



Universidade do Minho
Escola de Engenharia

Tactical Threat Modeling

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 não remediar!"**

Introdução

- Porquê, quando e como fazer modelação de ameaças ?
- Atualização de modelos de ameaças;
- **Falhas** na modelação de ameaças;
- Metodologias a adotar.

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.
- Durante o ciclo de desenvolvimento, como existem várias alterações de requisitos/funcionalidades, é necessário uma reestruturação prévia da modelação de ameaças!

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