# Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

## Scheme of Teaching & Examination

**M.Tech. (Information Security)**

**UNDER COMPUTER SCIENCE & ENGINEERING BOARD**

### 2nd Semester

<table>
<thead>
<tr>
<th>S. No</th>
<th>Board of Study</th>
<th>Subject Code</th>
<th>Subject</th>
<th>Periods per Week</th>
<th>Scheme of Examination</th>
<th>Total Marks</th>
<th>Credit L+(T+P)/2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>L</td>
<td>T</td>
<td>P</td>
<td>ESE</td>
</tr>
<tr>
<td>1</td>
<td>CSE</td>
<td>571211(22)</td>
<td>Network Simulation and Security</td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>2</td>
<td>CSE</td>
<td>571212(22)</td>
<td>Biometric Security Systems</td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>3</td>
<td>CSE</td>
<td>571213(22)</td>
<td>Cryptography and Security threats</td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>4</td>
<td>CSE</td>
<td>571214(22)</td>
<td>Software Engineering and Security</td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>5</td>
<td>Refer Table – II</td>
<td>Elective – II</td>
<td></td>
<td>3</td>
<td>1</td>
<td>-</td>
<td>100</td>
</tr>
<tr>
<td>6</td>
<td>CSE</td>
<td>571221(22)</td>
<td>Network Simulation and Security Lab.</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>75</td>
</tr>
<tr>
<td>7</td>
<td>CSE</td>
<td>571222(22)</td>
<td>Biometric Security Systems Lab.</td>
<td>-</td>
<td>-</td>
<td>3</td>
<td>75</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
<td></td>
<td>15</td>
<td>5</td>
<td>6</td>
<td>650</td>
</tr>
</tbody>
</table>

- L: Lecture, T: Tutorial, P: Practical, ESE: End Semester Examination, CT: Class Test, TA: Teacher's Assessment

<table>
<thead>
<tr>
<th>S.N.</th>
<th>Board of Study</th>
<th>Subject Code</th>
<th>Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Computer Science &amp; Engg.</td>
<td>571231 (22)</td>
<td>Intelligent Systems</td>
</tr>
<tr>
<td>2</td>
<td>Computer Science &amp; Engg.</td>
<td>571232 (22)</td>
<td>Information Security policies and Procedures</td>
</tr>
<tr>
<td>3</td>
<td>Computer Science &amp; Engg.</td>
<td>571233 (22)</td>
<td>Grid Computing</td>
</tr>
</tbody>
</table>

**Note (1) →** Choice of elective once made for an examination cannot be changed in future examinations.

**Note (2) →** Examination Duration of all Theory papers will be of THREE hours.
Unit – I OVERVIEW OF NETWORK SIMULATION
Simulator Preliminaries, Initialization and termination, Links and nodes, Agents and Applications, Scheduling events, Visualization using NAM (Network Animator), Tracing, Working with trace files using AWK, Grep, Fundamentals of Perl Scripting programming, Plotting with GNUPLOT and XGRAPH.

Unit - II PROTOCOL BASICS AND GATEWAYS

Unit - III SECURITY ISSUES AND MEASURES

Unit - IV NETWORK TYPES AND ISSUES

Unit - V NETWORK AUTHENTICATION AND MANAGEMENT

Text Books :

Reference Books :
Unit - I OVERVIEW OF BIOMETRICS
Introduction, Benefits of Biometrics over traditional authentication systems and identification systems, Selecting a Biometric for a system, Biometric Applications, Key Biometric terms and processes, Matching process of Biometrics, Limitations and Accuracy measures in Biometric systems.

Unit - II PHYSIOLOGICAL BIOMETRIC TECHNOLOGIES

Unit - III BEHAVIORAL BIOMETRIC TECHNOLOGIES

Unit - IV MULTI BIOMETRICS
Multi Biometrics and multi factor Biometrics, Two-factor Authentication with passwords, Tickets and Tokens, Executive decision, Implementation plan.

Unit – V CASE STUDIES
Case Studies on Physiological, Behavioral, and Multifactor Biometrics in Identification Systems.

Text / Reference Books:


Cryptography and Security threats

Introduction, Beginning with a simple communication game, Wrestling between Safeguard and Attack, Encryption Symmetric techniques, Encryption Asymmetric techniques, Bit Security of the basic public key cryptographic functions, Data Integrity Techniques, Authentication framework for public key cryptography.

Security Measures and Strategies
Formal and Strong security definitions for public-key crypto systems, Probable secure and efficient public-key cryptosystems, The optimal asymmetric encryption padding, The Cramer–Shoup Public-key crypto systems, An overview of probably secure hybrid cryptosystems, Literature notes on practical and probably secure public-key cryptosystems, Strong and probable security for digital signatures.

Sources of Security Threats

Security Threat Management

Firewalls and Intrusion Detection Systems

Text Books:

Reference Books:
Unit - I PROBLEM, PROCESS, AND PRODUCT
Problems of software practitioners, Approach through software reliability engineering, Experience with SRE, SRE process, Defining the product, Testing acquired software, Reliability concepts, Software and hardware reliability, Implementing Operational profiles - Developing, Identifying, Creating, Reviewing the operation, Concurrency rate, Occurrence probabilities, Applying operation profiles.

