Secure Systems Group, Aalto University

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

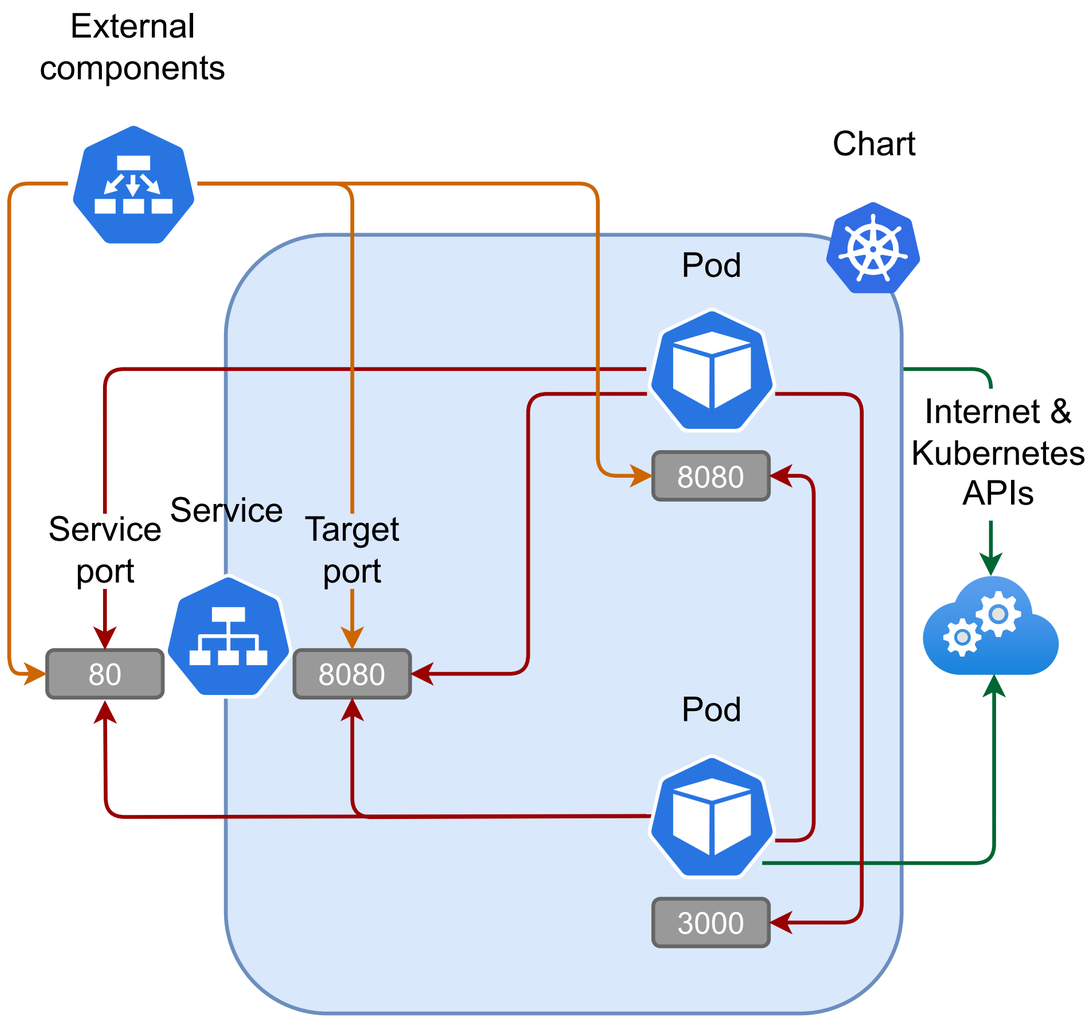
Helm-ET: Reducing Exposure to Lateral Movement in Kubernetes Artifacts

Problem

- Cloud applications are collections of containerized microservices orchestrated with tools like Kubernetes.
- The installation and configuration of these applications is simplified with package managers such as Helm.
- Publicly available applications often lack basic security measures such as network policies, which are crucial to block unintended and potentially harmful access between microservices and larger application components.
- Network access control rules are needed to decrease the lateral movement reach of an attacker, but creating them is a complex task that requires an error-prone manual inspection of the cloud applications.

