Universidade do Minho
Mestrado Integrado em Engenharia Informática
Segurança de Sistemas Informáticos

TP1 - Parte B
Threat Modelling

Diana Ribeiro Barbosa A78679

Francisco José Moreira de Oliveira A78416

Índice

Modelação do Sistema

O primeiro passo do "*4 steps framework*" de Threat Modelling é a modelação do sistema. Para este caso, consideramos que a modelação mais adequada que nos permitiria uma melhor compreensão do seu funcionamento envolveria um *Data Flow Diagram*. Estes são especialmente úteis na medida em que facilitam o processo de deteção de vulnerabilidades uma vez que permitem compreender o movimento dos dados pelo sistema e, portanto, perceber onde ataques podem ser realizados.

Na figura abaixo é possível visualizar o diagrama de *data flow* do sistema a ser estudado.

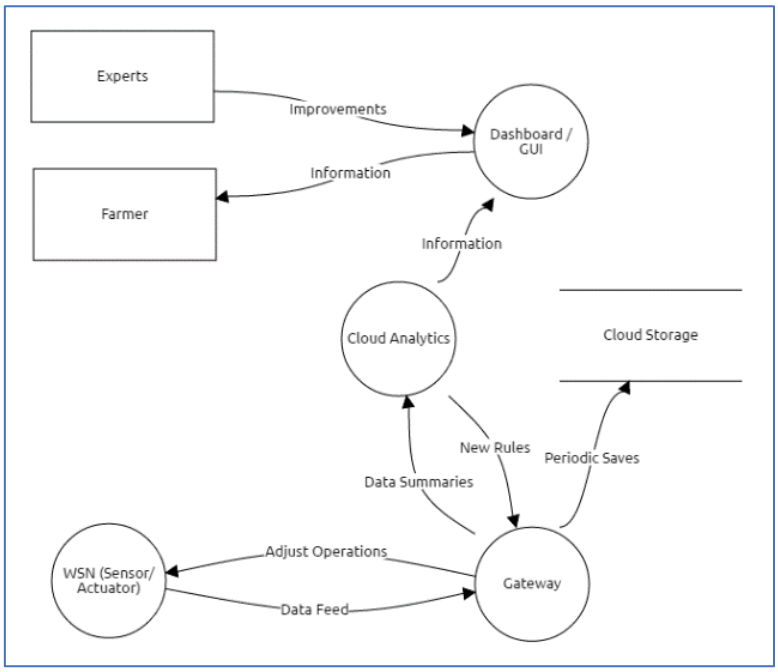

Figura 1 Data Flow Diagram do Precision Agriculture System

Ameaças

O segundo passo de Threat Modelling é a identificação de ameaças, isto é, identificar as vulnerabilidades do sistema relevantes no contexto da sua aplicação e como estas podem ser exploradas.

Um dos modelos de ameaças mais utilizados é o STRIDE (desenvolvido pela Microsoft). Cada letra deste acrónimo é a inicial de um dos seis tipos de ameaças, sendo que cada uma delas (*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service e Elevation of Privilege*) é o oposto das propriedades de um sistema seguro (Autenticação, Integridade, Não-repúdio, Confidencialidade, Disponibilidade, Autorização).

Spoofing

Um ataque de *Spoofing* acontece quando há comunicação com um utilizador, na qual a origem personifica uma fonte (sistema ou pessoa) que é conhecida ao recetor, violando a propriedade Autenticação.

Utilizando o modelo STRIDE, a identificação de vulnerabilidades que possam ser exploradas desta forma passa pela resposta à pergunta "*É possível um atacante ganhar acesso ao sistema usando uma identidade falsa*?".

A nível de requisitos de segurança do sistema, no que toca a autenticação, é requerido que este consiga evitar a injeção de pacotes adicionais e que não permita que os nodos aceitem falsas tarefas administrativas como por exemplo a reprogramação da rede.

As várias possibilidades de spoofing passam por:

- Spoofing do *gateway*, isto é, o atacante fingir ser o *gateway* e enviar ordens maliciosas aos actuators uma vez que é o *gateway* de uma WSN que ajusta as suas operações.
- Spoofing do *Analytics Module* enviando regras de aplicação maliciosas aos *gateways*.

Tampering

Um ataque de Tampering consiste da modificação não autorizada de dados através da sua destruição, manipulação ou edição violando a propriedade de Integridade de um sistema. Isto pode acontecer durante a transmissão de dados podendo o atacante intercetar mensagens não protegidas e modificar o seu conteúdo, mas também por exemplo com *data* em memória.

Utilizando o modelo STRIDE, a identificação de vulnerabilidades que possam ser exploradas desta forma passa pela resposta à pergunta "*É possível um atacante alterar dados do sistema*?". No caso de estudo, a nível de Integridade, os requisitos de segurança passam por impossibilitar a corrupção de dados de modo a não permitir que os serviços prestados sejam afetados.