Unit – II ENGINEERING “JUST RIGHT” RELIABILITY
Defining “failure” of the product, Choosing a common measure for all associated systems, Setting system failure intensity and objectives, Determining user needs for reliability and availability, Overall reliability and availability objectives, Common failure intensity objectives, Developed software failure intensity objectives, Engineering software reliability strategies, Preparing for Test, Preparing test cases, Planning number of new test cases for current release, Allocating new test cases, Distributing new test cases among new operations, Detailing test cases, Preparing test procedures.

Unit – III EXECUTING TEST
Planning and allocating test time for the current release, Invoking test, Identifying failures, Analyzing test output for deviations, Determining which deviations are failures, Establishing when failures occurred, Guiding Test, Tracking reliability growth, Estimating failure intensity using failure intensity patterns to guide test, Certifying reliability for workers and stakeholders, Executing the deployment through a consultant.

Unit - IV USING UML FOR SECURITY

Unit - V APPLICATIONS AND CASE STUDIES

Text / Reference Books :
Unit-I ARTIFICIAL INTELLIGENCE
Some Applications of AI-Production Systems, AI-Different types of Production Systems, Search Strategies for AI-Backtracking, Graph-search, Un-uniformed and Heuristic Graph-Search Procedures, Related Algorithms and Applications.

Unit-II INTRODUCTION TO NEURAL COMPUTING
Differences between Human Brain and ANN, Knowledge Based Information Processing, Neural Information Processing, Hybrid Intelligence, Basic Concepts of Neural Networks, Inference and Learning, Classification, Association, Optimization and Self-Organization Models, Supervised and Unsupervised Learning.

Unit-III FUZZY SYSTEMS
Crisp sets and Fuzzy sets, Notion of Fuzzy Sets, Basic Concepts - Operations on Fuzzy sets, Uncertainty and Information, Types of Uncertainty, Principles of Uncertainty and Information, Applications.

Unit-IV NEURO-FUZZY SYSTEMS

Unit-V GENETIC ALGORITHMS
Introduction, Robustness of Traditional Optimization and Search Techniques, The goals of Optimization, Computer Implementation, Applications.

Text Books :

Reference Books :
Unit-I SECURITY AND COMPUTING

Unit-II ETHICAL ISSUES IN SECURITY

Unit-III SECURITY POLICIES AND PROCEDURES
Corporate policies, Legal requirements, Business requirements, Process Management, Planning and preparation, Developing policies, Asset classification policy, Developing standards.

Unit-IV RESPONSIBILITIES AND CLASSIFICATION

Unit-V CASE STUDIES

Text Books:

Reference Books:
Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Semester: M.Tech. – 2nd
Subject: Grid Computing (ELECTIVE – II)  Code: 571233 (22)
Total Theory Periods: 40  Total Tutorial Periods: 12
Minimum number of Class tests to be conducted: 02  Total Marks in End Semester Exam: 100

Unit - I
Grid Computing: values and risks – History of Grid computing, Grid computing model and protocols, Overview and types of Grids.

UNIT - II
Desktop Grids : Background, Definition, Challenges, Technology, Suitability, Grid server and practical uses, Clusters and Cluster Grids, HPC Grids, Scientific in sight, Application and Architecture, HPC application, Development Environment and HPC Grids, Data Grids, Alternatives to Data Grid, Data Grid architecture.

UNIT - III
The open Grid services Architecture, Analogy, Evolution, Overview, Building on the OGSA platform, Implementing OGSA based Grids, Creating and Managing services, Services and the Grid, Service Discovery, Tools and Toolkits, Universal Description Discovery and Integration (UDDI).

UNIT - IV

UNIT - V
Application integration, Application classification, Grid requirements, Integrating applications with Middleware platforms, Grid enabling Network services, Managing Grid environments, Managing Grids, Management reporting, Monitoring, Data catalogs and replica management, Portals, Different application areas of Grid computing.

Text Books :

Reference Books :
Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.)

Subject: Network Simulation and Security Lab.  
Code: 571221 (22)  
Total Practical Periods: 40

List of Experiments:

1. Installation and configuration of NS2.
2. Write a NS script for a simple network.
3. Write a Web Server simulation script and show its network topology.
4. Write a program to show network topology and simulation scenario.
5. Write a program for multicasting simulation script and show the NAM screen capture of the simulation.
6. Implementation of ALOHA protocol for random access method.
7. Write a simulation script for a dynamic network where the routing adjusts to a link failure.
8. Write a script to simulate a very simple 2-node wireless scenario.
10. Simulation of TCP protocol.

Text / Reference Books:

3. NS2 MANUAL.
List of Experiments:

1. Study of different Biometrical traits with respect to information security.
2. Enhancement of Biometrical trait Images using different enhancement techniques.
3. Segmentation of Biometrical trait Images using different segmentation techniques.
4. Implementation of Normalized Cut method for the study of Biometrical traits.
5. Case Based study for the extraction of features / parameters.
6. Case based study for the creation of a knowledge-based model as a database with secured data.
7. Case based study for the understanding of the knowledge-based model for the identification / recognition / verification of Biometrical traits with respect to Information Security.
8. Case based study for face recognition from frontal.
9. Case based study for face recognition from side-view.
10. Case based study on GAIT Analysis.
11. Case based study using ECG (Electro Cardiogram).
12. Case based Study using EEG (Electro Encephalogram) waveform.
13. Case based study using ERG (Electro Retinogram).

Text / Reference Books: