

Security Attacks in Kubernetes Cluster due to Security Best Practices Violation



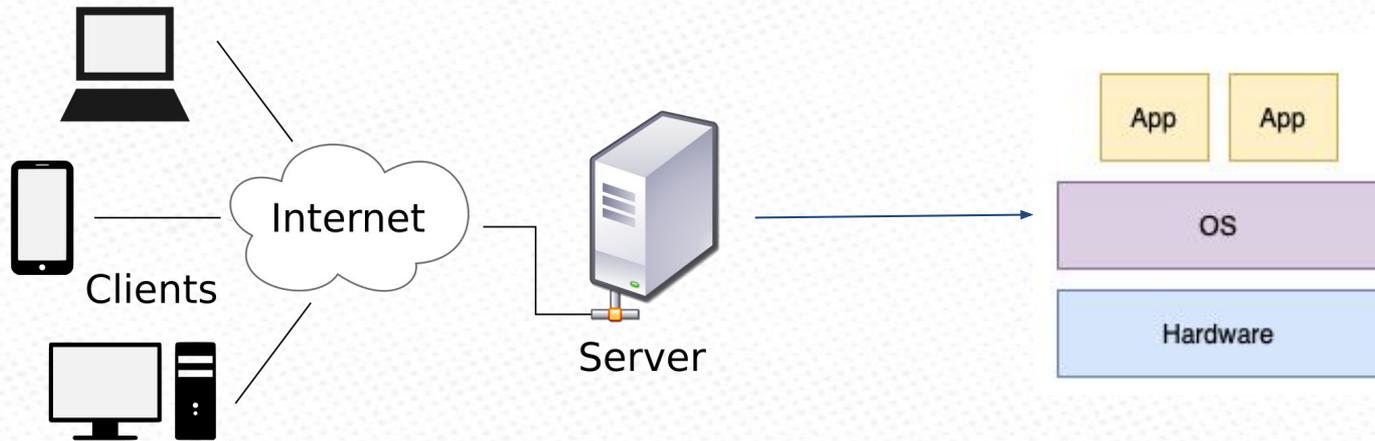
Shazibul Islam Shamim

PhD Student, Tennessee Tech University

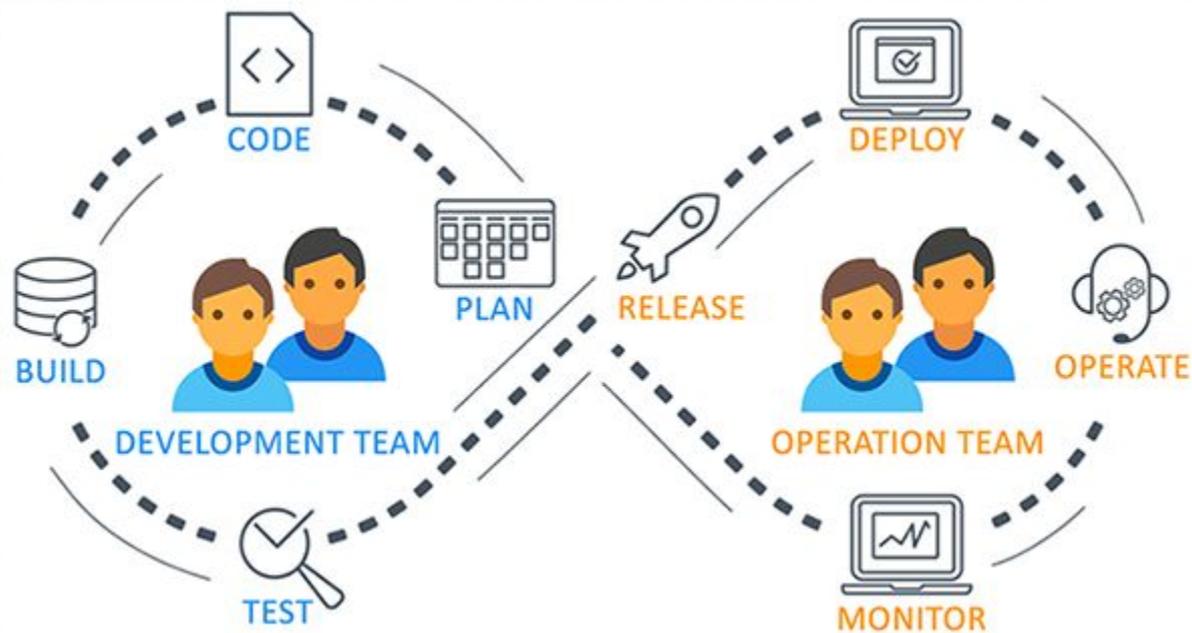
Advisor: Dr. Akond Rahman



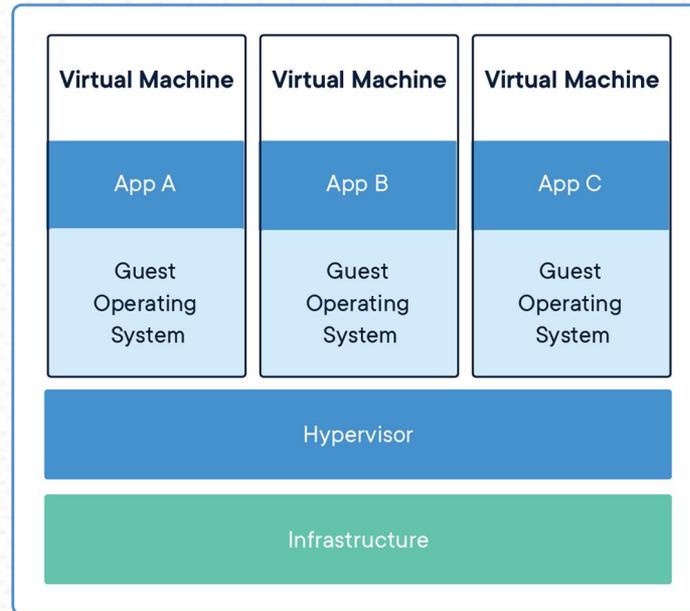
Overview of application Infrastructure



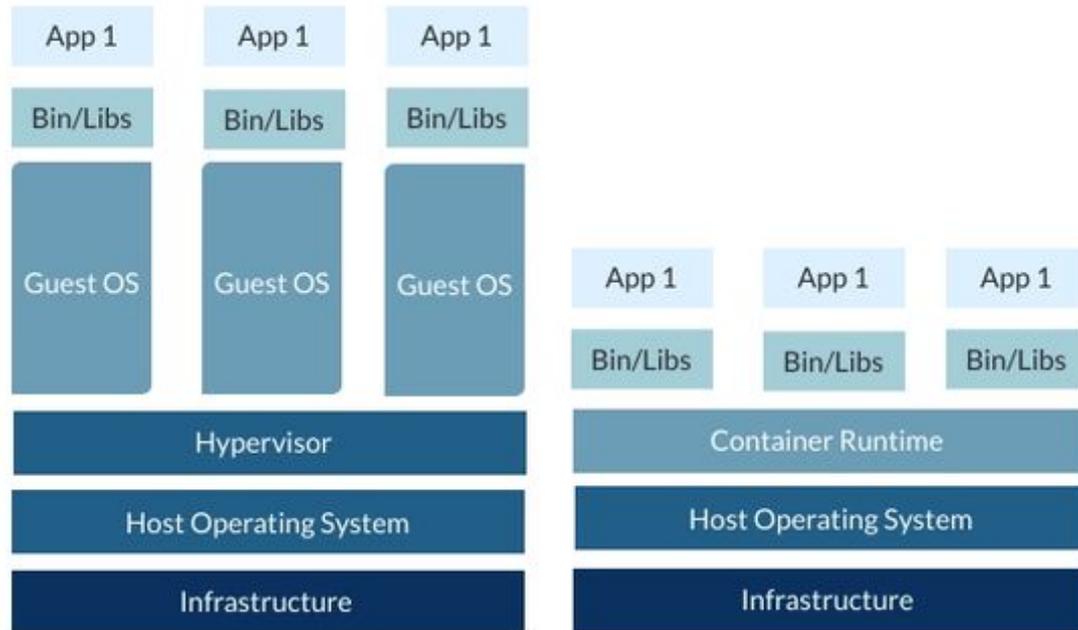
Development and Operations



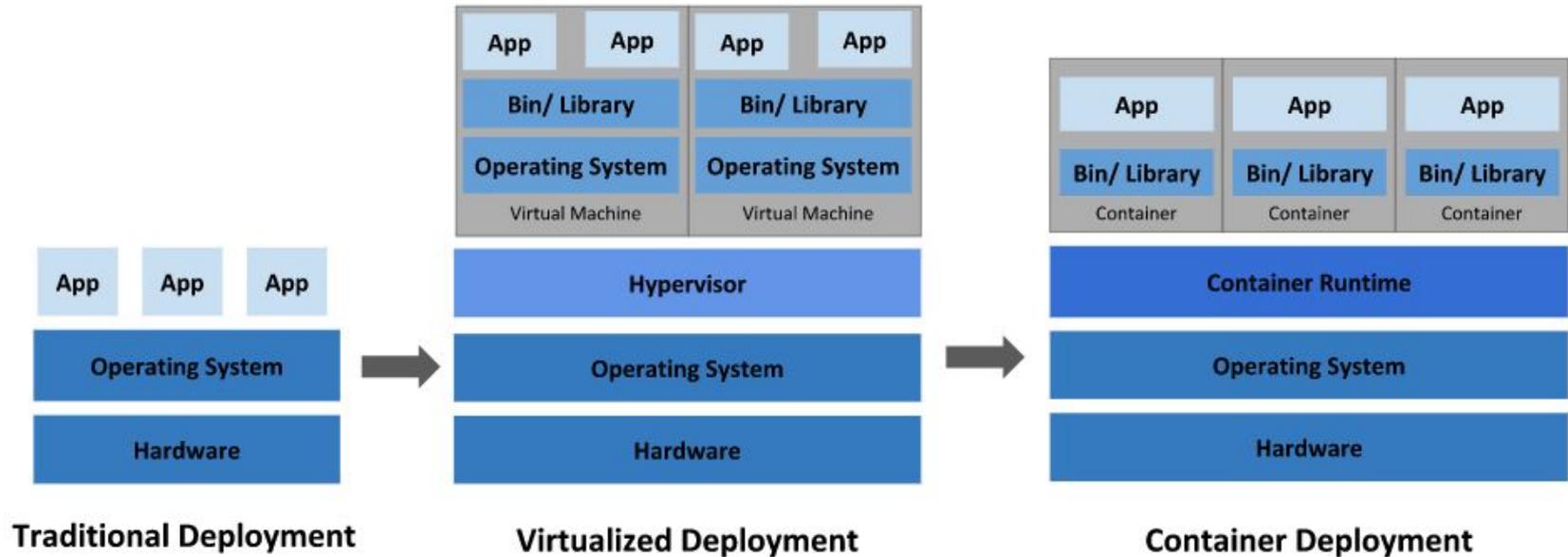
Virtualized Deployment



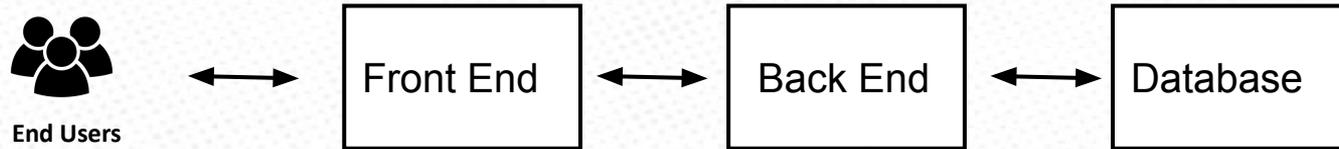
Containerized Deployment



Evolution of Application Deployment



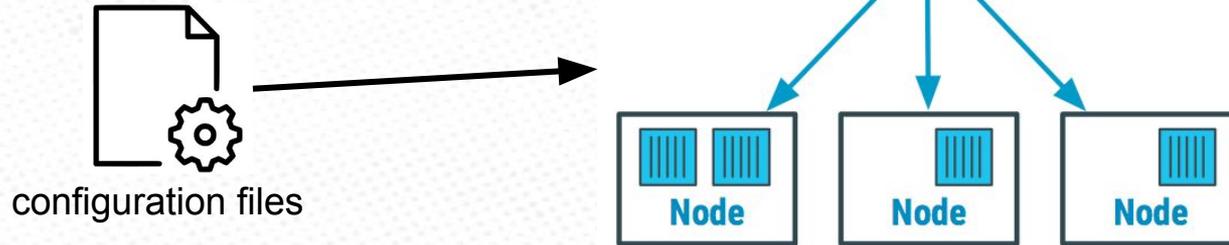
Why Container Orchestration?



- Real world applications use hundreds of services
- Need to manually define IP configurations, load balancer, storage
- Need to manually define number of instances, what happens a new service comes?
- Configuration management
- How to troubleshoot the containers?



Why Container Orchestration?



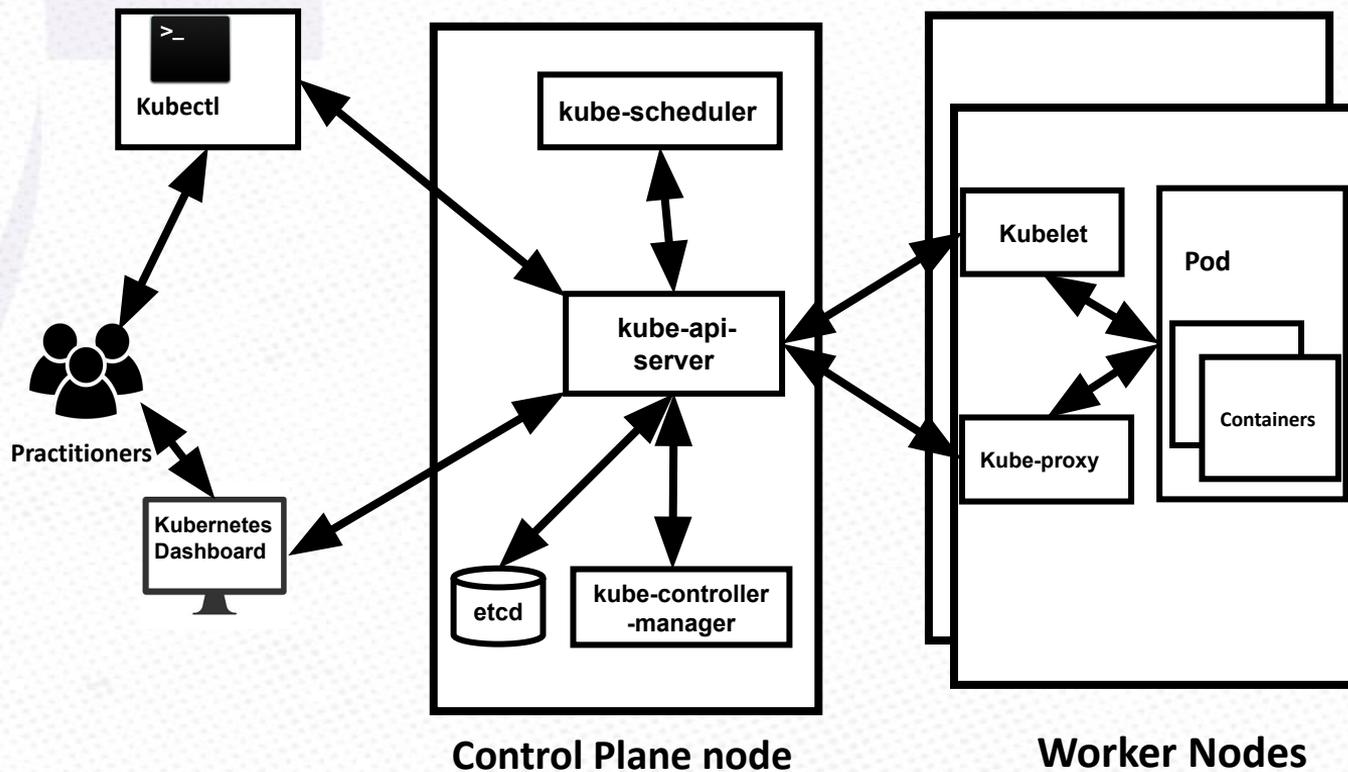
What is Kubernetes

- An open-source software for automating deployment, scaling and management of containerized applications.
- Initially developed by  in 2014
- Maintained by  since 2015