Ameaças que comprometam a integridade do sistema por Tampering são:

- Tampering com os sensores das WSN. Os sensores recolhem e enviam dados ao gateway que são analisados para ir ajustando o comportamento de vários *devices* no campo (e.g. o sistema de rega).
    - Redirecionando o *data flow* para a máquina do atacante, o gateway não recebe informação atualizada e, por conseguinte, não vai enviar ordens adequadas aos *actuators*.
    - As consequências seriam semelhantes caso o atacante modificasse os dados durante o seu envio para o *gateway*.
- Tampering com o *Gateway*.
    - Uma das tarefas dos *gateways* é correr aplicações de para o controle dos dispositivos de *IoT (Internet of things)* e análise dos dados. Um dos ataques

possíveis seria a modificação desse código o que por sua vez iria afetar negativamente o bom funcionamento do sistema.
    - Outro possível ataque seria a modificação ou redireccionamento das indicações de ajustes enviadas às WSNs.

Repudiation

Um ataque de Repudiation acontece quando uma aplicação ou sistema não aplica medidas de controlo apropriadas de rastreio e registo das ações dos utilizadores tornando possível a um atacante forjar e/ou manipular a sua identificação, isto é, atribuir ações a outros utilizadores do sistema ou utilizadores fictícios.

Utilizando o modelo STRIDE, a identificação de vulnerabilidades que possam ser exploradas desta forma passa pela resposta à pergunta "*É possível provar que o atacante foi a fonte do ataque*?".

No *Precision Agriculture System*, não-repúdio não é um dos requisitos de segurança.

Information Disclosure

Um ataque de Information Disclosure ocorre quando um atacante consegue aceder a informação à qual não era suposto ter acesso, violando a confidencialidade do sistema.

Utilizando o modelo STRIDE, a identificação de vulnerabilidades que possam ser exploradas desta forma passa pela resposta à pergunta "*É possível um atacante aceder a dados privados ou potencialmente prejudiciais?*".

No sistema que ao qual este relatório se refere, um dos requisitos de segurança é que a localização e identidade dos nodos que geram informação deve ser secreta ou protegida. Assim, ataques de information disclosure podem ser:

- Aceder aos dados que os sensores enviam ao *gateway*, e extrair daí a sua identidade e localização. Este ataque pode ocorrer tanto durante o envio como ser um ataque diretamente aos dispositivos.
- Aceder à *cloud* na qual são guardadas periodicamente *data sumaries*.

Denial of Service (DoS)

Um ataque de Denial of Service (DoS) ocorre quando os atacantes interferem com a disponibilidade do sistema absorvendo os recursos necessários à prestação do serviço impedindo os utilizadores de lhe acederem. Na prática, o ataque geralmente consiste do envio em grande escala de pedidos de autenticação cujos return addresses são inválidos, o que leva a

que o servidor espere antes de fechar a conexão mantendo-o ocupado e indisponível quando isto acontece para um elevado número de mensagens.

Utilizando o modelo STRIDE, a identificação de vulnerabilidades que possam ser exploradas desta forma passa pela resposta à pergunta "*É possível um atacante reduzir ou impedir a disponibilidade do sistema?*".

No *Precision Agriculture System,* é essencial que os utilizadores sejam capazes de aceder aos serviços sempre que assim queiram. Assim, possíveis ameaças deste tipo são:

- Ataque DoS ao GUI impedindo os utilizadores (agricultores) de acederem aos dados.
- Ataque DoS impedindo o envio dos dados dos sensores ao *gateway*, consumindo os recursos da rede.
- Ataque DoS ao *gateway*, ocupando toda a memória impedindo que este guarde os dados recolhidos pelos sensores.

Elevation of Privilege

Um ataque de elevation of privilege consiste em o sistema permitir que um utilizador ganhe acesso a recursos aos quais não deveria ter acesso por ausência de autorização, por exemplo, privilégios que apenas administradores deveriam ter.

Utilizando o modelo STRIDE, a identificação de vulnerabilidades que possam ser exploradas desta forma passa pela resposta à pergunta "*É possível um atacante assumir a identidade de um utilizador privilegiado?*".

Ataques de elevation of privilege neste sistema podem ser:

- Elevation of privilege por data Tampering.
    - O sistema vai sendo melhorado por *experts* que lhe fazem *updates* regularmente, sendo que estes são os administradores do sistema e por conseguinte possuem os privilégios necessários para o fazer. Um atacante que altere em disco os *updates* fazendo com que o sistema aja de maneira do que o administrador pretendia, está a cometer um ataque de elevation of privilege.

Bibliografia

https://www.toreon.com/application-security-training/threat-modeling-in-4-steps/

https://www.techopedia.com/definition/5398/spoofing

https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-065.pdf

https://www.csoonline.com/article/2969402/microsoft-subnet/researchers-exploit-zigbee-security-flaws-that-compromise-security-of-smart-homes.html

https://www.owasp.org/index.php/Repudiation_Attack

https://www.techopedia.com/definition/24841/denial-of-service-attack-dos