Department of Computer Science and Engineering

Malaviya National Institute of Technology
MTech Full Time (Computer Engineering and Information Security)
(2016-17 onwards)

CST701 Advanced Cryptography (3-0-0)

Introduction(10 T): Mathematical foundations: Group theory (Groups, Rings and Fields), Symmetric key cryptography vs. public key cryptography, One-way functions based on mathematical problems, Security problems of text book cryptosystems, Number theory, Algorithms in public key cryptography.

Lattice Based Cryptography(15 T): Introduction to Lattices, The Hermite normal form, Ajtai's worst-case/average-case connection, Discrete Gaussians, Smoothing Parameter, Leftover Hash Lemma, The lattice trapdoor construction of Micciciancio-Peikert, The Gorbunov-Vaikuntanathan-Wee LWE-based Attribute-Based Encryption Scheme, Attribute-Based Ecnryption, LWE-based homomorphic encryption, Continue LWE-based homomorphic encryption, Ideal Lattices, The NTRU cryptosystem, Multilinear maps from ideal lattices.

Advanced Topics in Cryptography(15 T): Interactive Proofs, Zero-Knowledge Proofs (concurrent zero knowledge, upper and lower bounds on round complexity, black-box vs. non-blackbox zero knowledge), Zero-Knowledge Proofs of Knowledge, Non-Interactive Zero-Knowledge Proofs, Secure Protocols. Two-party Secure Computation, Multiparty Secure Computation, Chosen Ciphertext Security. Oblivious transfer: Definitions, constructions, and applications, Byzantine agreement, private information retrieval, threshold cryptography, voting protocols, auctions, privacy preserving data mining, credential systems,

Text Books:

1. Cryptography: Theory and Practice, by Douglas R. Stinson.
2. A Course in Number Theory and Cryptography by Neal Koblitz ,Springer.
3. Algebraic aspects of cryptography Neal Koblitz ,Springer
4. Cryptography and Networks Security, William Stallings
5. Introduction to Modern Cryptography, Jonathan Katz and Yehuda Lindell
6. Security and cooperation in wireless networks, Levente buttyane and Jean-Pierre hubaux
7. Applied Cryptography, by Bruce Schneier
8. Lattice-based Cryptography, by Daniele Micciancio, Oded Regev
9. Complexity of Lattice problems: a cryptographic perspective, by Daniele Micciancio and Shafi Goldwasser's.
10. A Graduate Course in Applied Cryptography, by Dan Boneh and Victor Shoup

CST702 Special Topics in OS (3-0-0)

Advanced Topics: Advanced scheduling techniques for processes and threads; kernel architectures and implementation of CFS in recent kernels; Access control schemes in OS; Multimedia OS and design features; Introduction to networked, distributed file systems; Virtualisation and cloud OS; Introduction to embedded and Mobile OS;

Distributed shared memory: distributed scheduling, failure recovery, resource security and protection, Configuring Services Registry settings, System Configuration Settings, Manage Users Manage the system, Supporting address translation (NAT); **Introduction to Performance Tuning**: Maintenance and troubleshooting Introductions

Text:

Recent papers from USENIX and Journals

CST703 Advance Data Structures and Algorithms (3-0-0)

RAM model: Growth of functions, Notations, Recurrence analysis - Master's theorem and its proof, Probabilistic analysis, Amortized analysis.
Advanced Data Structures: B-Trees, Binomial Heaps, Fibonacci Heaps, AVL trees, Red-black trees, B-trees, Splay trees, Disjoint set, Hash tables, Bloom filters.
Graph Algorithms: DFS, BFS, Shortest path, MST, Articulation Point, Topological sorting, Connected components, Network Flow, Matchings.
Interval scheduling algorithms, Knapsack problem.
Dynamic programming: Longest common subsequence. Chain of matrix multiplication, Optimal binary tree.
Convex hull and Voronoi diagrams, line segments, Optimal polygon triangulation.
Approximate Algorithms: Vertex-cover, set-covering problems, Travelling Salesman problem.
Randomized algorithms: Use of probabilistic inequalities in analysis, applications using examples.
Randomized Algorithms
: Computing the Median, Randomized Divide-and-Conquer

Number-Theoretic Algorithms: Greatest common divisor, Modular arithmetic, Chinese remainder theorem, Cryptosystems , Primality testing, Integer factorization, Discrete logarithm,
Polynomial representations, Operations, FFT as an example.
Parallel algorithms: Basic techniques for sorting, seraching, merging.
Complexity classes - NP-Hard and NP-complete Problems - Cook's theorem, Undecidability, NP completeness reductions.

