VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM

SCHEME OF TEACHING AND EXAMINATION FOR

M.Tech. IN CYBER FORENSICS AND INFORMATION SECURITY

I Semester **CREDIT BASED**

Subject Code	Name of the Subject	Teaching hours/week		Duration of Exam in Hours	Marks for		Total Marks	CREDITS
		Lecture	Practical / Field Work / Assignment/ Tutorials		I.A.	Exam		
14SFC11	Ethical Hacking	4	2	3	50	100	150	4
14SFC12	Pragmatics of Information Security	4	2	3	50	100	150	4
14SFC13	Cyber Crime And Cyber Forensics	4	2	3	50	100	150	4
14SFC14	Basics of Forensic Psychology	4	2	3	50	100	150	4
14SFC15X	Elective 1	4	2	3	50	100	150	4
14SFC16	Ethical Hacking Laboratory	--	3	3	25	50	75	2
14SFC17	Seminar	--	3	--	25	--	25	1
Total		**20**	**16**	**18**	**300**	**550**	**850**	**23**

Elective – 1

01 14SFC151: Access control and Identity Management System

02 14SFC152: Cloud Security

03 14SFC153: Advanced Cryptography

04 14SFC154: Application and Web Security

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM

SCHEME OF TEACHING AND EXAMINATION FOR

M.Tech. IN CYBER FORENSICS AND INFORMATION SECURITY

II Semester **CREDIT BASED**

Subject Code	Name of the Subject	Teaching hours/week		Duration of Exam in Hours	Marks for		Total Marks	CREDITS
		Lecture	Practical / Field Work / Assignment/ Tutorials		I.A.	Exam		
14SFC21	Preserving & Recovering Digital Evidence	4	2	3	50	100	150	4
14SFC22	Operating System Security	4	2	3	50	100	150	4
14SFC23	Secured Programming	4	2	3	50	100	150	4
14SFC24	Cyber Laws & Ethics	4	2	3	50	100	150	4
14SFC25X	Elective 2	4	2	3	50	100	150	4
14SFC26	Secure Programming Laboratory		3	3	25	50	75	2
14SFC27	Seminar	--	3	--	25	--	25	1
	**Project Phase-I(6 week Duration)	--	--	--	--	--	--	--
Total		**20**	**16**	**18**	**300**	**550**	**850**	**23**

Elective – 2

01 14SFC251: Biometric Security

02 14SFC252: Trust Management in E-Commerce

03 14SFC253: Information Security Policies in Industry

04 14SFC254: Database Security

**** Between the II Semester and III Semester, after availing a vocation of 2 weeks.**

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM

SCHEME OF TEACHING AND EXAMINATION FOR

M.Tech. IN CYBER FORENSICS AND INFORMATION SECURITY

III Semester: INTERNSHIP **CREDIT BASED**

Course Code	Subject	No. of Hrs./Week		Duration of the Exam in Hours	Marks for		Total Marks	CREDITS
		Lecture	Practical / Field Work		I.A.	Exam		
14SFC31	Seminar / Presentation on Internship (After 8 weeks from the date of commencement)	-	-	-	25	-	25	1
14SFC32	Report on Internship	-	-	-		75	75	15
14SFC33	Evaluation and Viva-voce	-	-	-	–	50	50	4
	Total	**-**	**-**	**-**	**25**	**125**	**150**	**20**

* The student shall make a midterm presentation of the activities undertaken during the first 8 weeks of internship to a panel comprising **Internship** Guide, a senior faculty from the department and Head of the Department.

The College shall facilitate and monitor the student internship program.

The internship report of each student shall be submitted to the University.

****Between the III Semester and IV Semester after availing a vacation of 2 weeks.**

VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELGAUM

SCHEME OF TEACHING AND EXAMINATION FOR

M.Tech. IN CYBER FORENSICS AND INFORMATION SECURITY

IV Semester **CREDIT BASED**

Subject Code	Subject	No. of Hrs./Week		Duration of Exam in Hours	Marks for		Total Marks	CREDITS
		Lecture	Field Work / Assignment / Tutorials		I.A.	Exam		
14SFC41	File System Forensic Analysis	4	2	3	50	100	150	4
14SFC42x	Elective-3	4	2	3	50	100	150	4
14SFC43	Evaluation of Project Phase-I	-	-	-	25	-	25	1
14SFC44	Evaluation of Project Phase-II	-	-	-	25	-	25	1
14SFC45	Evaluation of Project Work and Viva-voce	–	-	3	-	100+100	200	18
Total		**8**	**04**	**09**	**150**	**400**	**550**	**28**
Grand Total (I to IV Sem.) : 2400 Marks; 94 Credits								

Elective – 3

01 14SFC421 Security Architecture Design

02 14SFC422 Steganography And Digital Watermarking

03 14SFC423 Mobile Device Forensics

04 14SFC424 Security Assessment and Verification

Note:

1) Project Phase – I**:** 6 weeks duration shall be carried out between II and III Semesters. Candidates in consultation with the guides shall carryout literature survey / visit to Industries to finalize the topic of dissertation.
2) Project Phase – II**:** 16 weeks duration during III Semester. Evaluation shall be taken during the Second week of the IV Semester. Total Marks shall be 25.
3) Project Evaluation: 24 weeks duration in IV Semester. Project Work Evaluation shall be taken up at the end of the IV Semester. Project Work Evaluation and Viva-Voce Examinations shall be conducted. Total Marks shall be 250 (Phase I Evaluation: 25 Marks, Phase –II Evaluation: 25 Marks, Project Evaluation marks by Internal Examiner (guide): 50, Project Evaluation marks by External Examiner: 50, marks for external and 100 for viva-voce).

   Marks of Evaluation of Project:

   - The I.A. Marks of Project Phase – I & II shall be sent to the University along with Project Work report at the end of the Semester.

4) During the final viva, students have to submit all the reports.
5) The Project Valuation and Viva-Voce will be conducted by a committee consisting of the following:

   a) Head of the Department (Chairman)
   b) Guide
   c) Two Examiners appointed by the university. (Out of two external examiners at least one should be present).

Course Title: ETHICAL HACKING	**Course Code: 14SFC11**
Credits(L:T:P): (4-0-0)	**Core/Elective: Core**
Type of Course: Lecture	**Total Contact Hours: 50**

UNIT I **10 Hours**

Casing the Establishment: What is foot printing, Internet Foot printing, Scanning, Enumeration, basic banner grabbing, Enumerating Common Network services. Case study: Network Security Monitoring.

UNIT II **10 Hours**

Securing permission: Securing file and folder permission, Using the encrypting file system, Securing registry permissions. Securing service: Managing service permission, Default services in windows 2000 and windows XP. Unix: The Quest for Root, Remote Access vs Local access, Remote access, Local access., After hacking root.

