



Universidade do Minho
Escola de Engenharia

Tactical Threat

GRUPO 1:
RICARDO PEREIRA
TIAGO RAMIRES

GRUPO 3:
ADRIANA MEIRELES
CARLA CRUZ


Introdução

- A grande maioria dos dispositivos com que lidamos necessita de proteção:
 1. sensores biométricos;
 2. *smartphones*;
 3. *routers*;
- Ocorrência de falhas básicas após ataques bem sucedidos;
- **"Prevenir para remediar!"**

2. Porque fazer Modelação de Ameaças?

- O que é modelação de ameaças?
- Objetivo principal
- Importância da modelação de ameaças

Em que é que realmente se concentram estas modelações?



Identificação de ameaças e problemas de segurança

Classificação das consequências e a probabilidade de ameaças.

3. Quando fazer Modelação de Ameaças

- Idealmente, a modelação de ameaças é aplicada assim que uma arquitetura é estabelecida.
- Começar muito tempo mais tarde pode significar que mudanças estruturais significativas ou adicionais necessárias para segurança.
- A modelação de ameaças é um exercício útil, independentemente de quão próximo o sistema esteja da implementação ou de quanto tempo ele esteja em uso.

4. Atualização da Modelação de Ameaças

Lista parcial de revisão que poderá indicar a necessidade de atualização:

- Alterações que afetam o processamento, a manipulação ou a classificação de dados pelo seu software.
- Adição de uma nova subcomponente, repositório de dados, mesmo que esta alteração pareça pequena e não esteja diretamente relacionada à segurança.
- Existem alterações adicionais nos controlos de segurança e funcionalidades:

Autenticação

Autorização

Registo, monitorização
e alerta

Criptografia

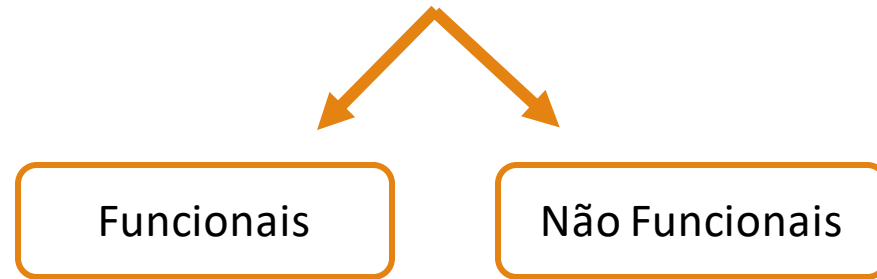
- Introdução ou alteração dos canais de comunicação entre as subcomponentes

5. Como fazer Modelação de Ameaças

- O processo de modelação de ameaças geralmente envolve algumas, distintas mas relacionadas, sub-atividades.
- Existem algumas maneiras populares de expressar esta descrição e identificação.
- O formato específico é menos importante do que a sua utilidade para os modeladores.
- Existem muitas maneiras possíveis de criar a modelação de ameaças.

5. Como fazer Modelação de Ameaças

Os objetivos do sistema são definidos em duas categorias de requisitos



- Cada requisito de segurança é composto por 3 partes

O problema

O control

Diretrizes de implementação

6. Falha na Modelação de ameaças

- São consideradas como "falhas de mentalidade" as seguintes:
 - O facto de se fazer testes de intrusão com ferramentas e pessoas;
 - O facto de o sistema já estar construído e implementado;
 - O facto de se ter criado um modelo de ameaças quando o sistema foi construído;
 - O facto da modelação de ameaças ser um processo complicado;
 - O facto de não possuir profissionais na área;
 - O facto de se estar a fazer modelação de ameaças nos momentos certos;

6. Falha na Modelação de ameaças

- As falhas que se seguem são falhas práticas :
 - falha em controlar o alcance da análise;
 - foco em áreas que já são bem conhecidas;
 - Não definir o que é o "Sucesso";
- As principais armadilhas :
 - Não incluir as partes interessadas no processo;
 - Falta de comunicação por parte dos membros da equipa;
 - As superfícies de ataque que podem ter sido derivadas de falhas na comunicação ;

7. Construção de uma Boa Equipa

- Podem ser considerados os seguintes especialistas na parte técnica:
 - **Arquitetos de solução:** possuem conhecimentos aprofundados da estrutura total de todo o sistema;
 - **Arquitetos:** pessoas que são especialistas na estrutura para partes definidas do sistema;
 - pessoas com experiência em rede, sistemas operativos, processos de implementação, cloud, garantia de qualidade, design de software;
 - A modelação de ameaças é para ser feito em equipa. Portanto, reduzir o número de membros da equipa pode ser prejudicial;
 - Para além de toda a parte técnica, é fundamental ter pessoas com diferentes abordagens/talentos;

8. Extensão da Modelação de Ameaças

- **Quão profundo vão os modeladores na estrutura de um sistema?**
- **Quais os pré-requisitos para o começo da modelação de ameaças?**
- **O que permite a finalização da modelação de ameaças?**

