Secure Systems Group, Aalto University
Jacopo Bufalino, Jose Luis Martin-Navarro, Mario Di Francesco, Tuomas Aura

Network misconfiguration abuse in Kubernetes

Security of microservice applications remains an issue, with security incidents occurring regularly. Securing the internal Kubernetes cluster network is a challenge due to the complexity of configuring resources across virtual network layers and mismatches between Kubernetes resource declarations and their runtime behavior. These issues have been mostly overlooked by both industry and academia.

ID	Description	Vulnerability	Attack	Scope	Analysis
M1	Port open on container is not declared	Listening on all interfaces by default	Command and control Sensitive port information	App	Runtime
M2	Container allocates dynamic ports	Dynamic ports cannot be controlled	Loosened security policies	App	Runtime
M3	Port declared on container is not open	Missing checks on declared ports	Data interception Data spoofing Data exfiltration	App	Runtime
M4A **M4B** **M4C**	Compute unit collision Service label collision Compute unit subset collision	Missing checks on label collision	Men in the middle Server impersonation	App Cluster*	Static
M5A **M5B** **M5C** **M5D**	Service targets unopened port Service targets undeclared port Headless service port is not available Service without target	Missing checks on declared ports Missing checks on target label	Data interception Data spoofing Denial of service Bypassing security checks	App	Runtime Static
M6	Lack of network policies	No isolation between containers	Data interception Data spoofing Privilege escalation	App	Static
M7	Container binds to host network	Network policies do not apply to host	Bypassing network controls	App	Static

Table 1: Classification of network-layer misconfigurations, along with the corresponding vulnerabilities, attacks, and properties.

Contribution

- We performed a systematic review [1] of academic and grey literature on Kubernetes network security and related tools from the last five years. The inclusion/exclusion criteria filtered works with insufficient dept or those focused on platforms different than Kubernetes.
- We compared existing knowledge and best practices with the actual capabilities of the Kubernetes network stack and application configuration.
- Table 1 shows the mismatches with security relevance. **M1-M7** are application misconfigurations and **M4*** cluster-wide. The majority are not detected by the state-of-the-art security tools (Table 2).
- We analyzed 280 real-world Kubernetes applications from six different organizations, revealing over 650 instances of misconfigurations (Table 3).

Dataset	Affected	Patched	M1	M2	M3	M4	M5	M6	M7
Banzai Cloud	51	0	13	2	17	12	2	51	0
Bitnami	158	22	106	26	40	40	19	156	7
EEA	8	3	7	0	1	1	0	0	0
Wikimedia	10	8	10	3	2	4	3	2	0
CNCF	7	1	10	0	4	0	6	7	0
Prometheus	25	0	42	4	3	0	5	25	4
Total	259	34	188	35	67	57	35	241	11

Table 2: Breakdown of misconfigurations by dataset. EEA stands for the European Energy Agency.

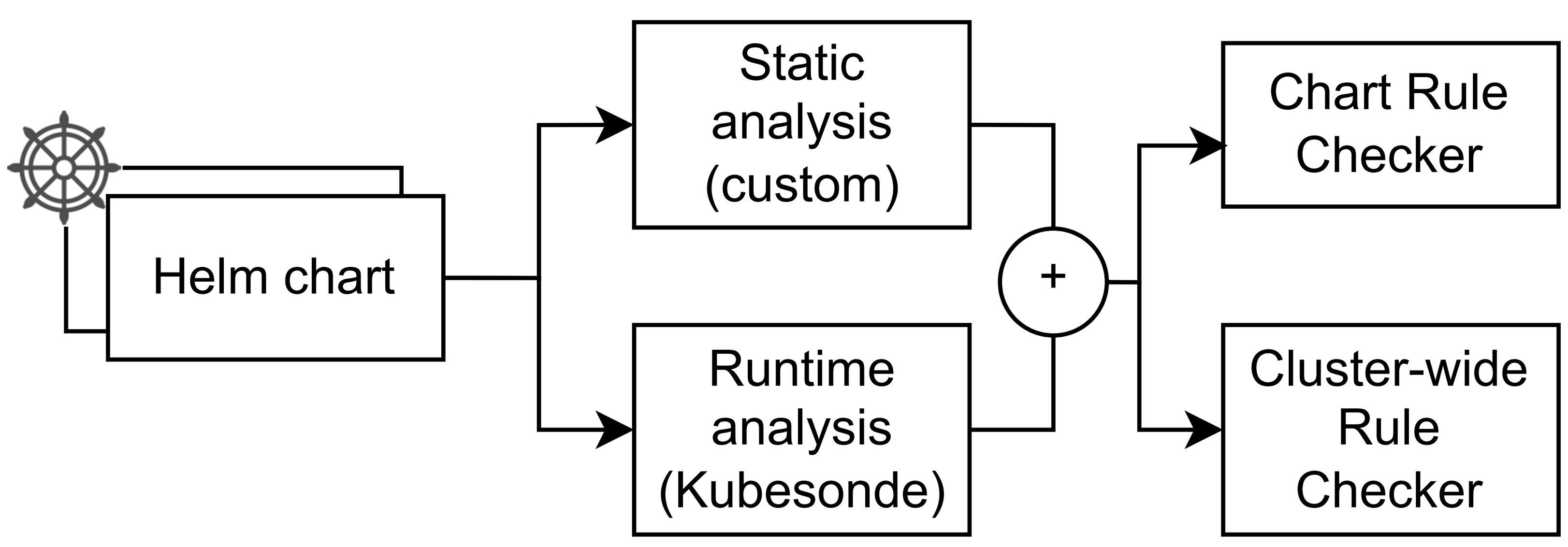

Figure 1: Evaluation flow of charts in each dataset.

Tool	Type	M1-2	M3	M4	M4*	M5A	M5B-C	M5D	M6	M7
Kubesec	Static	—	—	×	—	—	×	×	×	●
Checkov	Static	—	—	×	—	—	×	×	●	●
Kubeaudit	Static	—	—	×	—	—	×	×	●	●
KubeLinter	Static	—	—	×	—	—	×	●	×	●
Kube-score	Static	—	—	×	—	—	×	●	●	×
SLI-KUBE	Static	—	—	×	—	—	×	×	×	●
Kube-hunter	Runtime	×	×	×	—	×	×	×	◐	◐
Kube-bench	Runtime	×	×	×	—	×	×	×	×	●
Kubescape	Hybrid	×	×	◐	×	×	×	×	●	●
Trivy	Hybrid	×	×	×	×	×	×	×	×	●
StackRox	Platform	×	×	×	×	×	×	×	×	●
Neuvector	Platform	×	×	×	×	×	×	×	×	●
This work	Hybrid	●	◐	●	●	●	●	●	●	●

Table 3: Misconfigurations detected by the considered tools and our solution. The symbols indicate whether misconfigurations were ● found, ◐ partially found, × missed, or — not applicable.

[1] Barbara Kitchenham, O. Pearl Brereton, David Budgen, Mark Turner, John Bailey, and Stephen Linkman. Systematic literature reviews in software engineering – A systematic literature review. *Information and Software Technology*, 51(1):7–15, January 2009.

Aalto University
School of Science

Contact: jacopo.bufalino@aalto.fi, jose.martinnavarro@aalto.fi, mario.di.francesco@aalto.fi, tuomas.aura@aalto.fi