UNIT III **10 Hours**

Dial-up, PBX, Voicemail and VPN hacking, Preparing to dial up, War-Dialing, Brute-Force Scripting PBX hacking, Voice mail hacking, VPN hacking, Network Devices: Discovery Autonomous System Lookup, Public Newsgroups, Service Detection, Network Vulnerability, Detecting Layer 2 Media.

UNIT IV **10 Hours**

Wireless Hacking: Wireless Foot printing, Wireless Scanning and Enumeration, Gaining Access, Tools that exploiting WEP Weakness, Denial of Services Attacks, Firewalls: Firewalls landscape, Firewall Identification-Scanning Through firewalls, packet Filtering,

Application Proxy Vulnerabilities, Denial of Service Attacks, Motivation of Dos Attackers, Types of DoS attacks, Generic Dos Attacks, UNIX and Windows DoS.

UNIT V **10 Hours**

Remote Control Insecurities, Discovering Remote Control Software, Connection, Weakness.VNC, Microsoft Terminal Server and Citrix ICA, Advanced Techniques Session Hijacking, Back Doors, Trojans, Cryptography, Subverting the systems Environment, Social Engineering, Web Hacking, Web server hacking web application hacking, Hacking the internet Use, Malicious Mobile code, SSL fraud, E-mail Hacking, IRC hacking, Global countermeasures to Internet User Hacking.

TEXT BOOKS:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, Hacking Exposed 7: Network Security Secrets & Solutions, Tata Mc Graw Hill Publishers, 2010.

2. Bensmith, and Brian Komer, Microsoft Windows Security Resource Kit, Prentice Hall of India, 2010

REFERENCES:

1. Stuart McClure, Joel Scambray and Goerge Kurtz, "Hacking Exposed Network Security Secrets & Solutions", 5th Edition, Tata Mc Graw Hill Publishers, 2010.
2. Rafay Baloch, "A Beginners Guide to Ethical Hacking".

3. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, "Gray Hat Hacking The *Ethical Hackers* Handbook", 3rd Edition, McGraw-Hill Osborne Media paperback(January 27, 2011)

Course Title: PRAGMATICS OF INFORMATION SECURITY	**Course Code: 14SFC12**
Credits(L:T:P): (3-0-1)	**Core/Elective: Core**
Type of Course: Lecture & Practical	**Total Contact Hours: 50**

UNIT I **10 Hours**

Overview: Computer Security Concepts, Requirements, Architecture, Trends, Strategy Perimeter Security: Firewalls, Intrusion Detection, Intrusion Prevention systems, Honeypots

Case Study: Readings, Intrusion and intrusion detection by John McHugh.

UNIT II **10 Hours**

User Authentication: Password, Password-based, token based, Biometric, Remote User authentication.

Access Control: Principles, Access Rights, Discretionary Access Control, Unix File Access Control, Role Based Access Control

Internet Authentication Applications: Kerberos, X.509, PKI, Federated Identity Management.

UNIT III **10 Hours**

Cryptographic Tools: Confidentiality with symmetric encryption, Message Authentication & Hash Functions, Digital Signatures, Random Numbers.

Symmetric Encryption and Message Confidentiality: DES, AES, Stream Ciphers, Cipher Block Modes of Operation, Key Distribution.

UNIT IV **10 Hours**

Internet Security Protocols: SSL, TLS, IPSEC, S/ MIME. Public Key Cryptography and Message Authentication: Secure Hash Functions, HMAC, RSA, Diffie Hellman Algorithms Case Study: Readings, Programming Satan's Computer Ross Anderson and Roger Needham.

Unit V **10 Hours**

Malicious Software: Types of Malware, Viruses & Counter Measures, Worms, Bots, Rootkits Software Security: Buffer Overflows, Stack overflows, Defense, Other overflow attacks Case Study.

Readings: Smashing The Stack For Fun And Profit, Aleph One

http://www.phrack.com/issues.html?issue=49&id=14#article

TEXT BOOK:

1. Computer Security: Principles and Practice, William Stalling & Lawrie Brown, 2008, Indian Edition 2010, Pearson

REFERENCES:

1. Chuck Easttom, " Computer Security Fundamentals" Pearson, 2012.

LABORATORY

students have to carry out the mini project in the course with a team of two and shall be evaluated for 20 marks at the end of the semester.

Course Title: CYBER CRIME AND CYBER FORENSICS	**Course Code: 14SFC13**
Credits(L:T:P): (3-0-1)	**Core/Elective: Core**
Type of Course: Lecture & Practical	**Total Contact Hours: 50**

UNIT I **10 Hours**

Introduction and Overview of Cyber Crime, Nature and Scope of Cyber Crime, Types of Cyber Crime, Social Engineering, Categories of Cyber Crime, Property Cyber Crime.

UNIT II **10 Hours**

Unauthorized Access to Computers, Computer Intrusions, White collar Crimes, Viruses and Malicious Code, Internet Hacking and Cracking, Virus Attacks, Pornography, Software Piracy, Intellectual Property, Mail Bombs, Exploitation ,Stalking and Obscenity in Internet, Digital laws and legislation, Law Enforcement Roles and Responses.

UNIT III **10 Hours**

Introduction to Digital Forensics, Forensic Software and Hardware, Analysis and Advanced Tools, Forensic Technology and Practices, Forensic Ballistics and Photography, Face, Iris and Fingerprint Recognition, Audio Video Analysis, Windows System Forensics, Linux System Forensics, Network Forensics.

UNIT IV **10 Hours**

Introduction to Cyber Crime Investigation, Investigation Tools, eDiscovery, Digital Evidence Collection, Evidence Preservation, E-Mail Investigation, E-Mail Tracking, IP Tracking, E-Mail Recovery, Hands on Case Studies, Encryption and Decryption Methods, Search and Seizure of Computers, Recovering Deleted Evidences, Password Cracking.

UNIT V **10 Hours**

Laws and Ethics, Digital Evidence Controls, Evidence Handling Procedures, Basics of Indian Evidence ACT IPC and CrPC , Electronic Communication Privacy ACT, Legal Policies.

TEXT BOOKS:

1. Bernadette H Schell, Clemens Martin, “Cybercrime”, ABC – CLIO Inc, California, 2004.
2. ”Understanding Forensics in IT “, NIIT Ltd, 2005.
3. Nelson Phillips and Enfinger Steuart, “Computer Forensics and Investigations”, Cengage Learning, New Delhi, 2009.

REFERENCES:

1. Kevin Mandia, Chris Prosise, Matt Pepe, “Incident Response and Computer Forensics “, Tata McGraw -Hill, New Delhi, 2006.
2. Robert M Slade,” Software Forensics”, Tata McGraw - Hill, New Delhi, 2005.

