Attacks on Cloud Autoscaling Mechanisms
In the era of cloud-native computing, Kubernetes has emerged as a leading container orchestration platform, enabling seamless scalability and reliability for modern applications.

However, with its widespread adoption comes a new frontier in cybersecurity challenges, particularly low and slow attacks that exploit autoscaling features to disrupt services subtly yet effectively.

This project aims to delve into the intricacies of these attacks, examining their impact on Kubernetes' Horizontal Pod Autoscaler (HPA) and Vertical Pod Autoscaler (VPA), and proposing mitigation strategies for more resilient systems.

**Responsibilities:**

- Conduct a thorough literature review to identify existing knowledge gaps and research on similar attacks.
- Develop methodologies to simulate low and slow attack scenarios on Kubernetes clusters with varying configurations of autoscaling mechanisms.
- Analyze the impact of these attacks on resource utilization, service availability, and overall system performance.
- Evaluate current defense mechanisms and propose novel strategies to enhance the resilience of Kubernetes' autoscaling features.
- Implement and test selected mitigation approaches in a controlled environment.
- Document findings, present a comparative analysis of effectiveness, and discuss implications for future development in cloud security practices.

**Requirements:**

- A strong background in computer engineering, computer science or a related field.
- Familiarity with Kubernetes architecture and container orchestration concepts.
- Experience in deploying and managing applications on Kubernetes clusters.
- Proficiency in at least one scripting/programming language (e.g., Python, Go).
- Understanding of cloud computing and cybersecurity fundamentals.

**Nice to Have:**

- Prior research or hands-on experience in cloud security, particularly in the context of Kubernetes.
- Knowledge of network protocols and low-level system interactions.
- Experience with DevOps tools and practices.

**Contact**

**Email:** navid.asasdi@tum.de

**Advisors**

Navidreza Asadi