

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

Scheme of Teaching & Examination

M.Tech. (Information Security)

UNDER COMPUTER SCIENCE & ENGINEERING BOARD

2nd Semester

S. No	Board of Study	Subject Code	Subject	Periods per Week			Scheme of Examination			Total Marks	Credit L+(T+P) /2
							Theory/Practical				
				L	T	P	ESE	CT	TA		
1	CSE	571211(22)	Network Simulation and Security	3	1	-	100	20	20	140	4
2	CSE	571212(22)	Biometric Security Systems	3	1	-	100	20	20	140	4
3	CSE	571213(22)	Cryptography and Security threats	3	1	-	100	20	20	140	4
4	CSE	571214(22)	Software Engineering and Security	3	1	-	100	20	20	140	4
5	Refer Table – II		Elective – II	3	1	-	100	20	20	140	4
6	CSE	571221(22)	Network Simulation and Security Lab.	-	-	3	75	-	75	150	2
7	CSE	571222(22)	Biometric Security Systems Lab.	-	-	3	75	-	75	150	2
Total				15	5	6	650	100	250	1000	24

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

Table – II			
Elective – II			
S.N.	Board of Study	Subject Code	Subject
1	Computer Science & Engg.	571231 (22)	Intelligent Systems
2	Computer Science & Engg.	571232 (22)	Information Security policies and Procedures
3	Computer Science & Engg.	571233 (22)	Grid Computing

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.

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

Semester: M.Tech. – 2nd

Subject: **Network Simulation and Security**

Total Theory Periods: **40**

Minimum number of Class tests to be conducted: **02**

Branch: **Information Security**

Code: **571211(22)**

Total Tutorial Periods: **12**

Total Marks in End Semester Exam: **100**

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

ISO:OSI Model, Layer Protocols, Application Layer Protocols, TCP/IP, HTTP, SHTTP, LDAP, MIME,POP, POP3, RMON, SNMP, Presentation Layer Protocols, Light Weight Presentation Protocol, Session Layer Protocols, RPC Protocols, Transport Layer Protocols - ITOT, RDP, RUDP, TALI, TCP/UDP, Compressed TCP, Network Layer Protocols, Routing Protocols, Border Gateway Protocol, Exterior Gateway Protocol, Internet Protocols IPv4, IPv6, Internet Message Control Protocol, IRDP, Mobile IP, Mobile Support Protocol for IPv4 and IPv6, Resource Reservation Protocol, Multi-casting Protocol – VGMP, IGMP, MSDP.

Unit - III SECURITY ISSUES AND MEASURES

Data Link Layer Protocol – ARP, InARP, IPCP, IPv6CP, RARP, SLIP, Wide Area and Network Protocols, ATM Protocols, Broadband Protocols, Point-to-Point Protocols, Other WAN Protocols and Security issues.

Unit - IV NETWORK TYPES AND ISSUES

Local Area Network and LAN Protocols, ETHERNET Protocols, VLAN Protocols, Wireless LAN Protocols, Metropolitan Area Network Protocols, Storage Area Network and SAN Protocols, FDMA, WIFI and WIMAX Protocols, and Security issues.

Unit - V NETWORK AUTHENTICATION AND MANAGEMENT

Network Security and Technologies and Protocols, AAA Protocols, Tunneling Protocols, Secured Routing Protocols, GRE, Generic Routing Encapsulation, IPSEC, Security Architecture for IP, IPSEC AH, Authentication Header, ESP, IKE, ISAKMP, and Key Management Protocol, IEEE 802.11, Structure of 802.11 MAC, WEP- Problems with WEP, Attacks and Risk Station Security, Access Point Security, Gateway Security, Authentication and Encryption.

Text Books :

1. Jawin, "Networks Protocols Handbook", Jawin Technologies Inc., 2005.
2. Bruce Potter, Bob Fleck, "802.11 Security", O'Reilly Publications, 2002.
3. Lawrence Harte, "Introduction to WCDMA", Althos Publishing, 2004.

Reference Books :

1. Lawrence Harte, "Introduction to CDMA- Network Services Technologies and Operations", Althos Publishing, 2004.
2. Lawrence Harte, "Introduction to WIMAX", Althos Publishing, 2005.

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

Semester: M.Tech. – 2nd

Subject: **Biometric Security Systems**

Total Theory Periods: **40**

Minimum number of Class tests to be conducted: 02

Branch: **Information Security**

Code: **571212(22)**

Total Tutorial Periods: **12**

Total Marks in End Semester Exam: **100**

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

Fingerprints- Technical description, Characteristics, Strengths, Weaknesses, Deployment, Facial scan- Technical description, Characteristics, Strengths, Weaknesses, Deployment, Iris Scan - Technical description, Characteristics, Strengths, Weaknesses, Deployment, Retina Vascular pattern - Technical description, Characteristics, Strengths, Weaknesses, Deployment, Hand scan - Technical description, Characteristics, Strengths, Weaknesses, Deployment.

