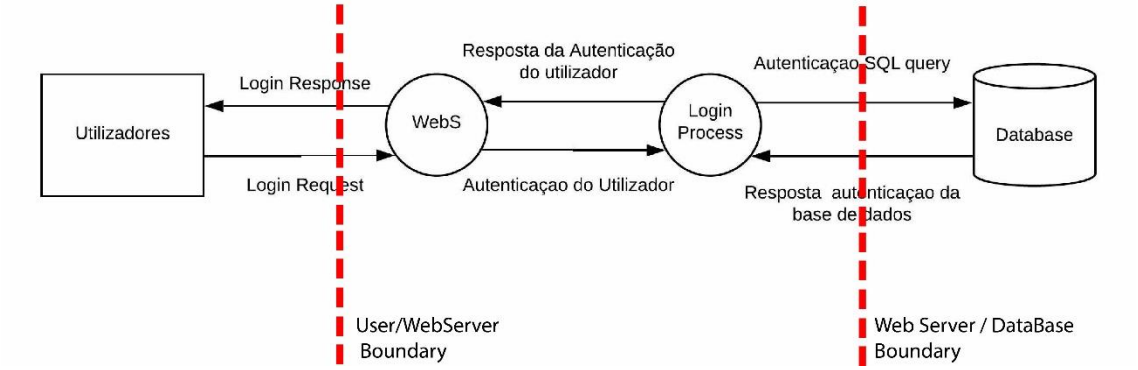


Figura 2- Fluxo de dados no front-end e com as fronteiras implementadas

Com isto estabelecido tentamos verificar quais as possíveis ameaças que poderiam ocorrer apenas nesta parte. Recorrendo ao STRIDE:

Spoofing

É possível concluir que a autenticação dos clientes Web pode ser fraca, pois é possível que um atacante efetue spoofing de Ip, de email ou até mesmo de DNS. No entanto serão impostos limites que melhorem a verificação da autenticidade do cliente. Limitar a dois tipos de utilizadores: agricultores e especialistas. Em relação a spoofing, no caso de o invasor utilizar falsificação de DNS pode vir a resultar no desvio do trafego para a maquina dele.

Tampering

A existência de lacunas nos módulos incluídos para autenticação fornecidos podem estar pouco controlados quanto às propriedades de segurança. Violando a integridade dos dados. O redireccionamento do fluxo de dados para outra máquina não confiável e ainda a modificação dos dados que fluem sobre alguma camada da nossa rede são ameaças predominantes neste modelo, no caso da modificação dos dados que fluem na rede pode tornar-se algo a atingir pois o nosso sistema de agricultura de precisão utiliza em grande parte wireless networks. O ataque man-in-the-middle é bastante recorrente nestes casos afetando a tampering e o spoofing. Em relação à memória pode acontecer que se o atacante conseguir ter acesso ao nosso código e conseguir modificá-lo de forma que este se torne "dele" ele pode manipular praticamente o que quiser.

Além disso há a possibilidade do utilizador já ter acesso á base de dados e assim manipule os dados dos perfis dos agricultores/especialista e mesmo os históricos de dados de cada campo, diretamente da base de dados.

Repudiation

No nosso esboço é possível ver que os registo no front-end são praticamente inexistentes. Além disso os logs existentes são criados na front-end e necessitam de ser enviados para o back end. E ainda há a possibilidade do atacante atacar os logs de modo que estes sejam modificados ou mesmo excluídos. Podendo acontecer que o sistema de logging seja "neutralizado", violando a non-repudiation.

A situação que também é bastante comum acontecer neste quesito seria o de ser analisado que um ou mais funcionários terem modificado ficheiros ou entrado em certos websites e alegarem que não o fizeram, claramente a propriedade afetada é non-repudiation.

Em suma as ameaças ao repudio deste sistema giram em torno dos logs, sendo necessário uma proteção extra, pois sem logs não poderemos provar nada que tenha acontecido com os agricultores ou especialistas ou qualquer outra coisa.

Information Disclosure

Podem existir interfaces de depuração e mensagens de erro, que revelam informações sobre os parâmetros de conexão do banco de dados.

