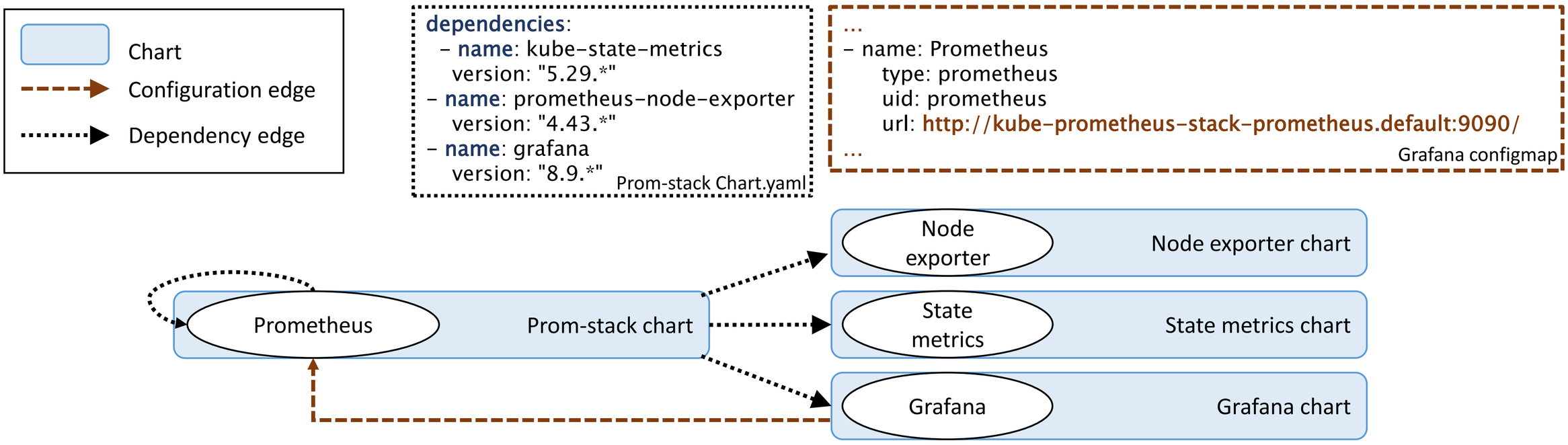
Secure Systems Group, Aalto University

Jacopo Bufalino, Jose Luis Martin-Navarro, Aleksi Peltonen, Tuomas Aura

Helm-ET: Reducing Exposure to Lateral Movement in Kubernetes Artifacts

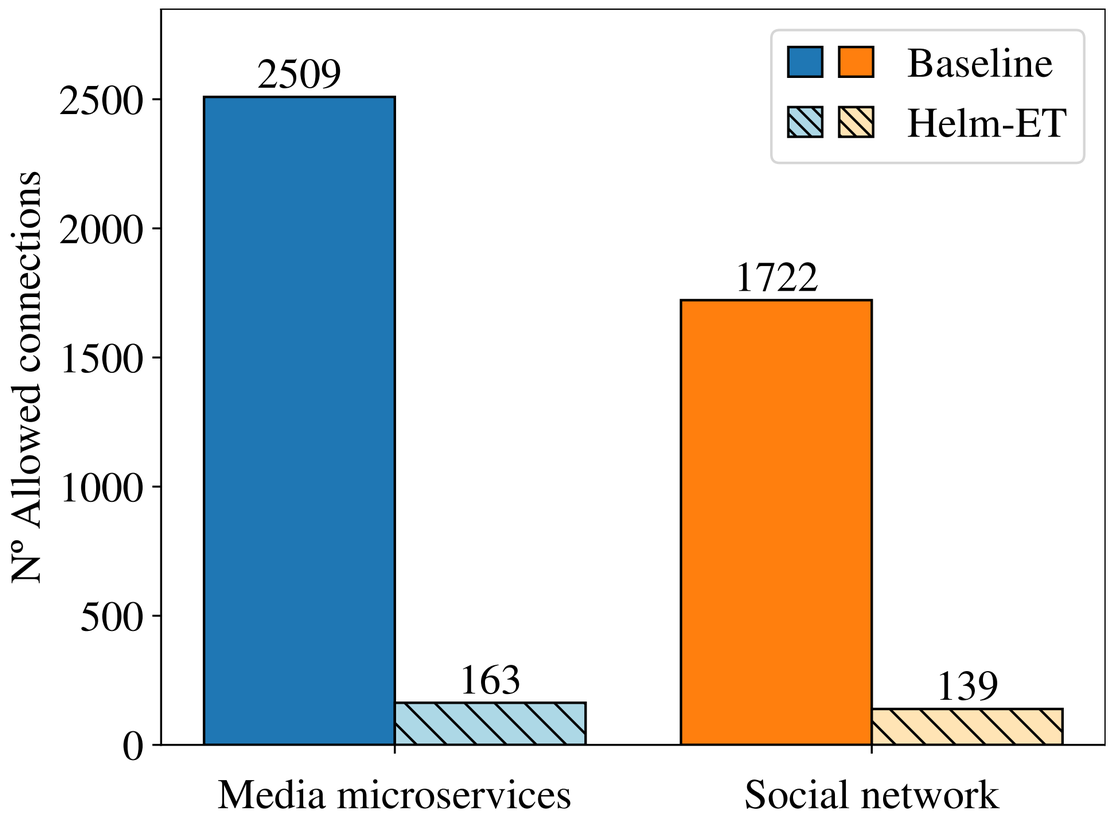
Problem

By default, Kubernetes allows connections between all microservices in the cluster, which can be abused by a compromised container to infect other services in the cluster, also called lateral movement.
Network policies restrict connections between microservices, but creating them is a complex and error prone manual process. Automatic tools require access to the source code or running the application with test traffic. The problem is more challenging with public available applications, because 90% of them lack network policies, lack test traffic and source code, and operators do not know the application details.



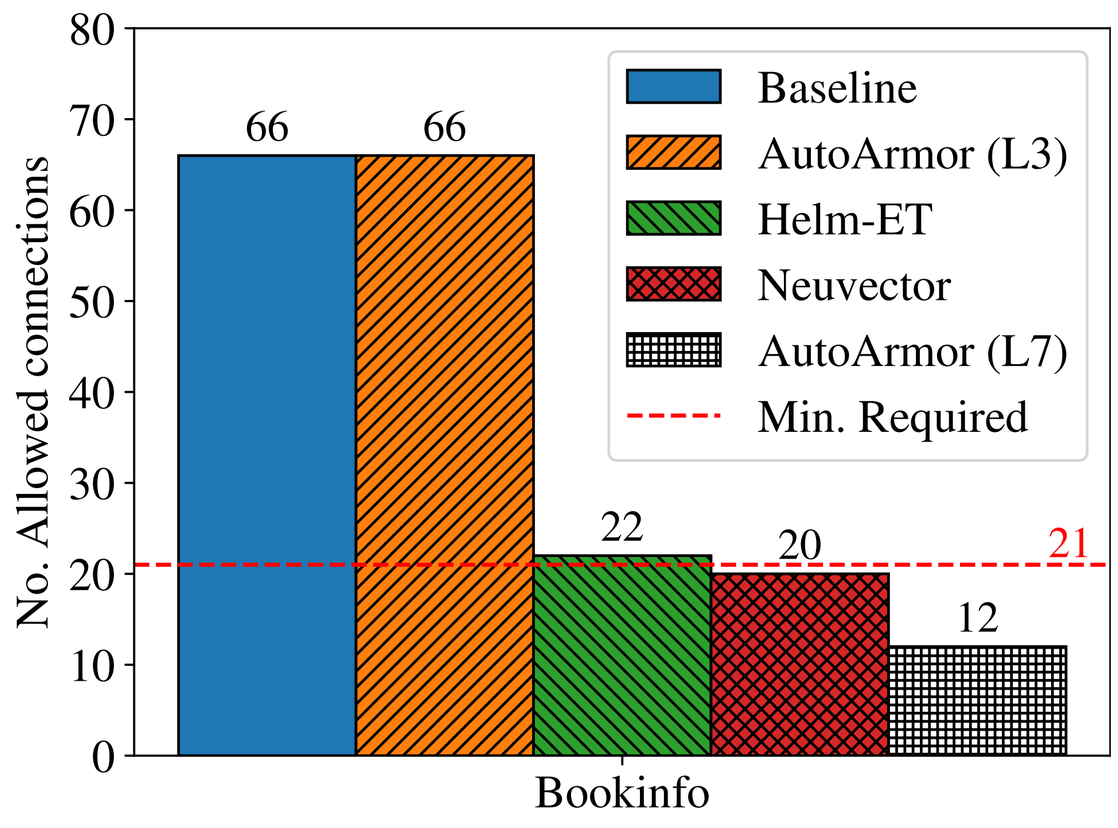
Solution

Helm-ET [1], an open-source static analysis tool designed to block unnecessary connections while allowing legitimate traffic. It automatically generates network policies based on the application's dependency hierarchy and configuration settings. It also provides high level configuration for cloud operators to define desired connectivity.



Evaluation & Results

Combined dataset of 451 cloud applications, with a reduction of 92.71% of connections in the cluster.
Comparable results to state-of-the-art tools, but with better performance (less than 100ms vs 79 seconds), and does not need traffic or source code, which makes Helm-ET less prone to blocking legitimate connections (e.g., Bookinfo).



[1] J. Bufalino, J. L. Martin-Navarro, A. Peltonen, and T. Aura, "Helm-et: Reducing exposure to lateral movement in kubernetes artifacts," in *IEEE 18th International Conference on Cloud Computing (CLOUD)*, 2025.

Aalto University
School of Science

Contact: jacopo.bufalino@aalto.fi, jose.martinnavarro@aalto.fi