Can we cross the line? Security Analysis of a multi-tenant SaaS cluster hosted in Kubernetes

Jonas Bührle
Advised by Dr. Mohammad Noureddine

SaaS

Software as a Service is:

- Subscription based
- Web-based
- On-demand

Multiple tenants share infrastructure which introduces isolation challenges.

Problem

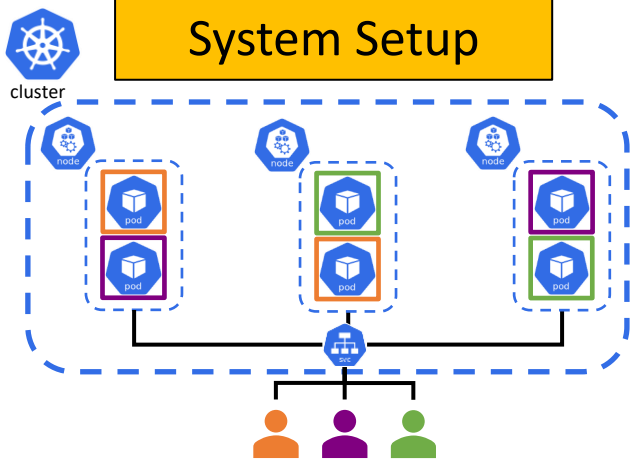
Cross tenant vulnerabilities in a SaaS cluster can result in:

- Data breaches
- Resource abuse
- Denial of service

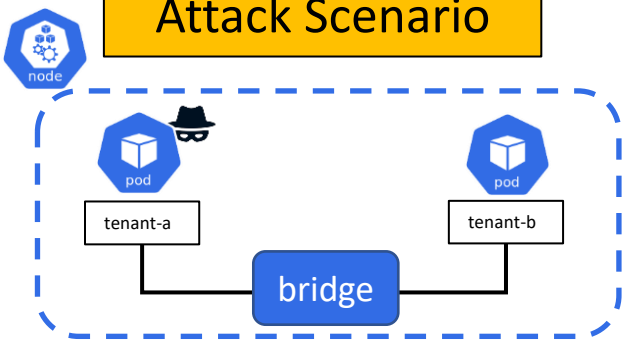
Therefore our hypothesis:

"Measuring the blast radius of a malicious tenant can lead to improved analysis of configuration files to harden multi-tenant K8 clusters."

System Setup



Attack Scenario



Methodology

- Perform attacks and analyze impact
- Write policies/recommendations based on the analysis

Results

Name	Stage	Success
Reconnaissance	Discovery	✓
ARP cache poisoning	Lateral Movement	✗
DoS Attack	Impact	⧗

Conclusion

- Multi-tenancy introduces new security challenges
- A malicious tenant can break out of its isolation and impact other tenants
- Analyzed the blast radius of a malicious container

Acknowledgements

This work was done in collaboration with Profect. PROFECT.