KubeCon | CloudNativeCon

North America 2020

Virtual

PKI the Wrong Way

Simple TLS Mistakes and Surprising Consequences

Tabitha Sable, Datadog

KubeCon | CloudNativeCon

North America 2020

Virtual

PKI the Wrong Way

Simple TLS Mistakes and Surprising Consequences

Tabitha Sable, Datadog

@tabbysable

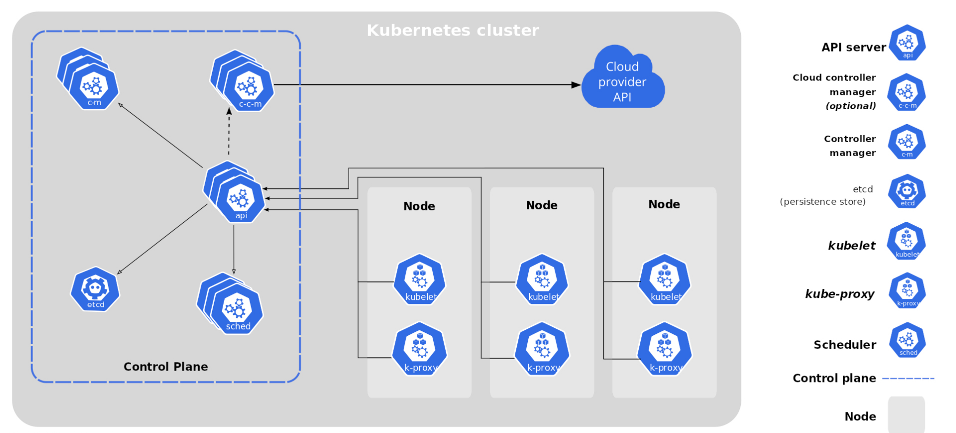
Hacker Agenda

- Kubernetes TLS Review
- Certifying Authority Capers
- Shared PKI Shenanigans
- Requestheader Auth Rowdiness
- PKI Chain Perpetrations

Kubernetes TLS Review

TMA

- TLS
- mTLS
- CA
- PKI



CC BY 4.0: https://kubernetes.io/docs/concepts/overview/components/

@tabbysable

Kubernetes TLS Review

- etcd
  - Mutual TLS authentication of clients
  - Mutual TLS authentication of peers

Kubernetes TLS Review

- kube-apiserver
  - Mutual TLS authentication of clients
  - Mutual TLS authentication to etcd
  - Mutual TLS authentication to kubelet

Kubernetes TLS Review

- apiserver front-proxy / aggregation layer
  - requestheader-* arguments
  - Mutual TLS authentication of front-proxy
  - Mutual TLS authentication to extension apiservers

Kubernetes TLS Review

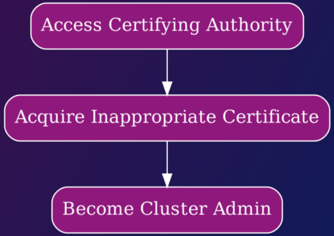
- kubelet and others
  - Mutual TLS authentication of clients
  - Mutual TLS authentication to apiserver

Kubernetes TLS Review

- Your Applications
  - TLS servers
  - mTLS servers
  - mTLS clients

Certifying Authority Capers

- CA signing controls Kubernetes RBAC



Access Certifying Authority

Acquire Inappropriate Certificate

Become Cluster Admin

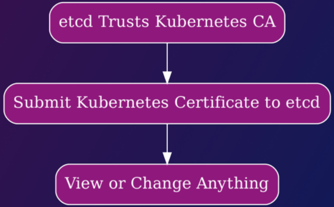
@tabbysable

Mitigations

- Treat CA permissions with care
- Use least-privilege

Shared PKI Shenanigans

- etcd sharing Kubernetes PKI
  - mTLS for clients
  - Every cert has full access


etcd Trusts Kubernetes CA
Submit Kubernetes Certificate to etcd
View or Change Anything

