# Systemic Risk & Vulnerability Analysis of Multi-Cloud Environments

This presentation was given at the 2023 National Cybersecurity Education Colloquium

**Program Name: INSuRE+C**

**Teams**: Mississippi State University, Rochester Institute of Technology
**Technical Directors**: National Security Agency

**October 2022 - September 2023**

# Team Members

This presentation was given at the 2023 National Cybersecurity Education Colloquium

**NSA**

- Dr. Josiah Dykstra
- Dr. Andy Sampson

**RIT**

- Dr. Nidhi Rastogi
- Matthew Stoffolano - MS Student

**MSU**

- Dr. Sudip Mittal
- Morgan Reece - PhD Student
- Teddy Lander - MS Student

# Agenda

- Introduction
  - Problem Motivation
  - Industry Modeling
- Modeling Framework
- Risk Analysis & Explanation
- Attack Implementation
- Results & Future opportunities

This presentation was given at the 2023 National Cybersecurity Education Colloquium

# Introduction

This presentation was given at the 2023 National Cybersecurity Education Colloquium

**Problem Statement**: Multi-Cloud application deployment has caused highly fragmented approach toward security, leading to a constant rise of new attack vectors and potential vulnerabilities.

**Project Phases:**

1) **Systemic Risk & Vulnerability Analysis of Multi-cloud Environments**
2) **Identify Novel Attacks Patterns & Risk Mitigation in Multi-cloud Environments**
3) **Develop & Evaluate Defensive Strategies to Secure Multi-cloud Environments**

# Phase 1 - **Systemic Risk & Vulnerability Analysis of Multi-cloud Environments**

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Architecture definition

3-tier mutli-cloud architecture

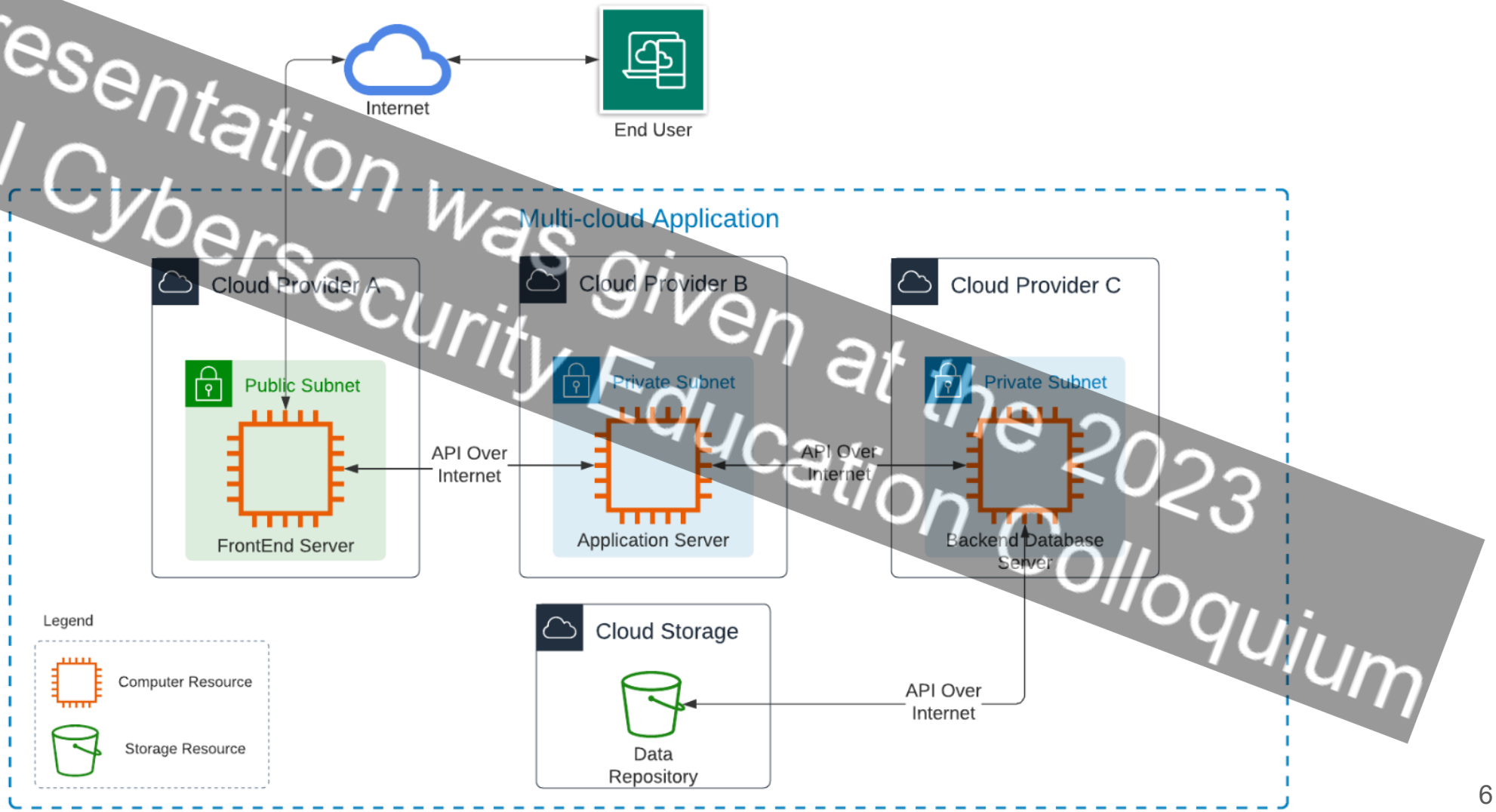
Identify industry for modeling and analysis