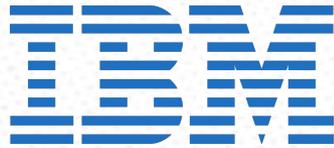
CLOUD NATIVE
COMPUTING FOUNDATION



Kubernetes Architecture



Kubernetes Usage and Benefits



-  The United States Department of Defense reduced their release time from 3~8 months to 1 week.
- According to CNCF 2020 survey, 91% respondents use Kubernetes compared to 78% in 2019 and 58% in 2018.



Kubernetes Usage and Benefits

- According to 2021 Kubernetes adoption survey, 89% of the 500 respondents mentioned that they use Kubernetes to deploy AI-based applications.
- Kubernetes has 77% of the market share in container orchestration technology compared to Mesos (4%), Docker Swarm (5%) and Openshift (9%).
- According to Enterprise open source survey, 78% practitioners reported Kubernetes as a clearly to go to choice.



Kubernetes Developer Community

- Kubernetes is considered one of the fastest growing community in the open-source software history with more than 2000 participant from Fortune 500 companies.
- According to the report of Bayern, Kubernetes related jobs search increased by 2,125% in last 4 years.
- According to Enlyft survey with 24,441 companies, 37% small companies, 43% medium sized companies and 20% large companies adopted Kubernetes.



