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

Scheme of Teaching & Examination

M. Tech. (e-Security)

Department: INFORMATION TECHNOLOGY

2nd Semester

S. No	Board of Study	Subject Code	Subject	Periods per Week			Scheme of Examination Theory / Practical			Total Marks	Credit L+(T+P) / 2
				L	T	P	ESE	CT	TA		
1	Information Technology	577211 (33)	Trusted Internet	3	1	-	100	20	20	140	4
2	Information Technology	577212 (33)	Business Ethics and Cyber Laws	3	1	-	100	20	20	140	4
3	Information Technology	577213 (33)	Advanced Cryptography	3	1	-	100	20	20	140	4
4	Information Technology	577214 (33)	Security Threats and Management	3	1	-	100	20	20	140	4
5	*Refer Table - II*		*Elective - II*	3	1	-	100	20	20	140	4
6	Information Technology	577221 (33)	Secured Operating System Lab	-	-	3	75	-	75	150	2
7	Information Technology	577222 (33)	Image Processing and Security Lab	-	-	3	75	-	75	150	2
Total				15	5	6	650	100	250	1000	24

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

TABLE –II			
ELECTIVE –II			
S. No	Board of Study	Subject Code	Subject
1	Information Technology	577231 (33)	Mobile Wireless Security
2	Computer Sc. & Engg.	571233 (22)	Grid Computing
3	Information Technology	577232 (33)	Steganography & Water Marking

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. IInd**
Subject: **Trusted Internet**
Total Theory Periods: **40**
Total Marks in End Semester Exam. : **100**
Minimum number of class test to be conducted: **02**

Specialization : e-Security
Code: 57211 (33)
Total Tutorial Periods: 12

UNIT I
Internet: Understanding the Internet, Hardware Requirements to connect to the internet, Software requirements and Internet Service Providers (ISP), Internet Addressing, Internet Protocol : Routing Information Protocol (RIP), User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Domain Name Service (DNS), Basic Connectivity: Telnet, FTP, Internet Relay Chat (IRC).

UNIT II
Access Attacks: Hacker Techniques – Snooping, Eavesdropping, interception, Hacker's motivation, Historical Hacking Techniques; Advance Techniques, Targeted Hacker, Information Security Services – Confidentiality, Integrity, Availability and Accountability.

UNIT III
Firewalls: Concepts, Types of Firewalls, Firewall Configuration, Design a Firewall Rule set, Purpose of Firewall, Security role of a Firewall, Advantages and disadvantages of firewall, Firewall Components, Procuring a Firewall, Administrating a firewall, firewall toolkits.

UNIT IV
Encryption: Basic Concepts, Private Key Encryption, Public Key Encryption, Digital Signature, Trust in the System, Encryption Algorithm – RSA Encryption, Blowfish Encryption.

UNIT V
Security Mechanism: User Authentication, Attacks from inside the system, Attacks from outside the system, Protection Mechanism: Snooping, Eavesdropping, interception, Trusted Systems, Trusted Computing Base, Formal Models of Secure system, Multi-level security, designing trusted Operating System.

TEXT BOOKS:

1. Marcus Goncalves., "Firewalls - A Complete Guide", Tata McGraw-Hill, 2000
2. Harley Hahn., "The Internet – Complete Reference", Tata McGraw-Hill, 1997.
3. William Stallings, "Cryptography and Network Security", Pearson Education (Singapore) Pvt. Ltd. 3rd Edition.

REFERENCES:

1. Andrew S. Tanenbaum, "Modern Operating Systems", Pearson Education (Singapore) Pvt. Ltd. 3rd Edition.
2. Ankit Fadia, "Unofficial Guide to Ethical Hacking", Macmillan India Ltd, 2001.
3. Charles P. Pleeger, Shari Lawrence Pleeger, "Security in Computing", Pearson Education (Singapore) Pvt Ltd, 3rd Edition.
4. Richard E. Smith, "Internet Cryptography", Pearson Education(Singapore) Pvt Ltd, 2000.

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

Semester: **M.TECH. IInd**
Subject: **Business Ethics and Cyber Laws**
Total Theory Periods: **40**
Total Marks in End Semester Exam. : **100**
Minimum number of class test to be conducted: **02**

Specialization : e-Security
Code: **57212 (33)**
Total Tutorial Periods: **12**

UNIT – I
Business Ethics: Principles of Business Ethics- Ethical philosophies, Ethical management. Corporate Governance - principles, mechanisms and control. Corporate Social Responsibility – approaches, social accounting, auditing and reporting, Benefits of Corporate Social Responsibility.

