**BIRLA INSTITUTE OF TECHNOLOGY & SCIENCE, PILANI**

**WORK INTEGRATED LEARNING PROGRAMMES**

**COURSE HANDOUT**

**Part A: Content Design**

|  |  |
| --- | --- |
| **Course Title** | **Cloud, IoT and Enterprise Security** |
| **Course No(s)** | SS ZG570 |
| **Credit Units** | 4 |
| **Course Author** | Nishit Narang |
| **Version No** | 1.0 |
| **Date** | 15/12/2020 |

**Course Description:**

This course introduces the security risks involves in the Cloud, IoT & other IT Infrastructure of an Enterprise and measures to foolproof.

**Course Objectives.**

|  |  |
| --- | --- |
| **No** | **Objective** |
| **CO1** | To introduce various security architectures involved in an enterprise IT infrastructure |
| **CO2** | To emphasize the specific risks involved in the cloud and IoT infrastructures |
| **CO3** | To introduce the identity management and access control in the cloud and IoT infrastructures |

**Text Book(s)**

|  |  |
| --- | --- |
| **T1** | Aaron Woody, **Enterprise Security: A Data-Centric Approach To Securing The Enterprise**. 1st ed. Birmingham: Packt Publishing Ltd., 2013. |
| **T2** | Ronald L. Krutz, Russell Dean Vines, **Cloud Security: A Comprehensive Guide to Secure Cloud Computing**, John Wiley & Sons, 2010 |
| **T3** | Shancang Li Li Da Xu, **Securing the Internet of Things**, Syngress, 1st Edition, 2017 |

**Reference Book(s)**

|  |  |
| --- | --- |
| **R1** | Johnson, T. **Cybersecurity**, CRC Press.2015 |
| **R2** | Ryan Ko and Kim-Kwang Raymond Choo, **The Cloud Security Ecosystem,** Syngress, 2015 |
| **R3** | Chris Dotson, **Practical Cloud Security**, O'Reilly Media, Inc., 2019 |
| **R4** | Ian Smith and Don A. Bailey, **IoT Security Guidelines for IoT Service Ecosystem**, GSM Association, Official Document CLP.12 |