Attack vector identification

Define Risk Analysis Methodology

STRIDE & DREAD to be used in conjunction with each other for full scoped analysis

# Multi-Cloud Architecture




This presentation was given at the 2023 National Cybersecurity Education Colloquium

# Healthcare Industry Modeling and Analysis

- Risk assessment begins with Business Impact Analysis (BIA)
  - BIA requires organizational operations to determine impact
  - Enables defining basis of value of data
- BIA drives organizational risk analysis
- Defined architecture found extensively in healthcare industry
  - Either through internal development or acquisition, 90% of healthcare organizations plan on using multiple cloud service providers[1]

[1] https://www.hitinfrastructure.com/features/pros-cons-and-strategies-for-implementing-healthcare-multicloud/

This presentation was given at the 2023 National Cybersecurity Education Colloquium

# Attack Vector Categories

Identifying attack vectors that are unique to multi-cloud application deployments.

1. Architecture
2. API
3. Authentication
4. Automation
5. Difference in Management
6. Mismatch in Cyber Legislation

This presentation was given at the 2023 National Cybersecurity Education Colloquium

# STRIDE use in Risk Analysis and Mitigation

This presentation was given at the 2023 National Cybersecurity Education Colloquium

**STRIDE Threat Modeling Methodology**

**Objective** - Identify, categorize, and analyze attacks into 6 types of threats: Spoofing, Tampering, Repudiation, Information disclosure (privacy breach or data leak), Denial of service, Elevation of privilege

**Benefits** - Proactive exercise in identifying threats and developing mitigations

**Selection of Methodology** - Used in all scenarios of threat modeling and risk analysis; one of the most commonly used threat modeling framework

# DREAD Methodology

This presentation was given at the 2023 National Cybersecurity Education Colloquium

**DREAD Risk Assessment Methodology**

**Objective** - Quantitatively assess the severity of a cyberthreat using a scaled rating system that assigns numerical values to risk categories

**Benefits** – Very customizable methodology requiring extensive cybersecurity experience to ensure accurate analysis

**Selection of Methodology** - Focuses on impact and operability

# Phase 2 - **Perform risk & vulnerability analysis**

Risk analysis

- Application of STRIDE and DREAD to threat vectors identified in Phase 1

Risk mitigation

- Utilizing MITRE ATT&CK Framework to support mitigation definition

Research and design simulation environment

- Cloud providers and possible applications

This presentation was given at the 2023 National Cybersecurity Education Colloquium

# Architecture Threat Risk Analysis

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Risk Score calculated from DREAD model:

avg_damage = (Legal + Reputation + Productivity)/3

threat_probability = (Reproducibility, Exploitability, Affected Users, Discoverability)

**DREAD Risk Score = (avg_damage) + Σ threat_attributes**

Overall Threat Rating from DREAD Risk Score

- **Critical (40–50):** Critical vulnerability; address immediately.
- **High (25–39):** Severe vulnerability; consider for review and resolution soon.
- **Medium (11–24):** Moderate risk; review after addressing severe and critical risks.
- **Low (1–10):** Low risk to infrastructure and data.

