IEEE COMPUTER SOCIETY

XI Commandments of Kubernetes Security: A systemization of Knowledge Related to Kubernetes Security Practices

Md Shazibul Islam Shamim, Farzana Ahamed Bhuiyan, Akond Rahman
Tennessee Technological University

Tennessee TECH

CERIAS Cybersecurity Education, Research and Outreach Center

#IEEESecDev https://secdev.ieee.org/2020

What is Kubernetes 

- An open-source software for automating management of containerized services.
- Initially developed by  in 2014
- Maintained by  since 2015

CLOUD NATIVE
COMPUTING FOUNDATION

Tennessee
TECH

Kubernetes usage


- 

reduced release time to 1 week from 3-8 months.

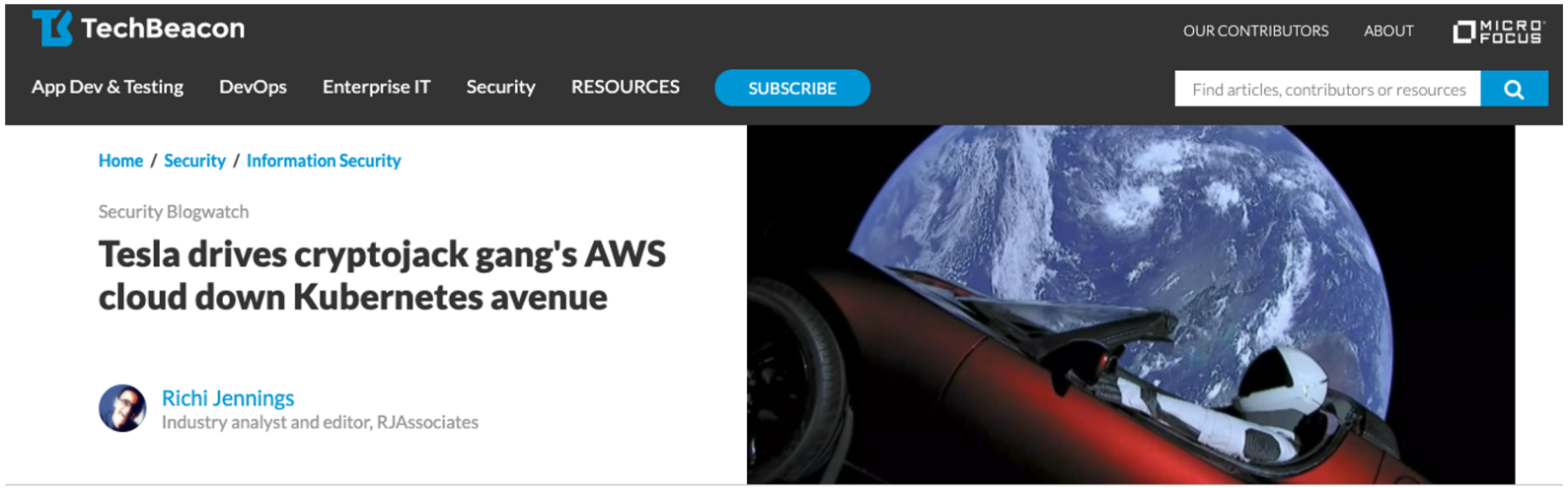
- 

improved release frequency 3~4 times a day from 4-6 weeks

Tennessee TECH

Why Kubernetes Security?

- According to 2019 CNCF survey, 40% among 1337 participants are concerned about security.



Tennessee TECH

Research objective

The goal of this paper is to help practitioners in securing their Kubernetes installations through a systematization of knowledge related to Kubernetes security practices.

Tennessee TECH

Our Research Question

What Kubernetes security practices are reported by practitioners?

Tennessee TECH

Our Contribution

1. A synthesized list of 11 security practices for Kubernetes security.
2. A curated dataset of 104 internet artifacts with a mapping between Internet artifact and the identified security practices.

