C S 55D: SECURITY IN AMAZON WEB SERVICES

Foothill College Course Outline of Record

Heading	Value
Effective Term:	Summer 2024
Units:	4.5
Hours:	4 lecture, 2 laboratory per week (72 total per quarter)
Advisory:	C S 30A, C S 50A, C S 55A and C S 55C.
Degree & Credit Status:	Degree-Applicable Credit Course
Foothill GE:	Non-GE
Transferable:	CSU
Grade Type:	Letter Grade (Request for Pass/No Pass)
Repeatability:	Not Repeatable

Student Learning Outcomes

- A successful student will be able to identify the role the Key Management Service and the best practices used in deployments.
- A successful student will be able to identify important security principles that web services applications must meet when deployed.
- A successful student will be able to describe use of the Shared Responsibility model in secure AWS deployments.

Description

This course focuses on information security principles for computing systems and data with respect to cloud computing. Students learn about governance, security frameworks, compliance, controls, layered security, and vulnerabilities in Amazon Web Services (AWS). The AWS Shared Responsibility model will be studied for specific XaaS cloud level deployments. The course presents a broad, hands-on approach to AWS security offerings and AWS services best security practices.

Course Objectives

The student will be able to:

1. Apply for an Amazon (AWS) account and Amazon Educate account
2. Understand industry security frameworks, such as the CIA triad and AAA security/controls
3. Understand compliance and how it differs from security
4. Review industry compliance frameworks, such as HIPAA, PCI DSS, ISO 27000, GDPR
5. Understand basic security controls (Physical, Technical, Administrative) and control classifications
6. Understand the AWS Well-Architected Framework and how the security pillar design principles of that framework apply to the overall security effort, including:
    a. Identity management
    b. Detection
    c. Infrastructure protection
    d. Data protection
    e. Incident response
7. Understand the AWS controls that AWS uses in practice and how those controls and audits can be used in governance/compliance efforts
8. Understand how AWS uses its hypervisor to secure underlying compute instances
9. Configure the AWS Identity Access Management (IAM) system
10. Use the AWS CloudTrail platform for logging actions within AWS
11. Use the AWS CloudWatch platform to collect resources log and act/analyze upon changes
12. Use the AWS Config service to monitor changes to asses/audit changes in configurations against internal guidelines
13. Automate changes in EC2 compute instances through AWS Systems Manager
14. Understand the industry consortiums to monitor and report vulnerabilities
15. Understand Inspector and Trusted Advisor services and how those services enable vulnerability inspections
16. Review intrusion detection/prevention and learn how AWS implements in AWS GuardDuty
17. Review sensitive data discovery with AWS Macie
18. Review IPv4 networking and build software defined networks (SDN) within AWS using AWS Virtual Private Cloud (VPC)
19. Set up out of region protection and Distributed Denial of Service (DDoS) via AWS Route 53, content distribution networks (AWS CloudFront), and AWS Web Application Firewall (WAF)
20. Understand security principles of serverless computing (AWS Lambda), Application Program Gateway (AWS API Gateway), and user authentication/authorization (Amazon Cognito)
21. Demonstrate the Key Management Service and AWS Secrets Manager and use best practices to configure
22. Review AWS organizational tools for security best practices, such as AWS Organizations, AWS Single Sign On, and AWS Control Tower

Course Content

1. AWS access
    a. AWS account acquisition
    b. AWS command line interface
    c. AWS Educate account acquisition
2. AAA framework for identity access security, processes for security
    a. Compliance
    b. Controls
    c. Layered security
3. AWS security concepts
    a. AWS Well-Architected Framework
    b. AWS Well-Architected Security Pillar
    c. AWS Shared Responsibility Model
    d. AWS Global Infrastructure
    e. AWS Nitro Hypervisor principles
    f. AWS security practices
        i. AWS Change Management
        ii. Communications and status
        iii. TLS
        iv. Secure logging
    g. Working under AWS Shared Security Model

i. AWS Acceptable Use Policy
ii. IaaS, PaaS considerations
iii. AWS Config assessment and auditing
iv. AWS Systems Manager instance management

h. Working with AWS Identity and Access Management (IAM)
i. IAM basics
ii. Users
iii. Groups
iv. Roles
v. Policies

i. Logging and measurement
i. CloudTrail event logging and management
ii. CloudTrail best practices
1. Detective
2. Preventive
iii. CloudWatch monitoring
1. Metrics collection
2. Metrics monitoring
3. Event action automation
4. Analysis

j. Vulnerabilities and mitigations
i. Industry efforts
1. Common Vulnerabilities and Exposures (CVE) group
2. National Institutes of Standards and Technology (NIST)
3. Cybersecurity and Infrastructure Agency (CIST)
4. Center for Internet Security (CIS)
ii. AWS Assessment Security tools
1. Amazon Inspector scanning service
2. Amazon Trusted Advisor