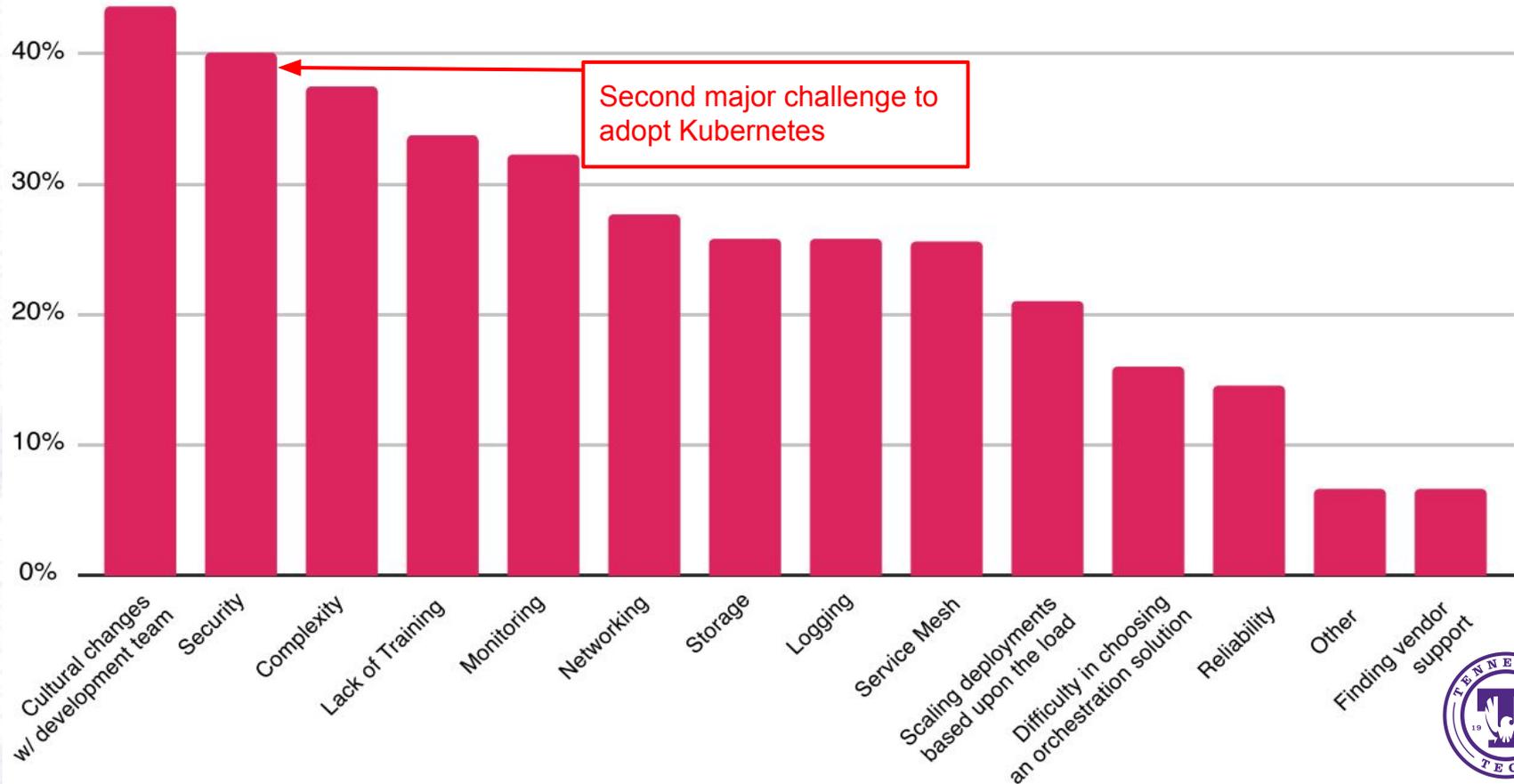
Kubernetes manifest

- Practitioners deploy containerized applications with the configurations file also known as 'manifests'

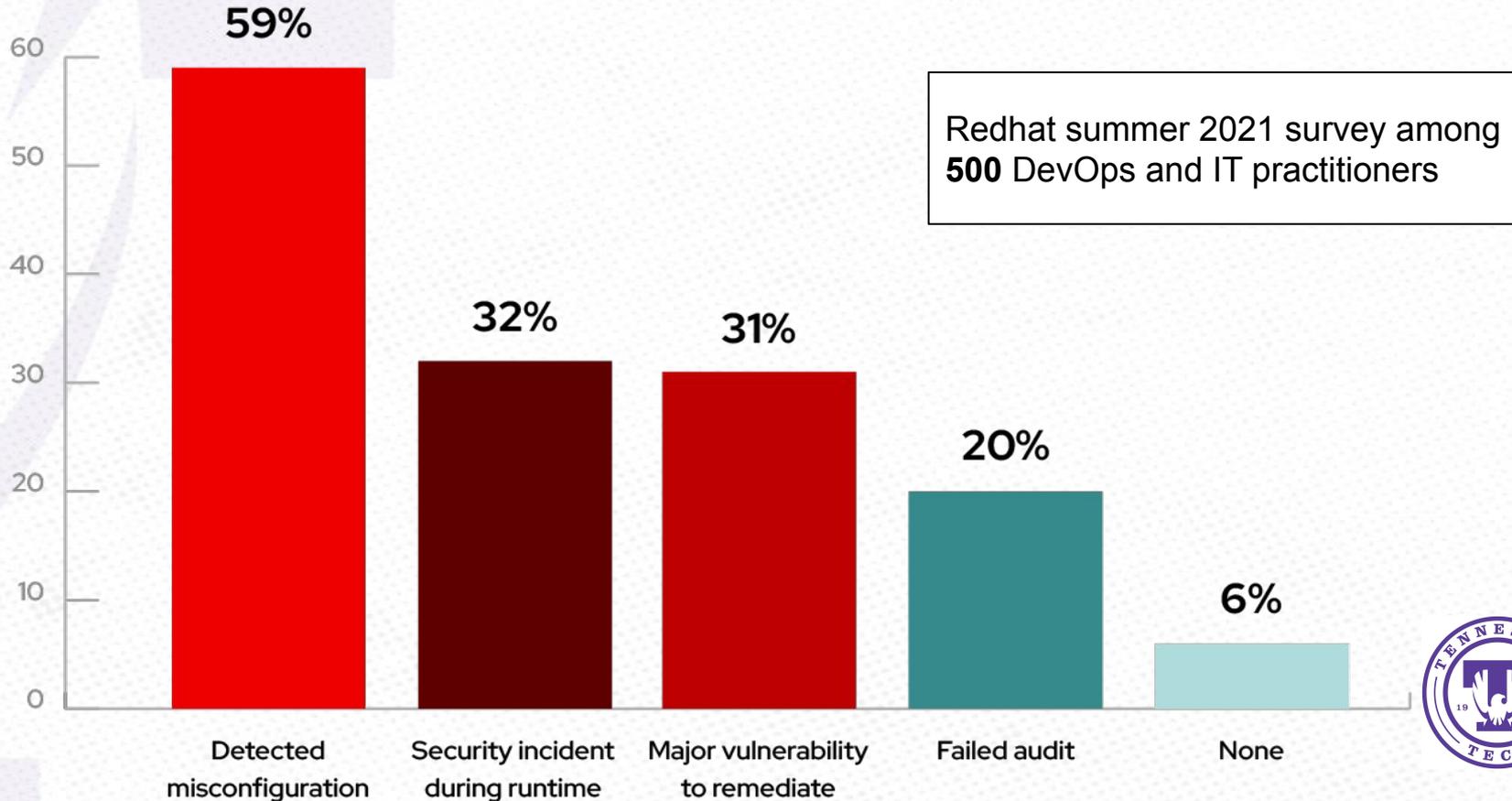
```
apiVersion: v1
kind: Pod
metadata:
  name: privileged-pod
spec:
  containers:
  - name: some-container
    image: glgl/py-kube:0.2
    command: ["/bin/bash", "-c", "while true ; do sleep 10 ; done"]
    securityContext:
      privileged: true
      allowPrivilegeEscalation: true
```



Security Concerns in Kubernetes



Practitioners Security Concerns in Kubernetes



Security Attacks in Kubernetes Cluster

ars TECHNICA [SUBSCRIBE](#) [SIGN IN](#)

CRYPTOCURRENCY JACKING —
Tesla cloud resources are hacked to run cryptocurrency-mining malware

Crooks find poorly secured access credentials, use them to install stealth miner.

DAN GOODIN - 2/20/2018, 1:21 PM



WIRED [BACKCHANNEL](#) [BUSINESS](#) [CULTURE](#) [MORE](#) [SUBSCRIBE](#)

LILY HAY NEWMAN SECURITY 02.20.2018 05:06 PM

Hack Brief: Hackers Enlisted Tesla's Public Cloud to Mine Cryptocurrency

The recent rash of cryptojacking attacks has hit a Tesla database that contained potentially sensitive information.

[f](#) [t](#) [✉](#) [🔖](#)

RedLock
A PAID ACTO NETWORKS COMPANY



< Back

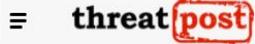
Research

Lessons from the Cryptojacking Attack at Tesla

by RedLock CSI Team | 02.20.18, 6:00 AM



Security Attacks in Kubernetes Cluster



Kubernetes Cloud Clusters Face Cyberattacks via Argo Workflows



EDITION: US ▾

ZDNet 🔍

BEST VPNS CLOUD SECURITY AI MORE ▾ NEWSLETTERS ALL WRITERS 👤

📄 MUST READ: [Quantum computing: How BMW is getting ready for the next technology revolution](#)

Researchers find new attack vector against Kubernetes clusters via misconfigured Argo Workflows instances

The report notes that other security teams have discovered large-scale cryptocurrency mining attacks against Kubernetes clusters.