Texts/References:

1) Cormen, Leiserson, Rivest: *Introduction to Algorithms*, Prentice Hall of India.
2) Jon Kleinberg
, Eva Tardos
: *Algorithm Design*, Pearson
3) Aho A.V , J.D Ulman: *Design and analysis of Algorithms*, Addison Wesley
4) Motwani and Raghavan: *Randomized Algorithms*, Cambridge University Press
5) Joseph Ja'Ja': *Introduction to Parallel Algorithms*, Addison-Wesley
6) Vaizirani: *Approximation Algorithms*, Springer Verlag

CST704 Critical Infrastructure Protection (3-0-0)
PRE-REQUISITES: Computer Networks, Network Security

COURSE OUTCOMES:

1. Describe what digital investigation is, the sources of evidence, and the limitations of forensics.
2. Describe the legal requirements for use of seized data, data collection, and storage
3. Reconstruct application history from application artifacts and replay of attack
4. Capture and interpret network traffic, analyze mobile devices, and inspect for presence of malware
5. Apply forensics tools to investigate security breaches and identify anti-forensic methods.

COURSE OUTLINE:

Introduction to Critical Infrastructure Assurance and Protection: Critical Infrastructure Functions, Evolution of Critical Infrastructure
Demand, Capacity, Fragility, and the Emergence of Networks
Beyond National Frameworks: Areas of Potential Risk or Concern
The Reinvention of Information Sharing and Intelligence: Data vs Information vs Intelligence, Open-Source Information and Intelligence
Emergency Preparedness and Readiness: First Responder, First Responder Classifications
Know Protocols to Secure, Mitigate, and Remove HAZMAT, Importance of Implementing an Emergency Response Plan
Security Vulnerability Assessment: Risk Assessment, Threat Risk Equations, Quantitative vs Qualitative Risk Assessments, Threat, Vulnerability, Countermeasures, Vulnerability Assessment Framework
Information Sharing and Analysis Centers: Critical Infrastructure Asset, Supply Chain, Public Transit, Transportation Technology, Water, Financial Services, Electricity, Information Technology, Internet Infrastructure, Cyber Threats & Cyber Security, Telecommunications, Energy Resource, Chemical, Healthcare, Food and Agriculture
Supervisory Control and Data Acquisition: Vulnerability Concerns about Control Systems, Insecure Connectivity to Control Systems, Issues in Securing Control Systems
Critical Infrastructure Information: Enforcement of FOUO Information, Export-Controlled Information, Source Selection Data, Privacy Information, Unclassified Controlled Nuclear Information, Critical Energy Infrastructure Information, Controlled Unclassified Information

TEXT BOOKS:

1. Robert S. Radvanovsky and Allan McDougall, Critical Infrastructure: Homeland Security and Emergency Preparedness, Third Edition, CRC Press, 2013
2. Tyson Macaulay, Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies, CRC Press, 2008
3. Robert Radvanovsky and Jacob Brodsky, Handbook of SCADA / Control Systems, Second Edition, CRC Press, 2016
4. Eric D. Knapp and Joel Thomas Langill, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Second Edition, CRC Press, 2014

CST705 Machine Learning (3-0-0)
Introduction: Basic concepts. Supervised learning: Supervised learning setup. LMS. Logistic regression. Perceptron. Exponential family. Generative learning algorithms. Gaussian discriminant analysis. Naive Bayes. Support vector machines. Model selection and feature selection. Ensemble

methods: Bagging, boosting. Evaluating and debugging learning algorithms.

Learning theory: Bias/variance tradeoff. Union and Chernoff/Hoeffding bounds. VC dimension. Worst case (online) learning.

Unsupervised learning: Clustering. K-means. EM. Mixture of Gaussians. Factor analysis. PCA (Principal components analysis).
ICA (Independent components analysis).

Reinforcement learning and control: MDPs. Bellman equations.Value iteration and policy iteration.
Linear quadratic regulation (LQR). LQG. Q-learning. Value function approximation.
Policy search. Reinforce. POMDPs.