I. Authentication and Authorization (82)

- The practice of applying authentication and authorization rules to prevent malicious users from getting access and performing unauthorized activities inside the Kubernetes cluster.
  - Disable all default configurations
  - Enable Role Based Access Control (RBAC)
  - Controlled use of impersonation feature
- Failure to follow the practice can allow malicious users to get access to Kubernetes API server. For example: Kubernetes default configuration allows anonymous access to Kubernetes server.

Tennessee TECH

II. Implementing Kubernetes-specific Security Policies (81)

- The practice of applying policies to secure Kubernetes components, pods and network of Kubernetes clusters to prevent security breaches
  - Network-specific policies
  - Pod-specific security policies
  - Generic policies
- If not implement can make entire Kubernetes cluster vulnerable.
  For example: If security context for a pod is not defined then a container can run as root user with write permission.

Tennessee TECH

III. Vulnerability Scanning (63)

- The practice of scanning Kubernetes components and continuous delivery (CD) components for vulnerabilities.
  - Check vulnerability of code and scan images.
  - Pull images from private registry.
- In 2017 researchers found docker images embedded with malicious malware.

Tennessee TECH

IV. Logging (47)

- The practice of enabling and monitoring logs for the Kubernetes cluster.
  - Logs must be monitored at a regular interval.
  - Alerts must be set up for any drastic change.
- Without logging root cause analysis for attack from malicious users or troubleshooting for any unexpected consequences will not be possible.

Tennessee TECH

V. Namespace separation (36)

- The practice of separating namespaces so that the resources of one namespace are not shared with another.
  - Create separate namespace for separate team in a company.
  - Avoid default namespace.
- Any malicious user can attack default namespace to gain control to all the resources in the default namespacce.

Tennessee TECH

VI. Encrypt and restrict access to etcd (34)

- The practice of encrypting and restricting access to ‘etcd’ server.
  - Make etcd only available from API server and isolate behind a firewall to restrict access from outsiders.
  - By default, Kubernetes stores secret data as plaintext in etcd. Use secret management tool such as vault for additional security.
- A malicious user can take over entire Kubernetes cluster if the malicious user gets access to etcd server.

Tennessee TECH

VII. Continuous Update (28)

- The practice of applying security patches to keep Kubernetes cluster updated with latest security fixes.
- For example- two vulnerabilities CVE-2019-16276, and CVE-2019-11253 discovered in October 2019 were susceptible to denial of Service attack.

Tennessee TECH

VIII. Limit CPU and memory quota (18)

- The practice of limiting CPU and memory to a pod or namespace so that malicious attacks can be mitigated.
  - Assign CPU and memory quota to a pod or a namespace.
  - Limit maximum number of instances of a container.
- A malicious user can successfully initiate denial of service attack if this practice is violated.

Tennessee TECH

IX. Enable SSL/TLS support (18)

- The practice of enabling secure sockets layer (SSL) or transport layer security (TLS) protocol to ensure secure and encrypted communication between Kubernetes components.
  - Enable TLS and SSL certificates for all Kubernetes components.
- Without SSL/TLS support, the communication between the components can be susceptible to man in the middle attack.