**Content Structure**

1. Enterprise Security Overview

1.1. The façade of enterprise security

1.2. Enterprise security pitfalls

1.3. The road map to securing the enterprise

2. Security Architectures

2.1. Redefining the network edge

2.2. Defining the building blocks of trust models

2.3. Enterprise trust models

2.4. Micro architectures

2.5. Data risk-centric architectures

2.6. BYOD initiatives

3. Security as a Process

3.1. Risk analysis

3.2. Security policies and standards

3.3. Security exceptions

3.4. Security review of changes

4. Securing the Network

4.1. Securing the Network

4.2. Next generation firewalls

4.3. Advanced persistent threat detection and mitigation

4.4. Securing network services

4.5. Network segmentation

4.6. Applying security architecture to the network

5. Securing Systems

5.1. System classification

5.2. File integrity monitoring

5.3. Application whitelisting

5.4. Host-based intrusion prevention system

5.5. Host firewall

5.6. Anti-virus

5.7. User account management

5.8. Policy enforcement

6. Securing Enterprise Data

6.1. Data classification

6.2. Data Loss Prevention

6.3. Encryption and hashing

6.4. Tokenization

6.5. Data masking

6.6. Authorization

6.7. Developing supporting processes

7. Securing the Internet of Things

7.1. Introduction

7.2. Security Requirements in IoT Architecture

7.3. Security in Enabling Technologies

7.4. Security Concerns in IoT Applications

8. Security Requirements in IoT and Current Vulnerabilities

8.1. Security Requirements in IoT

8.2. Insufficient Authentication/Authorization

8.3. Insecure Access Control

8.4. Threats to Access Control, Privacy, and Availability

8.5. Attacks Specific to IoT

9. Security Architecture in the Internet of Things

9.1. Secrecy and Secret-Key Capacity

9.2. Authentication/Authorization for Smart Devices

9.3. Transport Encryption

9.4. Secure Cloud/Web Interface

9.5. Secure Software/Firmware

9.6. Physical Layer Security

10. Device Security and Node Authentication

10.1. Security Goals in IoT

10.2. Public-Key-Based Authentication

10.3. Identify-Based Authentication, Encryption, and Digital Signature

10.4. IP Connectivity

10.5. Lightweight Cryptography

11. Data Security Schemes for IoT and Social IoT Concerns

11.1. Data Security and Privacy

11.2. Data Confidentiality and Key Management

11.3. Security Concerns in Social IoT

12. Cloud Computing Fundamentals

12.1. Essential Characteristics

12.2. Architectural Influences

12.3. Technological Influences

12.4. Operational Influences

12.5. Cloud Delivery Models

12.6. Cloud Deployment Models

13. Cloud Computing Software Security Fundamentals

13.1. Cloud Information Security Objectives

13.2. Cloud Security Services

13.3. Relevant Cloud Security Design Principles

13.4. Secure Cloud Software Requirements

13.5. Secure Cloud Software Testing

13.6. Cloud Computing and Business Continuity Planning/Disaster Recovery

14. Cloud Computing Risk Issues

14.1. The CIA Triad

14.2. Privacy and Compliance Risks

14.3. Threats to Infrastructure, Data, and Access Control

14.4. Cloud Service Provider Risks

15. Cloud Computing Security Challenges

15.1. Security Policy Implementation

15.2. Virtualization Security Management

16. Cloud Computing Security Architecture

16.1. Architectural Considerations

16.2. Identity Management and Access Control

16.3. Autonomic Security

**Learning Outcomes:**

|  |  |
| --- | --- |
| **No** | **Learning Outcomes** |
| **LO1** | Relate an insecure incident to each type of security architecture and estimates the value and risk propositions to the business |
| **LO2** | Explain the cloud security fundamentals, risks and challenges |
| **LO3** | Design a secure IoT ecosystem |
| **LO4** | Explain the existing security scheme for IoT |

**Part B: Contact Session Plan**

|  |  |
| --- | --- |
| **Academic Term** | First Semester 2022-2023 |
| **Course Title** | **Cloud, IoT and Enterprise Security** |
| **Course No** | SS ZG570 |
| **Lead Instructor** | Nishit Narang |