Lab Exercises:

1. Introduction to Hardware tool and how to use them. (Search and seizure methods.)
2. Introduction to commonly used Forensic software. (Imaging Process.)
3. Introduction to commonly used OS and their file structure (Windows, DOS).
4. Introduction to commonly used OS and their file structure (UNIX, LINUX).
5. Introduction to AccessdataFTK forensic software suite. (All stages of Investigations.)
6. Introduction to Encase Forensic software compilations. (All stages of Investigations.)
7. Introduction to Encryption and Decryption software stores. (How & when to use.)
8. Introduction to other useful software commonly used. (Knowledge base of common software handling and understanding techniques.)
9. Perform all stages of Investigation on a Forensic Image provided. (Assignment work.)

Course Title: BASICS OF FORENSIC PSYCHOLOGY	**Course Code: 14SFC14**
Credits(L:T:P): (4-0-0)	**Core/Elective: Core**
Type of Course: Lecture	**Total Contact Hours: 50**

UNIT I **10 Hours**

Historical roots, Modern major perspectives of psychology, distinguishing professional and pseudo-psychology, types of psychological professionals. The science and research methods, professional ethics of research, research challenges.

UNIT II **10 Hours**

The biology underlying behavior: Nerves and neurons, structure and functions of neurons, neurotransmitters, Central Nervous System, peripheral nervous system. The human brain: its structure and function, sensory system and endocrine system, Stages of sleep, REM sleep, sleep disturbances, States of consciousness, altered states of consciousness, attention and awareness, sensation of perception, problems in attention and perception.

UNIT III **10 Hours**

Learning process: Latent learning, observational learning. Memory: Recalling long term memories, Retrieval clues, constructive purposes in memory, memory in courtroom, autobiographical memory. Stages in memory: Encoding, storage and retrieval of memory. Forgetting: Proactive and retroactive interference. Memory dysfunctions: Afflictions of forgetting.

UNIT IV **10 Hours**

Cognition: Thinking and reasoning, Thinking mental images, concepts, reasoning. Problem solving: Production, judgment, impediments to problems solving. Language and Intelligence Language: Grammar, language development, influence of language on thinking. Intelligence: Measuring intelligence (IQ), practical intelligence-measuring commonsense. Motivation and Emotion: Types of approaches of motivation. Emotion: Understanding emotional experiences, functions of emotions and determining range of emotions, Coping with stress.

UNIT V **10 Hours**

Personality: Theories-Psychoanalytic approaches to personality, Trait approaches, learning approaches, biological approaches, and humanistic approaches. Assessing personality: Self-report measures of personality, projective methods and behavioral assessment.

TEXTBOOKS:

1. Understanding Psychology by Robert S. Feldman, 4th edition, Mcgraw Hill, 1996.

REFERENCES:

1. Study Guide for Psychology: from science to practice by Baron, R.A. & Kolsher MJ
2. Forensic Psychology by Christopher Cronin
3. Introduction to Psychology by Dennis Coon
4. Introduction to forensic psychology: Research and Application, 3rd edition (paperback) by Curt R Bartol, Anne M Bartol

Course Title: ACCESS CONTROL AND IDENTITY MANAGEMENT SYSTEM	**Course Code: 14SFC151**
Credits(L:T:P): (4-0-0) **Type of Course: Lecture**	**Core/Elective: Elective** **Total Contact Hours: 50**

UNIT I **10 Hours**

Access control: Introduction, Attenuation of privileges, Trust and Assurance, Confinement problem, Security design principles, Identity Management models, local, Network, federal , global web identity, XNS approach for global Web identity, Centralized enterprise level Identity Management.

UNIT II **10 Hours**

Elements of trust paradigms in computing, Third party approach to identity trust, Kerberos, Explicit third party authentication paradigm, PKI approach to trust establishment, Attribute certificates, Generalized web of trust models, Examples.

UNIT III **10 Hours**

Mandatory access control, comparing information flow in BLP and BIBA models, Combining the BLP and BIBA models, Chinese wall problem.

UNIT IV **10 Hours**

Discretionary access control and Access matrix model, definitions, Safety problem, The take grant protection model, Schematic protection model, SPM rules and operations, Attenuating, Applications

UNIT V **10 Hours**

Role based access control, Hierarchical Access Control, Mapping of a mandatory policy to RABC, Mapping discretionary control to RBAC, RBAC flow analysis, Separation of Duty in

RBAC, RBAC consistency properties, The privileges perspective of separation of duties, Functional specification for RBAC.

TEXT BOOKS:

1. Messoud Benantar, “Access Control Systems: Security, Identity Management and Trust Models”, Springer, 2009.

REFERENCES:

1. Elena Ferrari and M. Tamer A-zsu , “Access Control In Data Management Systems”, Morgan & Claypool Publishers, 2010.

Course Title: CLOUD SECURITY	**Course Code: 14SFC152**
Credits(L:T:P): (4-0-0)	**Core/Elective: Elective**
Type of Course: Lecture	**Total Contact Hours: 50**

UNIT I **10 Hours**

Cloud Computing Architectural Framework: Cloud Benefits, Business scenarios, Cloud Computing Evolution, cloud vocabulary, Essential Characteristics of Cloud Computing, Cloud deployment models, Cloud Service Models, Multi- Tenancy, Approaches to create a barrier between the Tenants, cloud computing vendors, Cloud Computing threats, Cloud Reference Model, The Cloud Cube Model, Security for Cloud Computing, How Security Gets Integrated.

UNIT II **10 Hours**

Compliance and Audit: Cloud customer responsibilities, Compliance and Audit Security Recommendations.

Portability and Interoperability: Changing providers reasons, Changing providers expectations, Recommendations all cloud solutions, IaaS Cloud Solutions, PaaS Cloud Solutions, SaaS Cloud Solutions.

UNIT III **10 Hours**

Traditional Security, Business Continuity, Disaster Recovery, Risk of insider abuse, Security baseline, Customers actions, Contract, Documentation, Recovery Time Objectives (RTOs), Customers responsibility, Vendor Security Process (VSP).

UNIT IV **10 Hours**

Data Center Operations: Data Center Operations, Security challenge, Implement Five Principal Characteristics of Cloud Computing, Data center Security Recommendations.

Encryption and Key Management: Encryption for Confidentiality and Integrity, Encrypting data at rest, Key Management Lifecycle, Cloud Encryption Standards, Recommendations.

UNIT V **10 Hours**

Identity and Access Management: Identity and Access Management in the cloud, Identity and Access Management functions, Identity and Access Management (IAM) Model, Identity Federation, Identity Provisioning Recommendations, Authentication for SaaS and Paas customers, Authentication for IaaS customers, Introducing Identity Services, Enterprise Architecture with IDaaS , IDaaS Security Recommendations.

Virtualization: Hardware Virtualization, Software Virtualization, Memory Virtualization, Storage Virtualization, Data Virtualization, Network Virtualization, Virtualization Security Recommendations

TEXT BOOK:

1. Tim Mather, Subra Kumaraswamy, Shahed Latif, “Cloud Security and Privacy, An Enterprise Perspective on Risks and Compliance”, Oreilly Media 2009.