Com a carência de access controls poderá ocorrer Divulgação de informação de todas as formas imagináveis sejam elas internas ou externas; um exemplo prático que pode acontecer é um funcionário que sofra engenharia social, onde lhe é induzido em erro que partilhe informações do sistema sem que este dê por ela. Claro que isto terá um impacto direto com a credibilidade

e reputação. Com os access controls bem definidos que determina quem acede a determinado objeto. Fornecendo confidencialidade e até integridade. Ainda seria possível analisar o tráfego ou direcioná-lo de modo a que o atacante pudesse ler os dados. De qualquer forma poderia enumerar diversas ameaças presentes neste modelo, sejam elas contra processos ou mesmo contra o fluxo de dados, mas se apostássemos na criptografia dos dados este parâmetro seria atenuado de certa forma, pois o atacante até podia "roubar os dados", mas não os conseguiria ler, afetando assim a confidencialidade dos dados em questão.

A questão dos logs seria algo que poderia pôr em causa a divulgação de informação, mas para isso era necessário que o invasor tivesse acesso à nossa base de dados.

Denial of Service DoS (User<->WebS)

A possibilidade de ocorrer um flooding (Threat) é altamente provável, se for transformada num vetor de ataque que pode derrubar a rede do sistema de agricultura ou até mesmo processos importantes, isto acontece quando a rede é inundada com uma quantidade absurda de tráfego. O atacante nesta ameaça pode realizar um ataque que caso a rede ou mesmo um serviço se tornem tao sobrecarregados com pacotes, acabam por iniciar solicitações de conexão incompletas que por consequência não permitem processar direito as solicitações de login ou outro de conexões verdadeiras. E claro isto leva ao preenchimento do buffer de memória do nosso host e quando este está completamente cheio, poderá ocorrer a tal negação de Serviços neste caso, contra o processo de aceder à página web/ à base de dados e também ao fluxo de dados caso não aconteça a negação do serviço este pode ficar mais lento.

Elevation of Privilege

Aqui pode haver ataques de injeção de comandos ou códigos, este tipo de ameaça é explorado quando o atacante fornece um carater de controlo e depois um comando. O uso de SQL injection pode fazer com que o sistema interprete certos símbolos como comandos, por exemplo se o nosso sistema lidar com scripts Shell unix, o Shell pode ver o <;> como o final da entrada assim assumindo qualquer coisa como comando – Elevation through data tampering/elevation of privilegie contra o processo de login através da corrupção do processo.

Cliente web e o servidor(Front end)

Resumidamente, o nosso modelo do sistema de agricultura de precisão demostra diversas ameaças que poderão ser transformadas em ataques, de forma breve a baixo temos a descrição de quadro hipóteses que facilmente poderiam ser descritas numa àrvore de ameaças (threat tree). Estas ameaças e cenários afetarão em grande parte a CIA.

Na hipótese de o atacante ser capaz de ler mensagens de utilizadores, sejam eles agricultores ou especialista. Tal suposição pode ser atingida no caso de um utilizador não tenha se desconectado ou mesmo tendo guardado, acidentalmente, as credenciais num computador público. (Confidencialidade e autenticação)

No caso de ocorrer uma falha de validação de dados se o cliente forneça inputs inválidos na entrada. Um exemplo prático, pode ser quando um user digita <script> e o campo em questão é validado, mas a validação de entrada falha porque <script> não é um input válido a ser inserido. Com isto permitindo ao invasor fornecer uma instrução SQL que posteriormente irá correr no banco de dados do nosso sistema.

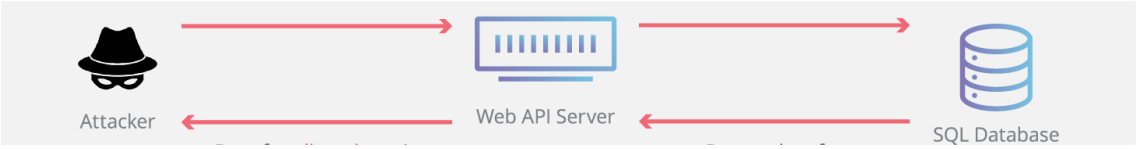


Figura 3 - Imagem meramente ilustrativa de um ataque de injeção SQL

Neste seguimento, algo parecido poderia acontecer, a autorização poder falhar permitindo acesso não autorizado, com a Implementação de verificações de autorização resolveríamos esta ameaça. No caso anterior a solução estaria na implementação de verificação e validação dos dados inseridos.

Por último algo comum como o cache do browser poderia conter conteúdos de mensagens sigilosas ou mensagens nos cabeçalhos que não deveriam ser visíveis para o comum utilizador e o são em certa altura.