MORE FROM JONATHAN GREIG

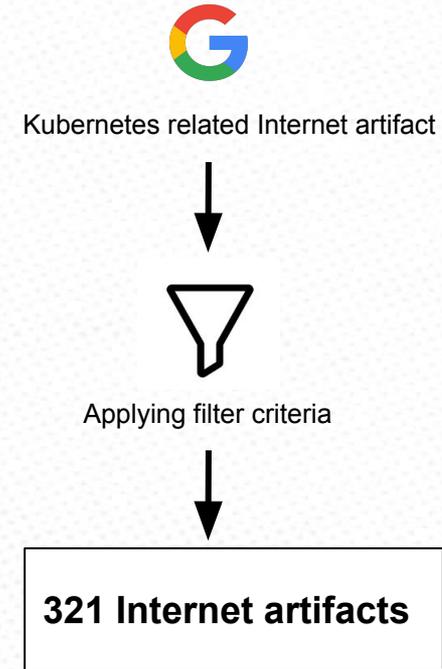
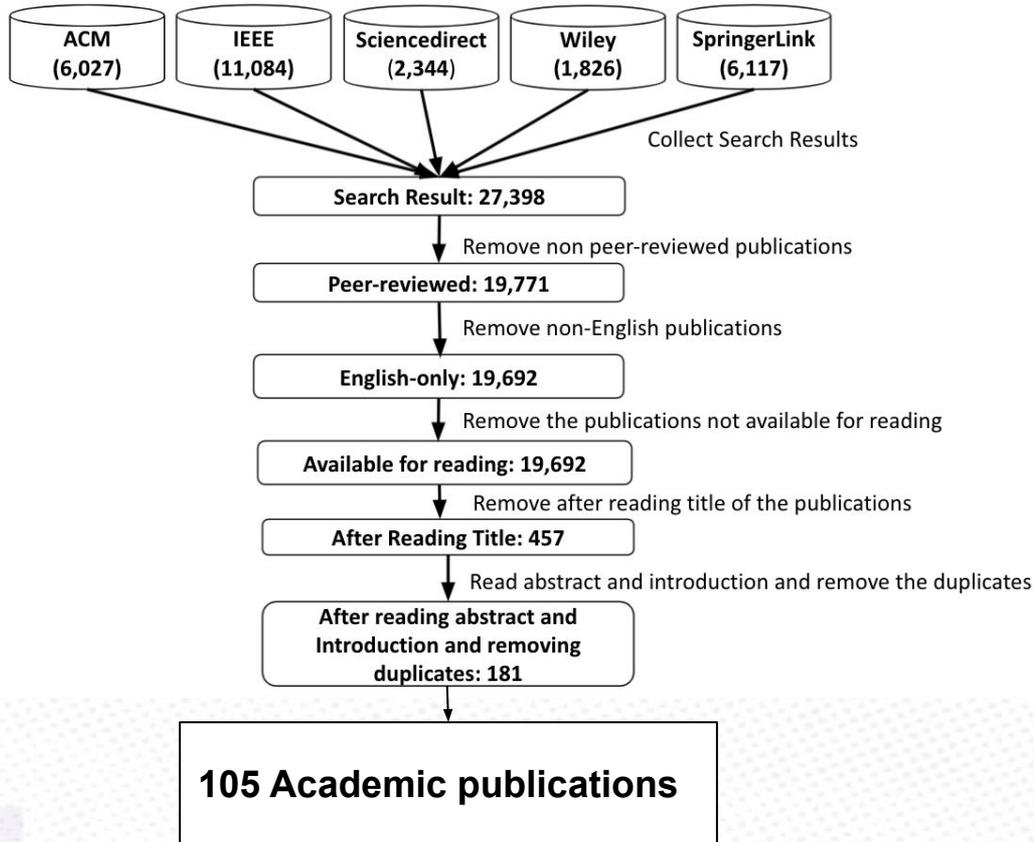
By [Jonathan Greig](#) | July 23, 2021 – 14:00 GMT (07:00 PDT) | Topic: [Cloud](#)

🗨️ [in](#) [📺](#) [f](#) [🐦](#) [✉️](#) 

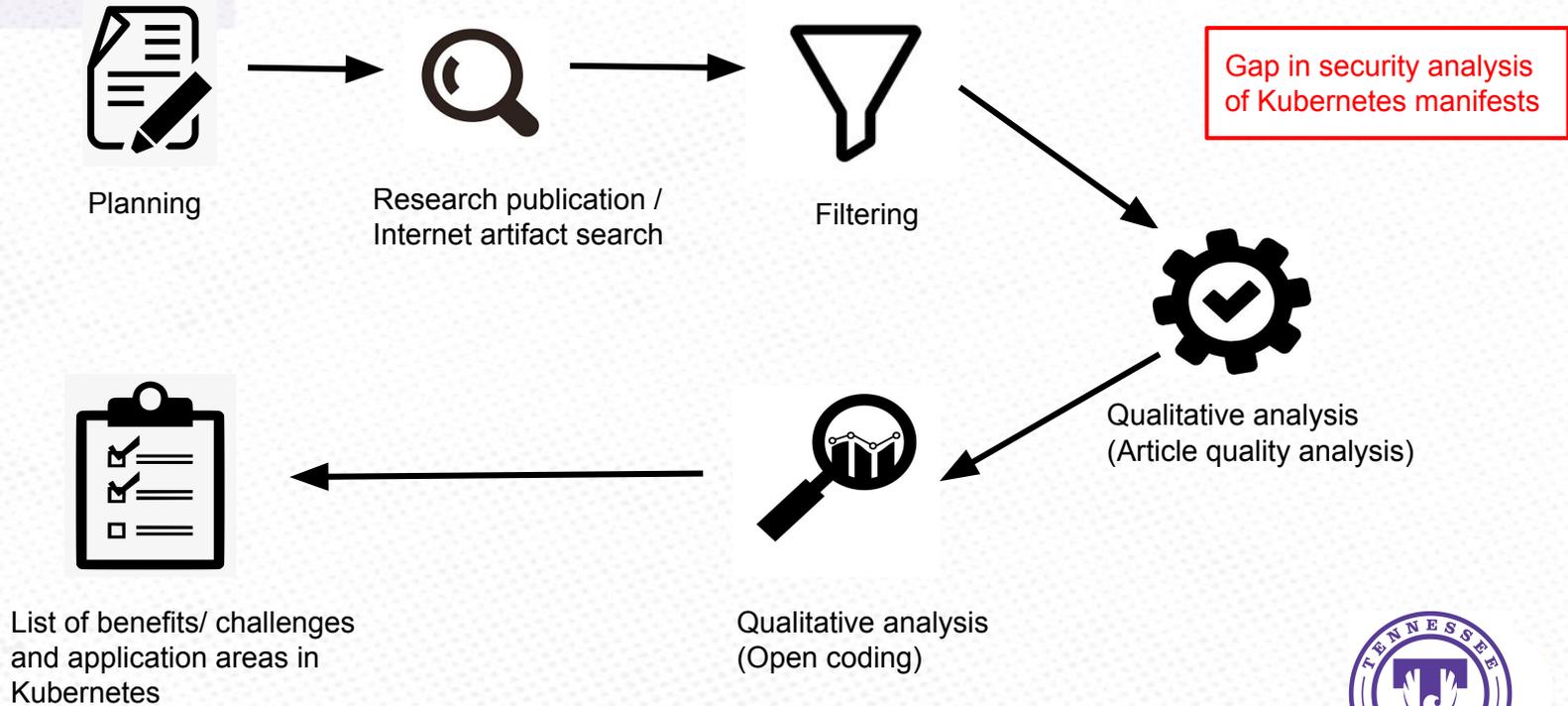
 Security
Nearly one million credit cards offered



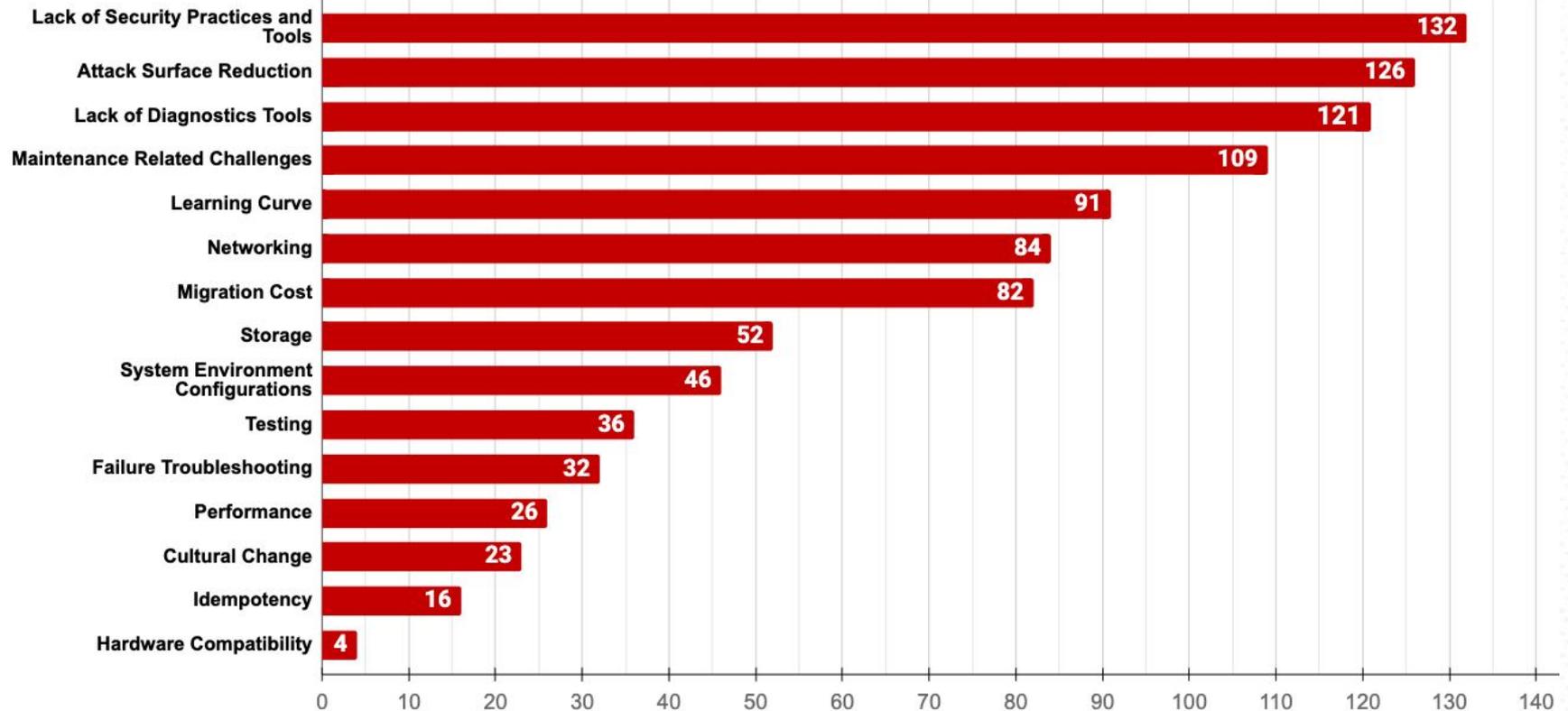
Multi-vocal Literature Review of Kubernetes