REFERENCES:

1. Vic (J.R.) Winkler, “ Securing the Cloud, Cloud Computer Security Techniques and Tactics”, Syngress, April 2011.

Course Title: ADVANCED CRYPTOGRAPHY	**Course Code: 14SFC153**
Credits(L:T:P): (4-0-0)	**Core/Elective: Elective**
Type of Course: Lecture	**Total Contact Hours: 50**

UNIT I **10 Hours**

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 **10 Hours**

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 **10 Hours**

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 **10 Hours**

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 **10 Hours**

Future trends: Review of recent experimental achievements, studyon 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.

Course Title: APPLICATION AND WEB SECURITY	**Course Code: 14SFC154**
Credits(L:T:P): (4-0-0)	**Core/Elective: Elective**
Type of Course: Lecture	**Total Contact Hours: 50**

UNIT I **9 Hours**

Web Application (In)security: The Evolution of Web Applications, Common Web Application Functions, Benefits of Web Applications , Web Application Security.

Core Defense Mechanisms: Handling User Access Authentication, Session Management, Access Control, Handling User Input, Varieties of Input Approaches to Input Handling, Boundary Validation.

Multistep Validation and Canonicalization: Handling Attackers, Handling Errors, Maintaining Audit Logs, Alerting Administrators, Reacting to Attacks.

UNIT II **9 Hours**

Web Application Technologies: The HTTP Protocol, HTTP Requests, HTTP Responses, HTTP Methods, URLs, REST, HTTP Headers, Cookies, Status Codes, HTTPS, HTTP Proxies, HTTP Authentication, Web Functionality, Server-Side Functionality, Client-Side Functionality, State and Sessions, Encoding Schemes, URL Encoding, Unicode Encoding, HTML Encoding, Base64 Encoding, Hex Encoding, Remoting and Serialization Frameworks.

UNIT III **9 Hours**

Mapping the Application: Enumerating Content and Functionality, Web Spidering, User-Directed Spidering, Discovering Hidden Content, Application Pages Versus Functional Paths, Discovering Hidden Parameters, Analyzing the Application, Identifying Entry Points for User Input, Identifying Server-Side Technologies, Identifying Server-Side Functionality, Mapping the Attack Surface.

UNITI IV **11 Hours**

Attacking Authentication: Authentication Technologies, Design Flaws in Authentication Mechanisms, Bad Passwords, Brute-Forcible Login, Verbose Failure Messages, Vulnerable Transmission of Credentials, Password Change, Functionality, Forgotten Password Functionality, "Remember Me" Functionality, User Impersonation, Functionality Incomplete, Validation of Credentials, Nonunique Usernames, Predictable Usernames, Predictable Initial Passwords, Insecure Distribution of Credentials.

Attacking Access Controls: Common Vulnerabilities, Completely Unprotected, Functionality Identifier-Based Functions, Multistage Functions, Static Files, Platform Misconfiguration, Insecure Access Control Methods.

UNIT V **12 Hours**

Attacking Data Stores: Injecting into Interpreted Contexts, Bypassing a Login, Injecting into SQL, Exploiting a Basic Vulnerability Injecting into Different Statement Types, Finding SQL Injection Bugs, Fingerprinting the Database, The UNION Operator, Extracting Useful Data, Extracting Data with UNION, Bypassing Filters, Second-Order SQL Injection, Advanced Exploitation Beyond SQL Injection: Escalating the Database Attack, Using SQL Exploitation Tools, SQL Syntax and Error Reference, Preventing SQL Injection.

TEXT BOOK

1. The Web Application Hacker's Handbook: Finding And Exploiting Security Defydd Stuttard, Marcus Pinto Wiley Publishing,Second Edition,

REFERENCES

1. Professional Pen Testing for Web application, Andres Andreu, Wrox Press

2. Carlos Serrao, Vicente Aguilera, Fabio Cerullo, "Web Application Security" Springer; 1st Edition

3. Joel Scambray, Vincent Liu, Caleb Sima ,"Hacking exposed", McGraw-Hill; 3rd Edition, (October, 2010)

4. OReilly Web Security Privacy and Commerce 2nd Edition 2011

5. Software Security Theory Programming and Practice, Richard sinn, Cengage Learning

6. Database Security and Auditing, Hassan, Cengage Learning

Course Title: ETHICAL HACKING LABORATORY	**Course Code: 14SFC16**
Credits(2)(L:T:P): (0-0-3)	**Core/Elective: Core**
Type of Course: Practical	**Total Contact Hours: 42**

1. Wireshark: Experiment to monitor live network capturing packets and analyzing over the live network.

1. LOIC: DoS attack using LOIC.
2. FTK: Bit level forensic analysis of evidential image and reporting the same.
3. Darkcomet : Develop a malware using Remote Access Tool Darkcomet to take a remote access over network.
4. HTTrack: Website mirroring using Httrack and hosting on a local network.
5. XSS: Inject a client side script to a web application.
6. Emailtrackerpro: Email analysis involving header check, tracing the route. Also perform a check on a spam mail and non-spam mail.

Course Title: PRESERVING & RECOVERING DIGITAL EVIDENCE	Course Code: 14SFC21
Credits(L:T:P): (3-0-1)	Core/Elective: Core
Type of Course: Lecture & Practical	Total Contact Hours: 50

UNIT I **10 Hours**

Digital evidence and computer crime: history and terminals of computer crime investigation, technology and law, the investigate process, investigate reconstruction, modus operandi, motive and technology, digital evidence in the court room.

UNIT II **10 Hours**

Computer basics for digital investigators: applying forensic science to computers, forensic examination of windows systems, forensic examination of Unix systems, forensic examination of Macintosh systems, forensic examination of handheld devices.

UNIT III **10 Hours**

Networks basics for digital investigators: applying forensic science to networks, digital evidence on physical and datalink layers, digital evidence on network and transport layers, digital evidence on the internet.

UNIT IV **10 Hours**

Investigating computer intrusions, investigating cyber stalking, digital evidence as alibi.

UNIT V **10 Hours**

Handling the digital crime scene, digital evidence examination guidelines

TEXTBOOKS:

1. Digital Evidence and Computer Crime Forensic science, Computers and Internet - Eoghan Casey, Elsevier Academic Press, Second Edition

REERENCES:

1. A Electronic Discovery and Digital Evidence in a Nut Shell-Shira A scheindlin, Daniel J Capra, The Sedona Conference, Academic Press, Third Edition (No where available)
2. Digital Forensic for Network, Internet, and Cloud Computing A forensic evidence guide for moving Targets and Data' – Terrence V.Lillard, Glint P.Garrison, Craig A..Schiller, James Steele, Syngress
3. The Best Damn Cybercrime and Digital Forensics Book Period' [Paperback] Jack Wiles , Anthony Reyes , Jesse Varsalone, Syngress Edition, 2007

Lab Exercises:

1. Advanced knowledge on using Hardware tools. (Search and seizure methods.)
2. Search and seizure methods continuation.
3. How to set up a Forensic Lab and considerations.
4. Deconstructing all OS, understanding where to find what.
5. Introduction to network forensic software, sniffer tools, Linux tools.
6. Network Forensic tools and experiments to capture wifi-data.
7. Wifi-data capture continued. Analysis of captured data.
8. Email stores all stages of Forensic processes.
9. Analysis of emails. Metadata analysis.
10. Performing an actual Investigation involving all the stages of a Forensic Investigation. (Part of Assignment work.)- To be graded.