References:

1. Tom M. Mitchell, Machine Learning, McGraw Hill, 2014

2. Bishop, C. M. Pattern Recognition and Machine Learning. Springer. 2007.

3. Marsland, S. Machine Learning: An Algorithmic Perspective. CRC Press. 2009. (Also uses Python.)

4. Richard O. Duda, David G.Stork,Peter E. Hart, Pattern Classification, Wiley 2007

5. Dougherty, Pattern Recognition and Classification, Springer 2011.
6. Bayesian Reasoning and Machine Learning, David Barber, CRC Press
7. A First Course in Machine Learning , Simon Rogers and Mark Girolami, Chapman & Hall/CRC

CST706 Malware Analysis (3-0-0)

Malware: Types – Virus, Worms, Trojans, Logic Bombs, etc., infection modes, payload and its delivery mechanisms.
Analysis Tools and their design: Disassemblers, Unpackers, Scanners, Decompilers, Emulators, Virtualization techniques
Anti-analysis techniques: Obfuscation techniques, Packing, Encryption, Polymorphism, metamorphism.
Analysis Techniques: Signature based, Non-signature based, Static, dynamic, behavioral, anomaly detection.
Case Study: Android Malware

Text/Reference Books

1. Peter Szor: The Art of Computer Virus Research and Defense, Addison Wesley Professional.
2. Eric Filiol: Computer Viruses: from theory to applications, Springer.
3. Michael Sikorski and Andrew Honig: Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, No Starch Press
4. Christopher Elisan: Advanced Malware Analysis, McGraw-Hill Osborne Media.
5. Michael Hale Ligh, Andrew Case: The Art of Memory Forensics: Detecting Malware, Wiley.
6. Bruce Dang, Alexandre Gazet: Practical Reverse Engineering, Wiley.

CST 707 Security Engineering (3-0-0)

Introduction to Security Engineering: Passwords and their limitations, attacks on passwords, CAPTCHA, Biometrics.

Access Control: ACL, sandboxing, virtualization, trusted computing. Multi-level and Multi-lateral security.

Secure systems: hardware, software and communication systems – design issues and analysis. Secure software architecture: models and principles, hardware design related security – smart cards and other security solutions, communication protocols and application systems associated with security.

Securing services: Security in Metered Services, pre-payment meters. Secure printing and Seals. Tamper resistance mechanisms.

References:

1. Ross Anderson's *Security Engineering,* Second Edition

2. Bruce Schneier. Secrecy, Security, and Obscurity. Crypto-Gram, 2002

Additional References :

1. Latest reputed conference and journal articles as chosen by the instructor.
2. William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin. Firewalls and Internet Security, Second Edition, Addison-Wesley, 2003.

3. Bruce Schneier. Applied Cryptography, Second Edition, Wiley, 1996.
4. Niels Ferguson and Bruce Schneier. Practical Cryptography, Wiley, 2003.
5. Matt Bishop. Introduction to Computer Security, Addison-Wesley, 2004.
6. Andrew Tanenbaum. Modern Operating Systems, Fourth Edition, Pearson, 2014.
7. Andrew Tanenbaum and David Wetherall. Computer Networks, Fifth Edition, Pearson, 2010.
8. Steven M. Bellovin. Thinking Security, Addison-Wesley, 2015.

CST708 Advance Database Systems (3-0-0)

Issues in the Implementation of Database Systems. Query Processing and Optimization – Implementation of Database operations, External Sorting, Size Estimations, Equivalence Rules, Heuristic-based Optimization, Materialized Views, Incremental View Maintenance.

Transaction Processing - Concurrency Control Management, Serializability, Two-phase Lock Protocol, Deadlock Prevention and Detection, Timestamp-based Ordering Protocol, Log-based Recovery Management.

Database System Architectures, Distributed Databases, Distributed Transactions, Data Storage, Two-Phase Commit Protocol, Distributed Query Processing, Parallel Databases, Times in Databases, Multimedia Databases.

Text and References:

1. Silberschatz A, Korth HF, Sudarshan S, Database System Concepts, McGrall Hill.
2. Elmasri R and Navathe SB, *Fundamentals of Database Systems,* 3rd Edition, Addison Wesley,2000. This book covers most of the material on the course.
3. Ceri S, Pelagatti G, Distributed Databases – Principles and Systems, McGraw Hill.
4. Date CJ, *An Introduction to Database Systems*, 7th Edition, Addison Wesley.
5. Khashafian S and Baker AB, *Multimedia and Imaging Databases*, Morgan Kaufmann.

CST710 Software Testing (3-0-0)

Introduction to Faults, Errors, and Failures, Basics of software testing, Testing objectives, Principles of testing, Requirements, behavior and correctness, Testing and debugging, Verification, Validation and Types of testing.