@tabbysable

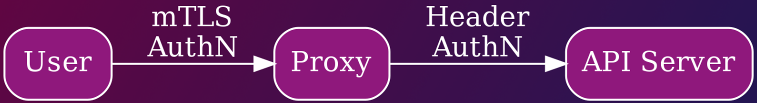
Mitigations

- Separate PKI for etcd and k8s
- Network policy
- etcd authorization

Requestheader Auth Rowdiness

@tabbysable

Requestheader Auth Rowdiness



User

mTLS AuthN

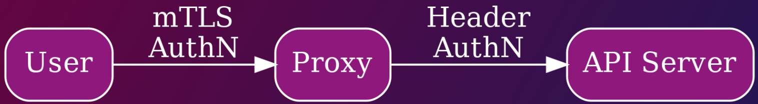
Proxy

Header AuthN

API Server

Front Proxy Authentication

Requestheader Auth Rowdiness



User

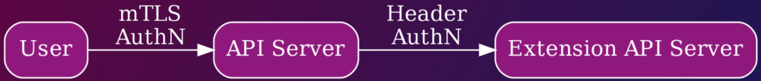
mTLS AuthN

Proxy

Header AuthN

API Server

Front Proxy Authentication



User

mTLS AuthN

API Server

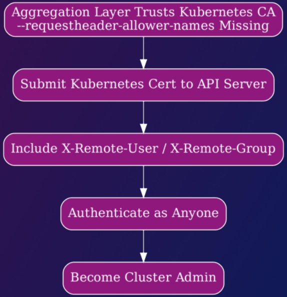
Header AuthN

Extension API Server

API Server Aggregation

Requestheader Auth Rowdiness

- Aggregation layer sharing main PKI
  - Enabled by --requestheader-*
  - Forgotten --requestheader-allowed-names


Aggregation Layer Trusts Kubernetes CA
--requestheader-allower-names Missing
Submit Kubernetes Cert to API Server
Include X-Remote-User / X-Remote-Group
Authenticate as Anyone
Become Cluster Admin

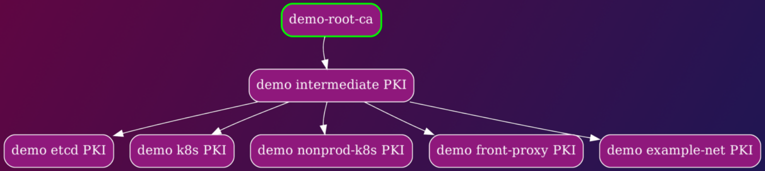
@tabbysable

Mitigations

- Use a separate PKI with strict access control
- Pass all requestheader-* arguments
- Pass no requestheader-* arguments
  - Extension apiservers won't autoconfigure

@tabbysable

PKI Chain Perpetrations



demo-root-ca

demo intermediate PKI

demo etcd PKI

demo k8s PKI

demo nonprod-k8s PKI

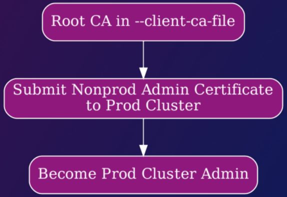
demo front-proxy PKI

demo example-net PKI

@tabbysable

PKI Chain Perpetrations

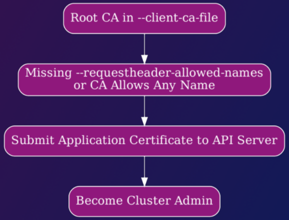
- mTLS trusted root CA
- Cross-cluster access


Root CA in --client-ca-file
Submit Nonprod Admin Certificate to Prod Cluster
Become Prod Cluster Admin

@tabbysable

PKI Chain Perpetrations

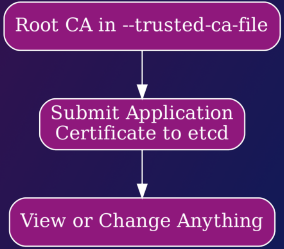
- mTLS trusted root CA
- Application certificate Kubernetes access


Root CA in --client-ca-file
Missing --requestheader-allowed-names or CA Allows Any Name
Submit Application Certificate to API Server
Become Cluster Admin

@tabbysable

PKI Chain Perpetrations

- mTLS trusted root CA
- Application certificate etcd access



Root CA in --trusted-ca-file

Submit Application Certificate to etcd

View or Change Anything

@tabbysable

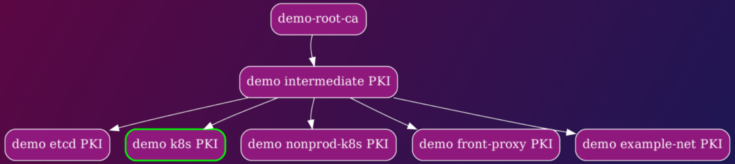
Mitigations

- Use standalone CAs

@tabbysable

Mitigations

- Use standalone CAs
- mTLS trust only the leaf cert



@tabbysable

Mitigations

- Use standalone CAs
- mTLS trust only the leaf cert
- Tight CA permissions
- Set "client auth" and "server auth" cert flags
- etcd authentication

@tabbysable

Wrapup

- PKI is complex
  - Details matter
- Be creative
  - These hacks are just examples

Take-Home

- Use 3 separate CAs per cluster
- Use standalone CAs
- Carefully understand all options

Thank You

- We're Hiring!
  - www.datadoghq.com/careers/
- I'm online
  - tsable@datadog.com
  - Kubernetes Slack
  - Twitter
- Play along
  - https://github.com/tabbysable/pki-the-wrong-way