UNIT – II
Ethical Practices: Creating an ethical organization. Workplace Ethics, Environment and Ethics, Ethics in Marketing and Consumer Protection, Ethics in Accounting and Finance, Ethics in Human Resource Management, intellectual property and skills.

Unit III
Cyber Crimes: Related concepts, distinction between cyber crimes and conventional crimes, Cyber criminals and their objectives, Kinds of cyber crimes cyber-stalking, cyber pornography, forgery and fraud, crime related to IPRs, cyber terrorism, computer vandalism etc. Cyber forensics, digital forensics and the law, forensic evidence, digital forensic tools.

Unit IV
Legal Issues in Cyber Crime: Issues relating to investigation, issues relating to jurisdiction, issues relating to evidence, relevant provisions under Information Technology Act 2000, Indian penal code, Pornography Act and Indian Evidence Act.

Unit V
Copyright Issues: Linking, framing, protection of content on web site, international treaties, trade mark issues in cyberspace, domain name dispute, cyber squatting, uniform dispute resolution policy, computer software and related IPR (Intellectual Property Rights) issues.

TEXT BOOKS:

1. Marianne Moody Jennings," Business: Its Legal, Ethical, and Global Environment", Cengage Learning India ,3rd Edition.
2. Jonathan Rosenoer," CyberLaw: The Law of the Internet", Springer, ,3rd Edition.
3. Zeinab Karake Shalhoub, Lubna Al Qasimi, Zeinab Karake Shalhoub "Cyber Law and Cyber Security in Developing and Emerging Economies", Springer, , 1st Edition.
4. M C Kuchhal, Business Law, Vikas publishing, New Delhi
5. Avtar Singh, "Principles of Mercantile Law," Eastern Book Company, Lucknow, 2006.

REFERENCES:

1. Nelson, Phillips, "Computer Forensics and Investigations", Cengage Learning India.
2. Vinod V. Sople, "Managing Intellectual Property" PHI Learning Private Limited.
3. Dr.R.K.Tiwari P.K.Sastri,K.V. Ravikumar, "Computer Crime and Computer Forensics", First Edition

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

Semester: **M.TECH. IInd**   Specialization : e-Security
Subject: **Advanced Cryptography**   Code: **57213 (33)**
Total Theory Periods: **40**   **Total Tutorial Periods: 12**
Total Marks in End Semester Exam. : **100**
Minimum number of class test to be conducted: **02**

UNIT I
OSI security architecture: Classical encryption techniques , Cipher principles ,Data encryption standard , Block cipher design principles and modes of operation ,Evaluation criteria for AES , AES cipher , Triple DES , Placement of encryption function , Traffic confidentiality.

UNIT II
Key management: Diffie Hellman key exchange , Elliptic curve architecture and cryptography, Introduction to number theory, Confidentiality using symmetric encryption , Public key cryptography and RSA.

UNIT III
Authentication requirements: Authentication functions , Message authentication codes , Hash functions , Security of hash functions and MACS , MD5 Message Digest algorithm , Secure hash algorithm , Ripend , HMAC digital signatures , Authentication protocols

UNIT IV
Quantum Cryptography and Quantum Teleportation: Heisenberg uncertainty principle, polarization states of photons, quantum cryptography using polarized photons, local vs. non local interactions, entanglements, EPR paradox, Bell's theorem, Bell basis, teleportation of a single qubit – theory and experiments.

UNIT V
Future trends: Review of recent experimental achievements, study on technological feasibility of a quantum computer, candidate physical systems and limitations imposed by noise.

TEXT BOOKS:

1.   William Stallings, "Cryptography and Network Security - Principles and Practices", 3rd Edition, Prentice Hall of India, 2003.
2.   Atul Kahate, "Cryptography and Network Security", Tata McGraw - Hill, 2003.
3.   William Stallings, "Network Security Essentials: Applications and Standards", Pearson Education Asia, 2000.

