Towards Securing Micro-Services

UNCC CSC 2016

By: John Melton
Y'ALL
AGENDA

1. WHAT IS MICRO-SERVICES?
2. WHAT IS MICRO-SERVICES SECURITY?
   - CHALLENGES
   - BENEFITS
   - HOW-TO
3. A (BRIEF) LOOK AT THE FUTURE
WHAT
EXACTLY
ARE
MICRO-SERVICES?
MICRO-SERVICE
MICRO-SERVICES

1 “APP,” MANY SERVICES
LIGHTWEIGHT COMM
AUTOMATED, INDEPENDENT DEPLOYMENT
LANGUAGE AGNOSTIC
DATA-STORAGE AGNOSTIC
WHAT IS MICRO-SERVICES SECURITY?
WHAT IS MICRO-SERVICES SECURITY?

- TEAM
- ARCH
- DEV
- OPS
TEAM
CHALLENGES

CULTURE

CHANGE NOOOOO!

TEAM CONFIGURATION
HOW TO EXPLOIT

DRIVE CULTURE CHANGE

TEAM OWNS PRODUCT

FOCUSED SEC TRAINING

SIMPLE SUCCESS MEASUREMENTS

CELEBRATE SUCCESSES
CHALLENGES

DIST. SYSTEMS ARE HARD

PEOPLE/TEAMS AFFECTS EVERYTHING

ARCH TOOLING

PARTIAL DATA + CACHING
CHALLENGES

I AM

⇒

ARCH IS HUGE

⇒

TOOLING STACK CHANGES
BENEFITS

ISOLATE SECURITY SERVICES

SECURITY SERVICES
(SEC AAS)

IAM
(BY NECESSITY)
BENEFITS

VS.

DATA HIDING

VS.

ATTACK SURFACE REDUCTION
HOW TO EXPLOIT

ISOLATE SECURITY SERVICES & THREAT MODEL

REQUIRE I AM

DISCUSS PRIVACY

LIMIT ARCH'S/LANG'S
HOW TO EXPLOIT

MAP

ATTACK SURFACE

LIVE ARCH DIAGRAMS
DEV
CHALLENGES

FAILURE MODES

LANG / FRAMEWORK SELECTION

PROTOCOL SELECTION

API CONTRACT SPRAWL
BENEFITS

- SECURITY
- UX

VS.

LIMITED LANGS & DSLs
HOW TO EXPLOIT

DDD + DDS

RELEASE

TRAINING CLOSEST TO DEVELOPER

SETUP HARNESS

TESTING
HOW TO EXPLOIT

- PICK ME!

- ME
- DEPS

- KNOW YOUR DEPENDENCIES

- STANDARD AND SECURITY TOOLING

- EXPLOIT CI
HOW TO EXPLOIT

Pick 1 Protocol per interaction

Validate everywhere

Common controls framework

Trust boundaries

Input validation

Code sensitive review components
CHALLENGES

RESOURCE SPRAWL vs. RESOURCE LIMITS

I'm tuning servers...???
CHALLENGES

I'm making network changes now???

Credentials everywhere

Differently scaled systems

VS. TLS complexity
CHALLENGES

AARON GRATTA FIORI'S PAPER IS OUTSTANDING

CONTAINERS!

AND ORCHESTRATION

I OWN ALL THE THINGS
BENEFITS

FORCES MONITORING

SECURITY TOUCHPOINTS IN CI

CONSTRAINTS DON'T ALLOW CRUFT

CONFIG MGMT TOOLING
Benefits

CRED STORAGE VAULT

VS.

SERVICE SCALING

TLS CA
BENEFITS

CONTAINERS & ORCHESTRATION

VS.

VISIBILITY & SELF-PROTECTION
HOW TO EXPLOIT

CAP

vs. ALPINE

BENCH

37
HOW TO EXPLOIT

CI
SCANNING

- PUPPET
- CHEF
- ANSIBLE
- SALT

LETS ENCRYPT

TLS

VAULT
CFSSL
HOW TO EXPLOIT

FOCUS ON MONITORING

SELF DEFENDING APPS

RUNTIME INTELLIGENCE

BLOW STUFF UP!
BATMAN, I CAN SEE THE FREAKIN FUTURE!

CAN YOU SEE THIS COMING?
TO THE FUTURE

- NETFLIX
- BEYOND CORP
- SPIFFE.10
- Aaron Gratta Fiori's Understanding & Hardening Containers

- JVNS.ca Slide Format

- Papers/Systems We Love
THANKS

? 

twitter: @-jtmelton

github: jtmelton

email: jtmelton@gmail.com