Static and Dynamic Testing: Static testing, static analysis tools, white box testing, Unit/Code functional testing, Code coverage testing, Code complexity testing, Black Box testing, Requirements based testing, Boundary value analysis, Equivalence partitioning, state/graph based testing, Model based testing and model checking, Differences between white box and Black box testing.

Integration, System, and Acceptance Testing: Top down and Bottom up integration, Bi-directional integration, System integration, Design/Architecture verification, Beta testing, Scalability testing, Stress testing, Security testing, Penetration testing, Vulnerability testing, Acceptance testing: Acceptance criteria, test cases selection and execution.

Test Selection & Minimization for Regression Testing: Regression testing, Regression test process, Initial Smoke or Sanity test, Selection of regression tests, Execution Trace, Dynamic Slicing, Test Minimization, Tools for regression testing, Defect seeding.

Test Management and Automation: Test Planning, Management, Execution and Reporting, Software Test Automation: Scope of automation, Design & Architecture for automation, Generic requirements for test tool framework, Test tool selection.

References:

1. S. Desikan and G. Ramesh, “Software Testing: Principles and Practices”, Pearson Education.
2. Aditya P. Mathur, “Fundamentals of Software Testing”, Pearson Education.
3. Naik and Tripathy, “Software Testing and Quality Assurance”, Wiley.
4. Myers, Glenford J., “The art of software testing”, John Wiley & Sons.

CST712 Advances in Compiler Design (3-0-0)

A Tour of Compiler Design, Structure of Compilers for Modern Programming Languages, LR Parsers and LR Grammars – Design and Development, Lex and Yacc Tools.

Optimizing Compiler, Control-flow Analysis, Control-flow Graphs, Basic Blocks, Data-flow Analysis, Dependence Analysis, Global Optimizations, Loop Optimizations, Peephole Optimization and Optimal Code Generation, Data Dependence Analysis in Loops, Loop Scheduling, Static Single Assignment, Just-In-Time (JIT) and Adaptive Compilation, Runtime System Architectures and Automatic Memory Management Techniques.

Text and References:

1. Aho, Alfred V., Sethi, Ravi, Ullman, Jeffrey D., Compilers: Principles, Techniques and Tools, Addison-Wesley.
2. Steven Muchnick, Advanced Compiler Design & Implementation, Morgan Kaufmann.
3. Keith Cooper and Linda Torczon, Engineering a Compiler, Morgan Kaufmann.

CST714 Advances in Real-time Systems (3-0-0)

Misconceptions about Real-Time computing. Real-time System requirements. Specification of timing constraints. Real-time scheduling, Requirements and Issues, Terminology, Modeling, Static and Dynamic Scheduling schemes, priority driven scheduling of periodic tasks, Schedulability Tests, Aperiodic Task Scheduling, Practical factors/overheads. Resources and resource access control, Multiprocessor Real Time Systems, Problems and Issues. Scheduling in Multiprocessor Systems. Scheduling flexible computations and tasks with Temporal Distance Constraints. Time Critical Applications and Recent Trends in Real Time Computing.

Reference Books

1. Real-Time Systems, Jane W.S.Liu, Pearson, 2006
2. Real-Time Systems, C.M.Krishna and Kang G.Shin, McGraw-Hill Education,1997.

CST716 Image Analysis (3-0-0)

Aim of the Course
By the end of the semester, students will be able to:

1. Students can able to understand and perform basic image analysis, modelling and visualization problems.
2. Students can able to comprehend challenging research topics and proposes solutions for a real-time in image analysis.

