FUJITSU

shaping tomorrow with you

Advanced Security on Kubernetes with Istio

20 June 2018

Shunsuke Miyoshi (s.miyoshi@jp.fujitsu.com)

Fujitsu Limited.

Outline

FUJITSU

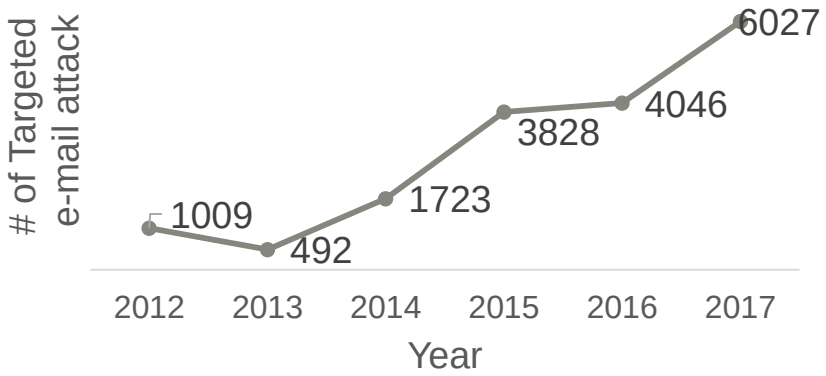
- Backgrounds
  - Recent Cyber Attack Trends
  - Conventional Network
  - Zero Trust Network Model
- Zero Trust Network in Kubernetes with Istio
- Demo
- Summary

Recent Cyber Attack Trends

FUJITSU

- Increasing the number of cyber attacks

The number of Targeted e-mail attack in Japan



- Advancing of Attacks
  - APT(Advanced Persistent Threat) Attack
    - continuously attack to special target with long period of time

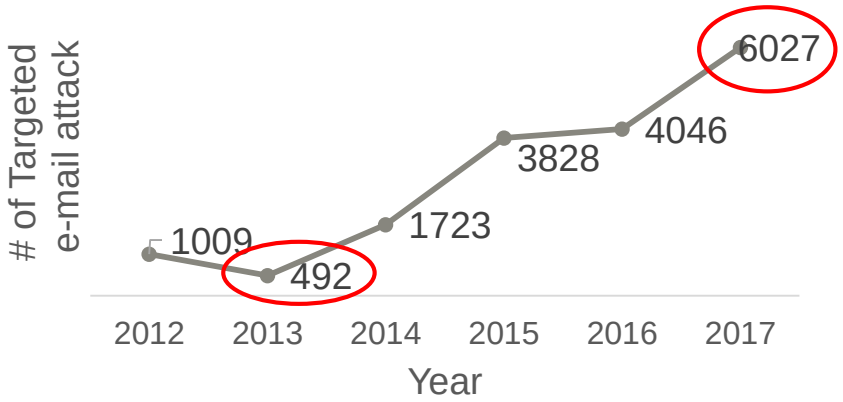
*) data from National Police Agency(http://www.npa.go.jp/)

Recent Cyber Attack Trends

FUJITSU

- Increasing the number of cyber attacks

The number of Targeted e-mail attack in Japan



- Advancing of Attacks
  - APT(Advanced Persistent Threat) Attack
    - continuously attack to special target with long period of time

*) data from National Police Agency(http://www.npa.go.jp/)

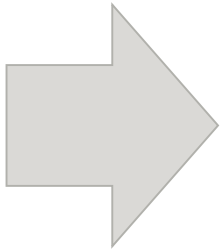
Advancing of Targeted e-Mail Attack

FUJITSU

Previous

e-Mail
From: bheojbr@gmail.com
To: your-address@example.com
Title: You won the prize money!
Dear member, You won the prize money! Please click http://mysite.com

Target: Anyone



Now

e-Mail
From: s.miyoshi@company.com
To: your-address@travel_egency.com
Title: Notification of attachment of e-ticket receipt
Attach: e-Ticket.pdf
Please check attached e-Ticket, and replay me.

Target: Individually

Advancing of Targeted e-Mail Attack

FUJITSU

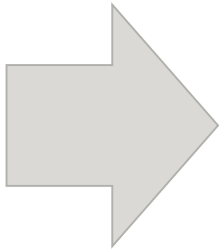
Previous

e-Mail
From: bheojbr@gmail.com
To: your-address@example.com
Title: You won the prize money!
Dear member, You won the prize money! Please click http://mysite.com

Free Address

Target: Anyone

Easy to find this is fake



Now

e-Mail
From: s.miyoshi@company.com
To: your-address@travel_egency.com
Title: Notification of attachment of e-ticket receipt
Attach: e-Ticket.pdf
Please check attached e-Ticket, and replay me.