Pode ocorrer na validação de entrada por parte do invasor uma SQL injection, permitindo assim que o atacante possa modificar dados da base de dados, afetando assim a integridade do sistema. (Integridade)

Visto que no nosso sistema o armazenamento de dados é remoto, como é dito no enunciado, pode ser executado no armazenamento conectado à rede, neste caso o controlador de armazenamento poderá ignorar todos os controlos nos dados. Ainda, as conexões de rede acabam por ser vulneráveis a ataques acima referidos. Podíamos prevenir grande parte desses ataques, sejam eles, de divulgação de informação, adulteração ou mesmo negação de serviço através da presença de um conjunto limitado de conexões, com estas conexões controladas pelas permissões do nosso sistema.

O back-end é responsável pelo processamento e armazenamento de dados. Neste caso o back-end é baseado na Cloud, e suporta múltiplos usuários simultâneamente, onde um usuário consegue aceder ao seu espaço alocado, mas não consegue aceder aos de outros usuários.

Mas um dos problemas de Cloud multilocatário (vários usuários) é que existe a partilha de recursos e serviços, que servem múltiplos usuários, o que significa que os recursos físicos, como o armazenamento e o processamento são partilhados.

Devido a isto, existe vários riscos associados este tipo de serviço.

Tempering

Um usuário malicioso devido a falhas na segregação de usuários, consegue aceder a dados guardados pelos usuários e apagá-los ou modifica-los.

Neste caso, em agricultura de precisão, isto resultaria na perda de dados relacionados com o bom funcionamento da plantação, armazenados para a criação de melhores estratégias agrícolas, importantes para a análise e melhoramento de produção.

Com a alteração de dados, a analise destes resultará na criação de gráficos de qualidade e produção com dados incorretos, sendo que seriam postos em prática soluções que contrariariam a necessidade real da plantação.

Information Disclosure

Segurança inadequada para conseguir segregar com sucesso os diferentes usuários (visto que estes partilham armazenamento, o processamento, base de dados) pode abrir espaço para vários ataques ou falhas críticas no sistema.

Os usuários maliciosos podem aproveitar-se da falta de segurança entre “inquilinos” e conseguir com sucesso roubar dados alheios.

Estes dados podem ser informações relativas ao funcionamento do sistema agrícola, como também pode haver informações pessoais (nomes e moradas de clientes) palavras-passe, entre outros dados.

Denial of Service

Um usuário malicioso consegue, devido a falha arquitetural da partilha de serviços, abusar e sobrecarregar o processamento, podendo causar um *denial of service*, afetando todos ou utilizadores.

Por outro lado, uma má configuração da partilha de serviços por parte de um especialista poderia também derrubar o serviço e impedir a sua utilização.

Isto poderá impedir o armazenamento de dados obtidos pelos sensores, fazendo com que se perca dados importantes sobre o bom funcionamento do sistema agrícola.

Gateways

Neste modelo os gateways serão habilitados com diversas interfaces de rádio, para a realização com os sensores e atuadores seja efetuada. É utilizada GSM mobile (Radio Frequência), GPRS / LTE para a conectividade à rede. Aqui os gateways estarão responsáveis pelo gerenciamento dos sensores e atuadores instalados nos campos, irão ajustar a sua operação conforme as analises dos processos do back-end.

Em suma, o gateway terá o propósito de receber os dados encaminhados pelos nodos sensores e efetuar diversos processos, entre eles, agregar dados dos sensores, executar aplicativos para gestão e analise desses dados e ainda enviar resumos periódicos do resumo dos dados. O processo de envio de dados é realizado através de serviços externos, internet, para que depois sejam armazenados na base de dados do sistema, de modo a serem acedidos pelos agricultores e especialistas.

A estratégia que seguimos nesta parte do sistema foi mais a de focar no invasor, aquilo que o invasor pode fazer, ou quer atacar e como defender.

Bem, a comunicação como já referido é feita utilizando GSM. Este sistema traz diversas ameaças, sendo, por exemplo, caso o tráfego de comunicação e sinalização não está protegido quando está conectado a rede fixa. Deste modo, se a rede fixa estiver comprometida o tráfego de comunicação realizado por GSM também está, pois esta conecta-se à rede fixa. Geralmente é complicado estar ciente da segurança dos dados.

