Secure Systems Group, Aalto University

Dat Doan, Jose Luis Martin Navarro, Tuomas Aura

Kubernetes Cluster Hardening

1. Problem

- Uncertainty about securing cluster due to Kubernetes' complexity and default configurations
- Lack of a comprehensive hardening strategy for Kubernetes clusters

2. Propose Approach

- Matrix for Kubernetes Hardening, based on Shift Left Security and Defence In Depth Principles
- Best practices from NSA, CISA, and CIS benchmarks
- Multi-layered security (Cluster, Workload, Resource, Container)
- Stage-specific actions (Development, Deployment, Runtime).

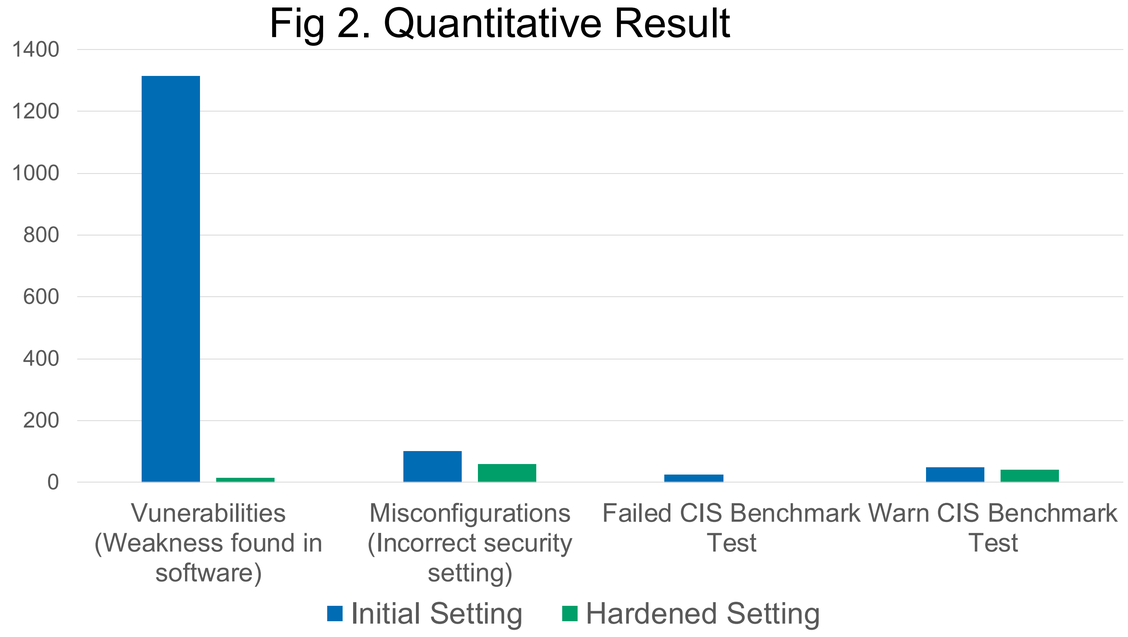
	Deployment Stage	Deployment Stage	Runtime Stage
Cluster Layer	Role-based Access Control Authentication And Authorization Secrets Management Namespace Boundaries Namespace Resource Quotas	Dynamic Admission Control	Monitoring, Alerting And Auditing
Workload Layer	Static Analysis of YAML file and configuration Network Policies LimitRanger Resource Management for Pods	Pod Security Admission Pod Security Standards	Pod Security Admission Pod Security Standards Honeypot Workload Monitoring, Alerting And Auditing
Resources Layer	CIS Benchmarks		CIS Benchmarks
Container Layer	Build Secure Image Image Scanning in build phase LimitRanger	Image Scanning in deployment phase	Image Scanning at the runtime stage Container Threat Analysis

Fig 1. Kubernetes Security Matrix

3. Case Study

- Implementation the proposed approach on an Anonymous Registration Anonymous Access Protocol application
- Environmental setup on Aalto VM
- Validate the feasibility and measure effectiveness

Fig 2. Quantitative Result



4. Evaluation and Takeaways

- Effectiveness on detecting and fixing and vulnerabilities, misconfigurations
- Each layer introduces interdependent challenges and deep expertise
- Balancing trade-off for security vs functionality (e.g., runAsNonRoot breaks apps)
- Future focus: cgroup and runtime hardening

Aalto University

Contact: tuan.doan@aalto.fi, jose.martinnavarro@aalto.fi

References:

[1] CIS Kubernetes Benchmark. Sept. 23, 2024, p. 328

[2] Kubernetes Hardening Guide. Cybersecurity Technical Report U/OO/168286-21. National Security Agency (NSA), Cybersecurity, and Infrastructure Security Agency (CISA), Aug. 2022, p. 59