Universidade de Pernambuco
Programa de Pós-Graduação em Engenharia da Computação (PPGEC)

Proposta de Tese de Doutorado

Área: Modelagem Computacional

Título: Quantificando o impacto de políticas de segurança no desempenho e na disponibilidade de serviços de computação em nuvem

Orientador: Gustavo Callou **(email:** gustavo.callou@ufrpe.br**)**
Co-orientador: Sergio Murilo **(email:** smurilo@ecomp.poli.br**)**

Descrição:

Em segurança cibernética, os sistemas de detecção de intrusão têm sido um componente crucial por vários anos. No entanto, devido à sua natureza reativa, respondendo apenas após a ocorrência de um ataque, a prevenção de um ataque pode não ser garantida. No mundo de hoje, onde as ameaças cibernéticas são persistentes e sofisticadas, os defensores precisam tomar medidas proativas para prevenir ataques. O *Moving Target Defense* (MTD) [1][2] representa uma estratégia de segurança que permite aos defensores se anteciparem e se prepararem para ataques potenciais, aumentando assim a segurança do sistema. Embora o MTD possa ser eficaz na melhoria da segurança de sistemas em nuvem, essa estratégia de segurança também tem algumas desvantagens. Por exemplo, para tornar a vida do invasor mais difícil, as estratégias de MTD impactam a disponibilidade e também o desempenho do sistema.

Em computação em nuvem, o termo disponibilidade se refere à acessibilidade e ao tempo de atividade de serviços e recursos, garantindo que aplicativos e dados permaneçam acessíveis apesar de falhas de hardware, bugs de software ou problemas de segurança, como ataques [3]. Já o desempenho está intimamente ligado à capacidade de aumentar ou diminuir recursos com base na demanda. Dado que tanto a disponibilidade como o desempenho são pilares fundamentais dos serviços de computação em nuvem, é essencial investigar o impacto das estratégias de MTD nesses requisitos críticos.

Este trabalho tem como objetivo a proposição de modelos para analisar a performabilidade de serviços hospedados em um ambiente de computação em nuvem (privada ou híbrida) sob a estratégia MTD. Por exemplo, modelos formais em redes de Petri estocásticas (SPN) poderão vir a serem propostos para dar suporte aos administradores de nuvem na definição de uma estratégia MTD baseada em métricas de desempenho (ex., tempo de resposta) e disponibilidade levando em consideração as VMs se movendo entre diferente hosts físicos. Vale destacar que estudo de casos serão realizados com medições em sistemas reais a fim de poder validar os modelos propostos. Posteriormente, com os modelos, serão porpostas melhorias da segurança de forma a se ter o impacto mínimo no desempenho e na disponibilidade do sistema em análise.

Referências Bibliográficas:

[1] J.-H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J. Moore, D. S. Kim, H. Lim, and F. F. Nelson, “Toward proactive, adaptive defense: A survey on moving target defense,” IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 709–745, 2020.

[2] E. Naderi, A. Asrari and B. Ramos, "Moving Target Defense Strategy to Protect a PV/Wind Lab-Scale Microgrid Against False Data Injection Cyberattacks: Experimental Validation," *2023 IEEE Power & Energy Society General Meeting (PESGM)*, Orlando, FL, USA, 2023

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” Commun. ACM, vol. 53, no. 4, p. 50–58, apr 2010.