Pela visão do atacante temos algumas ameaças a salientar:

O atacante pode ter a capacidade de intercetar informações do tráfego e dados associados aos usuários com maior privilégio (Especialistas). Basta que o atacante tenha um telefone modificado para transformar o vetor de ameaça para um vetor de ataque. (Information Disclosure afetando a confidencialidade dos dados dos agricultores e especialistas)

Algo que também pode acontecer é o atacante ter a capacidade de enviar dados não autorizados ou mensagens para a rede com a intenção de fazê-las aparecer por outro usuário, por exemplo

o invasor passar-se por especialista e enviar dados para os atuadores fazendo com que estes não funcionem corretamente (Spoofing, violando a autenticidade).

Outro caso que pode acontecer é o sistema, os gateways, serem vítimas de ataques de repetição, onde o atacante consegue repetir a transmissão de dados fraudulentos, vindos dos sensores ou da nuvem, basicamente o ataque é feito a algum dos protocolos do GPRS usando a tal repetição de mensagens de um contexto diferente para o contexto esperado, deste modo o ataque pode "enganar" processos e utilizadores. Se a ameaça for de nível maior pode mesmo ocorrer que o atacante execute ataques de "Man-in-the-middle. A proteção para esta ameaça seria a de implementações de limites de fluxo de dados, assim dificilmente haveria uma sobre carga na rede.

Com alguma pesquisa sobre a tecnologia GSM usada neste sistema, concluímos que é demasiado "frágil" contra-ataques de negação de serviços, sendo que nem é necessário muitos recursos para o fazer. Isto deve-se ao fato do protocolo de configuração de chamadas aloca recursos sem uma autenticação mínima. Permitindo assim que o invasor consiga realizar o ataque com sucesso. A solução reside na encriptação dos dados ou do próprio fluxo.

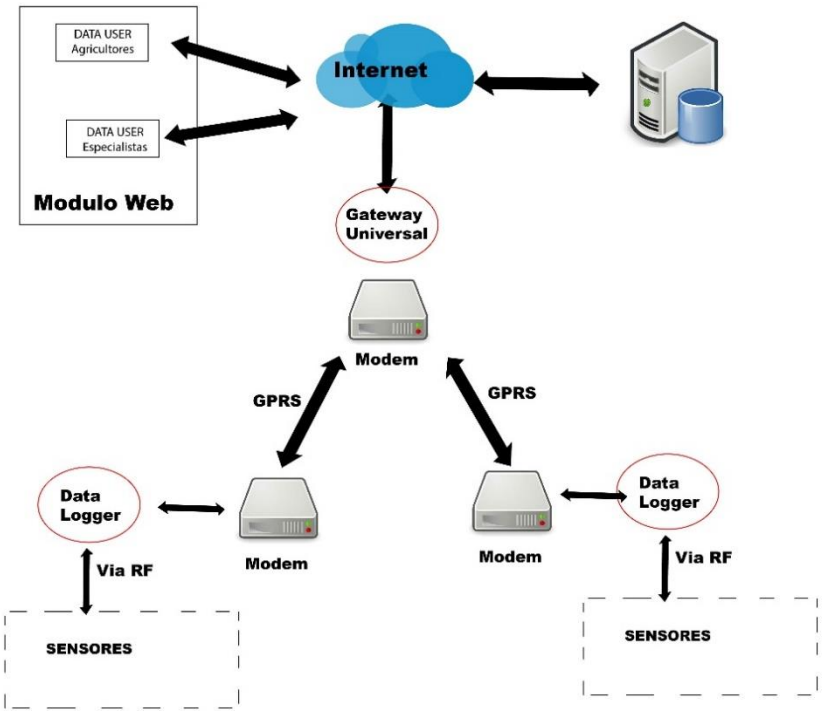


Figura 4 – DFD simplificado e com as respetivas formas de comunicação

Sensores/Atuadores

Sensores que transmitem informação via wireless com ligação a internet

Os sensores (Zigbee, telosb, arduinos ou raspberries)

Tipos de Vulnerabilidades

Fabricação de Informação – Um atacante injeta dados falsos, comprometendo o resto da informação.

Interrupção de comunicação - A comunicação entre sensores ou entre sensor e Cluster Leader/gateway perde-se, que impedem a transmissão da informação (exemplos: captura de nodes, adição de código malicioso)

Interceção de dados – A informação é intercetada pelo atacante, que ganha acesso indevido aos dados ou aos sensores.

Possíveis ataques (Sensores) (Stride)

Tampering

Uma forma mais física, mas que também provoca embaraçamento e prejuízo em negócios que dependem muito da tecnologia para o bom funcionamento do ecossistema empresarial é o vandalismo de material técnico.