Target: Individually

Advancing of Targeted e-Mail Attack

FUJITSU

Previous

e-Mail
From: bheojbr@gmail.com
To: your-address@example.com
Title: You won the prize money!
Dear member, You won the prize money! Please click http://mysite.com

Target: An

Too difficult to find
this is business e-Mail or not

Now

Forge to
<name>@<company's addr>

e-Mail
From: s.miyoshi@company.com
To: your-address@travel_egency.com
Title: Notification of attachment of e-ticket receipt
Attach: e-Ticket.pdf
Please check attached e-Ticket, and replay me.

individually targeted

Forge to PDF file

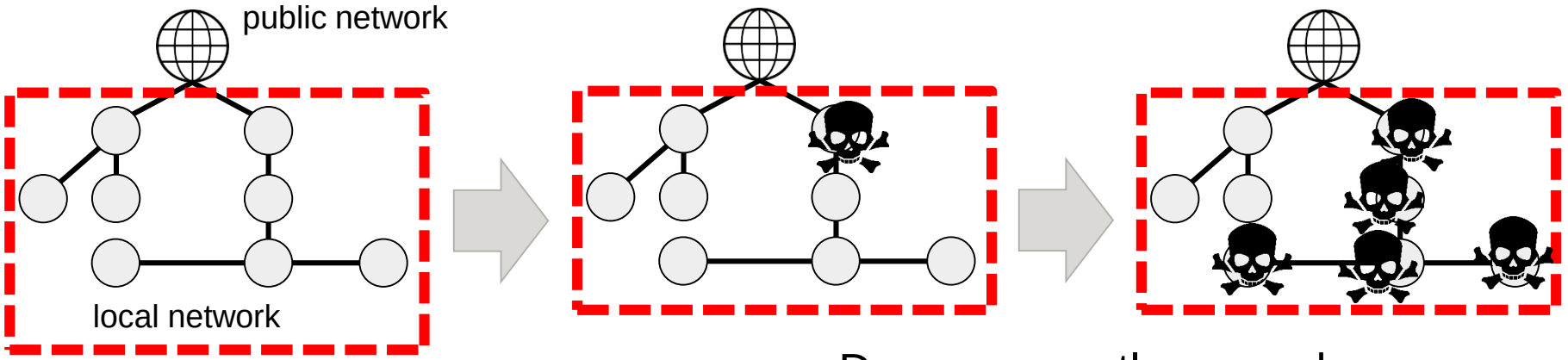
Target: Individually

Conventional Network

- Firewall-based Security
  - Policy: Inside a local network is safety

Service

Attacked Service



Once Attacked ・・・

Damage greatly expands

Zero Trust Network Model

FUJITSU

Zero Trust Network Model

Concept: **Never Trust, Always verify**

Ex. Service *'X'* is really Service *'X'* ?, Data is not wiretapped?, Authorized?