Course Title: OPERATING SYSTEMS SECURITY	**Course Code: 14SFC22**
Credits(L:T:P): (3-0-1)	**Core/Elective: Core**
Type of Course: Lecture & Practical	**Total Contact Hours: 50**

UNIT I **10 Hours**

Introduction: Secure Os, Security Goals, Trust Model, Threat Model, Access Control. Fundamentals: Protection system, Lampson's Access Matrix, Mandatory protection system.

UNIT II **10 Hours**

Multics: Fundamentals, multics protection system models, multics reference model, multics security, multics vulnerability analysis.

UNIT III **10 Hours**

Security in ordinary operating system: UNIX security, windows security Verifiable security goals: Information flow, information flow secrecy, models, information flow integrity model, the challenges of trusted, process, covert channels.

UNIT IV **10 Hours**

Security Kernels: The Security Kernels, secure communications, processor Scomp, Gemini secure OS, Securing commercial OS, Retrofitting security into a commercial OS, History Retrofitting commercial OS, Commercial era, microkernel era, UNIX era- IX, domain and type enforcement.

UNIT V **10 Hours**

Case study: Solaris Extensions Trusted extensions, access control, Solaris compatibility, trusted extensions, mediations process rights management, role based access control, trusted

extensions, networking trusted extensions, multilevel services, trusted extensions administration.

Case study: Building secure OS for Linux: Linux security modules, security enhanced Linux.

TEXT BOOKS:

1. Trent Jaeger, Operating system security, Morgan & Claypool Publishers, 2008

REFERENCES:

1. Michael Palmer, Guide to Operating system Security Thomson
2. Andrew S Tanenbaum, Modern Operating systems, 3rd Edition
3. Secure Operating Systems. John Mitchell. Multics-Orange Book-Claremont

LABORATORY EXPERIMENTS

1. Write programs using the following system calls of UNIX operating system: fork, exec,

getpid, exit, wait, close, stat, opendir, readdir

2. Write programs using the I/O system calls of UNIX operating system (open, read, write, etc)

3. Write C programs to simulate UNIX commands like ls, grep, etc.

4. Implement any file allocation technique (Linked, Indexed or Contiguous)

5. Implementation of Memory and Address Protection

6. Implementation of Access Control List

7. Setting of File Permissions and Protections.

Course Title: SECURED PROGRAMMING	**Course Code: 14SFC23**
Credits(L:T:P): (4-0-0)	**Core/Elective: Core**
Type of Course: Lecture	**Total Contact Hours: 50**

UNIT I **10 Hours**

Validating all input & Designing secure programs: Command line and environment variables, File descriptors, names and contents, Web based application inputs, Locale selection and character encoding, Filtering representable URIs, preventing cross site malicious input content, Forbidding HTTP Input to perform non-queries.

Good security design principles: Securing the interface, separation of data and control. Minimize privileges: Granted, time, modules, resources etc, Using chroot, careful use of setuid/setgid, Safe default value and load initializations. Avoid race conditions, Trustworthy channels and trusted path, Avoiding semantics and algorithmic complexity attacks.

UNIT II **10 Hours**

Declarations and Initializations and Expressions: Declare objects with appropriate storage durations, Identifier declaration with conflict linkage classifications, Using correct syntax for declaring flexible array member, Avoiding information leakage in structure padding, Incompatible declarations of same function or object.

Dependence on evaluation order for side effects: Reading uninitialized memory and dereferencing null pointers, Modifying objects with temporary lifetime, Accessing variable through (pointer) incompatible type, Modifying constant objects and comparing padding data.

UNIT III **10 Hours**

Integers and Floating Points: Wrapping of unsigned integers, Integer conversions and misrepresented data, Integer overflow and divide by zero errors, Shifting of negative numbers, Using correct integer precisions, Pointer conversion to integer and vice versa.

Floating point values for counters: Domain and range errors in math functions, Floating point conversions and preserving precision.

UNIT IV **10 Hours**

Arrays , Strings and Memory Management: Out of bounds subscripts and valid length arrays, Comparing array pointers, Pointer arithmetic for non-array object, scaled integer, Modifying string literals, Space allocation for strings (Null terminator), Casting large integers as unsigned chars, Narrow and wide character strings and functions.

Accessing freed memory: Freeing dynamically allocated memory, Computing memory allocation for an object, Copying structures containing flexible array members, Modifying object alignment by using realloc.

UNIT V **10 Hours**

I/O, Signals and Error Handing: User input and format strings, Opening an pre-opened file, Performing device operations appropriate for files, Dealing with EOF, WEOF, Copying FILE object, Careful use of fgets, fgetws, getc, putc, putwc. Use of fsetops and fgetops, Accessing closed files.

Using asynchronous safe functions and signal handlers: Shared objects and signal handlers, Using signal() within interruptible signal handlers, Returning computation exception signal handler.

Using errno: check and set, Depending upon indeterminate values of errno, Handling standard library errors.

TEXT BOOKS:

1. Robert C. Seacord, “The CERT ® C Coding Standard: 98 Rules for Developing Safe, Reliable, and Secure Systems, Second Edition”, Addison Wesley Professional, April 2014

2. David Wheeler, “Secure Programming for Linux and Unix HowTo”, Linux Documentation project, Aug 2004

REFERENCES:

1. JohnViega, Matt Messier, “Secure Programming Cookbook for C and C++”, O'Reilly Media, 1st Edition, July 2003.

Course Title: CYBER LAWS & ETHICS	**Course Code: 14SFC24**
Credits(L:T:P): (4-0-0)	**Core/Elective: Core**
Type of Course: Lecture	**Total Contact Hours: 50**

UNIT – I **10 Hours**

Introduction to Cyber Law and Cyber Ethics: Introduction to Cyber Crimes and Ethical Issues in IT**,** Basic concepts of Law and Information Security, overview of Information Security obligations under ITA 2008, Privacy and data protection concepts.

UNIT – II **10 Hours**

Law of Contracts applicable for Cyber Space transactions: introduction to Contract law, legal recognition of Electronic Documents, Authentication of Electronic Documents, Authentication of Electronic Documents, Cyber space contracts, Resolution of Contractual disputes, stamping of Contractual document.

UNIT – III **10 Hours**

Intellectual Property Law for Cyber Space: Concept of Virtual assests, nature of Intellectual property, Trade marks and domain names, copyright law, law of patents.

