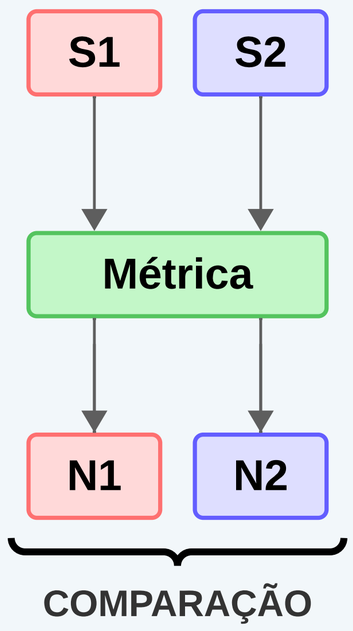
Métricas de privacidade

Revisão da literatura e aplicação em software científico na área de segurança de redes de computadores

Métrica sistemas



A partir de uma métrica podemos gerar uma nota para comparar sistemas considerando alguma característica

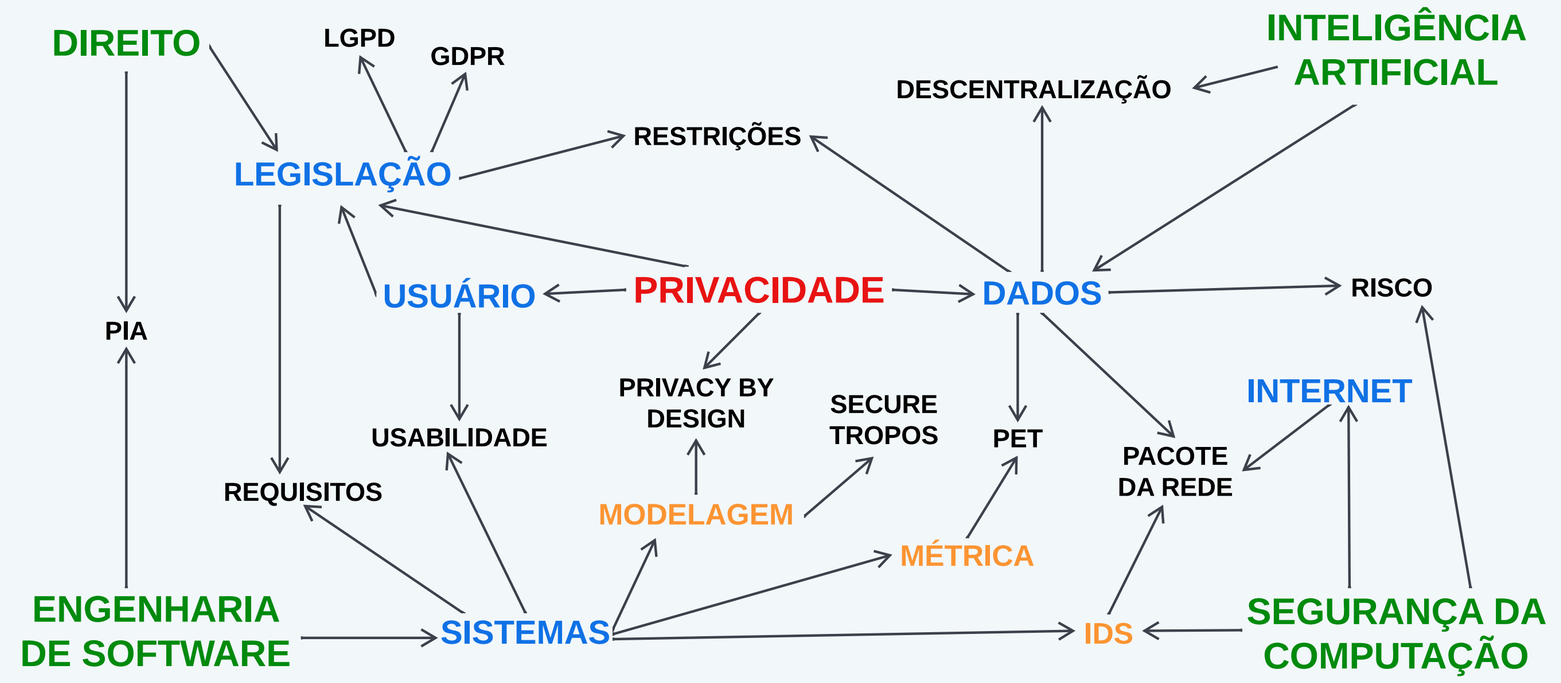
Motivação

Apesar das regulamentações recentes sobre privacidade, como a Lei Geral de Proteção de Dados Pessoais (LGPD) e a *General Data Protection Regulation* (GDPR), tem sido difícil encontrar trabalhos que avaliem o cumprimento dessas leis em sistemas de computação. No contexto de Segurança de Redes, é importante medir o quanto sistemas de detecção de intrusão (IDSs, do inglês *Intrusion Detection System*) conseguem cumprir o seu papel de monitorar o fluxo de pacotes e identificar uma possível intrusão, sem descumprir as regulamentações. Pelo melhor do nosso conhecimento, não existem trabalhos que tratem dessa avaliação. Isso é problemático, uma vez que IDSs estão cada vez mais utilizando técnicas de aprendizado de máquina supervisionado, necessitando de uma grande quantidade de informação potencialmente sigilosa. Esse trabalho estuda e avalia o balanço entre segurança e privacidade dos dados utilizados por um IDS: apesar dos dados serem essenciais para a segurança da rede, como lidar com o risco à privacidade dos usuários que terão seus dados acessados pelo detector?