Previous System

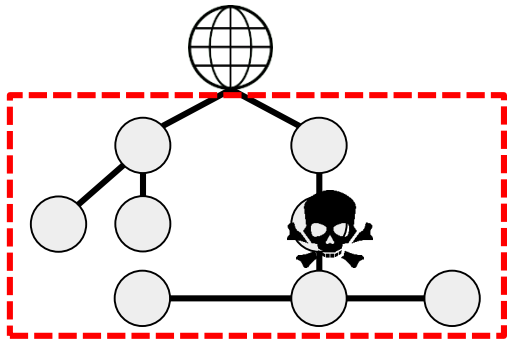
・Inside a local network is safety

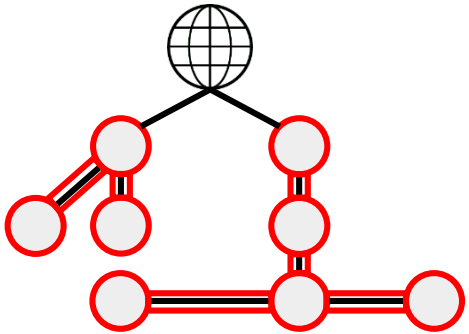
→ Firewall based system

Next Generation System

we never know where the enemy is

→ Zero Trust Network Model



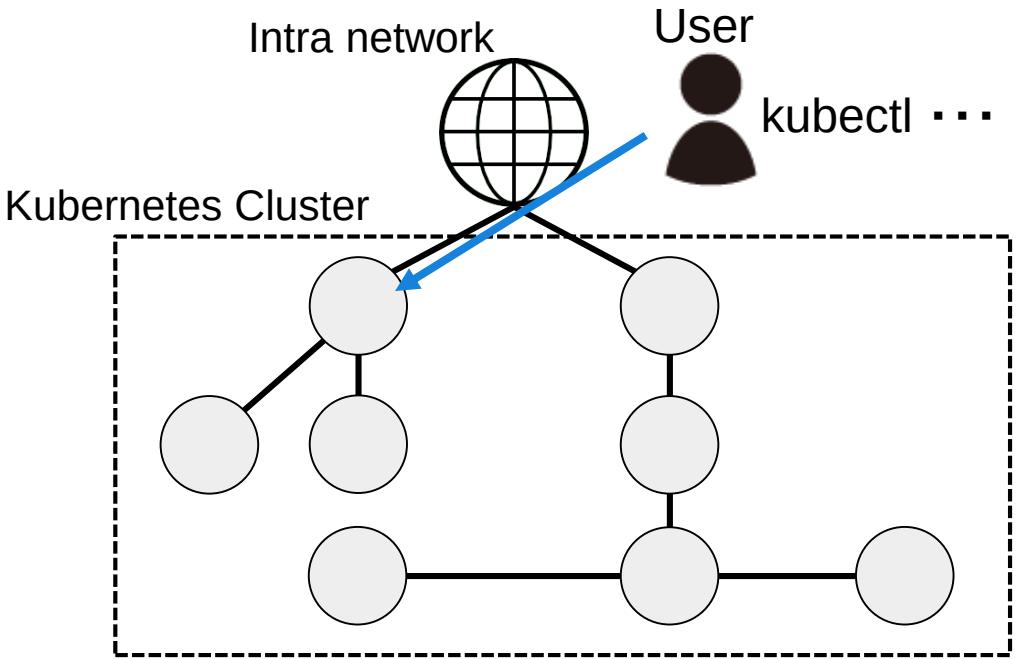


protecting-line

Zero Trust Network in Kubernetes

FUJITSU

- Image of Kubernetes



Zero Trust Network in Kubernetes

FUJITSU

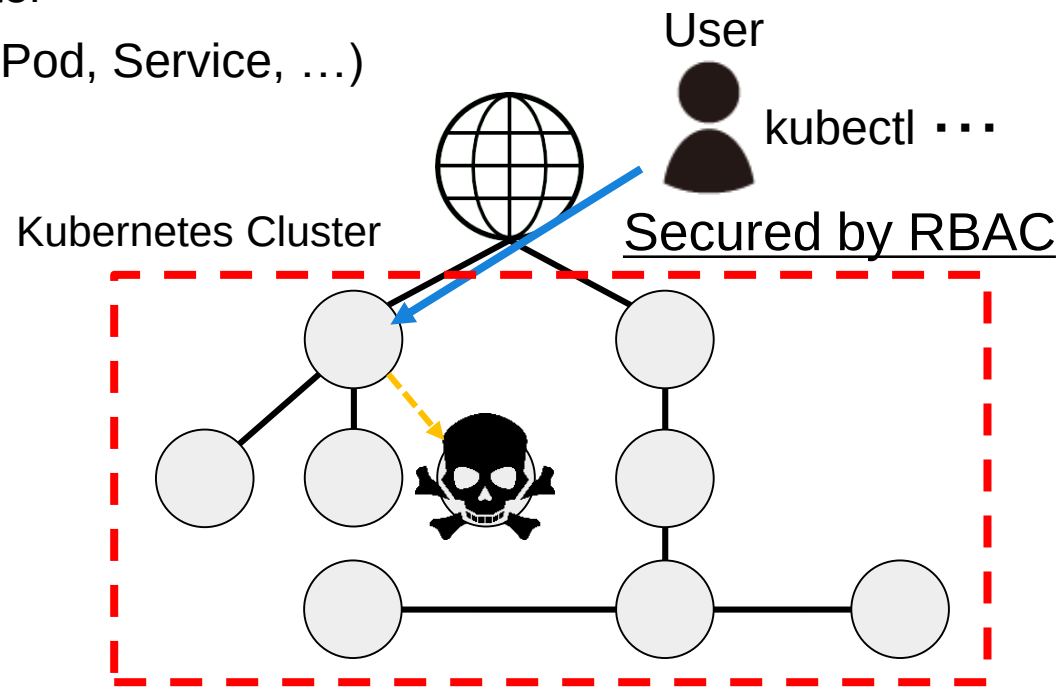
- Role Based Access Control(RBAC)
  - Access Control: User → Cluster

    Ex. allow get/edit resources(Pod, Service, …)

    of Namespace *'A'*

→ Unsafe yet

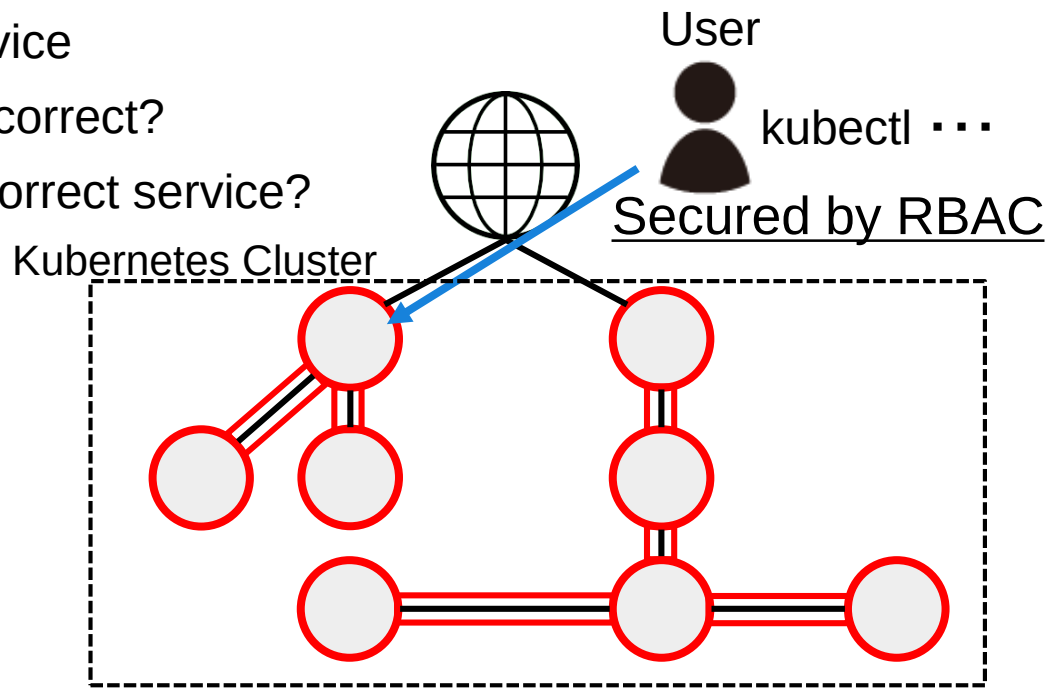
  - Wiretap from other Service
  - Spoofing of Regular Service