UNIT – IV **10 Hours**

Law of cyber Crimes: Different types of Cyber Crimes-Technical Perspective, Provisions of ITA 2008 on Cyber Crimes, System of Adjudication of Contraventions of ITA 2008, case studies.

UNIT – V **10 Hours**

Miscellaneous Issues in Cyber Crimes and Cyber Security: Cyber Crime Investigation and Prosecution, Digital evidence and Cyber forensics, Jurisdiction issues, Information Security Management in corporate Sector.

TEXT BOOK:

1. Cyber Laws for Engineers, Naavi, Ujvala Consultants Pvt Ltd, 2010.

REFERENCES:

1. Deborah G Johnson, Computer Ethics, Pearson Education Pub., ISBN : 81-7758-593-2.

2. Earnest A. Kallman, J.P Grillo, Ethical Decision making and Information Technology: An Introduction with Cases, McGraw Hill Pub.

3. John W. Rittinghouse, William M. Hancock, Cyber security Operations Handbook, Elsevier Pub.

4. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 2nd Edition, Cengage Learning Pub.

5. Randy Weaver, Dawn Weaver, Network Infrastructure Security, Cengage Learning Pub.

Course Title: BIOMETRIC SECURITY	Course Code: 14SFC251
Credits(L:T:P): (4-0-0)	Core/Elective: Elective
Type of Course: Lecture	Total Contact Hours: 50

UNIT I **10 Hours**

Biometrics: Introduction, benefits of biometrics over traditional authentication systems, benefits of biometrics in identification systems, selecting a biometric for a system, Applications, Key biometric terms and processes, biometric matching methods, Accuracy in biometric systems.

UNIT II **10 Hours**

Physiological Biometric Technologies: Fingerprints: Technical description, characteristics, Competing technologies, strengths, weaknesses, deployment. Facial scan: Technical description, characteristics, 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 , DNA biometrics.

UNIT III **10 Hours**

Behavioral Biometric Technologies: Handprint Biometrics, DNA Biometrics, signature and handwriting technology, Technical description, classification, keyboard / keystroke dynamics, Voice, data acquisition, feature extraction, characteristics, strengths , weaknesses deployment.

UNIT IV **10 Hours**

Multi biometrics: Multi biometrics and multi factor biometrics, two-factor authentication with passwords, tickets and tokens, executive decision, implementation plan.

UNIT V **10 Hours**

Case studies on Physiological, Behavioral and multifactor biometrics in identification systems.

TEXT BOOKS:

1. Samir Nanavathi, Michel Thieme, and Raj Nanavathi, Biometrics -Identity verification in a networked World, Wiley Eastern, 2002.
2. John Chirillo and Scott Blaul, Implementing Biometric Security, Wiley Eastern Publications, 2005.

REFERENCES:

1. John Berger, Biometrics for Network Security, Prentice Hall, 2004.

Course Title: TRUST MANAGEMENT IN E-COMMERCE	**Course Code: 14SFC252**
Credits(L:T:P): (4-0-0)	**Core/Elective: Elective**
Type of Course: Lecture	**Total Contact Hours: 50**

UNIT I **10 Hours**

Introduction to E-Commerce: Network and E-Commerce, Types of E-Commerce. E-commerce Business Models: B2C, B2B, C2C, P2P and M-commerce business models. E-commerce Payment systems: Types of payment system, Credit card E-Commerce transactions, B2C E-Commerce Digital payment systems, B2B payment system.

UNIT II **10 Hours**

Security and Encryption: E-Commerce Security Environment, Security threats in E-Commerce environment , Policies, Procedures and Laws.

UNIT III **10 Hours**

Inter-organizational trust in E-Commerce: Need, Trading partner trust, Perceived benefits and risks of E-Commerce, Technology trust mechanism in E-Commerce, Perspectives of organizational, economic and political theories of inter-organizational trust, Conceptual model of inter-organizational trust in E-Commerce participation.

UNIT IV **10 Hours**

Introduction to trusted computing platform: Overview, Usage Scenarios, Key components of trusted platform, Trust mechanisms in a trusted platform.

UNIT V **10 Hours**

Trusted platforms for organizations and individuals: Trust models and the E-Commerce domain.

TEXT BOOKS:

1. Kenneth C. Laudon and Carol Guercio Trave, Study Guide to E-Commerce Business Technology Society, Pearson Education, 2005.

2. Pauline Ratnasingam, Inter-Organizational Trust for Business-to-Business E- Commerce, IRM Press, 2005.

REFERENCES:

1. Siani Pearson, et al, Trusted Computing Platforms: TCPA Technology in Context, Prentice Hall PTR, 2002.

Course Title: INFORMATION SECURITY POLICIES IN INDUSTRIES	Course Code: 14SFC253
Credits(L:T:P): (4-0-0)	Core/Elective: Elective
Type of Course: Lecture	Total Contact Hours: 50

UNIT I **10 Hours**

Introduction to Information Security Policies: About Policies, why Policies are Important, When policies should be developed, How Policy should be developed, Policy needs, Identify what and from whom it is being protected, Data security consideration, Backups, Archival storage and disposal of data, Intellectual Property rights and Policies, Incident Response and Forensics, Management Responsibilities, Role of Information Security Department, Security Management and Law Enforcement, Security awareness training and support.

UNIT II **10 Hours**

Policy Definitions, Standards, Guidelines, Procedures with examples, Policy Key elements, Policy format and Basic Policy Components, Policy content considerations, Program Policy Examples, Business Goal Vs Security Goals, Computer Security Objectives, Mission statement Format, Examples, Key roles in Organization, Business Objectives, Standards: International Standards.

UNIT III **10 Hours**

Writing The Security Policies: Computer location and Facility construction, Contingency Planning, Periodic System and Network Configuration Audits, Authentication and Network Security, Addressing and Architecture, Access Control, Login Security, Passwords, User Interface, Telecommuting and Remote Access, Internet Security Policies, Administrative and User Responsibilities, WWW Policies, Application Responsibilities, E-mail Security Policies.

UNIT IV **10 Hours**

Establishing Type of Viruses Protection: Rules for handling Third Party Software, User Involvement with Viruses, Legal Issues, Managing Encryption and Encrypted data, Key Generation considerations and Management, Software Development policies, Processes Testing and Documentation, Revision control and Configuration management, Third Party Development, Intellectual Property Issues.

UNIT V **10 Hours**

Maintaining the Policies: Writing the AUP, User Login Responsibilities, Organization's responsibilities and Disclosures, Compliance and Enforcement, Testing and Effectiveness of Policies, Publishing and Notification Requirements of the Policies, Monitoring, Controls and Remedies, Administrator Responsibility, Login Considerations, Reporting of security Problems, Policy Review Process, The Review Committee, Sample Corporate Policies, Sample Security Policies.

