Emergent (In)Security of Multi-Cloud Environment

Morgan Reece[1], Teddy Lander[1], Sudip Mittal[1], Nidhi Rastogi[2], Josiah Dykstra[3], and Andy Sampson[3]
[1]Mississippi State University, [2]Rochester Institute of Technology, and [3]National Security Agency
mlr687@msstate.edu, tel127@msstate.edu, mittal@cse.msstate.edu, nxrvse@rit.edu, josiah.dykstra@cyber.nsa.gov, agsamps@uwe.nsa.gov

Project Statement

I. Objective

A. Understand and assess the risks and vulnerabilities exacerbated by the complexities of a multi-cloud environment

II. Motivation

A. Emerging proliferation of multi-cloud environment for organization's workloads

B. Risk escalation due to complexities of multi-cloud inter-communication and expanded attack surface

III. Methodology

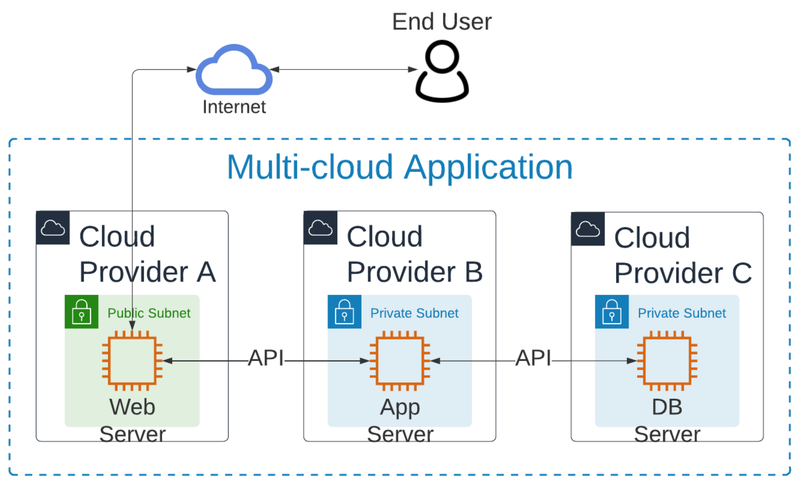
A. Utilization of industry standard risk analysis frameworks enabling holistic assessment

IV. Results development

A. Evaluate defensive techniques and gain an understanding of the multi-cloud specific risk priorities and mitigations

Methodology

I. Defined 3-tier cloud architecture for analysis



II. Healthcare provider as a use case to perform BIA

III. Defined **threat vectors** unique to multi-cloud utilizing MITRE ATT&CK framework

Methodology (cont.)

IV. Utilize STRIDE and DREAD risk frameworks to analyze

A. STIRDE - Categorization of **threat vectors**

B. DREAD – Risk scoring of **threat vectors**

C. EPSS – Exploit Prediction Scoring System

D. Support **threat vector** risk scoring

V. MITRE ATT&CK framework mitigation

Results

- Qualitative Analysis

Description of Threat	STRIDE Framework Category
Architecture:	
DoS attacks	Denial of Service
Differing Encryption Offerings and Capabilities	Information Disclosure
CVEs	ALL
VPN Infiltration	Information Disclosure
Guest OS, Hypervisor, and Host OS	Tampering with Data
Addition of Multiple Cloud Providers	ALL
API:	
Interface format consistency	Tampering with Data
Privilege Elevation	Elevation of Privilege
Multiple API Connections Conflict	Tampering with Data
Malformed packets	Denial of Service
Authentitcation:	
Session hijacking	Spoofing Identity
Substitution attack	Denial of Service
Man-in-the-Middle	Information Disclosure
Inconsistent user ACL	Elevation of Privilege
Automation:	
Dynamic changes to config causing inconsistency	Denial of Service
Data poisoning	Tampering with Data
Difference in Management:	
Service Level Agreement (SLAs)	Repudiation
Cloud Management Agreement	Repudiation
Monetization	Repudiation
Auto-Scaling	Denial of Service
Mismatch in Cyber Legislation:	
Data Privacy Laws	Information Disclosure
Data Control	Information Disclosure
Data Release/Sharing	Information Disclosure
Data Sovereignty Laws	Information Disclosure