Unit - III BEHAVIORAL BIOMETRIC TECHNOLOGIES

Handprint Biometrics, DNA Biometrics, Signature and Handwriting technology - Technical description, Classification, Keyboard / Keystroke dynamics, Voice–Data Acquisition (VDA), Feature Selection and Extraction, Characteristics, Strengths, Weaknesses, Deployment.

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 :

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, “Biometrics - Identity Verification in a Network”, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul, “Implementing Biometric Security”, Wiley Eastern Publications, 2005.
3. John Berger, “Biometrics for Network Security”, Prentice Hall, 2004.

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

Semester: M.Tech. – 2nd

Subject: **Cryptography and Security threats**

Total Theory Periods: **40**

Total Minimum number of Class tests to be conducted: 02

Branch: **Information Security**

Code: **571213 (22)**

Total Tutorial Periods: **12**

Total Marks in End Semester Exam: **100**

Unit - I OVERVIEW OF CRYPTOGRAPHY

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.

Unit - II 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.

Unit - III SOURCES OF SECURITY THREATS

About Security threats - Sources of Security threats, Motives, Target Assets and Vulnerabilities, Consequences of threats, E-mail threats, Web-threats, Intruders and Hackers, Cyber crimes, Active/Passive Interference, Active/Passive Interception, Active/Passive Impersonation, Worms, Viruses, Spams, Adware, Spy-ware, Trojans, Backdoors, Bots, IP Spoofing, ARP Spoofing, Session Hijacking, Sabotage, Internal threats, Environmental threats, Threats-to-Server Security.

Unit - IV SECURITY THREAT MANAGEMENT

Risk Assessment, Forensic Analysis, Security threat correlation, Threat awareness, Vulnerability sources and assessment, Vulnerability assessment tools, Threat identification, Threat Analysis, Threat Modeling - Model for Information Security, Planning, Access Rights, Access control systems, Authorization and Authentication, Types, Policies and techniques, Security Certification, Security Monitoring and Auditing, Security Requirements Specifications.

Unit - V FIREWALLS AND INTRUSION DETECTION SYSTEMS

Firewall–Types, Dynamic packet filtering, Content filtering, Crypto capable Routers, VPNs, Secure Modems, Intrusion Detection System–Types, Intrusion Detection Tools, Penetration testing, Intrusion Analysis, Log file Monitors, Honey pots, Intrusion Prevention Systems, Trusted Systems.

Text Books :

1. Wenbo Mao, “Modern Cryptography: Theory and Practice”, Pearson Education, 2004.
2. Atul Kahate, “Cryptography and Network Security”, Tata McGraw Hill, 2003.
3. William Stallings, “Cryptography and Network Security”, Pearson Education, Third Edition, 2003.
4. Joseph M Kizza, “Computer Network Security”, Springer, 2005.

Reference Books :

1. Thomas Calabrese, Tom Calabrese, “Information Security Intelligence Cryptographic: Principles & Application”, Thomson Delmar Learning, 2004.
2. Swiderski, Frank, Syndex, “Threat Modeling”, Microsoft Press, 2004.
- 3 William. R Cheswick, Steven M. Bellowin, Aviel D Rubin, “Firewalls & Internet Security – Repelling the Wily Hacker”, Addison Wesley Professional, 2nd Edition, 2003.

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

Semester: M.Tech. – 2nd

Subject: **Software Engineering and Security**

Total Theory Periods: **40**

Minimum number of Class tests to be conducted: 02

Branch: **Information Security**

Code: **571214 (22)**

Total Tutorial Periods: **12**

Total Marks in End Semester Exam: **100**

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, Concurrence 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

UML diagrams for security requirement, Security Business process, Physical Security, Security Critical Interaction, Security state, Analyzing Model – Notation, Formal semantics, Security analysis, Important security opportunities, Model based security engineering with UML, UML Security profile, Design principles for secure systems, Applying security patterns.

Unit - V APPLICATIONS AND CASE STUDIES

Tool support for UML Security, Extending UML CASE TOOLS with analysis tools, Automated tools for UML Security, Formal Foundations on UML machines, Rely guarantee specifications, Reasoning about security properties.

Text / Reference Books :

1. John Musa D, “Software Reliability Engineering”, Tata McGraw-Hill, 2nd Edition, 2005.
2. Jan Jürjens, “Secure Systems Development with UML”, Springer; 2004.

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

Semester: M.Tech. – 2nd

Subject: **Intelligent Systems (ELECTIVE – II)**

Total Theory Periods: **40**

Minimum number of Class tests to be conducted: 02

Branch: **Information Security**

Code: **571231 (22)**

Total Tutorial Periods: **12**

Total Marks in End Semester Exam: **100**

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

Introduction to Neuro - Fuzzy Systems, Fuzzy System Design Procedures, Fuzzy Sets and Logic Background, Fuzzy/ANN Design and Implementation.