TEXT BOOKS:

1. Scott Barman, Writing Information Security Policies, Sams Publishing, 2002.

2. Thomas.R.Peltier, Information Policies, Procedures and Standards, CRC Press, 2004.

REFERENCES:

1. Thomas R Peltier, Justin Peltier, John Backley, " Information Security Fundamentals", Auerbach publications, CRC Press, 2005.
2. Harold F. Tipton and Micki Krause "Information Security Management Handbook", Auerbach publications, 5th Edition, 2005.

Course Title: DATABASE SECURITY	Course Code: 14SFC254
Credits(L:T:P): (4-0-0)	Core/Elective: Elective
Type of Course: Lecture	Total Contact Hours: 50

UNIT I **10 Hours**

Introduction: Introduction to Databases, Security Problems in Databases Security Controls Conclusions. Security Models 1: Introduction, Access Matrix Model, Take-Grant Model, Acten Model, PN Model, Hartson and Hsiao's Model, Fernandez's Model, Bussolati and Martella's Model for Distributed databases.

UNIT II **10 Hours**

Security Models 2: Bell and LaPadula's Model, Biba's Model, Dion's Model, Sea View Model, Jajodia and Sandhu's Model, The Lattice Model for the Flow Control conclusion. Security Mechanisms: Introduction, User Identification/Authentication, Memory Protection, Resource Protection, Control Flow Mechanisms, Isolation, Security Functionalities in Some Operating Systems, Trusted Computer System, Evaluation Criteria.

UNIT III **10 Hours**

Security Software Design: Introduction, A Methodological Approach to Security, Software Design, Secure Operating System Design, Secure DBMS Design, Security Packages, Database Security Design.

UNIT IV **10 Hours**

Statistical Database Protection & Intrusion Detection Systems: Introduction, Statistics, Concepts and Definitions, Types of Attacks, Inference Controls, evaluation Criteria for Control Comparison, Introduction IDES System, RETISS System, ASES System Discovery.

UNIT V **10 Hours**

Models For The Protection Of New Generation Database Systems 1: Introduction, A Model for the Protection of Frame Based Systems, A Model for the Protection of Object-Oriented Systems, SORION Model for the Protection of Object-Oriented Databases. Models For The Protection Of New Generation Database Systems 2: A Model for the Protection of New Generation Database Systems, the Orion Model, Jajodia and Kogan's Model, A Model for the Protection of Active Databases Conclusions.

TEXT BOOKS:

1. Database Security and Auditing, Hassan A. Afyoun i, India Edition, CENGAGE Learning, 2009.

2. Database Security, Castano, Second edition, Pearson Education.

REFERENCE BOOK:

1. Database security by alfred basta, melissa zgola , CENGAGE learning.

Course Title: Secure Programming Laboratory	**Course Code: 14SFC26**
Credits(2)(L:T:P): (0-0-3)	**Core/Elective: Core**
Type of Course: Practical	**Total Contact Hours: 42**

LABORATORY EXPERIMENTS:

1. Writing programs that validate filenames. The filenames shouldn't allowing file globbing i.e. special characters e.g. '*', '?', '[', '..', control characters, leading dashes etc.

2. Validating input data to cgi scripts e.g URL encoded format. Ensure double encoding is not done e.g. %2500 should not result in %00 translating to NULL character. The script should also validate cookies to ensure that these corresponding to proper host domain.

3. Demonstrate dangers of unsafe programming e.g. use of strlen, strpy, strcat, sprintf, gets, and scanf family of functions etc.

4. Demonstrate buffer overflow using different sizes of integers especially between 64bits and 32 bits integers.

5. Demonstrate the dependence on evaluation order for side effects.

6. Demonstrate use of chroot to limit the files visible to programs.

7. Write program to create secure temporary files using mkstemp() and umask()

8. Write programs to demonstrate dangers of referencing freed memory.

Course Title: FILE SYSTEM FORENSIC ANALYSIS	**Course Code: 14SFC41**
Credits(L:T:P): (3-0-1)	**Core/Elective: Core**
Type of Course: Lecture & Practical	**Total Contact Hours: 50**

UNIT I **10 Hours**

Volume Analysis: Introduction, Background, Analysis Basics, Summary. PC-based Partitions: DOS Partitions, Analysis Considerations, Apple Partitions, Removable Media. Server-based Partitions: BSD Partitions, Sun Solaris Slices, GPT Partitions, Multiple Disk Volumes: RAID, Disk Spanning.

UNIT II **10 Hours**

File System Analysis: What Is a File System?, File System Category, Content Category, Metadata Category, File Name Category, Application Category, Application-level Search Techniques, Specific File Systems

FAT Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture, Other Topics.

FAT Data Structures: Boot Sector, FAT32 FSINFO, FAT, Directory Entries, Long File Name Directory Entries

UNIT III **10 Hours**

NTFS Concepts: Introduction, Everything is a File, MFT Concepts, MFT Entry Attribute Concepts, Other Attribute Concepts, Indexes, Analysis Tools.

NTFS Analysis: File System Category, Content Category, Metadata Category, File Name Category, Application Category, The Big Picture.

NTFS Data Structures: Basic Concepts, Standard File Attributes, Index Attributes and Data Structures, File System Metadata Files,

UNIT IV **10 Hours**

Ext2 and Ext3 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, Application Category. The Big Picture.

Ext2 and Ext3 Data Structures: Superblock, Group Descriptor Tables, Block Bitmap, Inodes, Extended Attributes, Directory Entry, Symbolic Link, Hash Trees, Journal Data Structures.

UNIT V **10 Hours**

UFS1 and UFS2 Concepts and Analysis: Introduction, File System Category, Content Category, Metadata Category, File Name Category, The Big Picture.

UFS1 and UFS2 Data Structures: UFS1 Superblock, UFS2 Superblock, Cylinder Group Summary, UFS1 Group Descriptor, UFS2 Group Descriptor, Block and Fragment Bitmaps, UFS1 Inodes, UFS2 Inodes, UFS2 Extended Attributes, Directory Entries

TEXT BOOKS:

1. Brian Carrier, File System Forensic Analysis, Pearson Education, 2005

REFERENCES:

1. Machtelt Garrels, “Introduction to Linux A Hands-On Guide”, Third Edition, Fultus Corporation Publisher, 2010.

WEBSITES:

1. http://sergiob.org/unam/DGSCA/forense/FileSystemAnalysis.pdf

LABORATORY EXPERIMENTS

1. Design a simple experiment to test whether a bootable CD/DVD examination altered the hard disk of the suspect's computer system when the system was booted using the bootable CD/DVD.

2. Design a simple experiments that shows that the correct application of a virtual environment approach results in a less time spent on analysing the evidence, giving more chance of discovering important data, and allowing less qualified personnel to be involved in a more productive way.

3. write a program to find a unique pattern in each sector of disk.

4. write a program to compare two partitions.

5. write a program to compare two disks.

6. write a program to change or corrupt one byte in a file.

The above experiments can be simulated using freely available forensic tool.

