

Modelagem

de ameaças

“Modelagem de ameaças serve para identificar, comunicar e entender ameaças e mitigações no contexto de proteger algo de valor.” (OWASP)





insecurity princess 🎉
@saraislet

"Privacy" doesn't mean anything in the absence of a threat model.

What privacy means to you (and your threat model) may leave me vulnerable to threats within my threat model, and what privacy means to me may not account for your threat model.

Privacy isn't a linear spectrum.

12:53 AM · Apr 27, 2020 · [Twitter for Android](#)

"Privacidade" não significa nada na ausência de um modelo de ameaça.

O que privacidade significa para você (e para seu modelo de ameaça) pode me deixar vulnerável a ameaças dentro do meu modelo de ameaça, e o que privacidade significa para mim pode não ser responsável por seu modelo de ameaça.

Privacidade não é um espectro linear.

Para falar em modelos de ameaças...

Quais são as ameaças que nós temos no dia a dia?

Quais são as ameaças que nós temos nos nossos sistemas?

Identificar

1. O que você quer proteger?
2. De quem você quer proteger?
3. Quão provável é que seja necessário proteger?
4. Quanto vai ser afetada pelas consequências, caso você falhe?
5. Quanto esforço você está disposta a fazer para prevenir que o que você quer proteger seja exposto ou comprometido?

1. O que você quer proteger?

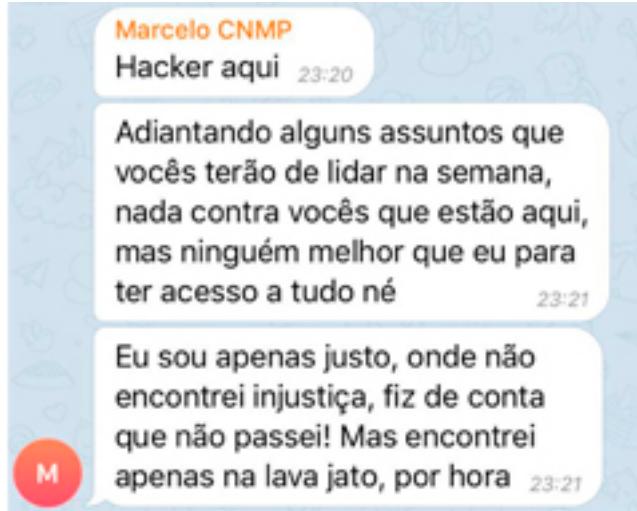


Alguns exemplos de assets (bens ou coisas que podem ser exploradas):

- Informações e dados de identificação pessoal
- Dados financeiros ou de negócio
- Metadados
- Dados e informações identificadoras de dispositivos
- Dados armazenados localmente nos dispositivos móveis ou nas servidoras, incluindo banco de dados dos contatos, banco de dados das mensagens de texto trocadas, calendário, notas, registro de chamadas, arquivos de mídia, acesso a redes sociais e identidades vinculadas.

