

Defesa de Qualificação de Tese: Francisco Rodrigo Parente da Ponte

Escrito por Marcus Vinícius

Qua, 17 de Agosto de 2022 00:00 - Última atualização Seg, 29 de Agosto de 2022 13:21



Título: FRAPE: A Framework for Risk Assessment, Prioritization and Explainability of Vulnerabilities

Data: 30/08/2022

Horário: 15h30

Local: Sala de seminários - Bloco 952

Resumo:

Práticas inadequadas de segurança, como o uso de métricas únicas, por exemplo, considerar

apenas o Sistema Comum de Pontuação de Vulnerabilidades -- Common Vulnerability Scoring System (CVSS) -- no processo de Gestão de Vulnerabilidades -- Vulnerability Management (VM) --, podem causar a superestimação do risco de exploração dos ativos. Idealmente, os analistas devem usar informações sobre a vulnerabilidade, inteligência de ameaças e contexto para avaliar a probabilidade e o risco de exploração de falhas de segurança. A falta de ferramentas especializadas torna essa tarefa complexa e passível de erros, pois os analistas precisam correlacionar manualmente as informações de diversas fontes de segurança com os milhares de ativos presentes na organização. Embora o Aprendizado de Máquina -- Machine Learning (ML) -- possa auxiliar nessa tarefa, sua aplicação na área de VM tem sido pouco explorada na literatura. Diante deste contexto, essa tese propõe o FRAPE, um framework de Gestão de Vulnerabilidades Baseada no Risco -- Risk-Based Vulnerability Management (RBVM) -- que utiliza uma técnica de rotulação de dados chamada de Aprendizado Ativo -- Active Learning (AL) -- em conjunto com a técnica de aprendizado supervisionado para criar um modelo de ML capaz de emular a experiência de especialistas de segurança na análise e avaliação do risco de exploração das vulnerabilidades. FRAPE é composto por 4 módulos que são: (i) Coleta de Dados, responsável por agregar as informações necessárias para a avaliação do risco; (ii) Classificação de Risco, onde será estipulado a probabilidade e o impacto da exploração das falhas de segurança; (iii) Priorização das Vulnerabilidades, onde as falhas com os maiores riscos para organização serão selecionadas; e por fim, (iv) Interpretação dos Resultados, onde oferecemos uma visão detalhada do porquê as vulnerabilidades foram selecionadas. Assim, este trabalho desenvolverá uma solução que consiga auxiliar os analistas de segurança a identificar as vulnerabilidades mais críticas da empresa e com isso, possam se defender de potenciais ataques de usuários mal-intencionados.

Banca examinadora:

- Prof. Dr. Emanuel Bezerra Rodrigues (MDCC/UFC - Orientador)
- Prof. Dr. César Lincoln Cavalcante Mattos (UFC)
- Prof. Dr. João Paulo Pordeus Gomes (UFC)
- Prof. Dr. Rafael Lopes Gomes (UECE)