Course Title: SECURITY ARCHITECTURE DESIGN	Course Code: 14SFC421
Credits(L:T:P): (4-0-0)	Core/Elective: Elective
Type of Course: Lecture	Total Contact Hours: 50

UNIT I **10 Hours**

Architecture and Security: Architecture Reviews**,** Software Process, Reviews and the Software Development Cycle, Software Process and Architecture Models, Software Process and Security, Architecture Review of System, Security Assessments**,** Security Architecture Basics**,** Architecture Patterns in Security.

UNIT II **10 Hours**

Low-Level Architecture: Code Review**,** importance of code review, Buffer Overflow Exploits, Countermeasures Against Buffer Overflow Attacks, patterns applicable, Security and Perl, Bytecode Verification in Java-Good Coding Practices Lead to Secure Code, Cryptography, Trusted Code, Secure Communications.

UNIT III **10 Hours**

Mid-Level Architecture: Middleware Security, Middleware and Security, The Assumption of Infallibility,The Common Object Request Broker Architecture,The OMG CORBA Security Standard, Vendor Implementations of CORBA Security, CORBA Security Levels, Secure Interoperability, Application, Unaware Security, Application, Aware Security, Application Implications, Web Security, Application and OS Security, Database Security.

UNIT IV **10 Hours**

High-Level Architecture: Security Components**,** Secure Single Sign-On- Public-Key Infrastructures, Firewalls, Intrusion Detection Systems, LDAP and X.500 Directories, Kerberos, Distributed Computing Environment,The Secure Shell, or SSH, The Distributed Sandbox, Security and Other Architectural Goals, Metrics for Non-Functional Goals, Force

Diagrams around Security, High Availability, Robustness, Reconstruction of Events, Ease of Use, Maintainability, Adaptability, and Evolution, Scalability, Interoperability, Performance, Portability.

UNIT V **10 Hours**

Enterprise Security Architecture: Security as a Process, Security Data, Enterprise Security as a Data Management Problem, Tools for Data Management, David Isenberg and the “Stupid Network”, Extensible Markup Language,The XML Security Services Signaling Layer, XML and Security Standards, The Security Pattern Catalog Revisited, XML-Enabled Security Data-HGP: A Case Study in Data Management, Business Cases and Security, Building Business Cases for Security

TEXT BOOKS:

1. Jay Ramachandran, Designing Security Architecture Solutions, Wiley Computer Publishing, 2010.

REFERENCES:

1. Markus Schumacher, Security Patterns: Integrating Security and Systems Engineering, Wiley Software Pattern Series, 2010.

Course Title: STEGANOGRAPHY AND DIGITAL WATERMARKING	**Course Code: 14SFC422**
Credits(L:T:P): (4-0-0)	**Core/Elective: Elective**
Type of Course: Lecture	**Total Contact Hours: 50**

UNIT I **10 Hours**

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 **10 Hours**

Survey of steganographic techniques: Substitution system and bit plane tools, Transform domain techniques, Spread spectrum and information hiding, Statistical Steganography, Distortion and code generation techniques, Automated generation of English text.

UNIT III **10 Hours**

Steganalysis: Detecting hidden information, Extracting hidden information, Disabling hidden information, Watermarking techniques, History, Basic Principles, applications, Requirements of algorithmic design issues, Evaluation and benchmarking of watermarking system.

UNIT IV **10 Hours**

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 **10 Hours**

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

WEBSITES:

1. http://www.armageddononline.org/PDF/Smuggling%20&%20Caching/Artech%20House%20Information%20Hiding%20Techniques%20for%20Steganography%20and%20Digital%20Watermarking.pdf

Course Title: MOBILE DEVICE FORENSICS	**Course Code: 14SFC423**
Credits(L:T:P): (4-0-0)	**Core/Elective: Elective**
Type of Course: Lecture	**Total Contact Hours: 50**

UNIT – I **10 Hours**

Android and mobile forensics: Introduction, Android platform, Linux, Open source software and forensics, Android Open Source Project, Internationalization, Android Market, Android forensics

UNIT – II **10 Hours**

Android hardware platforms: Overview of core components, Overview of different device types, Read-only memory and boot loaders, Manufacturers, Specific devices

UNIT – III **10 Hours**

Android software development kit and android debug bridge: Android platforms, Software development kit (SDK), Android security model, Forensics and the SDK.

UNIT – IV **10 Hours**

Android file systems and data structures: Data in the shell, Type of memory, File systems, Mounted file systems and directory structures. Android forensic techniques: Procedures for handling an Android device, Imaging Android USB mass storage devices, Logical techniques, Physical techniques

UNIT- V **10 Hours**

Android device data and app security: Data theft targets and attack vectors, Security considerations, Individual security strategies, Corporate security strategies, App development security strategies. Android application and forensic analysis: Analysis techniques, FAT forensic analysis, YAFFS2 forensic analysis, Android app analysis

TEXT BOOK:

1. Android Forensics Investigation, Analysis, and Mobile security for Google Android, Andrew Hoog, John McCash, Technical Editor, Elsevier, 2011.

REFERENCES:

1. Satish Bommisetty, Rohit Tamma, Heather Mahalik “Practical Mobile Forensics”, Kindle Edition, Packt Publishing (21 July 2014).

2. Andrew Martin,”Mobile Device Forensics”, © SANS Institute 2009

WEBSITES:

1. http://data.ceh.vn/Ebook/ebooks.shahed.biz/ANDROID/Android%20Forensics.pdf

2.For companion material including code, programs and updates please visit the website https://viaforensics.com/resources/android-forensics-mobile-security-book/

Course Title: SECURITY ASSESSMENT AND VERIFICATION	**Course Code: 14SFC424**
Credits(L:T:P): (4-0-0)	**Core/Elective: Elective**
Type of Course: Lecture	**Total Contact Hours: 50**

UNIT I **10 Hours**

Evolution of information security: information assets, security standards, organizational impacts, security certifications, elements of information security program, need for security assessment, security assessment process.

UNIT II **10 Hours**

Security assessment planning: Business drivers, scope definition, consultant's perspective, Client's perspective, Development of project plan. Initial information gathering, Initial preparation, analysis of gathered information.

UNIT III **10 Hours**

Business process evaluation, Technology evaluation, Risk analysis, Risk mitigation.

UNIT IV **10 Hours**

Security Risk assessment project management, Security risk assessment approaches and methods.

UNIT V **10 Hours**

Information security standards, Information security Legislation, Formal security verification, Security verification with SSL.

TEXT BOOKS:

1. Sudhanshu Kairab, A practical guide to security assessments, CRC press, 2005.

2. Douglas J.Landoll, A Security risk assessment Handbook, Auerbach publications, 2006.

REFERENCES:

1. Michael E. Whitman, Herbert J. Mattord, Principles of Information Security, 2nd Edition, Cengage Learning Pub.

2. Thomas R Peltier, Justin Peltier and John blackley, ”Information Security Fundamentals”, 2nd Edition, Prentice Hall, 1996