Tennessee TECH

X. Separate sensitive workload(18)

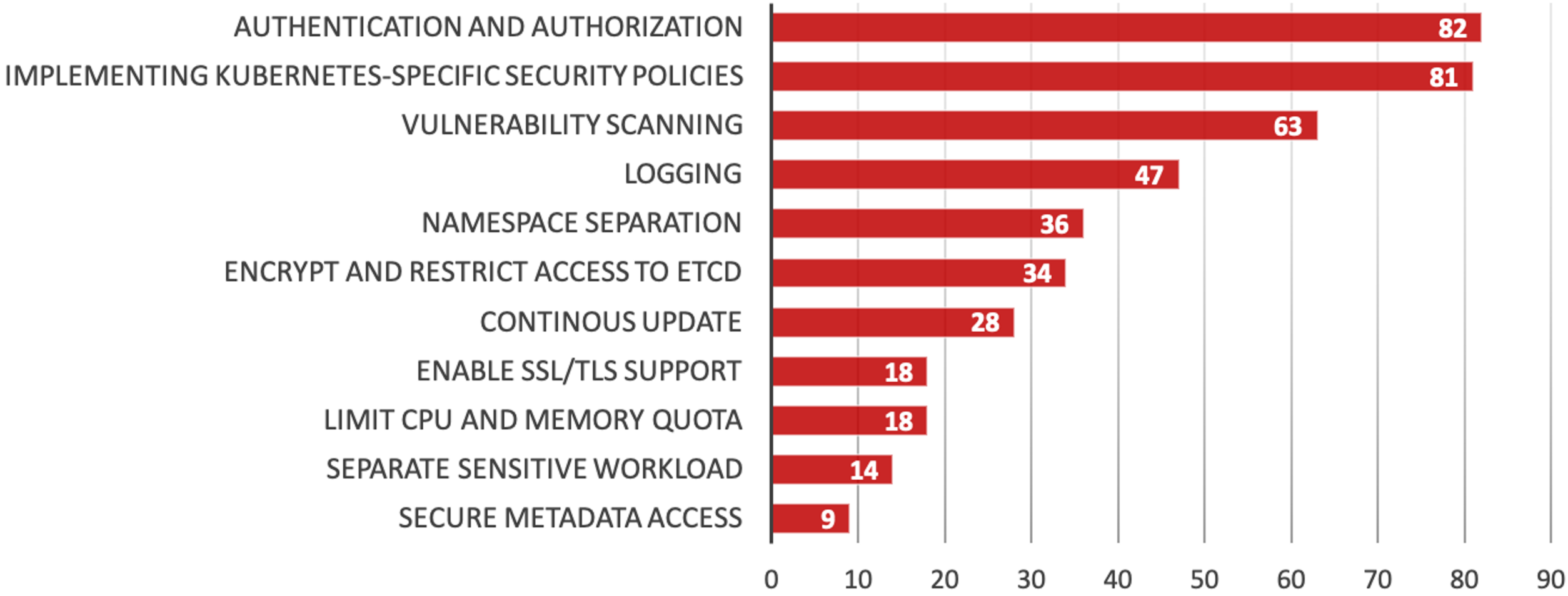
- The practice of running sensitive applications on a dedicated set of machines to limit the potential impact of a security breach.
  - Run sensitive applications on a dedicated set of machines to limit potential impact of a security breach.
  - Use Kubernetes namespaces, taints, tolerations to control where a pod might be deployed.
- For example, if a malicious user get access kubelet credential then he may get access to sensitive applications such as organization databases.

Tennessee TECH

XI. Secure metadata access(9)

- The practice of securing sensitive metadata of the Kubernetes cluster to avoid privilege escalation.
  - Use metadata concealment feature from Cloud providers such as ‘Workload Identity’ for Google Kubernetes Engine(GKE)
- In 2018, shopify bug bounty program disclosed how a user was able to escalate privileges to leak metadata of cloud provider.

Empirical Findings



Tennessee TECH

Implications

1. Practitioners can understand the components where security practices are applicable.

2. Practitioners who use Kubernetes can use our identified practices as a benchmark.

3. Our work can serve as the groundwork for future research in Kubernetes security such as how these security practices are used in practice.

4. Researchers can find possible mitigation strategies to inspect insecure practices in Kubernetes.

Tennessee TECH

Summary

Our Research Question

What Kubernetes security practices are reported by practitioners?

Our Contribution

1. A synthesized list of 11 security practices for Kubernetes security.
2. A curated dataset of 104 internet artifacts with a mapping between Internet artifact and the identified security practices.

Implications

1. Practitioners can understand the components where security practices are applicable.
2. Practitioners who use Kubernetes can use our identified practices as a benchmark.
3. Our work can serve as the groundwork for future research in Kubernetes security such as how these security practices are used in practice.
4. Researchers can find possible mitigation strategies to inspect insecure practices in Kubernetes.

Thank you!

Md. Shazibul Islam Shamim
PhD student, Tennessee Tech University
Email: mshamim42@tntech.edu
Website: https://shazibulislam.github.io