Neste caso, na produção agrícola, onde as regas, a exposição solar e a temperatura são controlados por sensores ligados a rede, e dependem do bom funcionamento e da precisão dos dados recolhidos pelo sensor, a falha destes pode ser prejudicial e critica na produção e no crescimento dos cultivos expostos.

A necessidade de colocar os sensores expostos é inevitável, pois estes são essenciais para a recolha de dados do solo e do ambiente em geral, mas que aumenta o risco de roubos, ou a destruição destes.

Quando os sensores são vandalizados de tal forma que a precisão dos dados fica comprometida, a informação por estes recolhida apenas compromete a viabilidade da informação de todos os sensores.

Para além do facto da exposição dos sensores ser um risco por si só, a necessidade de estes estarem conectados a rede também pode ser um ponto critico e alvo de ataques.

Um atacante mal-intencionado que consiga injetar dados falsos pela rede dos sensores, poderá com sucesso desequilibrar o funcionamento normal dos sistemas mecanizados.

Como os atuadores respondem conforme os dados fornecidos pelos sensores, a informação que foi previamente manipulada consegue com sucesso chegar as instruções dos atuadores. Como tal conforme os dados recebidos, o atuador responderá com a ação por estes enviados.

Se os dados recebidos por estes indicar que existe, sistematicamente, uma falta de água e uma necessidade de ser regado, poderá acontecer uma inundação no campo.

Se, por exemplo, a informação transmitida corresponder a uma temperatura inferior, a temperatura poderá subir drasticamente, ou a radiação solar apresentar ser maior do que realmente é, inibindo a exposição solar das plantações, podem pôr em causa os vários cultivos.

Uma forma de prevenir estes ataques seria pôr em prática o uso da criptografia para assegurar a integridade dos dados enviados.

Information Disclosure

Como os sensores estão conectados á rede, estes ficam expostos a ataques remotos.

Através destes ataques, o atacante consegue com sucesso aceder e roubar as várias informações que estão a ser fornecidas pelos sensores.

Uma das causas do vazamento de informação é a falta de encriptação sobre os dados enviados, sendo que assim o trabalho fica facilitado para o atacante.

Estas falhas podem não ser disruptivas para a produção agrícola, mas podem providenciar a concorrentes ou possíveis atacantes informações sobre o funcionamento geral do ecossistema agrícola.