Solution

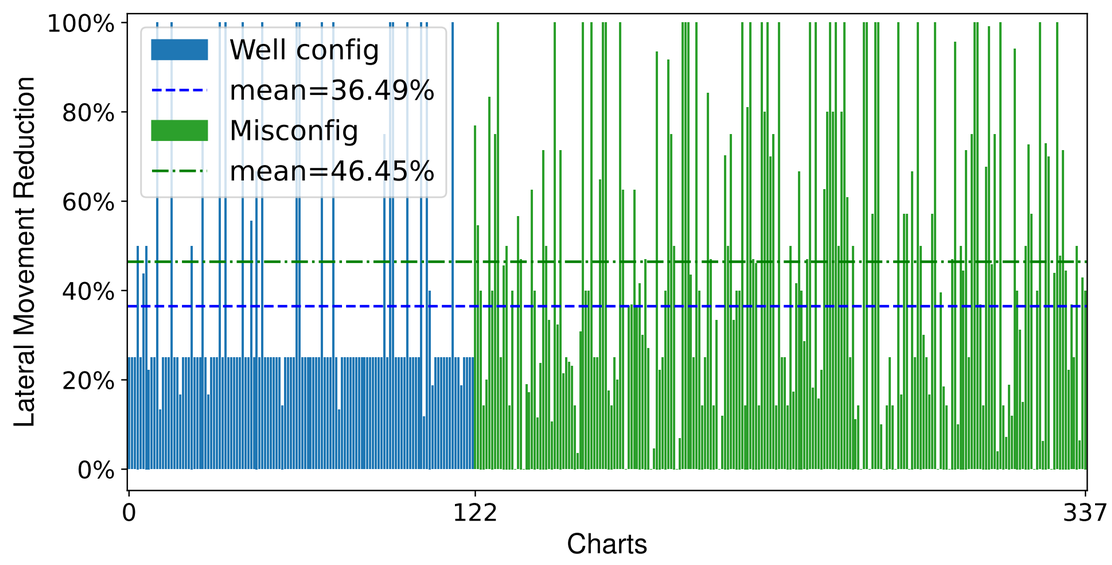
A novel approach for network boundary enforcement on unfamiliar applications is presented. The methodology allows the automatic creation of network policies based on the application description. It is based on a best-effort approach, blocking unnecessary connections without interrupting legitimate traffic.
We implemented Helm-ET, an open-source tool to automate the described process on Helm Charts.

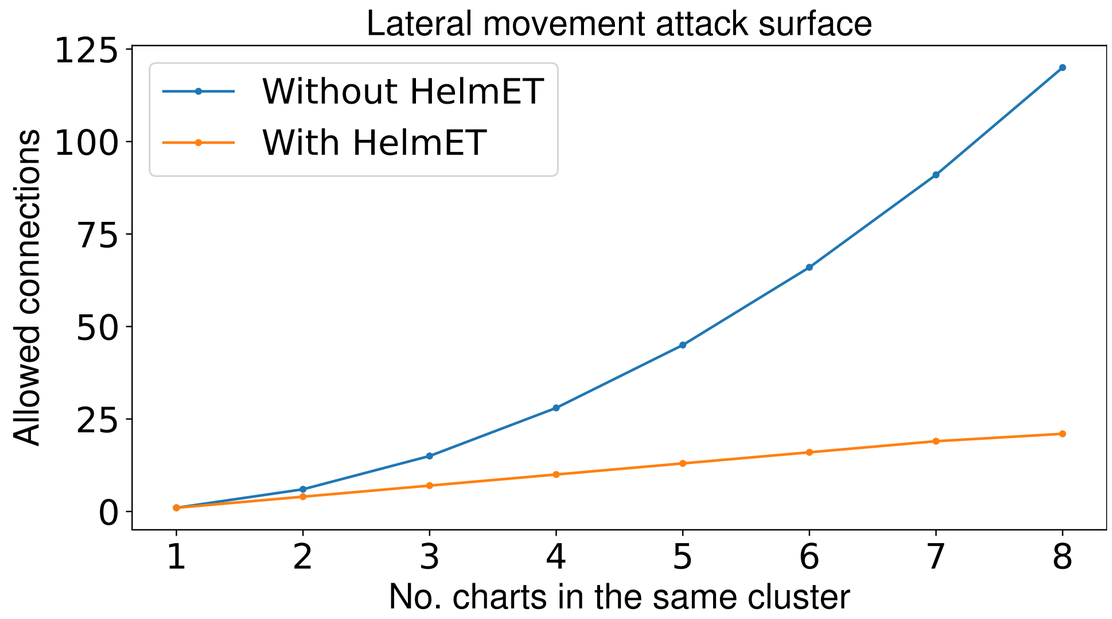


The figure illustrates the existing connections on a chart after applying Helm-ET. Outbound connections are shown in green, orange describes the inbound connections, and the red arrows show the connections within the chart components.

Evaluation

We evaluate our approach by analyzing 337 publicly available Helm charts lacking network policies. The results show that Helm-ET can significantly reduce the opportunities for attacker lateral movement in most cloud applications, achieving an average of 42.85% on the total amount of connections. On average, the tool shows an increased reduction in misconfigured charts, although it is still effective on well-declared applications.





The effectivity of the methodology increases with the number of applications installed in the same cluster.

Aalto University
School of Science

Contact: jacopo.bufalino@aalto.fi, jose.martinnavarro@aalto.fi, aleksi.peltonen@aalto.fi, tuomas.aura@aalto.fi