9. Metodologia

- Existem várias metodologias aceites pela indústria:
 - Processo de Modelação de ameaças da Microsoft;
 - P.A.S.T.A (Process for Attack Simulation and Threat Analysis);
 - Trike;
 - ATASM(Architecture, Threats, Attack Surfaces, and Mitigations);
 - Biblioteca de ameaças/ Abordagem de lista;
 - Modelação de Ameaças Rápida;
 - Existem outras para enumeração e descoberta de ameaça, tais como: **STRIDE**, **CVSS** (Common Vulnerability Scoring System), Open Group™ Factor Analysis of Information Risk (**FAIR**), **CWSS** (Common Weak-ness Scoring System) e **CWRAF** (Common Weakness Risk Analysis Framework).

10. Terminologia

- Equipas que "vendem" os projetos nem sempre são formadas pelas pessoas mais indicadas.
- **É possível vender algo sem saber exatamente aquilo que se está a vender?**
- Mal entendidos no que é acordado entre o cliente e o vendedor.
- Soluções?

10. Terminologia

- A contratualização de um projeto deve sempre ser acompanhada por alguém que saiba do que fala.
- Devem ser utilizados termos apropriados e estes têm que ser bem empregues.
 1. *Threat* - causa potencial de um acontecimento perigoso para uma organização/sistema;
 2. *Risk* - consequência da incerteza inerente nos objetivos;
 3. *Vulnerability* - um problema que se manifesta numa determinada implementação.
- Por exemplo, diferenças entre *weakness* e *vulnerability*.

11. Manuseamento de Sistemas Complexos

- Existem vários sistemas que podem ser difíceis de modelar.
- **Sistemas *IoT* :**
 1. serviços *cloud*;
 2. aplicações *web* e móveis;
 3. sensores;
 4. câmaras;
- Soluções?

11. Manuseamento de Sistemas Complexos

- Mote para a resolução destes problemas:

"Dividir para conquistar"

- **Primeira fase** - modelação do sistema na totalidade (**comportamentos** e **interações** entre os **principais constituintes**).
- **Segunda fase** - modelação específica de cada constituinte.

12. Tecnologias/Ferramentas

- Que **ferramentas** e que **tecnologias** existem disponíveis?
- Essas **ferramentas** são eficazes?
- **Cobrem todos os aspectos da modelação de ameaças?**

12. Tecnologias/Ferramentas

- soluções atuais não abrangem todos os mecanismos existentes;
- utilização de algumas ferramentas constitui uma **barreira** para trabalhar na área;
- iniciação do processo de modelação pode ser complicado;
- não é visível uma **consequência imediata**.

12. Tecnologias/Ferramentas

- **treino de pessoal** interessado e **destacamento de especialistas** para os formarem;
- **procura** e **interesse** na área tem vindo a crescer;
- garantidamente menos problemas de segurança a longo prazo.

12. Tecnologias/Ferramentas

- Necessidade de uma aplicação que preencha os seguintes requisitos:
 1. modelação da arquitetura usando **diagramas**;
 2. **anotação de problemas** insurgentes;
 3. **classificação** e **rastreamento** desses problemas;
 4. oportunidade do utilizador **poder escolher a abordagem** que quer ter;
 5. a modelação deve ser acompanhada da **construção de um relatório com layout editável**;
 6. possibilidade de **exportar/importar modelos já existentes** construídos com as ferramentas atualmente utilizadas no mercado