Zero Trust Network in Kubernetes

FUJITSU

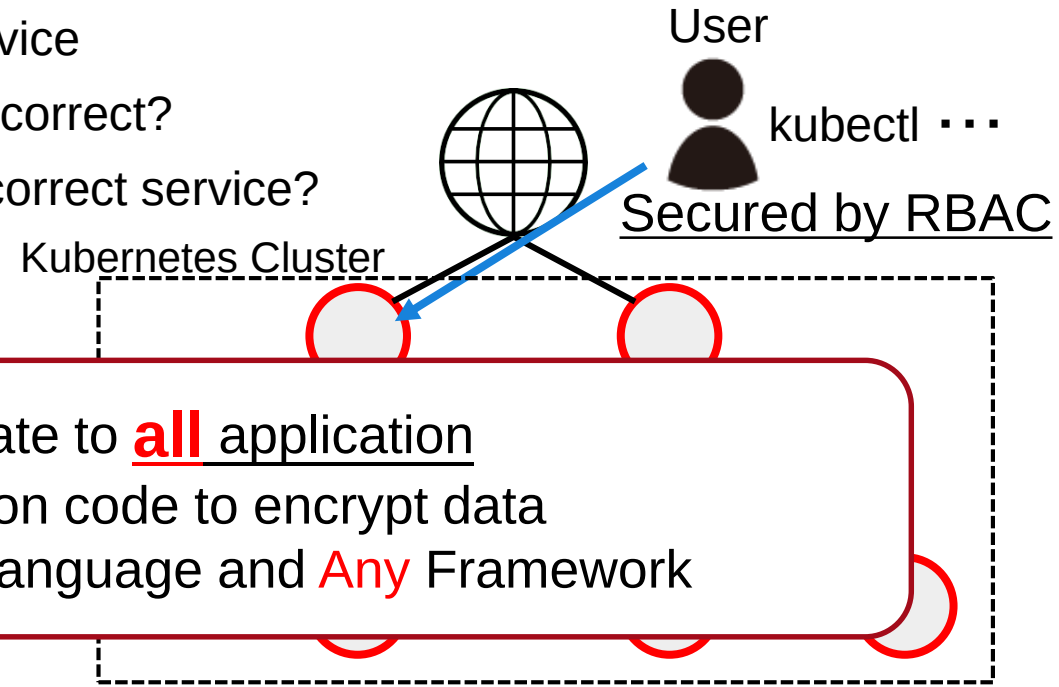
- Security of Communication between Services
  - Encryption of Communication Channel
  - Authentication of Destination Service
    - Is the destination service really correct?
    - Do you really receive from the correct service?



Zero Trust Network in Kubernetes

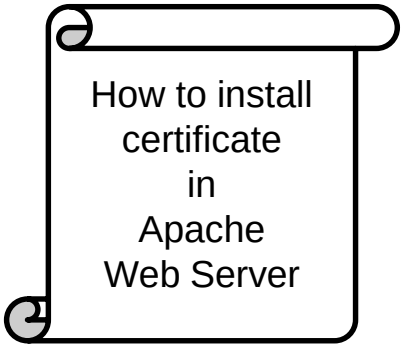
FUJITSU

- Security of Communication between Services
  - Encryption of Communication Channel
  - Authentication of Destination Service
    - Is the destination service really correct?
    - Do you really receive from the correct service?



Information that Service Owner Must Manage

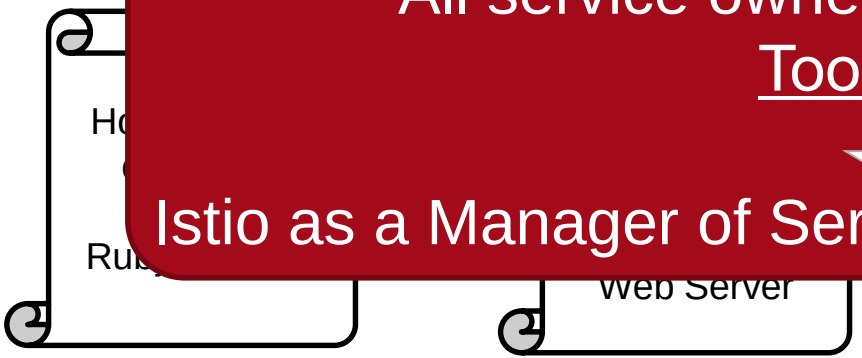
Service X		
Destination	Certificate Path	Expiration date
Service A	/etc/certs/svc_a.crt	2018/12
Service F	/etc/certs/new/svc_f.crt	2019/05
Service Y	/etc/certs/v2/svc_y.crt	2019/01
⋮	⋮	⋮



Information that Service Owner Must Manage

FUJITSU

Service X		
Destination	Certificate	Expiration date
Service A	/etc/certs/svc_a.crt	2018/12
Service F	/etc/certs/new/svc_f.crt	2019/05
Service Y	/etc/certs/v2/svc_y.crt	2019/01
.	.	.
.		
.		