# High Risk Attack Vectors – Risk Analysis Results

| | | | Damage | | | Threat Attributes | | | |
|---|---|---|---|---|---|---|---|---|---|
| Description of Threat | STRIDE Framework Category | Total Risk Score | Legal Damage | Reputation Damage | Productivity Damage | Reproducibility | Exploitability | Affected Users | Discoverability |
| Architecture: CVEs | ALL | 44.00 | 0 | 9 | 9 | 9 | 10 | 10 | 9 |
| Architecture: DoS attacks | Denial of Service | 42.67 | 0 | 10 | 10 | 8 | 8 | 10 | 10 |
| Automation : Data poisoning | Tampering with Data | 34.33 | 0 | 4 | 6 | 10 | 10 | 8 | 3 |
| Authentication : Man-in-the-Middle | Information Disclosure | 32.67 | 0 | 9 | 5 | 7 | 9 | 10 | 2 |
| API : Malformed packets | Denial of Service | 32.00 | 0 | 6 | 9 | 8 | 7 | 3 | 9 |
| Architecture: Differing Encryption Offerings and Capabilities | Information Disclosure | 30.33 | 0 | 6 | 7 | 7 | 8 | 4 | 7 |
| Authentication : Substitution attack | Denial of Service | 29.33 | 0 | 7 | 9 | 10 | 10 | 2 | 2 |
| API : Privilege Elevation | Elevation of Privilege | 28.00 | 0 | 9 | 6 | 8 | 10 | 3 | 2 |
| Automation : Dynamic changes to config causing inconsistency | Denial of Service | 27.33 | 0 | 5 | 8 | 5 | 8 | 7 | 3 |
| Difference in Management: Auto-Scaling | Denial of Service | 25.67 | 0 | 8 | 9 | 6 | 5 | 7 | 2 |
| Authentication : Session hijacking | Spoofing Identity | 25.67 | 4 | 6 | 4 | 7 | 8 | 1 | 5 |
| Architecture: VPN Infiltration | Information Disclosure | 25.33 | 0 | 8 | 5 | 6 | 9 | 2 | 4 |

This presentation was given at the 2023 National Cybersecurity Education Colloquium

# High Risk Attack Vectors – Countermeasures and mitigations

| Description of Threat | STRIDE Framework Category | Total Risk Score | Countermeasures | MITRE ATT&CK Mitigation |
|---|---|---|---|---|
| Architecture: CVEs | ALL | 44.00 | Patch Management - System Hardening | Patch |
| Architecture: DoS attacks | Denial of Service | 42.67 | WAF w/DDoS mitigation | Filter network traffic |
| Automation : Data poisoning | Tampering with Data | 34.33 | ICAM - Data Encryption - Secrets Management | Filter network traffic, IPS |
| Authentication : Man-in-the-Middle | Information Disclosure | 32.67 | Secrets Management - DNSsec | Static network config |
| API : Malformed packets | Denial of Service | 32.00 | API security & encryption | Monitoring |
| Architecture: Differing Encryption Offerings and Capabilities | Information Disclosure | 30.33 | ITIL - Change Management - Secrets Management | N/A |
| Authentication : Substitution attack | Denial of Service | 29.33 | Secure Block-cypher - timestamp | Audit, PAM, Cert Mgmt |
| API : Privilege Elevation | Elevation of Privilege | 28.00 | PAM - least privilege | Monitoring, Audit GPO, PAM, User Acct mgmt |
| Automation : Dynamic changes to config causing inconsistency | Denial of Service | 27.33 | SOAR Configuration Management - ITIL | N/A |
| Difference in Management: Auto-Scaling | Denial of Service | 25.67 | ITIL - Event Management | N/A |
| Authentication : Session hijacking | Spoofing Identity | 25.67 | TLS encryption on all sessions & MFA | MFA, delete persistent cookies |
| Architecture: VPN Infiltration | Information Disclosure | 25.33 | ICAM-MFA, Network segmentation | Network segmentation, MFA |