REFERENCES:

1.   R. P. Feynman, "Feynman lectures on computation", Penguin Books, 1996.
2.   Gennady P. Berman, Gary D. Doolen, Ronnie Mainiri & Valdmis Itri Frinovich, "Introduction to quantum computers", World Scientific, Singapore, 1998.
3.   Jonathan Katz, Yehuda Lindell," Introduction to Modern Cryptography" Principles And Protocols",CRC Press.

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

Semester: **M.TECH. IInd**   **Specialization : e-Security**
Subject: **Security Threats and Management**   **Code**: **57214 (33)**
Total Theory Periods: **40**   **Total Tutorial Periods: 12**
Total Marks in End Semester Exam. : **100**
Minimum number of class test to be conducted: **02**

UNIT I
Introduction: Security threats, Sources of security threats, Motives , Target Assets and vulnerabilities , Consequences of threats, E-mail threats , Web-threats , Intruders and Hackers, Cyber crimes.

UNIT II
Network Threats: Active/ Passive , Interference , Interception , Impersonation , Worms , Virus , Spams , Adware , Spy ware , Trojans , Backdoors , Bots, IP Spoofing , ARP spoofing , Session Hijacking , Sabotage-Internal treats, Environmental threats , Threats to Server security.

UNIT III
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 Panning.

UNIT IV
Security Privileges and Credentials: Access Rights , Access control systems , Authorization and Authentication , types, policies and techniques , Security certification , Security monitoring and Auditing , Security Requirements Specifications , Security Policies and Procedures.

UNIT V
Firewalls & Intrusion Detection Systems: Firewalls , Types, Dynamic packet filtering content filtering , Crypto capable Routers, VPNs , Secure Modems , Intrusion Detection Systems , Types , Intrusion Detection Tools , Penetration testing, Intrusion Analysis, Log file Monitors , Honey pots , Intrusion Prevention Systems , Trusted Systems.

TEXT BOOKS:
1. Joseph M Kizza, "Computer Network Security", Springer, 2005
2. Swiderski, Frank, Syndex, "Threat Modeling", Microsoft Press, 2004.
3. Alberto Partida, Diego Andina ," IT Security Management: IT Securiteers - Setting up an IT Security Function", Springer.

REFERENCES:
1. Thomas Calabrese,Tom Calabrese, "Information Security Intelligence: Cryptographic Principles & Application", Thomson Delmar Learning, 2004
2. William. R Cheswick, Steven M. Bellowin, Aviel D Rubin, "Firewalls & Internet Security – Repelling the Wily Hacker", 2nd Edition, Addison Wesley Professional, 2003.
3. Gerard Blokdijk, Ivanka Menken, Gerard Blokdijk" Information Security Management Best Practice ", Lulu Publication.
4. Karim H. Vellani," Strategic Security Management: A Risk Assessment Guide for Decision Makers", Butterworth-Heinemann publication.

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

Semester: **M.TECH. IInd**　　　　　　　　　　Specialization : **e-Security**
Subject: **Mobile Wireless Security (Elective II)**　　**Code**: **577231 (33)**
Total Theory Periods: **40**　　　　　　　　　　**Total Tutorial Periods: 12**
Total Marks in End Semester Exam. : **100**
Minimum number of class test to be conducted: **02**

UNIT I
Wireless Fundamentals: Wireless Hardware, Wireless Network Protocols, Wireless Programming, Wired Equivalent Privacy (WEP) Security. Wireless Cellular Technologies , concepts , Wireless reality , Security essentials , Information classification standards , Wireless Threats: Cracking WEP - Hacking Techniques, Wireless Attacks, Airborne Viruses.

UNIT II
Standards and Policy Solutions: Network Solutions , Software Solutions, Physical Hardware Security, Wireless Security , Securing WLAN , Virtual Private Networks , Intrusion Detection System, Wireless Public Key infrastructure, Tools , Auditing tools , Pocket PC hacking , wireless hack walkthrough.

UNIT III
Security Issues: Authentication , Access control and Authorization , Non-repudation, privacy and Confidentiality , Integrity and Auditing ,Security analysis process. Privacy in Wireless World , Legislation and Policy , Identify targets and roles analysis, Attacks and vulnerabilities , Analyze mitigations and protection.

UNIT IV
Implementation Issues: WLAN Configuration, IEEE 802.11, Physical layer ,media access frame format , systematic exploitation of 802.11b, WLAN, WEP – WEP Decryption script , overview of WEP attack , Implementation , Analyses of WEP attacks.