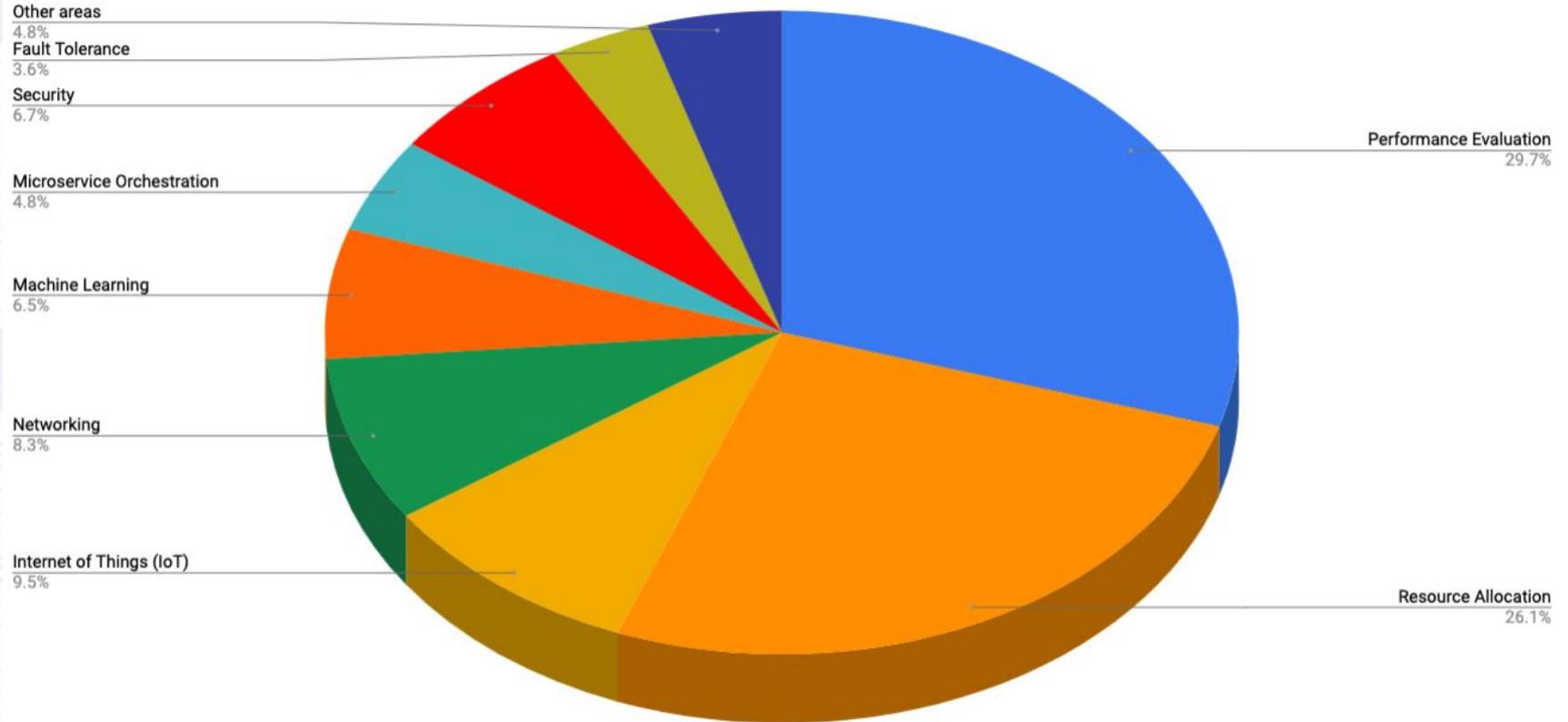
Multi-vocal Literature Review of Kubernetes



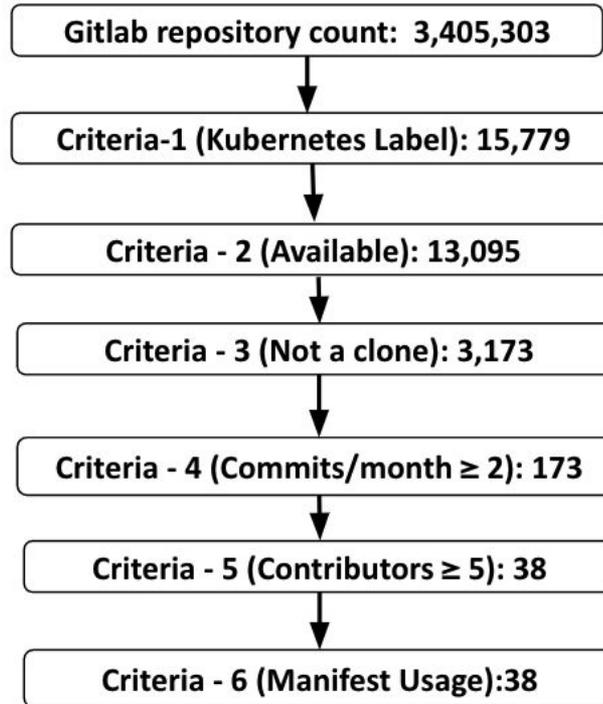
Multi-vocal Literature Review (Kubernetes Challenges)



Multi-vocal Literature Review (Current Kubernetes Research)



Security Defects in Kubernetes Manifests



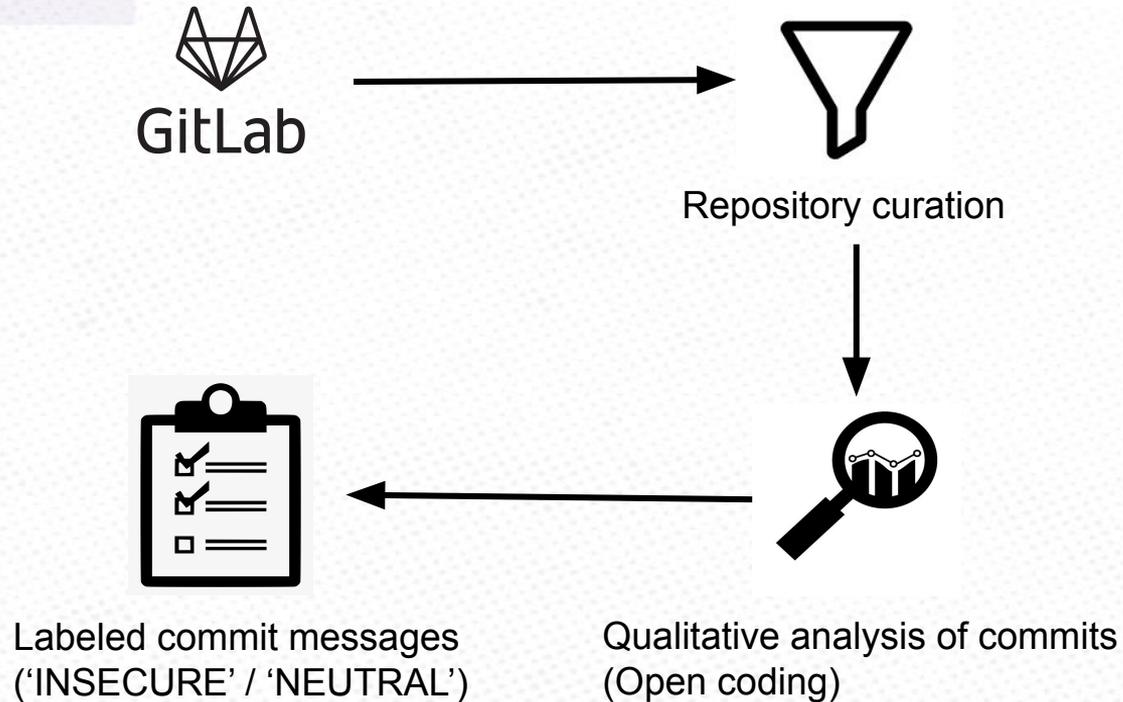
Security Defects in Kubernetes Manifests

- We curate 38 repositories that contain 1796 Kubernetes manifests that are modified with 5,193 commits.

| Attribute | Count |
|--------------------------|-----------------|
| Repositories | 38 |
| Manifests | 1,796 |
| Manifest-related Commits | 5,193 |
| Duration | 10/2015-07/2020 |



Security Defects in Kubernetes Manifests



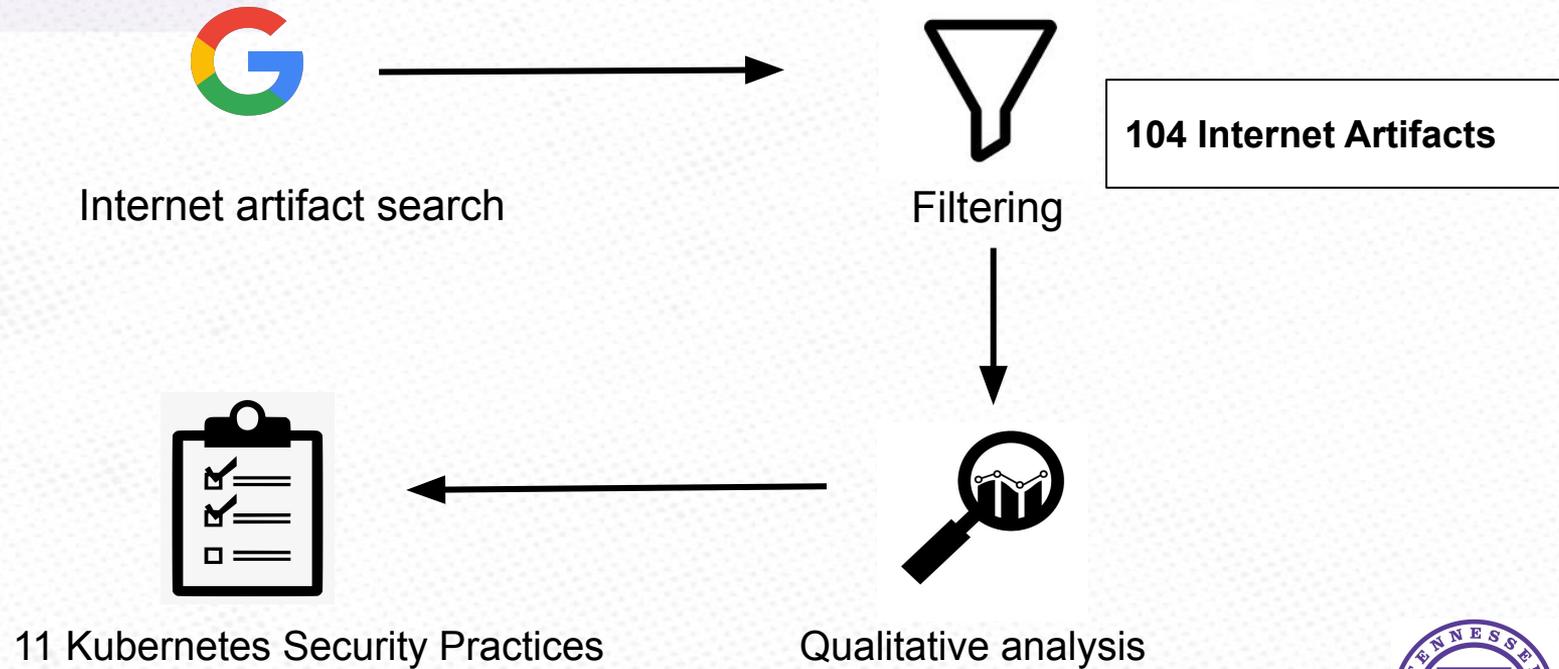
Security Defects in Kubernetes Manifests