IMAGE PRELIMINARIES and IMAGE PROCESSING
Digital image representation, Fundamental steps in image processing, *Image Acquisition*: Energy, the optical system, image sensor and digital image formation. Gray scale and color images. Elements of visual perception, Image model, Sampling and quantization, Relationship between pixels, imaging geometry. *Image Point Processing*: Gray-level mapping, non-liner gray-level mapping, image histogram, histogram stretching, histogram equalization, thresholding. *Neighborhood Processing*: Median filter, mean filter, correlation and image sharpening. *Color image processing*. *Morphology*: Dilation & Errosion, closing & opening and boundary detection.
Geometric transformations**:** Translation, rotation, scaling and shearing. *Frequency transformation*: Discrete Fourier transform (DFT), fast Fourier transform (FFT), short-time Fourier transform (STFT), ***Multi-resolution Expansions*****:** Wavelet Transforms in 1-D and 2-D. The Fast Wavelet Transform, Wavelet Packets Transform.
FEATURE EXTRACTION AND DIMENSION REDUCTION
Color, Texture, Shape and structure Features in spatial and frequency domains, Corner Detection, Hough Transform, Principal Component Analysis, Linear Discriminate Analysis, Feature Reduction in Input and Feature Spaces.
IMAGE SEGMENTATION
Gray-level thresholding, Supervised vs. Unsupervised thresholding, Binarization using Otsu's method, Locally adaptive thresholding, Color-based segmentation, Region oriented segmentation, Use of motion in segmentation, Spatial techniques, Frequency domain techniques.
FEATURES BASED IMAGE MATCHING:
Scale Space Image Processing, Different Feature descriptors: Key Point Detection, SIFT descriptor SURF descriptor Bag of Visual Words approach, Geometric consistency check, Vocabulary tree
PANORAMIC IMAGING
Template Matching, Mono Panorama, Stereo Panorama.

TEXT BOOKS
1. J G Proakis and D G Manolakis, "Digital Signal Processing," Pearson, Fourth edition
2. Rafael C. Gonzalez, Richard E. Woods, Digital Image Processing, Prentice Hall, 3rd Edition, 2007.
3. Bishop, Pattern Recognition and Machine Learning
4. Duda-Pattern Classification

CST718 Wireless Security (3-0-0)

Introduction(10 T): Wireless networking technology: fundamentals in wireless communication, Wireless MAC standards, Wireless networks: wireless sensor networks, MANETs, WMNs, CRNs, etc. Security definitions and concepts, Attacks and risks in wireless networks/communications.

Wireless MAC Security (7 T): attacks on IEEE 802.11, anonymity, confidentiality, availability and integrity in IEEE 802.11. WPA, WPA2 (IEEE 802.11i). Security issues IEEE 802.16, IEEE 802.15.

4, and IEEE 802.22.

RFID Security(10 T): Introduction to RFID security, Physical form factor, threat and target identification and Management of RFID security. **Tag data security :** Potential attacks: skimming and eavesdropping**,** Measures to protect RFID data transmission, Physical security, Protocol-based security (Encryption and mutual authentication, Effect of security protocols on performance, Frequencies and security, ePassports: standardized security protocols). **Safeguarding personal privacy:** Potential threats to personal privacy, EPCglobal: recommended industry practices for safeguarding consumer privacy, Regulatory measures: India, U.S., Europe, and Japan.

Advances in Wireless Security(13 T): Secure and resilient data aggregation, Key pre-distribution and management, Encryption and authentication, Security in group communication, Trust establishment and management, Denial-of-service attacks and Energy-aware security mechanisms.

Text books:

No text book and use selected research articles to teach.

CST720 Security and Privacy in Social Networks (3-0-0)

Brief introduction to OSNs: History and definition of Privacy; Vocabulary, history, terms; Types of consumers, privacy; Myths or why we don’t care?

Duality of privacy and security: Privacy and security; The role of usability; Crypto and its failure; Privacy and anonymity; Anonymization techniques; Why hasn’t privacy/security duality yielded more?

Terminology and key players: Tracking; Technologies for tracking; Technical vectors of leakage and ways of identifying them; Role of JavaScript; Role of protocols.

Personally Identifiable Information: What is personally identifiable information; People search engines;

Introduction to Mobile OSNs; Special purpose OSNs: Pinterest, SnapChat, Ask.fm, WhatsApp; Privacy settings in OSNs; PII leakage in OSNs

Linkage: Semantics and the compositional problem; Collateral Damage of Privacy;

Economics of Privacy: Privacy of mixed data sets, OSNs; Privacy across time

References:

1. Latest reputed conference and journal articles as chosen by the instructor.
2. Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security: Private Communication in a Public World, 2nd edition, 2002, Prentice Hall.
3. Simson Garfinkel, Gene Spafford, Web Security, Privacy and Commerce, 2002, O'Reilly
4. Ross Anderson, Security Engineering, John Wiley and Sons, 2001

5. Cryptography and Network Security: Principles and Practice, by William Stallings , Prentice Hall, Hardcover. Fifth Edition is out also. See http://williamstallings.com/Crypto3e/Crypto3e-student.html for student online help.
6. Network Security Essentials: Applications and Standards, by William Stallings. Prentice Hall, Hardcover, Published November 1999, 366 pages, ISBN 0130160938
7. Secrets and Lies: Digital Security in a Networked World by Bruce Schneier John Wiley, Published August 2000, 412 pages, ISBN 0471253111.Kruegel, and G. Vigna.