All service owner must manage them

Too hard …

Istio as a Manager of Service Communication Security

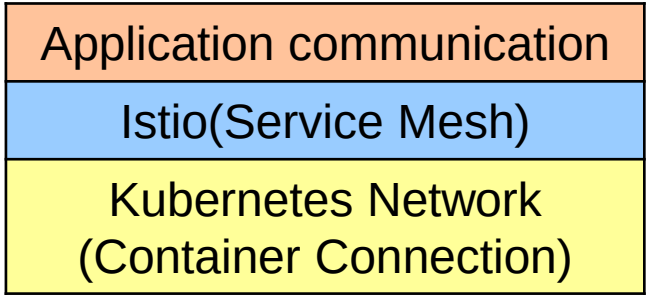
FUJITSU

Istio

Overview of Istio

FUJITSU

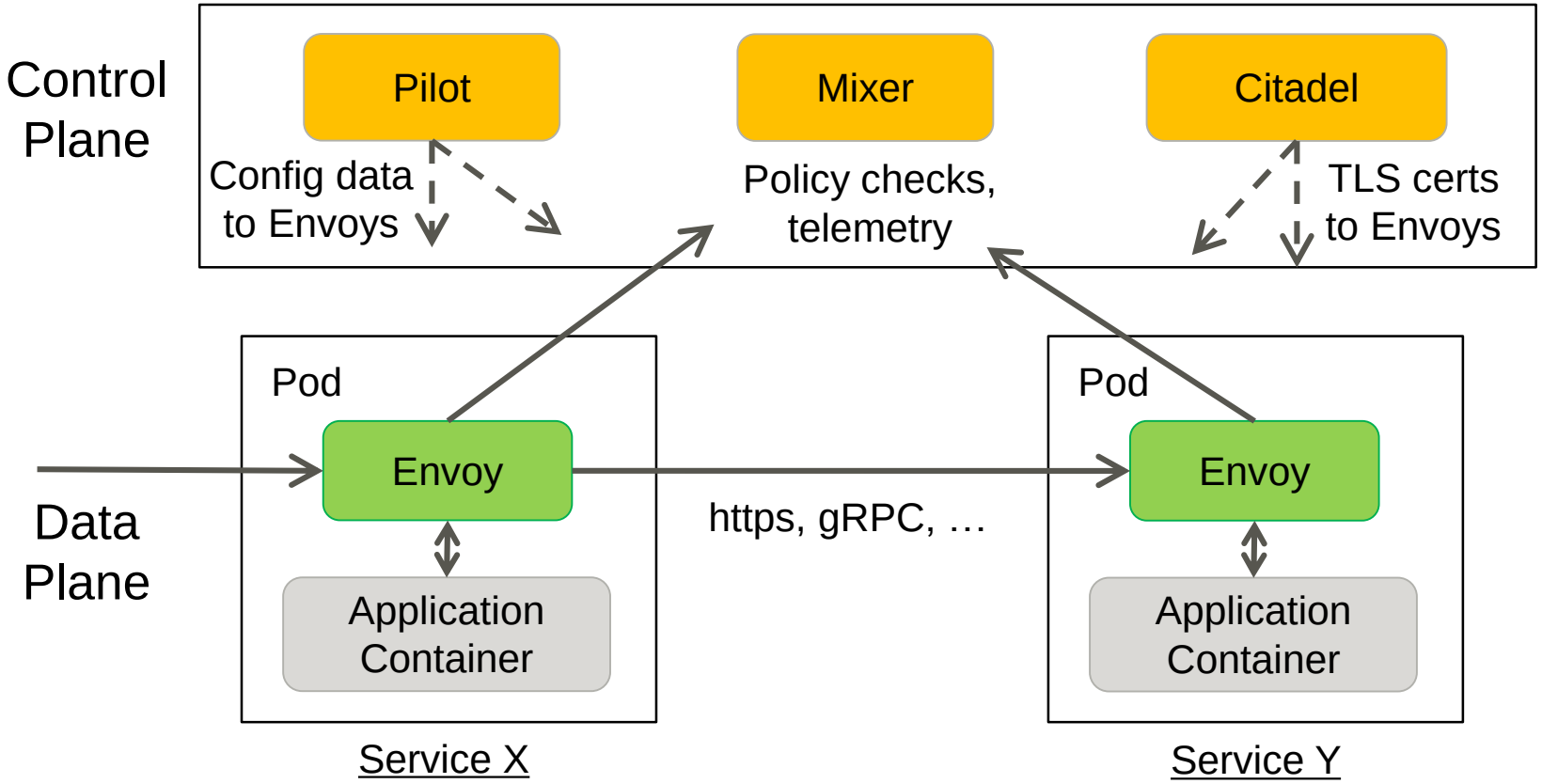
- What's Istio?
  - Network Infrastructure for services communication
  - Improve services communication
    without application code changing
- Features
  - Traffic Management
  - Policy Enforcement
  - Observability
  - Security