- We identify 41 commits to be labeled as a security dataset.
- We identify 39 Kubernetes manifests to be modified as a security defect.
- Proportion of security defect is 0.79%
- Cohen's Kappa between the raters is 0.7

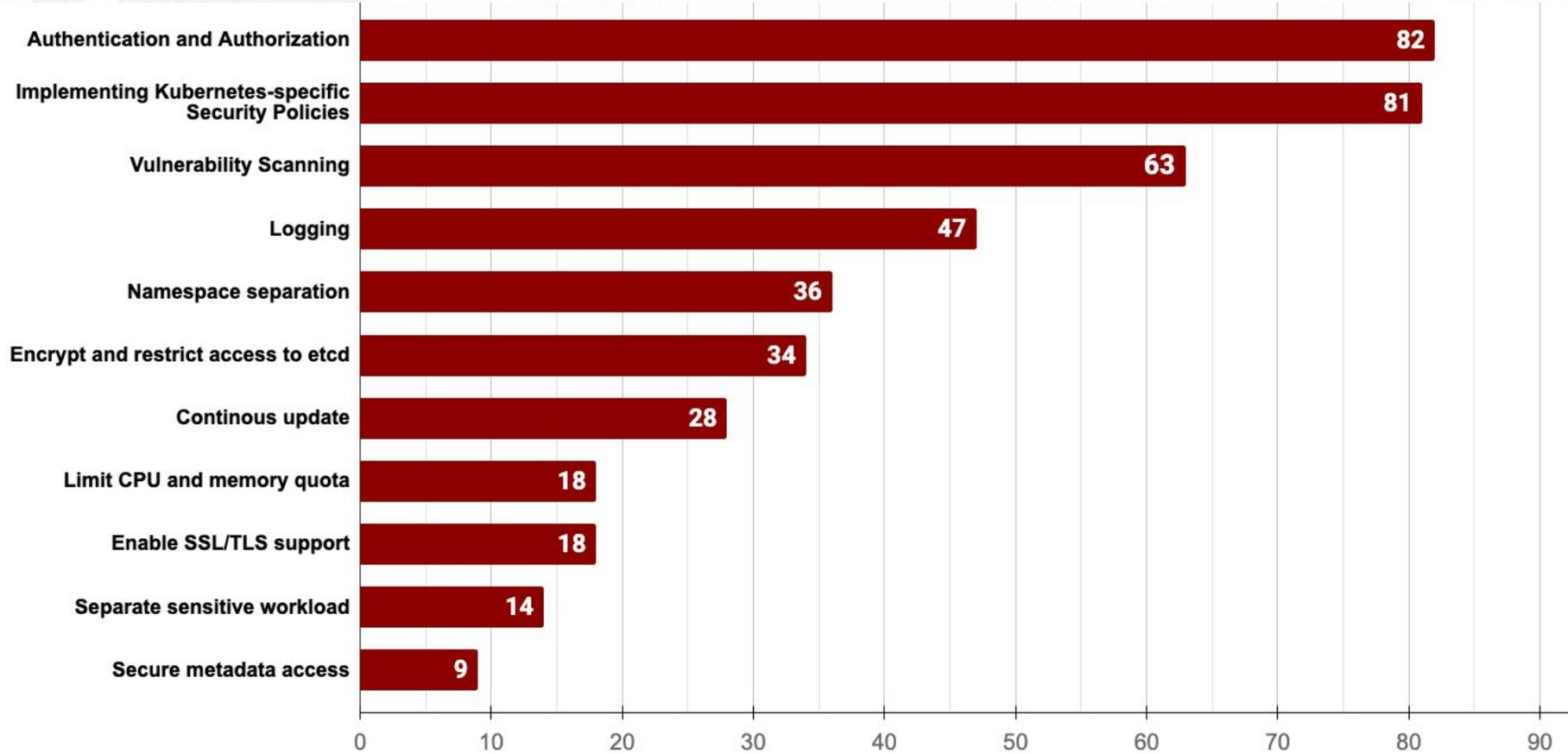
| Attribute | Count |
|--|-------|
| Repositories with ≥ 1 Security Defect | 9 |
| Manifests Modified in a Security Defect | 39 |
| Security Defects | 41 |



Kubernetes Security Best Practices



Kubernetes Security Best Practices

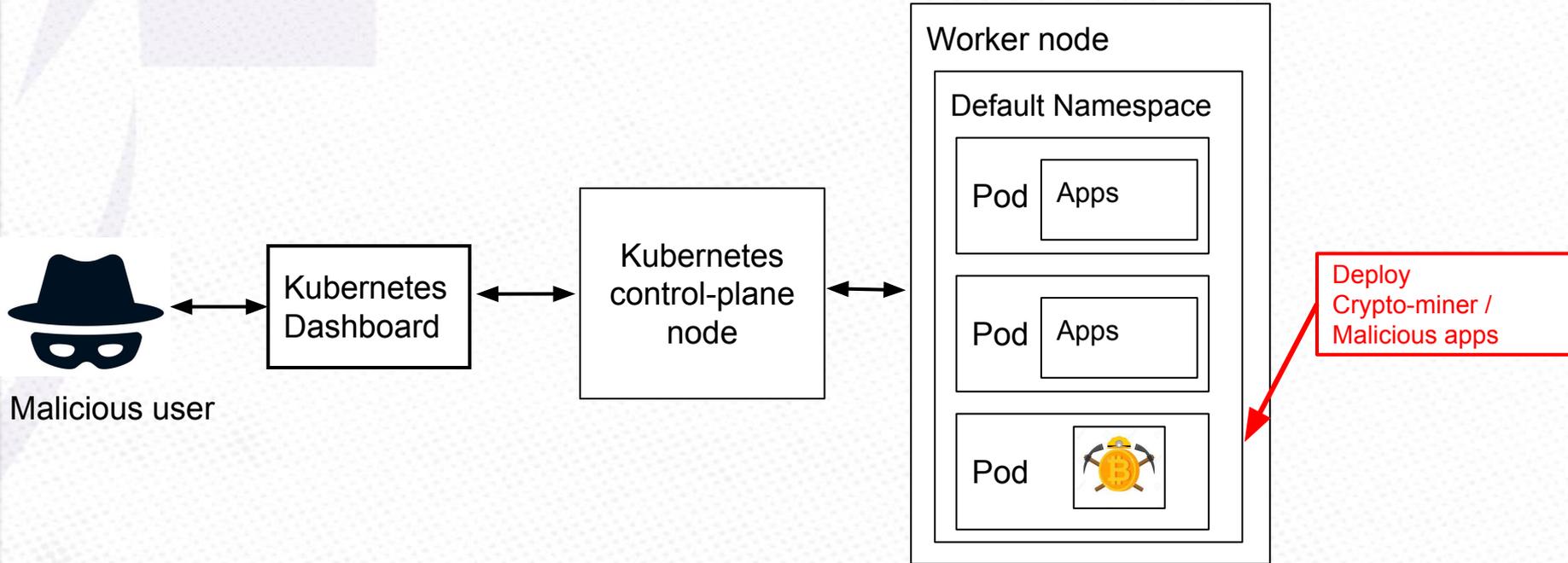


Threat Model for misconfigured RBAC

- RBAC is a built in authorization mechanism in Kubernetes.
- Over-privileged user has the unnecessary permission to perform an intended action.
- Consider a user uses Kubernetes dashboard as per default installation. By default the user will have admin privilege(no RBAC).
- The user can run malicious apps such as Crypto miner inside the Kubernetes cluster that can cause massive financial loss.



