Let us know what you think

Click ‘engage’ to rate sessions and ask questions

Follow us on Twitter @GOTOber

www.gotober.com
Microservices – a security nightmare?

GOTO Berlin - Dec 2, 2015
Maximilian Schöfmann
Container Solutions Switzerland
Jetzt reisen: ZU LAST MINUTE-PREISEN!

HolidayCheck

Wer nicht checkt, reist dumm.
microservices...

small, hence many services
talking over the network
built with different technologies
by autonomous teams with end-to-end responsibility
doing DevOps and Continuous Delivery
using containers
many small services
talking over the network
Java 7
(1.7.0_03)
built with different technologies

Java 8
nodejs 0.9
Ruby 2.1
Java 7
Go 1.4
by autonomous teams
with end-to-end responsibility
doing **DevOps**

**OWASP** ??
and Continuous Delivery
using containers
using containers

XEN Hypervisor - $10^5$ LOC

Linux Kernel - $10^7$ LOC
Welcome to your new nightmare.

A Nightmare on Elm Street
many small services
talking over the network

user_db

payment_data

cat_pictures

(stateless)

(stateless)
talking over the network
Authentication: Basic Auth

Authorization: Basic c21hcnc3Muc21hcnRhc3MuLi4uCg==
Authentication: Client certificates
Authentication: API Keys

X-My-API-Key: YWxsIHVyIGJhc2UgYXJlIGJlbG9uZ3MgMiAgdXMk
Authentication: HMAC

Authorization: AWS FOOBR7EXAMPLE:frJIUN8h81ADYpKg=
Secrets management

talking over the network

vaultproject.io

square.github.io/keywhiz
Single-Sign-On

talking over the network
Single-Sign-On

talking over the network

client
authenticate
token
request with token

SSO
verify
send response

service
Single-Sign-On

talking over the network
Authorization

talking over the network
Authorization

```json
{
    "iss":"myservice@developer.gserviceaccount.com",
    "scope":"https://www.googleapis.com/auth/bigquery",
    "aud":"https://www.googleapis.com/oauth2/v3/token",
    "exp":1328554385,
    "iat":1328550785
}
```
ID Tokens

```json
{
    "sub" : "bob",
    "email" : "bob@example.com",
    "name" : "Bob Example",
    "exp" : 1328672194,
    "https://mycorp.tld/groups" : ["admin", "publisher"]
}
```
Translating ID Tokens

talking over the network

Gateway

Service A

Service B

Service C

dumb token

JWT

JWT
The Confused Deputy
API Gateways

• Access control
• Rate limiting
• HTTPS termination

...
API Gateways
built with different technologies
by autonomous teams
with end-to-end responsibility
Trust by autonomous teams with end-to-end responsibility

Accountability
Expertise
Autonomy & Entrepreneurship
Collaboration & Support

Idea from A.T. Kearny Analysis
Definition of Done

“It’s not done, before it’s fast!”
Definition of Done

“It’s not done, before it’s secure!”

by autonomous teams with end-to-end responsibility
Rugged Software Manifesto

by autonomous teams with end-to-end responsibility

ruggedsoftware.org
doing DevOps

SecDevOps?

SecOps?

DevSec?
doing **DevOps**

SecDevOps = Mindset + Tooling
and **Continuous Delivery**
Test pyramid

from “Succeeding with Agile” (Mike Cohn)
Security-Test pyramid

- E2E security tests
- Vulnerability scanning
- static code analysis

and continuous delivery
BDD style

Scenario: Passwords should be case sensitive
Meta: @id auth_case
When the default user logs in with credentials from: users.table
Then the user is logged in
When the case of the password is changed
And the user logs in from a fresh login page
Then the user is not logged in
using **containers**

- **1982** chroot
- **2000** BSD Jails
- **2001** Virtuozzo
- **2004** Solaris Zones
- **2007** cgroups
- **2008** LXC
- **2013** Docker
- **2014** rkt
Defense in depth

payment service instance #2
docs upload service instance #1

bookmark manager instance #1

payment service instance #1
cat picture service instance #1
meme generator instance #1

using containers
Freeze & replace

- payment service instance #2
- docs upload service instance #1
- bookmark manager instance #1
- payment service instance #1
- cat picture service instance #1
- meme generator instance #1

using containers
Freeze & replace

- payment service instance #2
- docs upload service instance #1
- payment service instance #3
- bookmark manager instance #1
- cat picture service instance #1
- meme generator instance #1
Docker security

- read-only containers
- minimal base images
- drop capabilities
- verify signed images
- traditional hardening (AppArmor, SELinux...)

	tinyurl.com/docker-security
Scan images for vulnerabilities

**Nautilus** (Docker Inc.)

**Clair** (CoreOS)

**Twistlock**

**Scalock**
Secure deployments

Docker daemon - “just HTTP”

- TLS
- Authentication
- Authorisation
- Logging & Auditing
Summary

small, distributed services can limit the impact of breaches

isolate services with different security requirements

use standard mechanisms for auth, but make sure they are scalable

consider an API gateway, but don't overuse this pattern
Summary

Monocultures can do harm

Embrace rugged software principles

Accountability ensures security is built in, not bolted on

Invest in automation and tooling around security tools and security testing
Summary

use containers as additional line of defense

use containers as immutable infrastructure

if you need to, use containers to do forensics

secure your container hosts thoroughly

scan images centrally for vulnerabilities

abolish obsolete deployment methods
Nightmare?
Image References
(all CC-BY or public domain)

Pumpkin:
https://www.flickr.com/photos/wwarby/5144858705

Bill Gates:
https://c2.staticflickr.com/8/7331/16335705267_b6e9d9b223.jpg

Anarchy Symbol:
https://pixabay.com/p-32917/

Sandwich:
https://upload.wikimedia.org/wikipedia/commons/6/6a/Peanut-Butter-Jelly-Sandwich.png

Wasp:
https://pixabay.com/p-538470

Whack-a-mole:
https://c1.staticflickr.com/9/8484/8195620894_4b68d7df76_b.jpg

Rusty container:
https://www.flickr.com/photos/annspan/3912153466

Server:
https://upload.wikimedia.org/wikipedia/commons/0/0c/Chassis-Plans-3U.jpg

Rugged vehicle:
https://c1.staticflickr.com/5/4036/4669861882_742023ed7a_b.jpg

Certificate:
https://pixabay.com/p-576790

Confused Deputy:

Aphid:
container-solutions.com
Please Remember to rate session Thank you!

Follow us on Twitter @GOTOber

www.gotober.com