CST722 Advances in Data Mining (3-0-0)

UNIT-I

Data mining Overview

Data mining tasks – mining frequent patterns, associations and correlations, classification and regression for predictive analysis, cluster analysis , outlier analysis; advanced pattern mining in multilevel, multidimensional space – mining multilevel associations, mining multidimensional associations

UNIT-II

Classification, Clustering, Association Rule Mining

Classification by back propagation, support vector machines, classification using frequent patterns, other classification methods – genetic algorithms, roughest approach, fuzz>set approach;

Density - based methods –DBSCAN, OPTICS, DENCLUE; Grid-Based methods – STING, CLIQUE;
Exception – maximization algorithm; clustering High- Dimensional Data; Clustering Graph and Network Data.

Frequent Pattern matching, Association Rule Mining

UNIT-III

Web and Text Mining

Introduction, web mining, web content mining, web structure mining, we usage mining, Text mining –
unstructured text, episode rule discovery for texts, hierarchy of categories, text clustering.

UNIT-V

Temporal and Spatial Data Mining

Introduction; Temporal Data Mining – Temporal Association Rules, Sequence Mining, GSP algorithm,
SPADE, SPIRIT Episode Discovery, Time Series Analysis, Spatial Mining – Spatial Mining Tasks, Spatial Clustering. Data Mining Applications.

TEXT BOOKS:

1. Data Mining Concepts and Techniques, Jiawei Hang Micheline Kamber, Jian pei, Morgan Kaufmannn.
2. Data Mining Techniques – Arun K pujari, Universities Press.

REFERENCE BOOKS:

1. Introduction to Data Mining – Pang-Ning Tan, Vipin kumar, Michael Steinbach, Pearson.
2. Data Mining Principles & Applications – T.V Sveresh Kumar, B.Esware Reddy, Jagadish S Kalimani, Elsevier.

CST724 Web Security (3-0-0)

PRE-REQUISITES: Computer Networks, Operating System, Web Application Development

COURSE OUTCOMES:

3. Describe the browser security model including same-origin policy and threat models in web security.
4. Discuss the concept of web sessions, secure communication channels such as TLS and importance of
   secure certificates, authentication including single sign-on such as OAuth and SAML.
5. Describe common types of vulnerabilities and attacks in web applications, and defenses against them.
6. Use client-side security capabilities in an application.

COURSE OUTLINE:

Web Security Model: Browser security model including same-origin policy, Client-server trust boundaries
Session Management and Authentication: Single sign-on, HTTPS and certificates
Application Vulnerabilities and Defenses: SQL Injection, Cross Site Scripting (XSS), CSRF, Insecure Direct Object References, Security Misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control, Using Components with Known Vulnerabilities, Invalidated Redirects and Forwards (OWASP Top 10)
Client-Side Security: Cookies security policy, HTTP security extensions, Plugins, and web apps; Web user tracking
Server-Side Security: Tools, Web Application Firewalls (WAFs) and Fuzzers

TEXT BOOKS:

1. Dafydd Stuttard and Marcus Pinto, The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws, II Edition, Wiley Publishing Inc, 2011
2. Vincent Liu, Web Application Security - A Beginner's Guide, McGraw-Hill Osborne, 2012
3. Mike Shema, Seven Deadliest Web Application Attacks, Syngress, 2010
4. Jeremiah Grossman, Robert “RSnake” Hansen, Petko “pdp” D. Petkov, Anton Rager, Cross Site Scripting Attacks: XSS Exploits and Defense, 2007
5. Justin Clarke, SQL Injection Attacks and Defense, II Edition, Syngress, 2012

CST726 Quantum Cryptography (3-0-0)

Preliminaries: Quantum Information Theory, Quantum Information Theory, Unconditional Secure Authentication and , Entropy.

Quantum Key Distribution: Quantum Channel, Public Channel, QKD Gain , Finite Resources, Adaptive Cascade: Introduction, Error Correction and the Cascade Protocol, Adaptive Initial Block-Size Selection, Fixed Initial Block-Size, Dynamic Initial Block-Size.