Attacks for Misconfigured RBAC

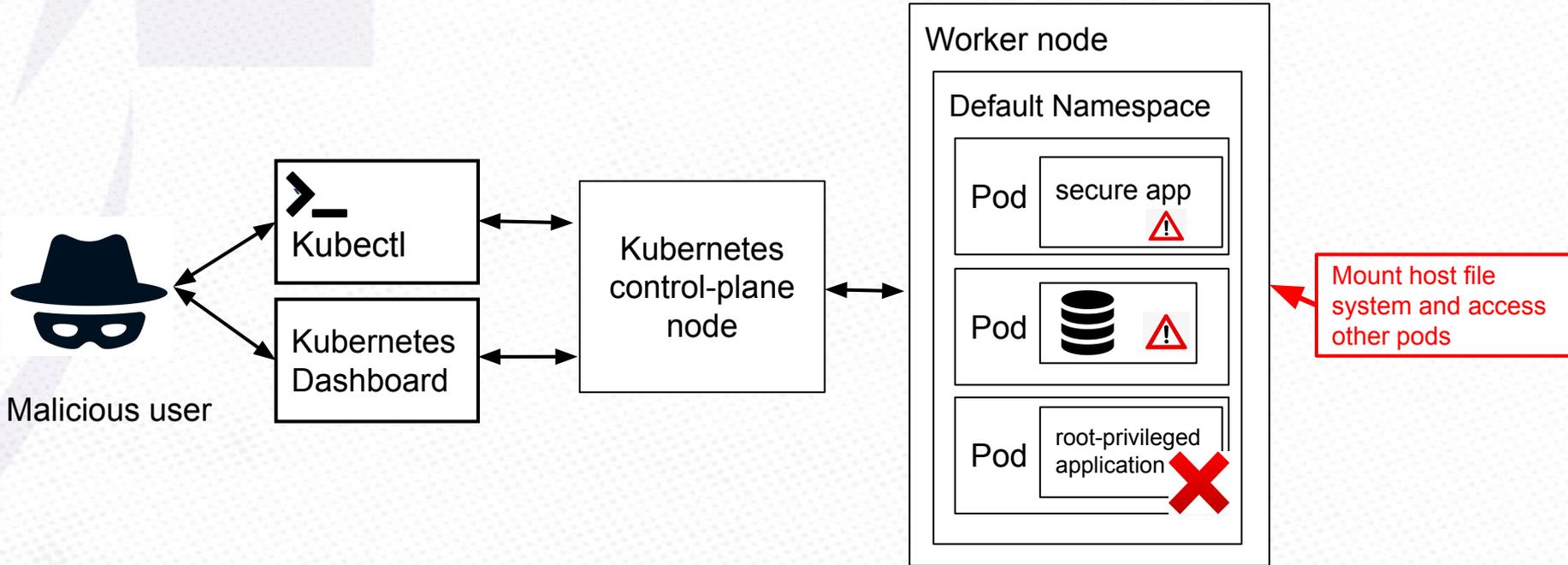


Threat Model for misconfigured Pod

- Pod Security policy is a cluster level resource that pods must comply and security context defines the access and privilege level of a container inside a pod.
- Let's say pod is running in a cluster without security context or pod security policy. If a malicious user has the permission to view and deploy a container then he perform remote code execution using shell of the container and can copy mounted host volume into the container storage.
- The user will get access to sensitive information from host file system.



Attack for misconfigured pod

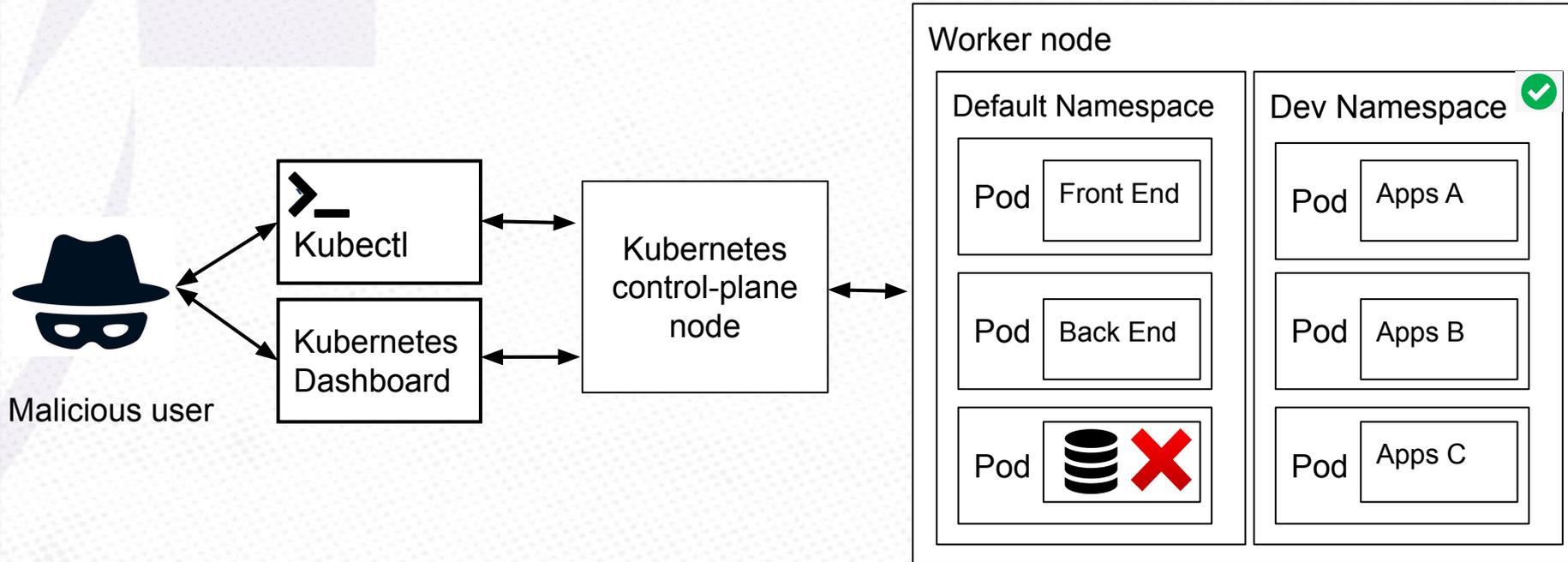


Threat Model for Default Namespace

- Namespace creates a logical isolation inside Kubernetes cluster. It is recommended that each team in an organization has separate namespace.
- If no namespace is specified while deploying the pod, Kubernetes assigns default namespace for the pod.
- For instance, in an organization all the applications are deployed in default namespace. If a malicious user gets access to view and deploy application in default namespace then he can access all the running applications in Kubernetes cluster.
- Malicious user can access sensitive application running in the default namespace.



Attack in the Default Namespace



Malicious user can exploit sensitive application such as database.

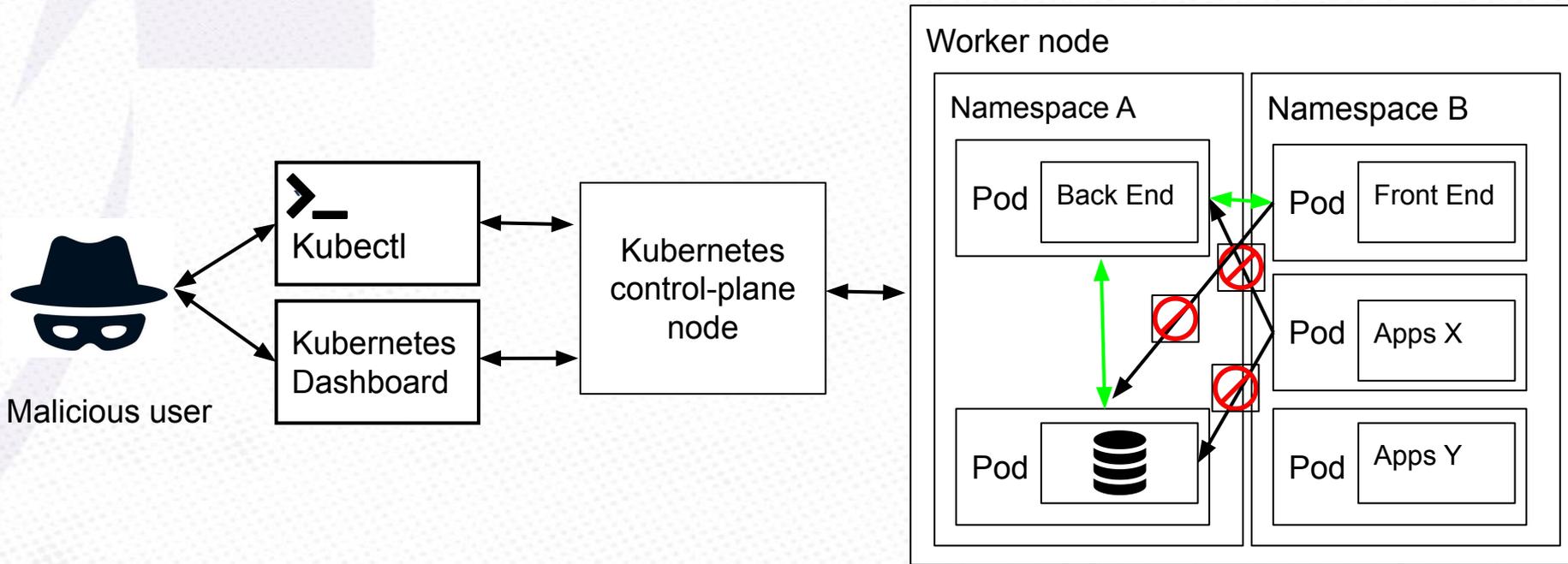


Threat Model for Network Policy

- Network policy controls the network traffic flow within a Kubernetes cluster. By default, all pods in a Kubernetes cluster can communicate with each other, and Network Policy enforces rules on the running pods.
- Let's consider an organization where no network policy is defined in the Kubernetes cluster. If a malicious user with the permission to deploy a pod can eventually access pods in different namespaces and request a connection.
- This can eventually lead to a successful connection or hamper other applications with unnecessary traffic.