This presentation was given at the 2023 National Cybersecurity Education Colloquium

# Phase 3 - **Develop & Evaluate Defensive Strategies to Secure Multi-cloud Environments**

This presentation was given at the 2023 National Cybersecurity Education Colloquium

Build of test environment

Define scoped attack methodologies

- Authentication

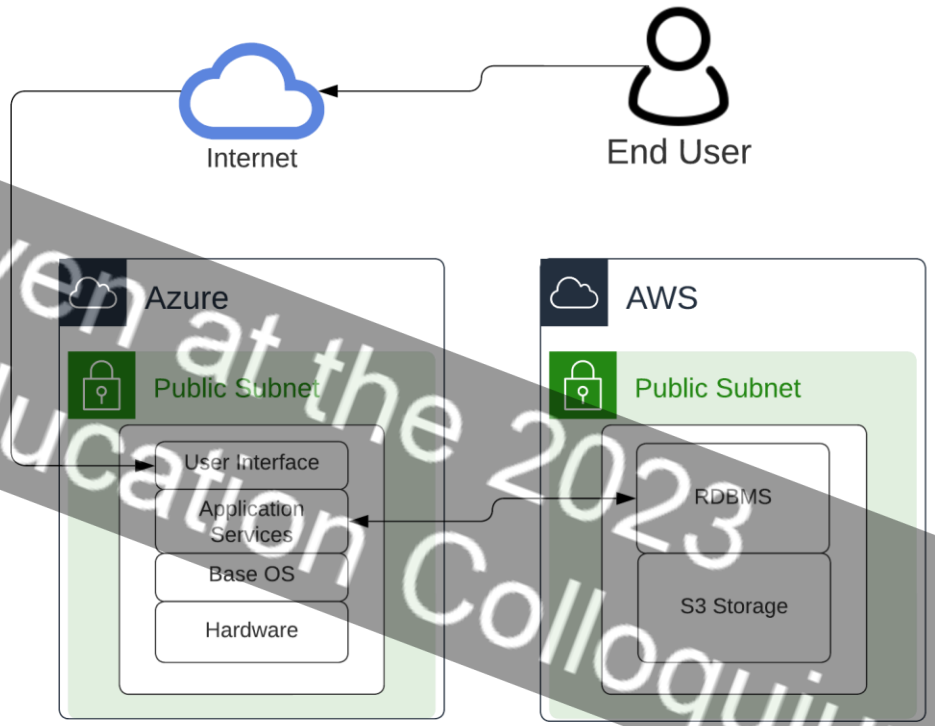
Execute attack

Implement mitigation

Retest attack identifying attack hinderances

# Test Env Architecture

- Utilizing Azure & AWS
- Collapse Front-end and application server
- Exposed UI and DB API
- Separate identity control systems




This presentation was given at the 2023 National Cybersecurity Education Colloquium

# Attack Execution on Authentication

This presentation was given at the 2023 National Cyber Security Education Colloquium

- Privilege Escalation
  - Gain illegal/illicit access to a system through the elevation of user privilege about the assign authorization level. This can be obtained through the exploitation of a system bug, misconfiguration, or inadequate access controls.

- Session Highjacking
  - Attackers use session cookies that have been stolen from a user's computer to impersonate the session/user gaining access to protected data and systems.

# Final Conclusions

This presentation was given at the 2023 National Cybersecurity Education Colloquium

- Multi-cloud deployments of applications continues to grow and a source of vulnerability
- Vulnerabilities in multi-cloud is similar to single cloud with a few exceptions
  - Multi-cloud adds **COMPLEXITY** to the security
  - Security **PRIORITIES** can change in multi-cloud because of unique exposed vulnerabilities

# Future Opportunities

This presentation was given at the 2023 National Cybersecurity Education Colloquium

- Multi-cloud security direction and research opportunities
  - Recurring mitigation across the attack vectors
    - Change management
      - Enabling coordination of configuration and changes
      - Centralized management
    - Further research
      - Unified management of multi-cloud configuration
      - Automated mitigation implementation across cloud providers

This presentation was given at the 2023 National Cybersecurity Education Colloquium

# Q&A