Attack Strategies on QKD Protocols: Attack Strategies in an Ideal Environment , Individual Attacks in an Realistic Environment. QKD Systems, Statistical Analysis of QKD Networks in

Real-Life Environment: Statistical Methods, Results of the Experiments, Statistical Analysis.

QKD Networks Based on Q3P : QKD Networks, PPP, Q3P, Routing and Transport. Quantum-Cryptographic Networks from a Prototype to the Citizen. The Ring of Trust Model, Model of the Point of Trust Architecture, Communication in the Point of Trust Model, Exemplified Communications, A Medical Information System Based on the Ring of Trust.

Text books:

1. Quantum Cryptography and Secret-Key Distillation, Gilles van Assche, Cambridge University Press, 2006.

Paul Kaye, Raymond Laflamme, and Michele Mosca, An Introduction to Quantum Computing, Oxford University Press (2007).

2. Michael A. Nielsen and Isaac L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press (2000).

CST728 Trust Management System (3-0-0)

Introduction: Definition – Sociological perspective, technical perspective; Concept of Trust Evolution, Trust over Security and Privacy; Important of trust in future networks; properties of trust.

Traditional Trust Management: Identification and Authentication mechanism; Overview of Public Key Infrastructure (PKI), Entities, Standards, design issues, implementation and deployment, Trust management challenges.

Re-invention of "Trust" paradigm on future internet: Social Psychology to Social Network; Sociology of the Internet and Digital Sociology; Digital Personality; Trust origin, types, properties, models.

Trust and Social Network: Overview of Social network, social agents, importance of trust, social capital and social trust, information collection, evaluation of trust.

Trust and Internet of Things: Overview of Internet of Things, importance of trust, objective, frameworks, types of trust for IoT, evaluation models. Social IoT, trust in social IoT.

Attacks on Trust: Classification criteria, system model, classification of trust attacks. Attack's assumptions, characteristics, setup, effect in trust evaluation.

Text and References:

1. Roles, Trust, and Reputation in Social Media Knowledge Markets: Theory and Methods, Elisa Bertino, Sorin Adam Matei, Springer.
2. The Internet of Things: Key Applications and Protocols, David Boswarthick, Olivier Hersent, and Omar Elloumi, Wiley.
3. Latest research articles.

CST730 Cloud Security (3-0-0)

PRE-REQUISITES: Computer Networks, Operating System

COURSE OUTCOMES:

7. Understand the characteristics in terms of the systems, protocols and mechanisms in Cloud
8. Examine virtualization & its types, hypervisors and various aspects of VM management

9. Comprehend the design of Cloud Architectures with reference to scalability
10. Understand the vulnerabilities, threats and attacks in Cloud Environment and the defense mechanisms
11. Realize the post attack scenario and evaluate investigation and forensic techniques for Cloud

COURSE OUTLINE:

Introduction of Cloud Computing: Taxonomy and related technologies, Essential Characteristics, Service and Deployment Models
Virtualization: Types of Virtualization and Hypervisors, Virtualization at Storage, Compute and Network, Hypervisors (Types and Case studies), Virtual Machine Provisioning, Virtual Machine Migration
Architectures: Standards, Orchestration, Provisioning, Portability, Interoperability, Federated Cloud,
Security: CIA Triad, Vulnerabilities in Cloud, Threats to Infrastructure, Data and Access Control; Identity Management; Multi Tenancy Issues; Attack taxonomy; Intrusion Detection, VM Specific attacks, VM Introspection, Management; Trusted Cloud Initiative of Cloud Security Alliance (CSA).
Forensics: NIST Forensics Reference Architecture, Forensic Science Challenges, Architectural Issues, Evidence Collection and Analysis, Anti-Forensics, Incident Response, Standards and Framework

TEXT BOOKS:

1. K. Hwang, G. C. Fox, and J. Dongarra, Distributed and Cloud Computing, 1st ed.: Morgan Kaufmann, 2011
2. R. Buyya, J. Broberg, and A. M. Goscinski, Cloud Computing: Principles and Paradigms: Wiley-Blackwell, 2011
3. S. Dinkar and G. Manjunath, Moving to the Cloud: Developing Apps in the New World of Cloud Computing Syngress Media, U.S., 2012.
4. W. Stallings, Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud, 1st ed.: Addison-Wesley Professional, 2015
5. T. Erl, Z. Mahmood, and R. Puttini, Cloud Computing: Concepts, Technology & Architecture: Prentice Hall/Pearson PTR, 2014
6. R. L. Krutz and R. D. Vines, Cloud Security - A Comprehensive Guide to Secure Cloud Computing, Wiley Publishing, 2010
7. T. Mather, S. Kumaraswamy, and S. Latif, Cloud Security and Privacy - An Enterprise Perspective on Risks and Compliance, O Reilley Publishers, 2009
8. V. (J. R.) Winkler, G. Speake, P. Foxhoven, Securing the Cloud: Cloud Computer Security Techniques and Tactics, Syngress, 2011

CST732 Database Security (3-0-0)

Security and Information Technology, Database Security Architecture, Profiles, Password policies, Privileges and Roles, Virtual Private Databases, and Database Auditing.