Possible Attacks for Undefined Network Policy



Without Network policy pods can communicate with each other

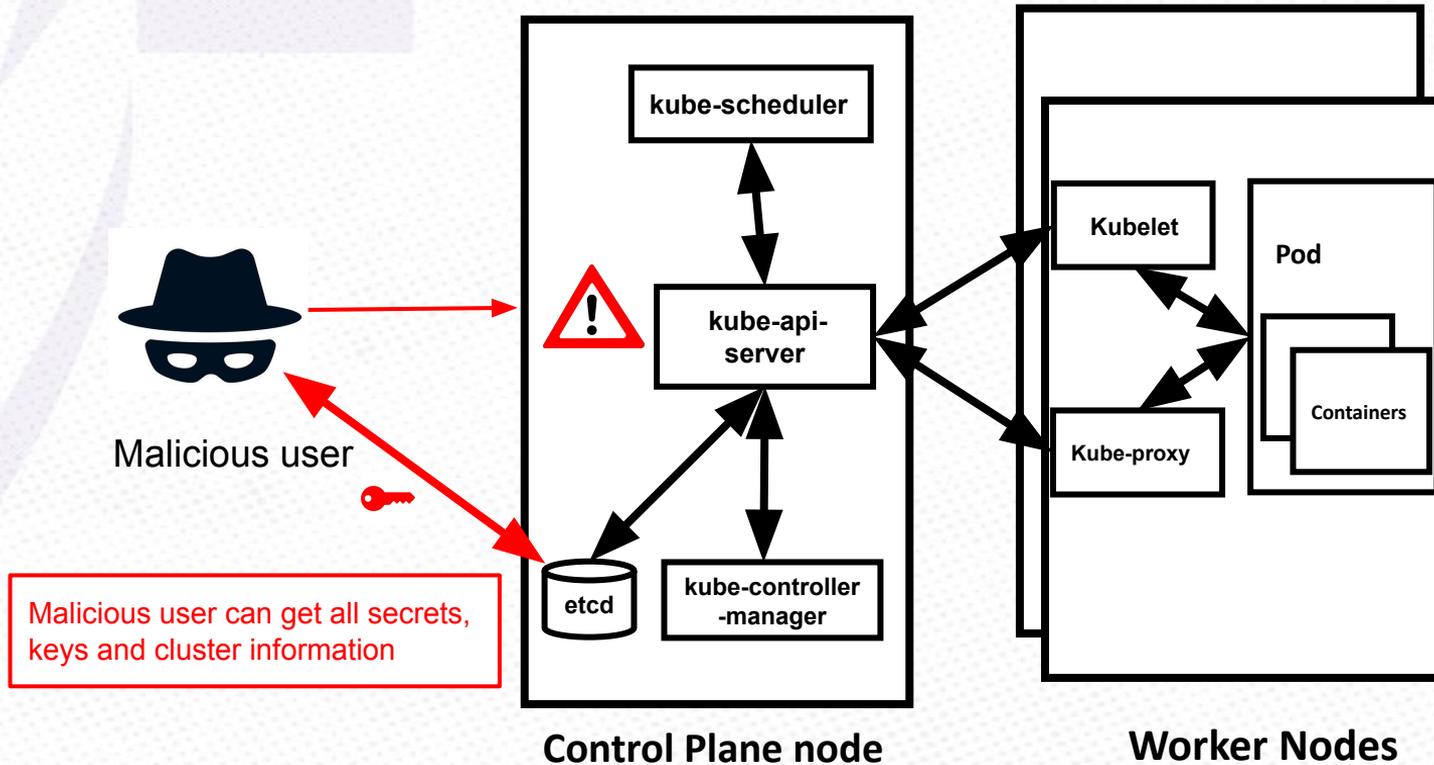


Threat Model for ETCD secret

- ETCD contains all the secrets and the back up information of the cluster. By default the secrets in ETCD is not encrypted.
- Let's say a malicious user compromised the host of a Kubernetes cluster and ETCD database is not encrypted with KMS service then the hacker access all the cluster information and potential secrets of the Kubernetes cluster.



Attack for Unencrypted ETCD

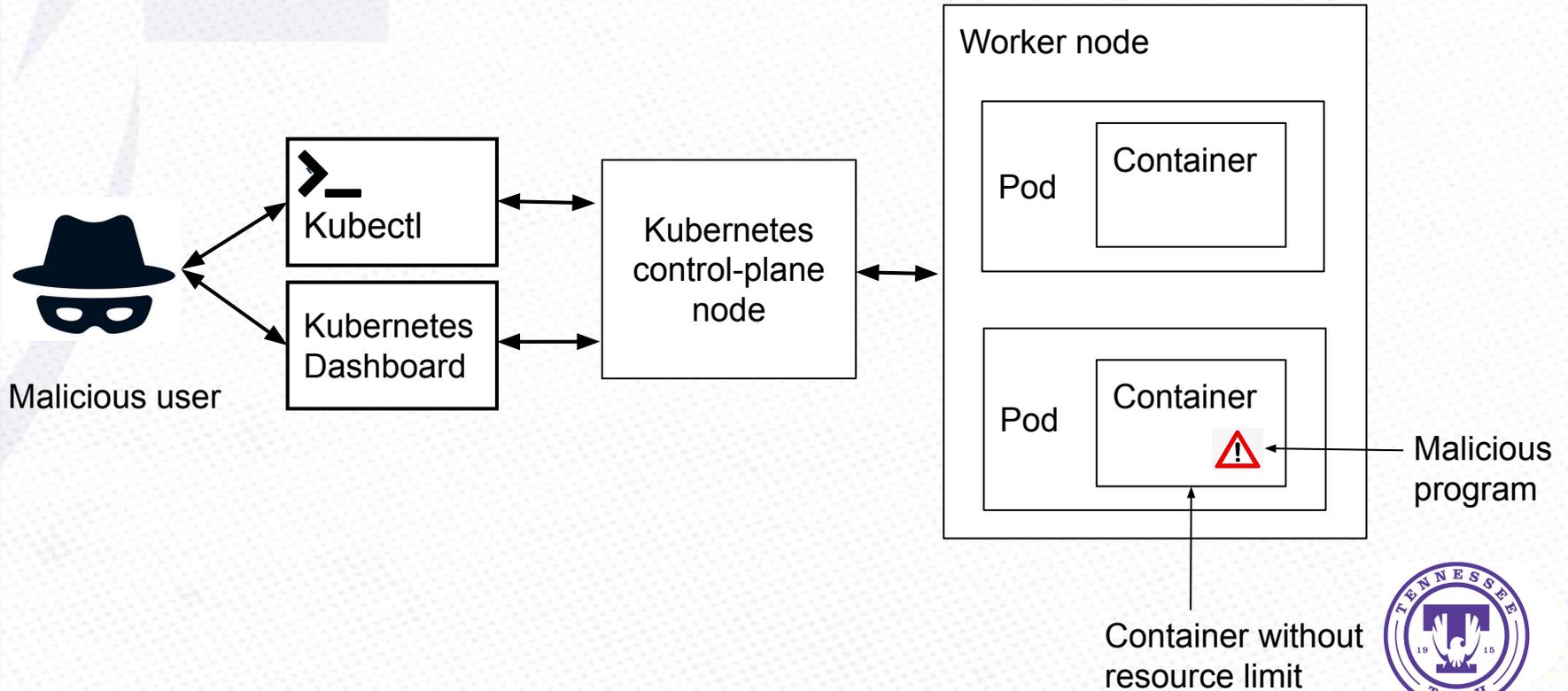


Threat Model for Resource Limit

- Specifying resource limit restricts a pod to consume upto a maximum allowable resource limit.
- Let's a developer deployed a pod without resource limit that contains a malicious code or a malicious user who has the permission to view, and deploy and delete the pod in a namespace can inject malicious code into the container that can consume all the available resource for the node.
- This condition will lead to denial of service (DoS) attack.



Attacks for Resource Limit



Conclusion and Future Work

- I demonstrate that the Kubernetes security best practices violation can actually lead to exploit.
- In future work, I want to explore more attacks for security best practices violations in the Kubernetes manifests and also propose the mitigation strategies.



Summary

Security Attacks in Kubernetes Cluster

RedLock

Hack Brief: Hackers Enlisted Tesla's Public Cloud to Mine Cryptocurrency

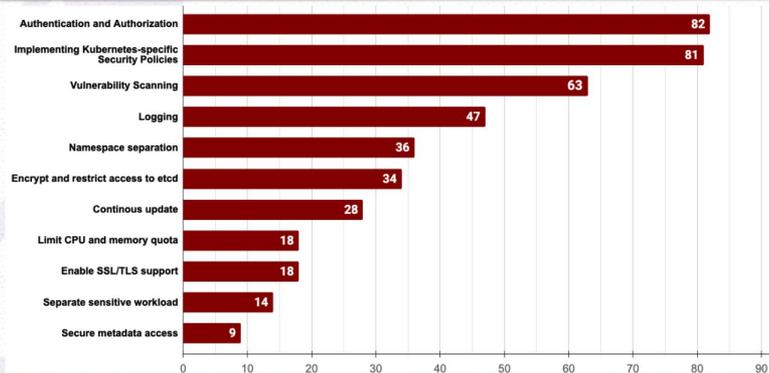
The recent rash of cryptojacking attacks has hit a Tesla database that contained potentially sensitive information.

Lessons from the Cryptojacking Attack at Tesla

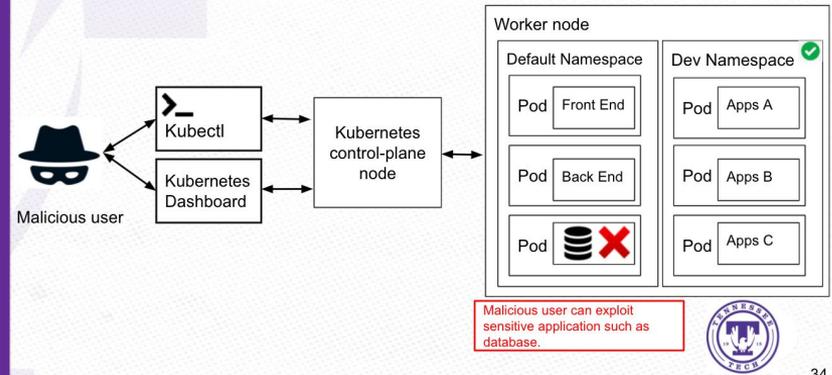


17

Kubernetes Security Best Practices (SecDev 2020)



Attack in the Default Namespace



THANK YOU!

Email: mshamim42@tntech.edu
Website: <https://shazibulislam.github.io>



Questions