13. Inclusão da modelação de ameaças no ciclo de vida do desenvolvimento

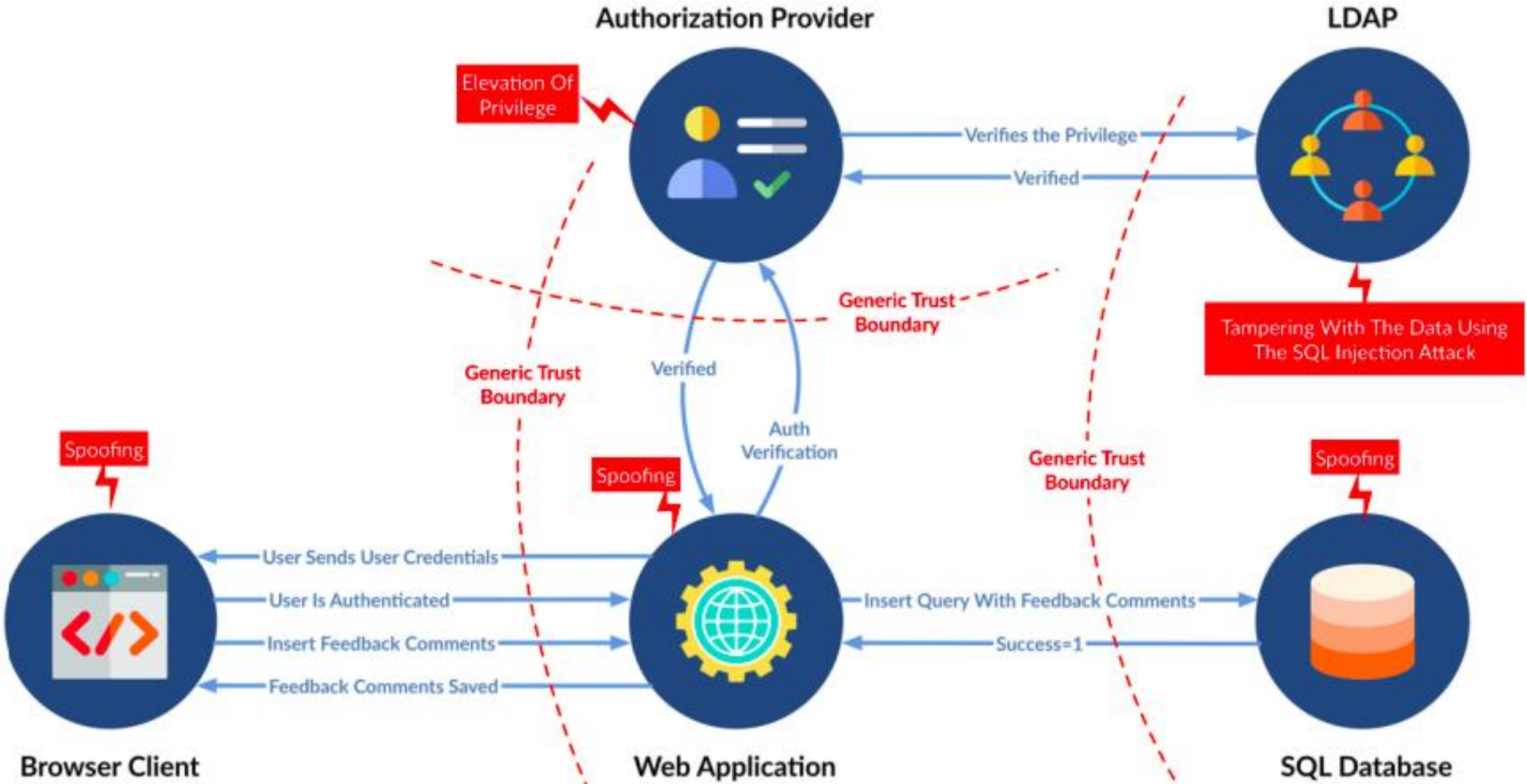
- o ciclo de desenvolvimento um sistema de software raramente inclui a modelação de ameaças;
- exemplos de modelos que **antecipam problemas** nos sistemas que modelam:
 1. página *web* que permite o teste de dispositivos médicos;
 2. modelo de verificação do sistema de controlo de velocidade de automóveis.

13. Inclusão da modelação de ameaças no ciclo de vida do desenvolvimento

- **sequência das fases do ciclo de vida de desenvolvimento:**
 1. **definição da estratégia** de segurança;
 2. avaliação da **arquitetura**;
 3. conceção do **modelo de ameaças**;
 4. análise ao *design*; (...)
 5. plano de teste. (...)

14. Exemplos de Modelação de Ameaças

- aplicação *web* de atribuição de *feedbacks*:
 1. identificação das entidades intervenientes;
 2. definição das zonas de confiança;
 3. pontos críticos com ameaças inerentes;
 4. ações realizadas entre entidades.



14. Exemplos de Modelação de Ameaças

- **autenticação em dispositivos *IoT*:**

1. pessoa \leftrightarrow dispositivo
2. dispositivo \leftrightarrow serviço
3. computador \leftrightarrow serviço
4. serviço \leftrightarrow serviço
5. dispositivo \leftrightarrow dispositivo

"A **autenticação** é um método de segurança que deve ser implementado sempre que possível!"

15. Práticas de Modelação de Ameaças e Desenvolvimento *Agile*

- **Modelação de ameaças e metodologia *Agile*:**
 1. *Sprint 0* - Iniciação e construção do modelo de ameaças com base no projeto geral;
 2. *Sprint 1* - Sempre que surja uma alteração ao código ou algo que invalide o modelo de ameaças, o mesmo deve ser alterado;
 3. *Release* - Fase em que se verifica se o modelo de ameaças reflete a segurança a ser implementada naquele sistema.
- **Modelação de ameaças em ambiente *DevOps*:** necessidade de ter cuidado com alguns sistemas automáticos que adicionam componentes ao *software*.

Conclusão

- Devem ser tidas em conta **boas práticas** para a construção de *software*;
- Modelação de ameaças é fulcral para garantir *softwares* **fidedignos** e **funcionais**;
- **Não é uma "perda de tempo"!**
- Os resultados são sempre visíveis a longo prazo;
- Existem **atividades de formação** e o nº de interessados tem crescido.



Universidade do Minho
Escola de Engenharia

Tactical Threat Modeling

GRUPO 1:
RICARDO PEREIRA
TIAGO RAMIRES

GRUPO 3:
ADRIANA MEIRELES
CARLA CRUZ