UNIT V
Mobile Commerce: Reputation and Thrust, Intrusion detection , Vulnerabilities analysis of mobile commerce platform, Secure authentication for mobile users , Mobile Commerce security , Payment methods, Mobile Coalition key evolving Digital Signatures scheme for wireless mobile networks.

TEXT BOOKS:
1. Russel Dean Vines,"Wireless Security Essentials: Defending Mobile from Data Piracy", John Wiley & Sons, First Edition – 2002.
2. Cyrus, Peikari, Seth Fogie, "Maximum Wireless Security", SAMS Publishing 2002.
3. S. Kami Makki,"Mobile and Wireless Network Security and Privacy", Springer, Second Edition

REFERENCES:
1. Tara M. Swaminathan, Charles R. Eldon, "Wireless Security and Privacy- Best Practices and Design Techniques", Addison Wesley –2002.
2. Bruce Potter, Bob Fleck, "802.11 Security", O'Reilly Publications,2002.
3. Wen Chen hu, Chang Wiu Lee, Weidong kou, "Advances in Security and Payment Methods for Mobile Commerce", Idea Group Inc-2004**.**

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

Semester: **M.TECH. IInd**
Subject: **Grid Computing (Elective II)**
Total Theory Periods: **40**
Total Marks in End Semester Exam. : **100**
Minimum number of class test to be conducted: **02**

Specialization : **e-Security**
Code: **571233 (33)**
Total Tutorial Periods: 12

UNIT - I
Introduction: 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
Architecture and Services: 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
Computing Paradigms: 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
Emerging Areas: 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.

REFERENCES :

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.
3. Janakiram , Grid Computing ,TMH Publications

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

Semester: **M.TECH. IInd**   Specialization : e-Security
Subject: **Steganography & Water Marking (Elective II)**   **Code**: 577232 (33)
Total Theory Periods: **40**   **Total Tutorial Periods: 12**
Total Marks in End Semester Exam. : **100**
Minimum number of class test to be conducted: **02**

UNIT I
Introduction to Information hiding: Brief history and applications of information hiding, Principles of Steganography, Frameworks for secret communication , Security of Steganography systems , Information hiding in noisy data, Adaptive versus non adaptive algorithms , Laplace filtering Using cover models, Active and malicious attackers, Information hiding in written text, Examples of invisible communications.

UNIT II
Survey of Steganographic techniques: Substitution system and bitplane tools ,Transform domain techniques , Spread spectrum and information hiding , Statistical Steganography , Distortion and code generation techniques, Automated generation of English text.

UNIT III
Steganalysis: Detecting hidden information: text, audio, video and images, Extracting hidden information, Disabling hidden information, Watermarking techniques, Basic Message Coding, Error Correction coding , Information Theoretic analysis and design issues, Evaluation and benchmarking of watermarking system.

UNIT IV
Survey of current watermarking techniques: Cryptographic and psycho visual aspects, Choice of a workspace: binary image, audio, video.Formatting the watermark beds - Digital watermarking schemes: Spread Spectrum, DCT (Discrete Cosine Transform),Domain and Quantization schemes , Watermarking with side information , Robustness to temporal and geometric distortions.

UNIT V
Data Right Management: DRM Products and Laws, Fingerprints – Examples, Protocols and Codes– Boneh-Shaw finger printing Scheme , Steganography and watermarking applications – Military, Digital copyright protection and protection of intellectual property.

TEXT BOOKS:

1. Stefan Katzenbelsser and Fabien A. P. Petitcolas, Information hiding techniques for Steganography and Digital Watermarking, ARTECH House Publishers, January 2004.
2. I.J. Cox, M.L. Miller, J.Fridrich and T.Kalker, Digital Water Marking and Steganography, 2nd Edition, Morgan Kauffman Publishers, 2008.
3. Johnson, Neil F. / Duric, Zoran / Jajodia, Sushil G ,Information Hiding: Steganography and Watermarking - Attacks and Countermeasures (Advances in Information Security, Volume 1),2001.

REFERENCES:

1. Peter Wayner, "Disappearing Cryptography: Information Hiding, Steganography and Watermarking 2/e", Elsevier.

2. Practical Cryptography, N.Ferguson and B.Schneier, Wiley Publishing Inc., 2003.
3. Bolle, Connell et. al., "Guide to Biometrics", Springer
4. John Vecca, "Computer Forensics: Crime scene Investigation", Firewall Media
5. Christopher L.T. Brown, "Computer Evidence: Collection and Preservation", Firewall Media.

