ChaoSlingr: Introducing Security-Based Chaos Testing

Aaron Rinehart  
*Chief Enterprise Security Architect*  
UnitedHealth Group

Grayson Brewer  
*IT Security Consultant*  
UnitedHealth Group
Security + Chaos = Security Experimentation
About Aaron

Aaron Rinehart
Chief Enterprise Security Architect
UnitedHealth Group

Contact Info
Rinehart.Aaron@gmail.com
@aaronrinehart
About Grayson

Grayson Brewer
Security Consultant
UnitedHealth Group

Contact Info
e.grayson.brewer@gmail.com
@BrewerSecurity
Overview UnitedHealth Group

**The Challenge: We are Large & Complex**

- Fortune 6 Company
- 360+ Companies & Growing
- 28,000+ Developers
- 8,000+ Applications
- HIPAA, HITRUST, FISMA, MARS-E, GDPR, ICFR(++++++)
- United Nations of Technology
- Largest Healthcare Company in World
- 1000+ Security Professionals
- Multinational Business
- Some DevOps
- Waterfall, Agile, & Others
- Security Testing: Mostly Human Driven
- Cloud Journey: Mixed
IN This Session We will Cover
A Tool to Build or a Weapon to Destroy?

Failure
A Tool to Build
Or a
Weapon to Destroy?
The Reality is......

**FAILURE HAPPENS.**

*Saturday, January 13*

**Emergency Alert**
BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL.
Slide for more
Failure is Necessary

Humans need failure to learn & grow
So... what does this have to do with Security?
2017 Causes of Data Breaches

- Malicious Attacks: 47%
- Human Error: 25%
- System Glitches: 28%
Where do Security Failures come from?

- Bugs
- Assumptions
- Code Quality
- Misconfiguration
- Complexity in Distributed Systems
- Complexity in Security Control
- Defect
- Coverage Gaps
- Miscommunication
- Human Error
- Computer Error
- Lack of Monitoring
- Poor Testing Practices
- Untested Scalability
- Single Points of Failure
- Failures in External Dependencies
- Vulnerabilities
The Gap b/t Modern Software & Security

**Modern**

**Software is...**
- Highly Distributed
- Stateless
- Iterative
- Rapid Change Evolution
- Very Complex

**Security is...**
- Mostly Monolithic
- State Dependant
- Static
- Preventative Design
- Complex

UNITEDHEALTH GROUP™
Distributed Systems Are Tricky

Distributed Systems can have unpredictable outcomes
Distributed Systems Are Tricky
Don't Drift into the Unknown

How do we avoid drifting into the unknown?
Don’t look for a better answer, instead...
Ask better questions
How does my security really work?
Ask yourself.........

AM I SURE IT WORKS
THAT WAY?
Ask yourself........

How would I know?

Ask
So in fact do we identify Security Failures?

Logs??

Security Scans??

Penetration Tests?

Monitoring Tools??

Security Incidents!!!!
Its tooooooo late.....

SECURITY INCIDENTS ARE NOT DETECTIVE MEASURES
It worked for Rebel Alliance but not here

IS NOT A STRATEGY
Build Confidence through Instrumentation

BUILD CONFIDENCE IN WHAT ACTUALLY WORKS
What is Chaos Engineering?

"Chaos Engineering is the discipline of experimenting on a distributed system in order to build confidence in the system's ability to withstand turbulent conditions."

UNIVERSAL

UNITED HEALTH GROUP®

RSA® Conference 2018
A brief history of Chaos
The New Playbook

Security Experimentation
Do Less, Better

DON'T JUST TEST.... EXPERIMENT
Testing vs. Experimentation
What's the Difference?

- **Testing** is assessment or validation of an expected outcome

- **Experimentation** seeks to derive new insights and information that were previously unknown
Security Experimentation: A Definition

“THE SECURITY DISCIPLINE OF EXPERIMENTATION IN ORDER TO BUILD CONFIDENCE IN THE SYSTEM’S ABILITY TO DEFEND AGAINST MALICIOUS CONDITIONS.”
Be Objective & Use Failure as a Tool

- Drive out failure.
- Observe failure.
- Learn from failure.
- Build resilient systems.
“Wow, I wasn’t expecting that to happen.” - You, learning something
Why do it?

- **Build Confidence** in Security Measures
- **Strengthen** Incident Management
- **Measure** Incident Response Readiness
- **Identify Security Failures** within the Security Control Plane
- **Proactively Detect** Security Failures
- **Measure Investments** in Security Technology
GameDays + Post Mortem

GAME DAY EXERCISES
Value of Game Day Exercises

- Provides Objective Measurement for Security Incident Response
- Identify Control Coverage Gaps
- Keeping the Team Sharp and “Battle Ready”

“If you’re not cultivating a Learning Culture, you will probably end up losing to someone else who is.”
Open Source Security Experimentation Tool

ChaoSlingr

AN OPEN SOURCE TOOL
So, eh, what is it exactly
FYI ChaoSlingr is on Github (FREE!)

ChaoSlingr

- ChatOps Integration
- Configuration-as-Code
- Example Code & Open Framework
- Serverless App in AWS
- 100% Native AWS
- Configurable Operational Mode & Frequency
- Opt-In | Opt-Out Model
An Example Experiment Using ChaoSlingr

PortSlingr

*Example ChaoSlingr Experiment*

*Unauthorized Port Change*
An Example Security Experiment

**Example: Unauthorized Port Change**

1. List **Available EC2 VPC Security Groups** within Account
2. Select **only** those **Security Groups** that are "Tagged" with the **Opt-In Tag** for Chaos Testing
3. Randomly Select a **Security Group within the Opt-In Model Pool**
4. Apply a Random **Open or Close Port Action** based on Existing Port Configuration

PortSlingr
How the experiment works

**Experiment Framework**

Applies the configured change

Kicks off the experiment, Performs **Target Acquisition**, and Stages **Target** for changes

Tracks changes made by Generatr. Triggered by monitoring events that are monitoring for changes.
Summary: Takeaways

- Security Problems in Distributed Systems
- Chaos Engineering
- Security Experimentation
- ChaoSlingr: Open Source Tool
- Think Differently, Be Objective
Apply What You Have Learned Today

- Next week you should:
  - Start asking yourself the Right Questions
  - Go to Github and check out ChaoSlingr
  - Find out if your organization has an Site Reliability Engineer and tell them what you learned in this talk.

- In the first three months following this presentation you should:
  - Conduct your first GameDay Exercise and manual Security Chaos Experiment
  - Attend a Chaos Engineering Community Event near you

- Within six months you should:
  - Write your own experiments for ChaoSlingr or your own tool.
  - Run your first automated Security Chaos Experiment
The New Normal: Continuous Evolution

THINK DIFFERENTLY

"If it ain’t broke, try harder.
Chaos Philosophy"
Hit us with some questions

Questions

@aaronrinehart
@BrewerSecurity

BE EXCELLENT TO EACH OTHER