Network Layer Stack

Istio Architecture

FUJITSU



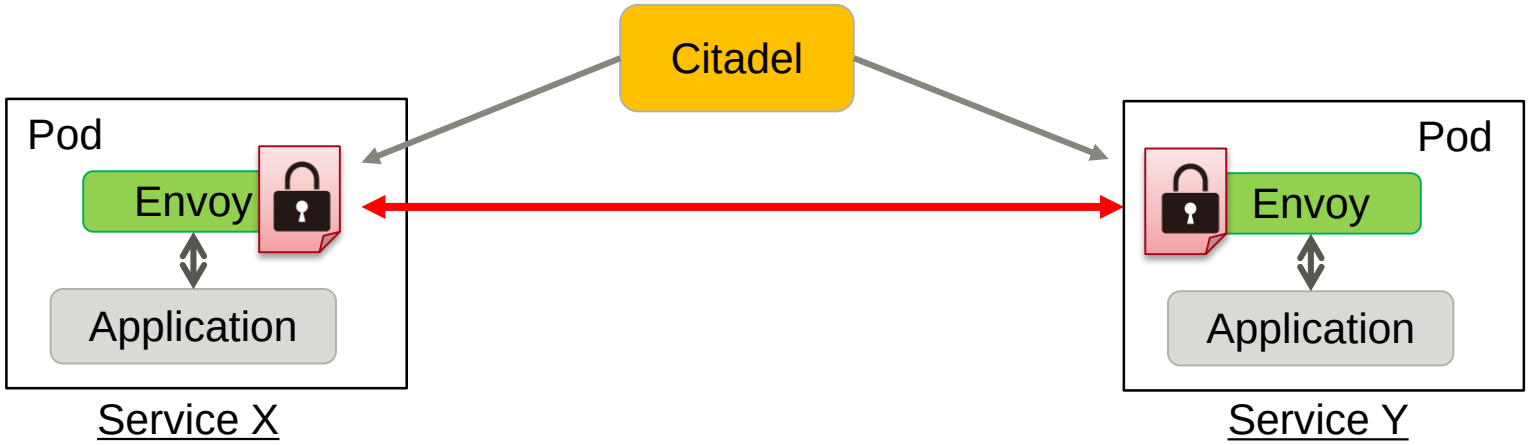
Security of Istio

FUJITSU

- How Istio secures communication between services
  1. Distribute Certificate to Envoy from Citadel
  2. Secure Communication with the Certificate

※ Citadel manage certificate

- **Automate** key and certificate generation, distribution, rotation, and revocation

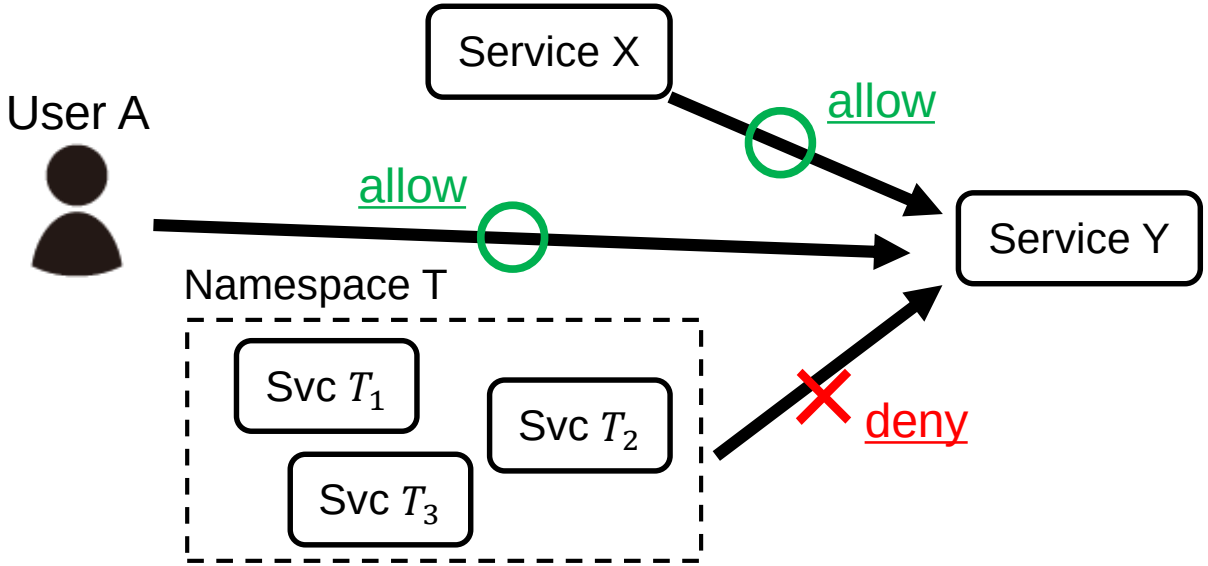


Istio Role Based Access Control(RBAC)

FUJITSU

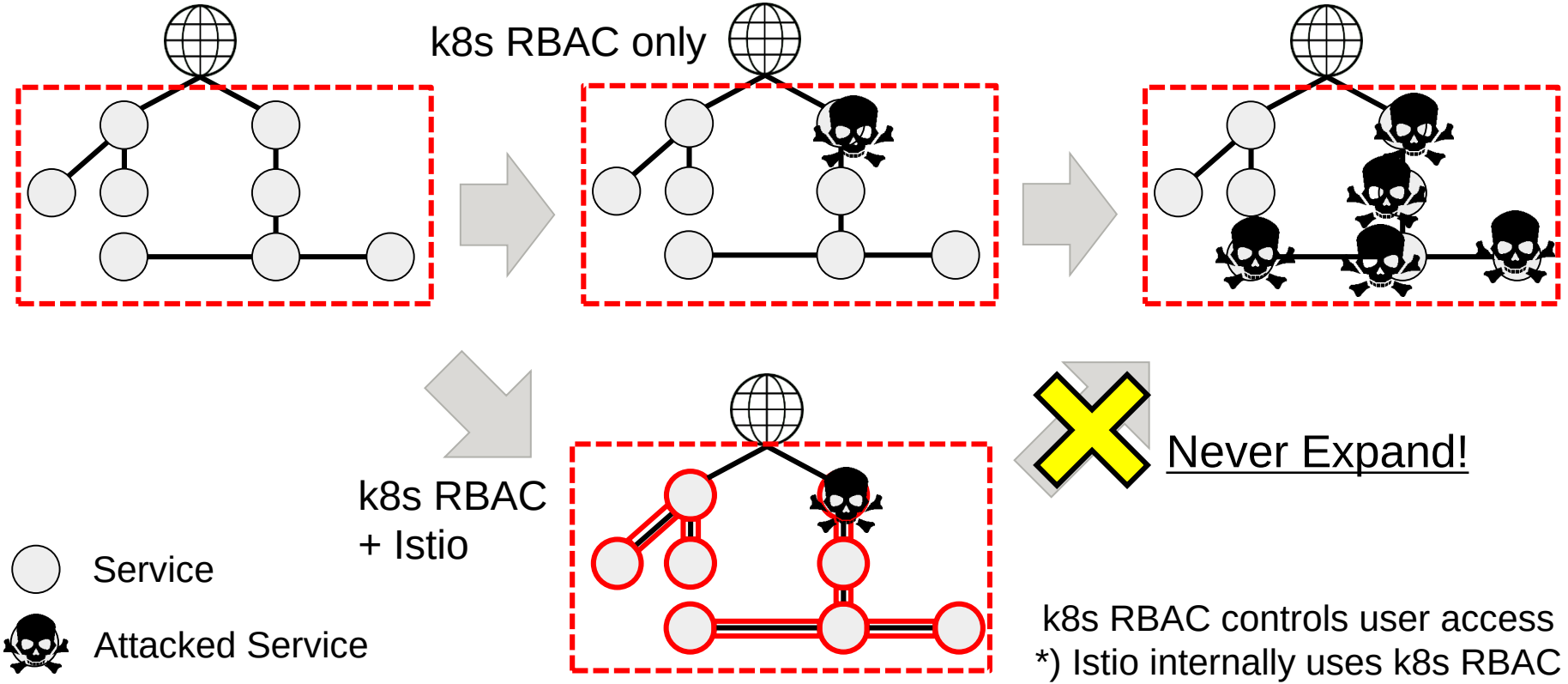
- Authorize
  - Service to Service
  - End User to Service

Istio RBAC Policy	
Service X	allow
User A	allow
Namespace T	deny



Zero Trust Network Kubernetes with Istio

FUJITSU



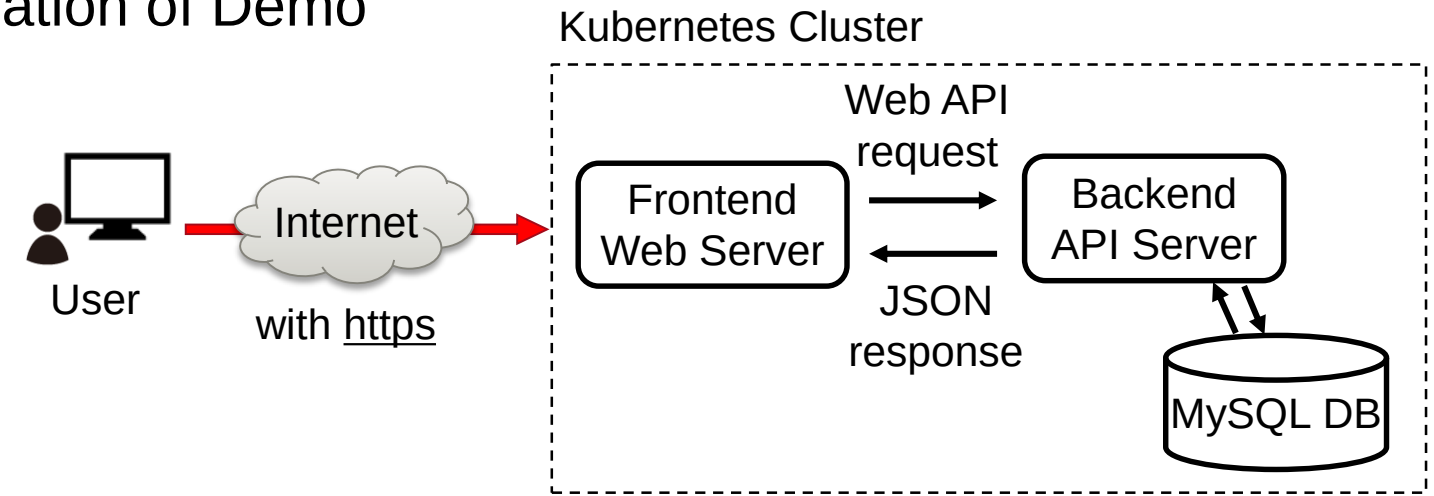
FUJITSU

Demo

*source code: https://github.com/sh-miyoshi/sectest

Demo

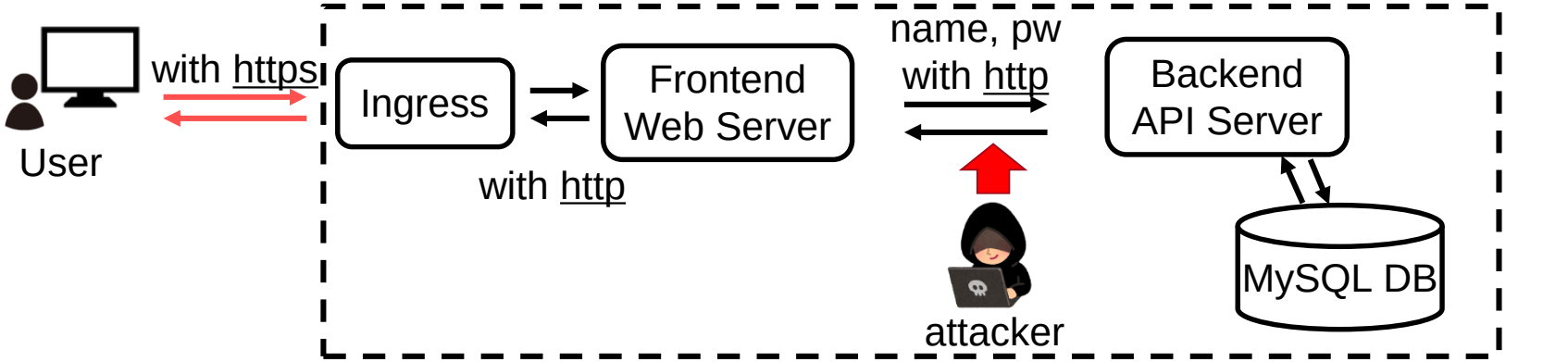
- Contents
  - Wiretap
  - Spoofing1(Already Password Leaked)
  - Spoofing2(Already Password and Certificate Leaked)
- Configuration of Demo