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

Semester: **M.TECH. IInd**   **Specialization : e-Security**
Subject: **Secured Operating System Laboratory**   **Code**: **577221 (33)**
Total Theory Periods: **40**   **Total Tutorial Periods: 12**
Total Marks in End Semester Exam. : **100**
Minimum number of class test to be conducted: **02**

List of Experiments:

(Implement the following on LINUX platform. Use C for high level language implementation)
1.   Shell programming
             - command syntax
             - write simple functions
             - basic tests
2.   Shell programming
             - loops
             - patterns
             - expansions
             - substitutions
3.   Write programs using the following system calls of UNIX operating system:
        fork, exec, getpid, exit, wait, close, stat, opendir, readdir
4.   Write programs using the I/O system calls of UNIX operating system (open, read, write, etc)
5.   Write C programs to simulate UNIX commands like ls, grep, etc.
6.   Given the list of processes, their CPU burst times and arrival times, display/print the Gantt chart   for FCFS and SJF. For each of the scheduling policies, compute and print the average waiting time and average turnaround time
7.   Given the list of processes, their CPU burst times and arrival times, display/print the Gantt   chart for Priority and Round robin. For each of the scheduling policies, compute and print the average waiting time and average turnaround time
8.   Implement the Producer – Consumer problem using semaphores.
9.   Write a shell script to scan current operating system security settings.

10.   Write a program to create a secured pipe for Inter-Process Communication.

11.   Identify Vulnerabilities (Potential Threats) of Operating System and Security features.

12.   Identify and analyze Buffer overflow problem.

13.   Implement some memory management schemes – I for e.g.
      Free space is maintained as a linked list of nodes with each node having the starting byte address and the ending byte address of a free block. Each memory request consists of the process-id and the amount of storage space required in bytes. Allocated memory space is again maintained as a linked list of nodes with each node having the process-id, starting byte address and the ending byte address of the allocated space.
14.   Implement some memory management schemes – II for e.g.
      When a process finishes (taken as input) the appropriate node from the allocated list should be deleted and this free disk space should be added to the free space list. [Care should be taken to merge contiguous free blocks into one single block. This results in deleting more than one node from the free space list and changing the start and end address in the appropriate node. For allocation use first fit, worst fit and best fit.

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

Semester: **M.TECH. IInd**   **Specialization : e-Security**
Subject: **Image Processing & Security Lab**   **Code**: **577222 (33)**
Total Theory Periods: **40**   **Total Tutorial Periods: 12**
Total Marks in End Semester Exam. : **100**
Minimum number of class test to be conducted: **02**

List of Experiments:

1. Study and Analyze important Image Processing toolbox functions with at least two standard images like Cameraman, Lena, Monkey, and others.
2. Write a program for Image reading and displaying the results in matrix form and hence changing the matrix elements by multiplying with the factor 0.001 and hence writing to a file with extension .jpeg format and hence plot a histogram.
3. Write a program for performing Point-to-point transformation.
4. Write a program for performing Morphological operations .(The operations that can be performed are erosion, dilation, opening, closing, open-close, close-open.)
5. Write a program to hide a word in an image file and retrieve it (Stenography).
6. Histogram equalization. This experiment illustrates the relationship among the intensities (gray levels) of an image and its histogram. It shows how to improve the image by equalizing the histogram.
7. Write a program for performing Geometric transformations by using translation , rotation scaling of given image.
8. Write a program for performing Linear filtering using convolution. After completing this experiment every student should understand the concepts of filtering using linear convolution.
9. Write a program for applying highly selective filters upon input images. In this experiment students appreciate the effects on an image after a highly selective filter is applied to it.
10. Write a program for performing Non Linear filtering upon input images using convolution masks. This experiment allows students to understand the effects of a median filter on an image corrupted with impulsive noise.
11. Write a program to use Entropy as a compression measure upon input images. This experiment introduces students to entropy as compression measurement to the DPCM compression measure.
12. Write a program for performing Edge detection upon input images. This experiment enables students to understand the concept of edge detectors and their operation in noisy images.
13. Write a program for Converting Color to Gray Scale and hence enhancement with segmentation.