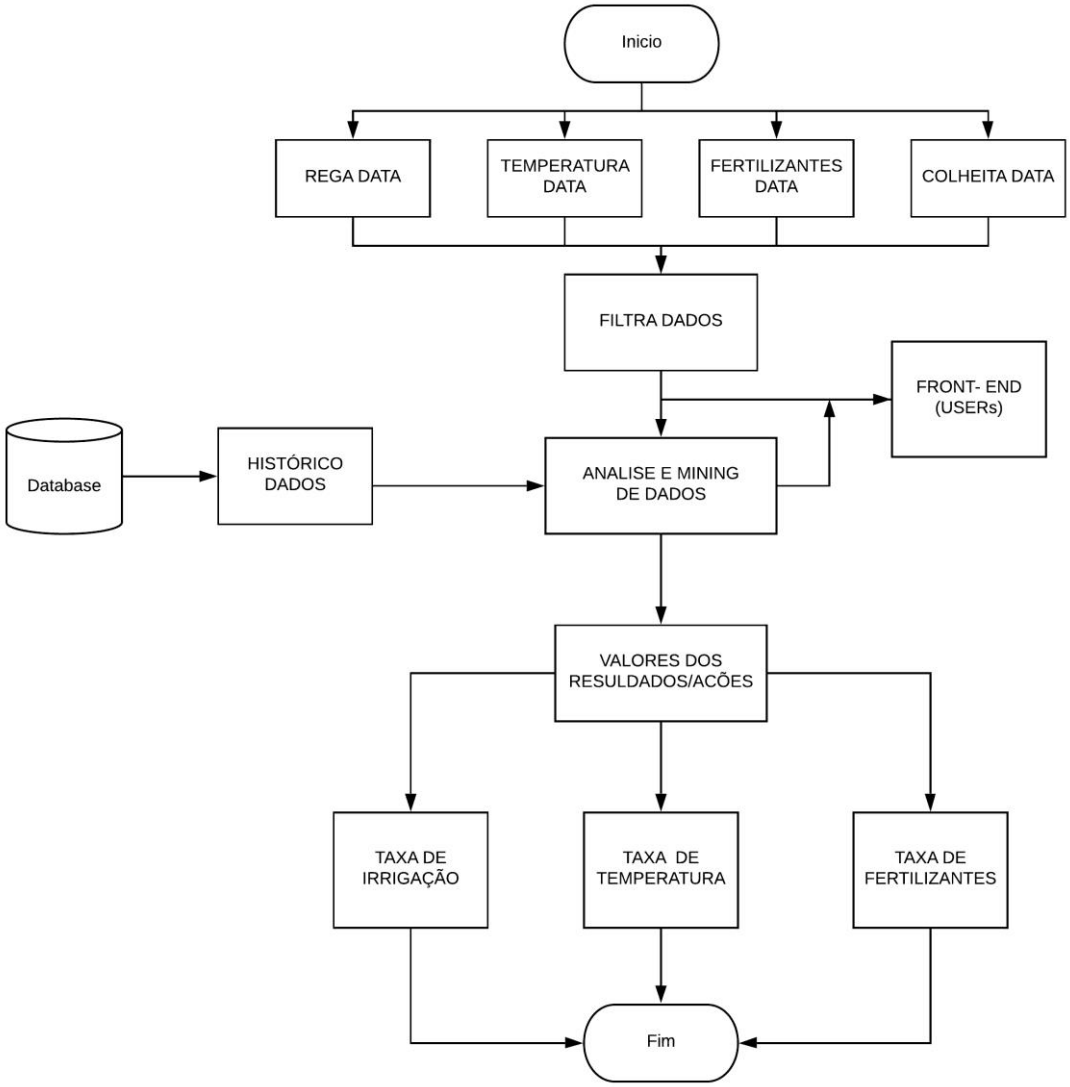
Denial of Service

Uma forma física de bloquear o envio de informações de rede é usar um atolamento de radio (radio *jammer*), que atua na mesma frequência que a comunicação dos sensores. Isto impedirá com que os sensores comuniquem entre si, e com o *gateway*.

Os sensores são aparelhos que dependem de bateria para o seu funcionamento, como tal, quando não estão em uso estes entram num modo de poupança de energia. Ataques que impedem o sensor de poupar bateria e obrigar ao seu funcionamento constante leva a uma exaustão muito rápida da bateria, assim desativando o sensor.

Um atacante que consegue enviar pacotes excessivos para a rede poderá obstruir a rede com pacotes maliciosos, conseguindo assim evitar com que o sistema envie e receba pacotes legítimos.

Modificação de informação – Um atacante consegue aceder a dados, como também os modifica. Isto permite a alteração dos pacotes de dados, inundando a rede com informação falsa, podendo causar um Dos (*Denial of service*)



Conclusão

A realização deste modelo de ameaça tinha como objetivo analisar e descobrir falhas de segurança que podem afetar um sistema de agricultura de precisão, sendo que este teria que aplicar as várias estratégias conforme o que foi ensinado nas aulas para ser realizado com sucesso um modelo de ameaças detalhado e bem estruturado.

Ao longo desta análise foram apresentados vários componentes e elementos que integram o ecossistema que é a agricultura de precisão, sendo que cada um foi analisado, seguindo uma das duas estratégias: focado em Assets, e a partir do ponto de vista do atacante.

Cada componente foi escrutinado e analisado de maneira a ser possível apresentar as fraquezas que os elementos que incorporam o ecossistema continham, sendo que utilizado o método STRIDE como meio para encontrar possíveis ameaças, apontamos com base nas suas seis categorias as várias falhas de segurança que poderiam afetar o modelo.

Como tal e aplicando os conhecimentos aprendidos em aula foi possível realizar este modelo com sucesso, e como consequência, foram consolidados as várias estratégias e métodos aprendidos em aula, sendo que agora existe uma maior compreensão na importância da análise e na realização destes modelos para o desenvolvimento de sistemas mais seguros.

Referências

Albert, Z. T. (2016). *Security Issues in Wireless Sensor Network.* Sydney.

owasp. (30 de Agosto de 2010). Obtido de https://www.owasp.org/index.php/Cloud-10_Multi_Tenancy_and_Physical_Security

owasp. (06 de Junho de 2016). Obtido de https://www.owasp.org

Shostack, A. (2014). *Threat Modeling Designing for Security .* Wiley.

Shostack, A. (03 de Julho de 2018). *Misti*. Obtido de https://misti.com/infosec-insider/threat-modeling-what-why-and-how

Os diagramas aqui presentes foram desenhados com apoio das seguintes ferramentas:

Lucidchart e Illustration cc.