Unit-V GENETIC ALGORITHMS

Introduction, Robustness of Traditional Optimization and Search Techniques, The goals of Optimization, Computer Implementation, Applications.

Text Books :

1. Limin Fu , “Neural Network in Computer Intelligence”, McGraw-Hill International Editions, 1994.
2. Timothy J. Ross , “Fuzzy Logic with Engineering Applications”, McGraw-Hill, 2004.

Reference Books :

1. Nils J. Nilsson, “Principles of Artificial Intelligence”, Narosa Publishing House, 1980.
2. Elaine Rich and Kelvin Knight, “Artificial Intelligence”, McGraw-Hill Edition.1991.
3. David E. Goldberg , “Genetic Algorithms : Search, optimization and Machine Learning”, Pearson Education, 1999.
4. George J. Klin and Bo Yuan , “Fuzzy Systems & Fuzzy Logic – Theory and Applications”, Prentice Hall of India, 1995.

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

Semester: M.Tech. – 2nd

Branch: **Information Security**

Subject: **Information Security policies and Procedures (ELECTIVE – II)** Code: **571232 (22)**

Total Theory Periods: **40**

Total Tutorial Periods: **12**

Minimum number of Class tests to be conducted: 02

Total Marks in ESE: **100**

Unit-I SECURITY AND COMPUTING

Characteristics of Computer Intrusion, Attacks, Security goals, Criminals, Methods of defense control, Cryptography, Digital Signatures, Program Security, Protection in Operating System, Design of trusted Operating Systems.

Unit-II ETHICAL ISSUES IN SECURITY

Database Security, Security in networks, Network Controls, Firewalls, Intrusion detection Systems, Secure Email, Administrating Security, Organization Security polices, Legal privacy ethical issues in computer 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

Information Security, Fundamentals, Employee responsibilities, Information classification, Information handling, Tools of information security, Information processing, Secure program administration.

Unit-V CASE STUDIES

Organization Security Model, Information handling procedures, Developing Information standard manual, Developing Information security manual.

Text Books :

1. Willis H Ware, Charles P Pfleeger, and Shari Lawrence Pfleeger, "Security in Computing", Prentice Hall, 2003.
2. Thomas R. Peltier, "Information Security policies and procedures: A Practitioner's Reference", 2nd Edition Prentice Hall, 2004.

Reference Books :

- 1 Thomas R Peltier, Justin Peltier, and John Blackley," Information Security Fundamentals", Second Edition, Prentice Hall, 1996.
2. Jonathan Rosenoer, "Cyberlaw: the Law of the Internet", Springer-Verlag, 1997.

Chhattisgarh Swami Vivekananda Technical University, Bilai (C.G.)

Semester: M.Tech. – 2nd

Branches: **Information Security & Computer Technology.**

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

Desktop Supercomputing, Parallel Computing, Parallel Programming Paradigms, Problems of Current parallel Programming Paradigms, Desktop Supercomputing Programming Paradigms, Parallelizing Existing Applications, Grid Enabling Software Applications, Needs of the Grid users, methods of Grid Deployment, Requirements for Grid enabling Software, Grid Enabling Software Applications.

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 :

1. Ahmar Abbas, "Grid Computing: A Practical Guide to Technology and Applications", Firewall Media, 2004.
2. Joshy Joseph and Craig Fellenstein, "Grid Computing", Pearson Education, 2001.

Reference Books :

1. Ian Foster and Carl Kesselman, "Grid Blue Print for New Computing Infrastructure", Morgan Kaufmann, 2000.
2. Fran Berman, Geoffrey Fox and Anthony J. G. Hey, "Grid Computing: Making the Global Infrastructure a Reality", Willy Publisher, 2001.

Chhattisgarh Swami Vivekananda Technical University, Bilai (C.G.)

Semester: M.Tech. – 2nd
Subject: **Network Simulation and Security Lab.**
Total Theory Periods: **NIL**
Total Marks in End Semester Exam: **75**

Branch: **Information Security**
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.
9. Simulation of UDP protocol.
10. Simulation of TCP protocol.

Text / Reference Books :

1. William Stallings, "Network Security", PHI, Second Edition, 2005.
2. B. Forouzan, "Cryptography and Network Security", McGraw-Hill, 2004.
3. NS2 MANUAL.

Chhattisgarh Swami Vivekananda Technical University, Bilai (C.G.)

Semester: M.Tech. – 2nd
Subject: **Biometric Security Systems Lab.**
Total Theory Periods: **NIL**
Total Marks in End Semester Exam: **75**

Branch: **Information Security**
Code: **571222 (22)**
Total Practical Periods: **40**

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).
14. Case based study using EMG (Electro Myogram).

Text / Reference Books :

1. John Chirillo and Scott Blaul, "Implementing Biometric Security", Wiley Eastern Publications, 2005.