Demo 1

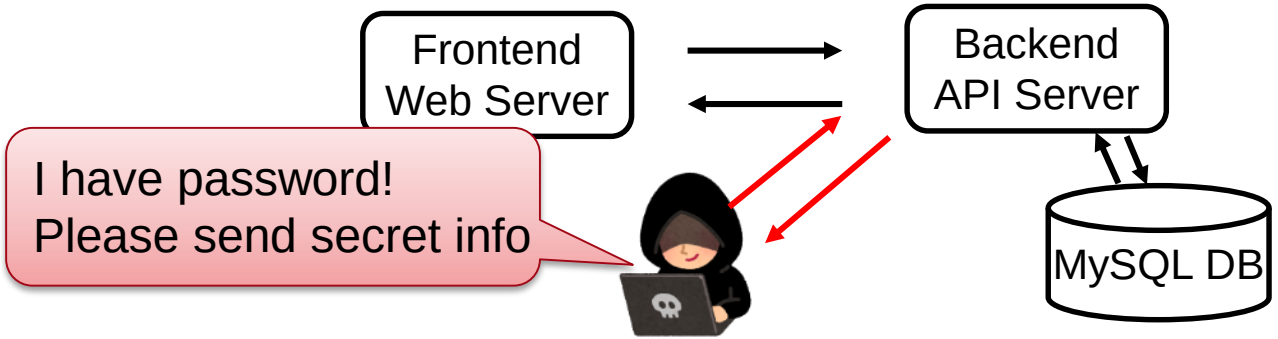
FUJITSU

- Wiretap
  - Overview of attack
    - Web Server communicate to API Server via http(not encrypt)
    - Attacker is trying to wiretap the communication
  - Countermeasure
    - All communication use https



Demo 2

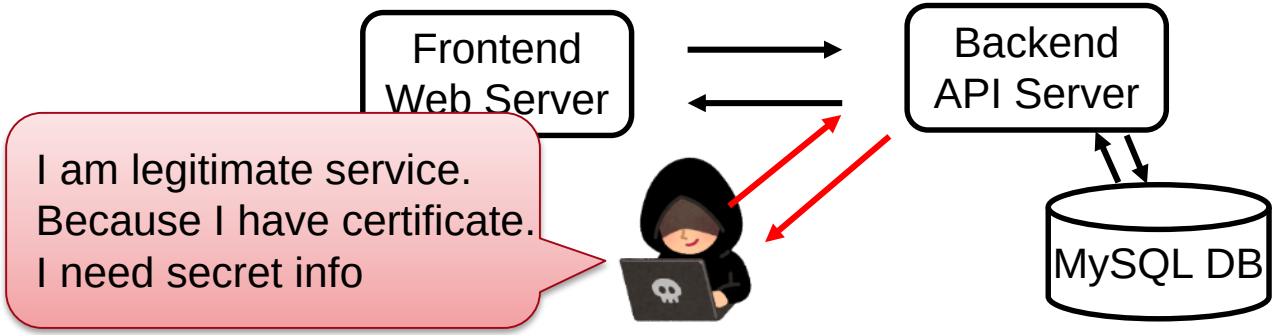
- Spoofing1(Already Password Leaked)
  - Overview of attack
    - Password of DB was already leaked. (e.g. leaked by other service)
  - Countermeasure
    - Mutual Authentication
      - Authenticate Frontend ⇔ Backend



Demo 3

FUJITSU

- Spoofing2(Already Password and Certificate Leaked)
  - Overview of attack
    - Password and Istio certificate are leaked due to sloppy management.
  - Countermeasure
    - Setting Access Policy to Service
      - default: deny
      - allow: only from Service '*Frontend*'

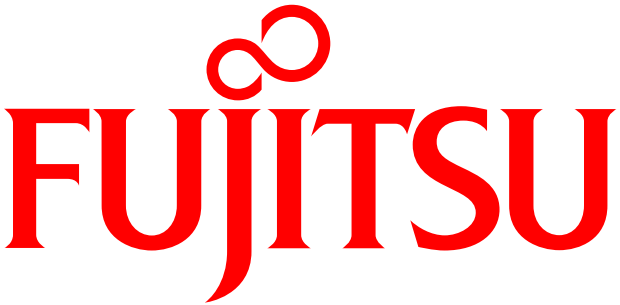


Summary

FUJITSU

- Introduction of Zero Trust Network Model
  - Attacks become more sophisticated
  - Serious damage to your business when attacked

  → Never increase the damage
- Kubernetes + Istio
  - Become more secure <u>without application code changing</u>



shaping tomorrow with you