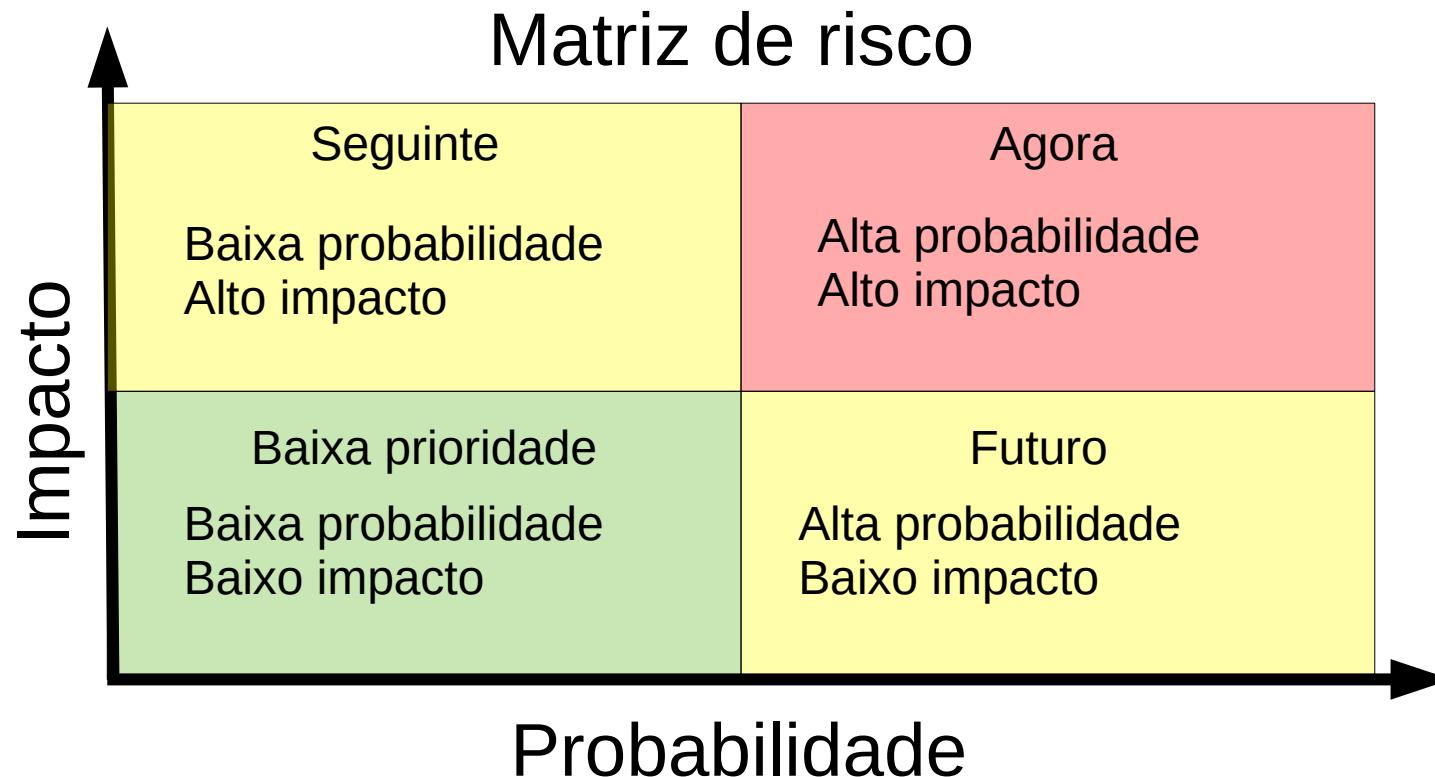
Confidencialidade, Integridade, Disponibilidade, Autenticação, Autorização...

2. De quem você quer proteger?



Descoberta accidental, pessoas cujos objectivo principal é atacar (o sistema / a pessoa), atacantes internos

3. Quão provável é que seja necessário proteger?
4. Quanto vai ser afetada pelas consequências, caso você falhe?



5. Quanto esforço você está disposta a fazer para prevenir que o que você quer proteger seja exposto ou comprometido?

Responder

aos riscos

O que é possível fazer diante de um risco?

