CHAOS SECURITY ENGINEERING: INTEGRATING SECURITY THROUGH CHAOS

By: Nikki Robinson, DSc, PhD
All thoughts, feelings, views expressed in this presentation are my own. They do not reflect my employer/s. All views or opinions expressed in this presentation are personal and belong solely to me. They do not reflect the people, institutions, or organizations that I may or may not be associated with in a professional / personal capacity. Any views or opinions are not intended to malign any person, place, or organization.
INTRODUCTION

• Security Architect, IBM
• Adjunct Professor, Capitol Technology University
• ICIT Fellow (2022–2023)
• President, InfraGard Maryland
• Doctorate of Science (DSc), Cybersecurity
• PhD, Human Factors
AGENDA

• DevSecOps
• Chaos Engineering
• Chaos Security Engineering (CSE)
• Hypothesis-Based Testing
• Benefits of CSE
• Open-Source Information
DevSecOps

Integration of developers, security, operations

More than tools or process - but communication between teams

Security in Agile - continuous iteration

Security engineers working during design and development phases
Not actually based in chaotic functions or methods

Hypothesis-based approach to testing, breaking, fixing

Build research questions and hypotheses based on possible problems

Identify misconfigurations before they become a major problem

Similar to penetration test methodology – how can I break (into) this?

Reference: https://principlesofchaos.org/
CHAOS SECURITY ENGINEERING

Build a hypothesis / steady state behavior
What security baselines exist? Are configurations similar across configurations?

Real-World Events
Threat intelligence data injected into code?

Experiments in Production
Authentication, encryption, security control expectation, passwords saved

Automate / Iterate
Integrate security testing / continuous monitoring

Reference: https://principlesofchaos.org/
HYPOTHESIS-BASED TESTING

- Confirmation Bias - expectations vs reality
- Environmental factors - cloud-based? Micro-application development?
- Causation vs correlation
- Identifying / defining variables
- Anchoring and Accessibility

MATURING A DEVSSECOPS PROGRAM

• What is the current / steady state of the program
• What skills / characteristics do your developers have?
• What is the ultimate goal of the project?
• Who do you need to hire? Who can be upskilled?
• Once program is in place – sprinkle in a little chaos
BENEFITS OF CHAOS SECURITY ENGINEERING (CSE)

• Integrate more security engineering skills/practitioners on the team
• Improve the reputation and usability of the product
• Security is not a point in time - able to measure the moving needle
• Reduce cost of security at the end of projects
• Don’t rely just on tools and processes - use hypotheses
• Move to a predictive security model
Combination of vulnerabilities to create critical attacks

Consider low and medium vulnerabilities for hypothesis-based testing

Not just chaining vulnerabilities - it’s about the methodology

What are the known-knowns and unknown-unknowns

Vulnerability Chaining Blindness (VCB)

OPEN-SOURCE INFORMATION

• Security Chaos Engineering (Rinehard, A, and Shortridge, K.)
  • https://www.oreilly.com/library/view/security-chaos-engineering/9781492080350/

• DevSecCon – Security Chaos Engineering - What is it and why should you care?

• Tools to conduct security chaos engineering tests
  • https://www.techtarget.com/searchsecurity/feature/Tools-to-conduct-security-chaos-engineering-tests

• ChaoSlingr
  • https://github.com/Optum/ChaoSlingr
QUESTIONS/THOUGHTS?