Objetivos

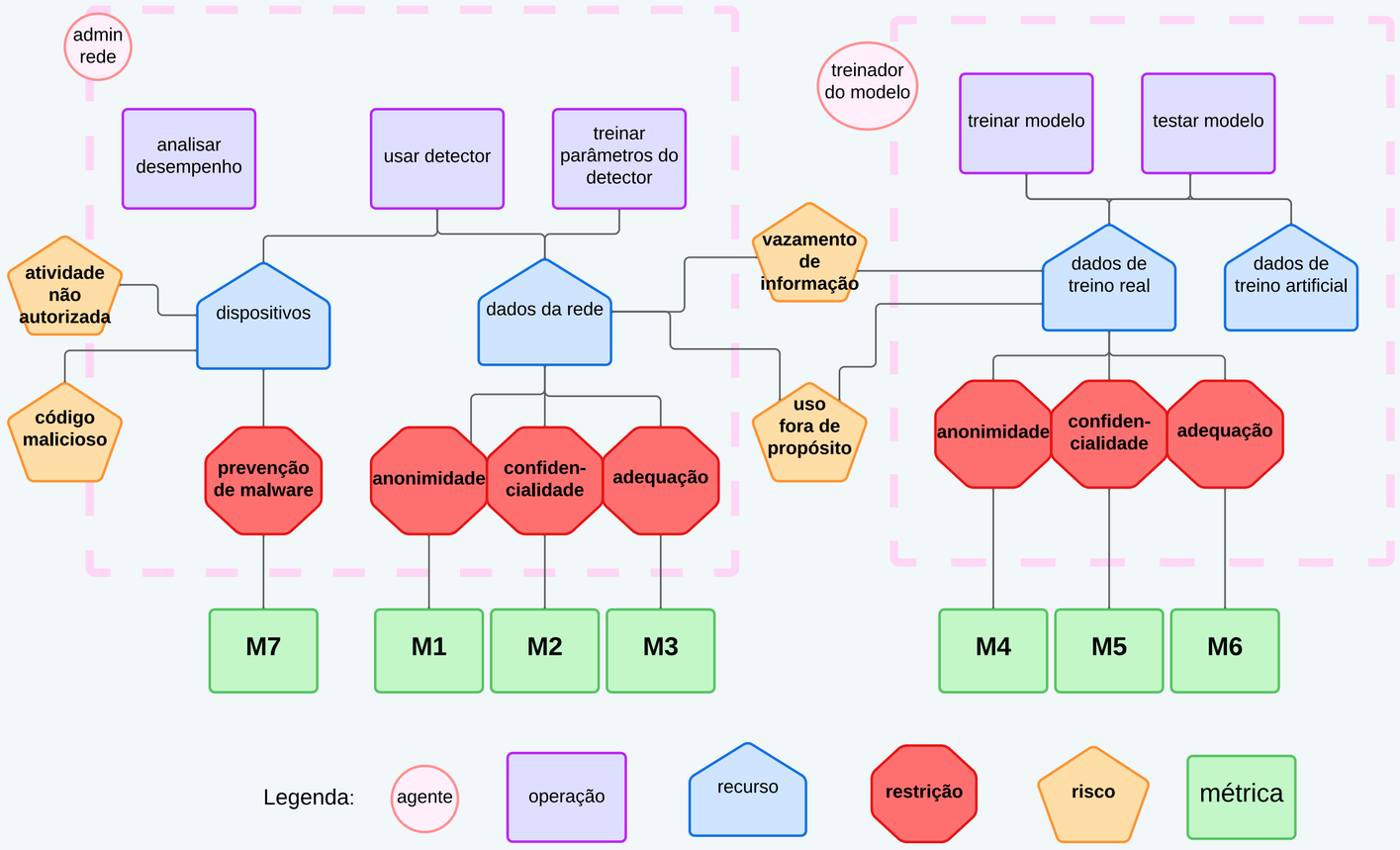
- Estudar e revisar trabalhos que:
  - tratem de privacidade em sistemas e suas legislações
  - discorrem sobre métricas de privacidade
  - propõem IDSs que melhorem a privacidade
- Analisar os riscos e restrições que um IDS tem que considerar para garantir a privacidade dos usuários da rede
- Propor uma métrica capaz de avaliar a privacidade de um IDS

Conceitos Básicos



PIA = *Privacy Impact Assessment* PET = *Privacy-Enhancing Technologies*

Rascunho da métrica



Resultados e Conclusões

- Revisão da literatura
- Modelagem de IDS baseado em aprendizado de máquina
- Planejamento de uma métrica utilizando a modelagem
- Disseminação dos resultados preliminares no Workshop de Graduação do Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais
- É necessário ainda mais estudo sobre os requisitos e restrições relacionados à privacidade

Autora: **Jessica Yumi Nakano Sato** (jyns1703@usp.br)

Orientador: **Daniel Macêdo Batista** (dbatista@ime.usp.br)

Departamento de Ciência da Computação – Universidade de São Paulo

CNPq