Advanced Security on Kubernetes with Istio

20 June 2018
Shunsuke Miyoshi (s.miyoshi@jp.fujitsu.com)

Fujitsu Limited.
Outline

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

■ Increasing the number of cyber attacks

The number of Targeted e-mail attack in Japan

<table>
<thead>
<tr>
<th>Year</th>
<th># of Targeted e-mail attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>1009</td>
</tr>
<tr>
<td>2013</td>
<td>492</td>
</tr>
<tr>
<td>2014</td>
<td>1723</td>
</tr>
<tr>
<td>2015</td>
<td>3828</td>
</tr>
<tr>
<td>2016</td>
<td>4046</td>
</tr>
<tr>
<td>2017</td>
<td>6027</td>
</tr>
</tbody>
</table>

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

■ Advancing of Attacks

■ APT(Advanced Persistent Threat) Attack
  • continuously attack to special target with long period of time
Recent Cyber Attack Trends

- 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

<table>
<thead>
<tr>
<th>Previous</th>
<th>Now</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>e-Mail</strong></td>
<td><strong>e-Mail</strong></td>
</tr>
<tr>
<td>From: <a href="mailto:bheojbr@gmail.com">bheojbr@gmail.com</a></td>
<td>From: <a href="mailto:s.miyoshi@company.com">s.miyoshi@company.com</a></td>
</tr>
<tr>
<td>To: <a href="mailto:your-address@example.com">your-address@example.com</a></td>
<td>To: <a href="mailto:your-address@travel_egency.com">your-address@travel_egency.com</a></td>
</tr>
<tr>
<td>Title: You won the prize money!</td>
<td>Title: Notification of attachment of e-ticket receipt</td>
</tr>
<tr>
<td>Dear member, You won the prize money! Please click <a href="http://mysite.com">http://mysite.com</a></td>
<td>Attach: e-Ticket.pdf</td>
</tr>
<tr>
<td>Target: Anyone</td>
<td>Please check attached e-Ticket, and replay me.</td>
</tr>
</tbody>
</table>
Advancing of Targeted e-Mail Attack

Previous

<table>
<thead>
<tr>
<th>e-Mail</th>
<th>Free Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>From: <a href="mailto:bheojbr@gmail.com">bheojbr@gmail.com</a></td>
<td></td>
</tr>
<tr>
<td>To: <a href="mailto:your-address@example.com">your-address@example.com</a></td>
<td></td>
</tr>
<tr>
<td>Title: You won the prize money!</td>
<td></td>
</tr>
<tr>
<td>Dear member, You won the prize money! Please click <a href="http://mysite.com">http://mysite.com</a></td>
<td></td>
</tr>
</tbody>
</table>

Target: Anyone

Easy to find this is fake

Now

<table>
<thead>
<tr>
<th>e-Mail</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>From: <a href="mailto:s.miyoshi@company.com">s.miyoshi@company.com</a></td>
<td></td>
</tr>
<tr>
<td>To: <a href="mailto:your-address@travel_egency.com">your-address@travel_egency.com</a></td>
<td></td>
</tr>
<tr>
<td>Title: Notification of attachment of e-ticket receipt</td>
<td></td>
</tr>
<tr>
<td>Attach: e-Ticket.pdf</td>
<td></td>
</tr>
<tr>
<td>Please check attached e-Ticket, and replay me.</td>
<td></td>
</tr>
</tbody>
</table>

Target: Individually
**Advancing of Targeted e-Mail Attack**

### Previous

<table>
<thead>
<tr>
<th>e-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From:</strong> <a href="mailto:bheojbr@gmail.com">bheojbr@gmail.com</a></td>
</tr>
<tr>
<td><strong>To:</strong> <a href="mailto:your-address@example.com">your-address@example.com</a></td>
</tr>
<tr>
<td><strong>Title:</strong> You won the prize money!</td>
</tr>
</tbody>
</table>
| Dear member,  
You won the prize money!  
Please click [http://mysite.com](http://mysite.com) |