- Quantitative Analysis

Description of Threat	Total Risk Score	Damage			Threat Attributes			
		Legal Damage	Reputation Damage	Productivity Damage	Reproducability	Exploitability	Affected Users	Discoverability
Architecture:								
DoS attacks	42.67	0	10	10	8	8	10	10
Differing Encryption Offerings and Capabilities	30.33	0	6	7	7	8	4	7
CVEs	44.00	0	9	9	9	10	10	9
VPN Infiltration	25.33	0	8	5	6	9	2	4
Guest OS, Hypervisor, and Host OS	22.33	0	7	6	5	8	2	3
Addition of Multiple Cloud Providers	19.33	0	7	6	5	6	2	2
API:								
Interface format consistency	18.00	0	7	8	2	2	2	7
Privilege Elevation	28.00	0	9	6	8	10	3	2
Multiple API Connections Conflict	19.33	0	5	8	2	3	2	8
Malformed packets	32.00	0	6	9	8	7	3	9
Authentitcation:								
Session hijacking	23.33	0	6	4	7	8	1	4
Substitution attack	29.33	0	7	9	10	10	2	2
Man-in-the-Middle	32.67	0	9	5	7	9	10	2
Inconsistent user ACL	24.67	0	9	5	3	9	6	2
Automation:								
Dynamic changes to config causing inconsistency	27.33	0	5	8	5	8	7	3
Data poisoning	34.33	0	4	6	10	10	8	3
Difference in Management:								
Service Level Agreement (SLAs)	22.67	0	4	4	4	4	6	6
Cloud Management Agreement	20.67	0	4	4	4	4	4	6
Monetization	19.33	0	5	5	4	4	4	4
Auto-Scaling	25.67	0	8	9	6	5	7	2
Mismatch in Cyber Legislation:								
Data Privacy Laws	22.00	10	6	2	1	3	6	6
Data Control	23.00	10	6	2	1	4	6	6
Data Release/Sharing	23.33	10	7	2	1	4	6	6
Data Sovereignty Laws	22.67	10	5	2	1	4	6	6

Results (cont.)

- MITRE ATT&CK mitigations & countermeasures

Description of Threat	Countermeasures	MITRE ATT&CK Mitigation
Architecture:		
DoS attacks	WAF w/DDoS mitigation	Filter network traffic
Differing Encryption Offerings and Capabilities	ITIL - Change Management - Secrets Management	N/A
CVEs	Patch Management - System Hardening	Patch
VPN Infiltration	ICAM-MFA, Network segmentation	Network segmentation, MFA
Guest OS, Hypervisor, and Host OS	Patch Management - System Hardening	User Acct Mgmt
Addition of Multiple Cloud Providers	ITIL - Change Management - CMDB	N/A
API:		
Interface format consistency	ITIL - Change Management - CMDB	N/A
Privilege Elevation	PAM - least privilege	Monitoring, Audit GPO, PAM, User Acct mgmt
Multiple API Connections Conflict	ITIL - Change Management - CMDB	N/A
Malformed packets	API security & encryption	Monitoring
Authentitcation:		
Session hijacking	TLS encryption on all sessions & MFA	MFA, delete persistent cookies
Substitution attack	Secure Block-cypher - timestamp	Audit, PAM, Cert Mgmt
Man-in-the-Middle	Secrets Management - DNSsec	Static network config
Inconsistent user ACL	ICAM - SCIM/SAML	ICAM
Automation:		
Dynamic changes to config causing inconsistency	SOAR Configuration Management - ITIL	N/A
Data poisoning	ICAM - Data Encryption - Secrets Management	Filter network traffic, IPS
Difference in Management:		
Service Level Agreement (SLAs)	ITIL - Service Level Management - CMDB	N/A
Cloud Management Agreement	ITIL - Supplier Management	N/A
Monetization	ITIL - Supplier Management	N/A
Auto-Scaling	ITIL - Event Management	N/A
Mismatch in Cyber Legislation:		
Data Privacy Laws	Regulatory Compliance Management	N/A
Data Control	Data Governance	N/A
Data Release/Sharing	Data Governance	N/A
Data Sovereignty Laws	Data Governance	N/A

Conclusion

I. Multi-cloud environments have similar risk and vulnerabilities as single cloud environments with the primary differences being:

A. Expanded attack surface

B. Increased complexity of security design

C. Different mitigation priorities

II. Change management is a significant administrative security practice addressing threats across multiple categories

III. Research to address multi-cloud specific security risks and vulnerabilities should be prioritized considering the proliferation and complexity of the multi-cloud environments.

A. Current focus of research is on software development for a multi-cloud

1. Limited research has focused on multi-cloud systems and infrastructure integration

B. Future research opportunities

1. Unified cloud environment management

2. Multi-cloud threat modeling standard