Reducir / Mitigar

Transferir

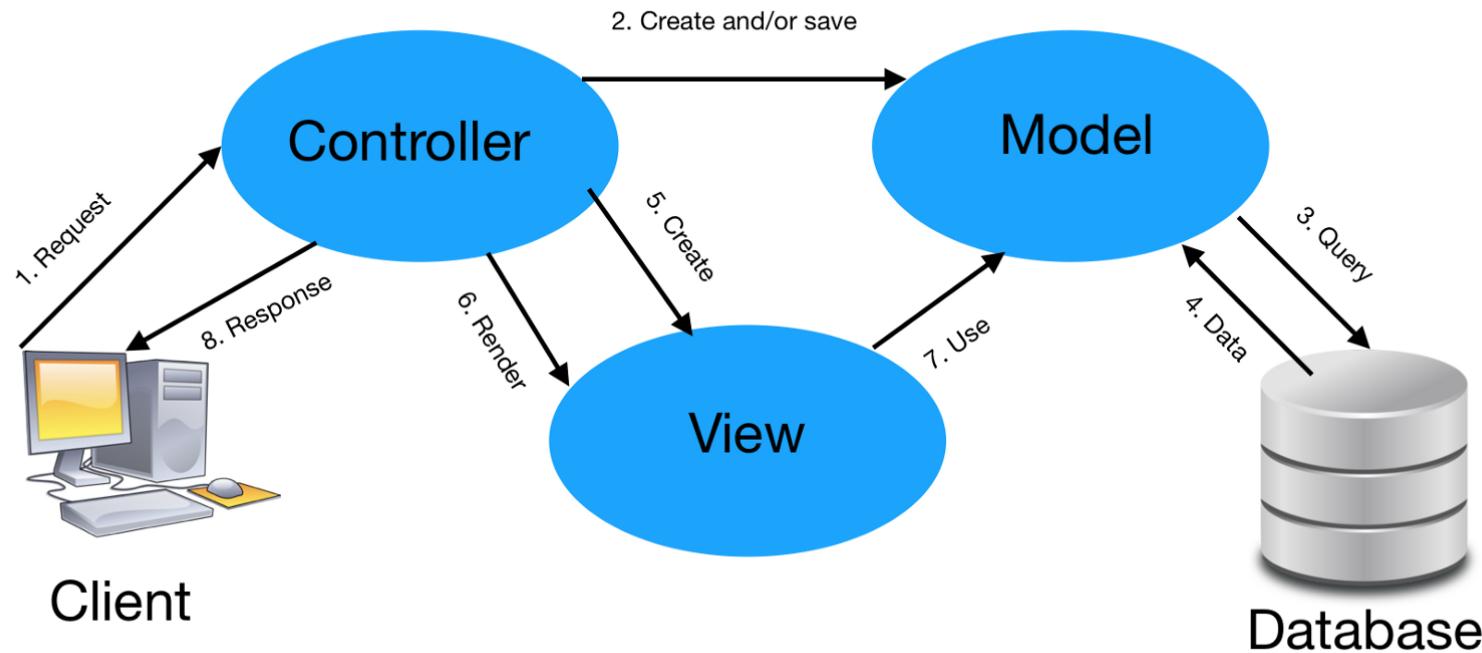
Evitar

Aceitar

E como fazer a

modelagem de ameaças?

Faça um perfil do seu sistema / aplicação / daquilo que você quer proteger



Organize contextos e cenários...

Crie “fronteiras de confiança” entre as diferentes partes do sistema

Mapeie entradas e saídas do sistema

Mapeie os fluxos de dados, para identificar vulnerabilidades

Identifique as ameaças e vulnerabilidades para cada um e coloque na matriz, para determinar o que vai ser “atacado” primeiro.

E depois?

1. Os riscos podem mudar com o tempo

- Descobertas de novas vulnerabilidades
- Sistemas/bibliotecas desatualizados
- Patches que mitigam ameaças existentes...

2. Por isso, é importante constantemente reavaliá-los, para ver se ainda fazem sentido ou se novas ameaças surgiram

Recursos adicionais:

OWASP Threat Modelling Control Cheat Sheet:

https://cheatsheetseries.owasp.org/cheatsheets/Threat_Modeling_Cheat_Sheet.html

OWASP Threat Dragon (ferramenta utilizada pra criar modelos de ameaças para aplicações web e desktop, registrando possíveis ameaças e decidindo em suas mitigações): <https://owasp.org/www-project-threat-dragon/>

Threat Modeling: Architecting & Designing with Security in Mind (OWASP):

<https://owasp.org/www-pdf-archive/AdvancedThreatModeling.pdf>