Target: Anonymously

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

### Now

<table>
<thead>
<tr>
<th>e-Mail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>From:</strong> <a href="mailto:s.miyoshi@company.com">s.miyoshi@company.com</a></td>
</tr>
<tr>
<td><strong>To:</strong> <a href="mailto:your-address@travel_egency.com">your-address@travel_egency.com</a></td>
</tr>
<tr>
<td><strong>Title:</strong> Notification of attachment of e-ticket receipt</td>
</tr>
<tr>
<td>Attach: e-Ticket.pdf</td>
</tr>
<tr>
<td>Please check attached e-Ticket, and replay me.</td>
</tr>
</tbody>
</table>

Target: Individually

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

individually targeted

Forge to PDF file
Conventional Network

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

Once Attacked • • •

Damage greatly expands
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

---

Copyright 2018 FUJITSU LIMITED
Zero Trust Network in Kubernetes

- Image of Kubernetes
Zero Trust Network in Kubernetes

- **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

Secured by RBAC

---

Copyright 2018 FUJITSU LIMITED
Zero Trust Network in Kubernetes

- 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?

Kubernetes Cluster

Secured by RBAC
Zero Trust Network in Kubernetes

- 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?

For realization

Install certificate to all application
change application code to encrypt data
※ Any Programming Language and Any Framework

Copyright 2018 FUJITSU LIMITED
# Information that Service Owner Must Manage

## Service X

<table>
<thead>
<tr>
<th>Destination</th>
<th>Certificate Path</th>
<th>Expiration date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service A</td>
<td>/etc/certs/svc_a.crt</td>
<td>2018/12</td>
</tr>
<tr>
<td>Service F</td>
<td>/etc/certs/new/svc_f.crt</td>
<td>2019/05</td>
</tr>
<tr>
<td>Service Y</td>
<td>/etc/certs/v2/svc_y.crt</td>
<td>2019/01</td>
</tr>
</tbody>
</table>

- How to install certificate in Ruby on Rails
- How to install certificate in Apache Web Server

...
Information that Service Owner Must Manage

<table>
<thead>
<tr>
<th>Service X</th>
<th>Destination</th>
<th>Certificate</th>
<th>Expiration date</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Service A</td>
<td>/etc/certs/svc_a.crt</td>
<td>2018/12</td>
</tr>
<tr>
<td></td>
<td>Service F</td>
<td>/etc/certs/new/svc_f.crt</td>
<td>2019/05</td>
</tr>
<tr>
<td></td>
<td>Service Y</td>
<td>/etc/certs/v2/svc_y.crt</td>
<td>2019/01</td>
</tr>
</tbody>
</table>

All service owner must manage them

Too hard …

Istio as a Manager of Service Communication Security
Istio
Overview of Istio

What's Istio?
- Network Infrastructure for services communication
- Improve services communication without application code changing

Features
- Traffic Management
- Policy Enforcement
- Observability
- Security
Istio Architecture

Control Plane

- **Pilot**: Config data to Envoys
- **Mixer**: Policy checks, telemetry
- **Citadel**: TLS certs to Envoys

Data Plane

- **Pod**: Envoy
  - Application Container
  - Service X: https, gRPC, ...

- **Pod**: Envoy
  - Application Container
  - Service Y
Security of Istio

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)

- Authorize
  - Service to Service
  - End User to Service

<table>
<thead>
<tr>
<th>Istio RBAC Policy</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Service X</td>
<td>allow</td>
</tr>
<tr>
<td>User A</td>
<td>allow</td>
</tr>
<tr>
<td>Namespace T</td>
<td>deny</td>
</tr>
</tbody>
</table>

Service Y

Service X

User A

allow

Namespace T

Svc $T_1$

Svc $T_2$

Svc $T_3$

deny
Zero Trust Network Kubernetes with Istio

Service
Attacked Service

k8s RBAC only

Never Expand!

k8s RBAC controls user access
*) Istio internally uses k8s RBAC

k8s RBAC + Istio
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

![Diagram of Demo configuration including Internet, User, Frontend Web Server, Backend API Server, Kubernetes Cluster, and MySQL DB with https connection.]
Demo 1

- **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

![Diagram of communication flow](image_url)
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

I have password! Please send secret info
Demo 3

- 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'

I am legitimate service. Because I have certificate. I need secret info
Summary

- 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 without application code changing
FUJITSU
shaping tomorrow with you