k. Threat detection, data discovery, monitoring
i. Introduction to intrusion detection/prevention
1. AWS GuardDuty threat detection
ii. Introduction to data discovery and sensitive data
1. AWS Macie sensitive data discovery
iii. Security monitoring via AWS Security Hub

l. Network security
i. IPv4 review
ii. Creating networks within AWS using Amazon Virtual Private Cloud (VPC)
1. Design of subnetworks
2. VPC Flow Logs
3. VPC security best practices

m. Out of region protection
i. DNS using AWS Route 53
ii. Content distribution using AWS CloudFront
iii. Amazon web application firewall (WAF)
iv. Distributed Denial of Service (DDoS) mitigation using AWS Shield
v. Firewall management using VPC, AWS Security Groups, and AWS Firewall Manager

n. Cryptography
i. Cryptography basics
ii. Encryption
iii. Key Management
1. Hardware security modules
2. AWS Key Management System (KMS) basics
3. AWS KMS Security
4. AWS Cloud Hardware Security (CloudHSM)
iv. Applications secrets using AWS Secrets Manager

o. AWS account management and provisioning
i. AWS Organizations multiple account provisioning
ii. AWS Single Sign On (SSO)
iii. Management of multiple AWS accounts with respect to security via AWS Control Tower

Lab Content

1. Create AWS working environment including AWS account, AWS Educate Account, and AWS Command line interface on local computer
2. Creating AWS Config rules to insure EC2 compute instance managed by AWS Systems Manager
3. Creating IAM user accounts with granular permissions
   a. IAM restrictions demonstration
   b. Multi factor authentication demonstration using IAM and S3
4. CloudTrail and CloudWatch
   a. CloudTrail trail creation and analysis
   b. CloudWatch rule and event automation
   c. CloudWatch monitoring of EC2 instance
5. Trusted Advisor demonstration of a PaaS platform and security notifications
6. EC2 instance configuration vulnerability discovery via Amazon Inspector
7. Amazon Macie sensitive data discovery in S3
8. N-tier demonstration of security of IaaS service using VPC
9. Content distribution protection using AWS WAF on AWS CloudFront
10. REST API demonstration to AWS Serverless Lambda
11. Granular storage security methods in AWS S3 using encryption, Access Control Lists (ACLs), private access, network access control via VPCs, and confirmation via AWS Config
12. Using KMS secrets to lock S3 objects
13. Using Secrets Manager to protect a secret

Special Facilities and/or Equipment

1. Access to a computer with a web browser compatible with the Foothill learning management system and AWS Console.
2. A payment method for accessing AWS services (credit/debit/stored value card). AWS as a commercial service requires all accounts to be paid for accounts. AWS will provide credits and no actual spending with normal class use would be incurred.
3. A learning management system with an assignment posting component (through which all lab assignments are to be submitted) and a forum component (where students can discuss course material and receive help from the instructor). This applies to all sections, including on campus (i.e., face-to-face) offerings.
4. The college will provide a fully functional and maintained course management system through which the instructor and students can interact.
5. Students must have email accounts and ongoing access to computers with internet capabilities.

Method(s) of Evaluation

Methods of Evaluation may include but are not limited to the following:

Tests and quizzes
Written laboratory assignments, which include detailed instructions, sample runs, and documentation
Completion of class project implementing and describing real world IaaS threat detection and automation of remediation
Final examination

Method(s) of Instruction

Methods of Instruction may include but are not limited to the following:

Lectures which include motivation for the architecture of the specific topics being discussed
In-person or online labs (for all sections, including those meeting face-to-face/on campus), consisting of:
1. An assignment webpage located on a college-hosted course management system or other department-approved internet environment. Here, the students will review the specification of each assignment and submit their completed lab work
2. A discussion webpage located on a college-hosted course management system or other department-approved internet environment. Here, students can request assistance from the instructor and interact publicly with other class members
Detailed review of laboratory assignments which includes model solutions and specific comments on the student's submissions
In-person or online discussion which engages students and instructor in an ongoing dialog pertaining to all aspects of designing, implementing, and analyzing programs
When course is taught fully online:
1. Instructor-authored lecture materials, handouts, syllabus, assignments, tests, and other relevant course material will be delivered through a college-hosted course management system or other department-approved internet environment
2. Additional instructional guidelines for this course are listed in the addendum of C S department online practices

Representative Text(s) and Other Materials

All course materials provided by instructor through the online course management system.

Types and/or Examples of Required Reading, Writing, and Outside of Class Assignments

1. Reading:
    a. Reading the supplied handouts and modules averaging 30 pages per week
    b. Reading online resources as directed by instructor though links pertinent to the course
    c. Watching video presentations by AWS and other cloud providers as contained in the course
    d. Reading library and reference material directed by instructor through course handouts
2. Writing:
    a. Writing technical prose documentation that supports and describes the assignments that are submitted for grades

Discipline(s)

Computer Science