## Course Contents

|  |  |  |
| --- | --- | --- |
| **Contact Session** | **List of Topics** | **Reference** |
| 1 | 1. **Enterprise Security Overview**    1. The façade of enterprise security    2. Enterprise security pitfalls    3. The road map to securing the enterprise 2. **Security Architectures**    1. Redefining the network edge    2. Defining the building blocks of trust models    3. Enterprise trust models | **T1: Chapter 1,2** |
| 2 | **Security Architectures**   * 1. Micro architectures   2. Data risk-centric architectures   3. BYOD initiatives  1. **Security as a Process**    1. Risk analysis    2. Security policies and standards    3. Security exceptions    4. Security review of changes | **T1: Chapter 2,3** |
| 3 | 1. **Securing the Network**    1. Securing the Network    2. Next generation firewalls    3. Advanced persistent threat detection and mitigation    4. Securing network services    5. Network segmentation    6. Applying security architecture to the network | **T1: Chapter 4** |
| 4 | 1. **Securing Systems**    1. System classification    2. File integrity monitoring    3. Application whitelisting    4. Host-based intrusion prevention system    5. Host firewall    6. Anti-virus    7. User account management    8. Policy enforcement | **T1: Chapter 5** |
| 5 | 1. **Securing Enterprise Data**    1. Data classification    2. Data Loss Prevention    3. Encryption and hashing    4. Tokenization    5. Data masking    6. Authorization    7. Developing supporting processes | **T1: Chapter 6** |
| 6 | 1. **Securing the Internet of Things**    1. Introduction    2. Security Requirements in IoT Architecture    3. Security in Enabling Technologies    4. Security Concerns in IoT Applications | **T3: Chapter 01** |
| 7 | 1. **Security Requirements in IoT and Current Vulnerabilities**    1. Security Requirements in IoT    2. Insufficient Authentication/Authorization    3. Insecure Access Control    4. Threats to Access Control, Privacy, and Availability    5. Attacks Specific to IoT | **T3: Chapter 02, 05** |
| 8 | 1. **Security Architecture in the Internet of Things**     1. Secrecy and Secret-Key Capacity    2. Authentication/Authorization for Smart Devices    3. Transport Encryption    4. Secure Cloud/Web Interface    5. Secure Software/Firmware    6. Physical Layer Security | **T3: Chapter 03** |
| 9 | 1. **Device Security and Node Authentication**    1. Security Goals in IoT    2. Public-Key-Based Authentication    3. Identify-Based Authentication, Encryption, and Digital Signature    4. IP Connectivity    5. Lightweight Cryptography | **T3: Chapter 04** |
| 10 | 1. **Data Security Schemes for IoT and Social IoT Concerns**    1. Data Security and Privacy    2. Data Confidentiality and Key Management    3. Security Concerns in Social IoT | **T3: Chapter 07,08** |
| 11 | 1. **Cloud Computing Fundamentals**    1. Essential Characteristics    2. Architectural Influences    3. Technological Influences    4. Operational Influences | **T2: Chapter 01,02** |
| 12 | * 1. Cloud Delivery Models   2. Cloud Deployment Models  1. **Cloud Computing Software Security Fundamentals**    1. Cloud Information Security Objectives    2. Cloud Security Services | **T2: Chapter 02, 03** |
| 13 | * 1. Relevant Cloud Security Design Principles   2. Secure Cloud Software Requirements   3. Secure Cloud Software Testing   4. Cloud Computing and Business Continuity Planning/Disaster Recovery | **T2: Chapter 03** |
| 14 | 1. **Cloud Computing Risk Issues**    1. The CIA Triad    2. Privacy and Compliance Risks    3. Threats to Infrastructure, Data, and Access Control | **T2: Chapter 04** |
| 15 | * 1. Cloud Service Provider Risks  1. **Cloud Computing Security Challenges**    1. Security Policy Implementation    2. Virtualization Security Management | **T2: Chapter 04,05** |
| 16 | 1. **Cloud Computing Security Architecture**    1. Architectural Considerations    2. Identity Management and Access Control    3. Autonomic Security | **T2: Chapter 06** |

Important Information:

* Syllabus for Mid-Semester Test: Topics in CS 1-8.
* Syllabus for Comprehensive Exam: All topics given in plan of study

**Evaluation Scheme**:

Legend: EC = Evaluation Component; AN = After Noon Session; FN = Fore Noon Session

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No** | **Name** | **Type** | **Duration** | **Weight** | **Day, Date, Session, Time** |
| EC-1 | Quiz-I/ Assignment-I | Online | - | 5% | August 16-30, 2022 |
| Quiz-II | Online |  | 5% | September 16-30, 2022 |
| Quiz-III/ Assignment-II | Online |  | 20% | October 16-30, 2022 |
| EC-2 | Mid-Semester Test | Open Book | 2 hours | 30% | Friday, 23/09/2022 (AN) |
| EC-3 | Comprehensive Exam | Open Book | 2 hours | 40% | Friday, 25/11/2022 (AN) |

1. For Closed Book tests: No books or reference material of any kind will be permitted. Laptops/Mobiles of any kind are not allowed. Exchange of any material is not allowed.
2. For Open Book exams: Use of prescribed and reference text books, in original (not photocopies) is permitted. Class notes/slides as reference material in filed or bound form is permitted. However, loose sheets of paper will not be allowed. Use of calculators is permitted in all exams. Laptops/Mobiles of any kind are not allowed. Exchange of any material is not allowed.
3. If a student is unable to appear for the Regular Test/Exam due to genuine exigencies, the student should follow the procedure to apply for the Make-Up Test/Exam. The genuineness of the reason for absence in the Regular Exam shall be assessed prior to giving permission to appear for the Make-up Exam. Make-Up Test/Exam will be conducted only at selected exam centres on the dates to be announced later.

It shall be the responsibility of the individual student to be regular in maintaining the self-study schedule as given in the course handout, attend the lectures, and take all the prescribed evaluation components such as Assignment/Quiz, Mid-Semester Test and Comprehensive Exam according to the evaluation scheme provided in the handout.