SQL Injections- Identification and Defense. Security Testing.

Database Management Security Issues such as Administration of Users, Enforcing Access Controls, and related Issues.

Security Issues in New-generation Database Systems like Distributed, Frame-based and Object-oriented Databases.

Text:

1. Alfred Basta, Melissa Zgola, Database Security, Course Technology (Cengage Learning).
2. Hassan A. Afyduni, Database Security and Auditing: Protecting Data Integrity and Accessibility, Course Technology (Cengage Learning).
3. Ron Ben Natan, Implementing Database Security and Auditing, Elsevier.

CST734 Secure Software (3,0,0)

Unit 1: Introduction: Secure Software, assets, stakeholders, threats, security requirements, confidentiality, authentication, authorization, integrity.

Unit 2: Secure Software Development Life Cycle: Security practices, Common criteria, built-in security, Agile Processes, Security Development Lifecycle (SDL), Secure Software Development Methodology (SecSDM), Security Design Patterns.

Unit 3: Requirements Engineering: Functional and Non-functional requirements, security requirements, reliability, maintainability, portability, trustworthiness, robustness, usability, use cases, mis-use cases.

Unit 4: Threat Modeling and Secure Design: Asset, Threat, Attack, Dataflow Diagram (DFD), Attack Tree, STRIDE, DREAD, Security Principles, Guidelines for Secure Software Development, Access Control. SecUML, model based security engineering with UML

Unit 5: Secure Coding and Secure Testing: Secure Coding Practices, Vulnerabilities, Vulnerability Patterns, Code Checking Tools, Cross Site Scripting, Injection Flaws. Use of formal methods and verification for security, techniques for software protection.
Test Cases, Security Test Plan, White Box Testing, Black Box Testing, Penetration Testing, Code Reviews, Regression Testing, Performance Testing.

Recommended Books:

1. John Musa D, “Software Reliability Engineering”, 2nd Edition, Tata McGraw-Hill, 2005 (Units I, II and III)
2. Jan Jürjens, “Secure Systems Development with UML”, Springer; 2004 (Unit IV and V)
3. Frank Swiderski, Window Snyder, “Threat Modeling”, Microsoft Press, First Edition, 2005.
4. J. Viega and G. McGraw, “Building Secure Software: How to Avoid Security Problems the Right Way”, Addison-Wesley, 2002

5. A. Cockburn, “Writing Effective Use Cases”, Addison- Wesley, Boston, MA, 2001

CST-736 Fault Tolerant Computing (3-0-0)

Introduction to Fault Tolerant Paradigm: Fault Classification, Byzantine Failures, Basic Measures of Fault Tolerance. Failure Rate, Reliability and Mean Time to Failure. Redundancy in Hardware, Software, Time and Information. **Software Fault Tolerance** : Acceptance Tests, Single-Version Fault Tolerance, N-Version Programming, Recovery Block Approach, Preconditions, Post conditions and Assertions, Exception-Handling, Software Reliability Models, Fault-Tolerance Remote Procedure Calls. **Fault Tolerance Strategies in Distributed Systems:** Fault detection and Prediction, Location, Masking, Containment, Reconfiguration, Self-Repairing, Self-Healing and Recovery. Simulation Techniques**.**

Reference Books

1. Fault-Tolerant Systems, Israel Koren and C. Mani Krishna, Morgan Kaufmann Publishers, 2007
2. Fault Tolerance in Distributed Systems, Pankaj Jalote, PTR Prentice Hall, 1994.
3. Fault Tolerant Computer System design by D. K. Pradhan, Prentice Hall.

CST738 Pattern Classification (3-0-0)

Introduction to Pattern Recognition: Clustering vs. Classification; Applications; Linear Algebra, vector spaces, probability theory, estimation techniques.

Classification:Tree Classifiers Getting our feet wet with real classifiers: Decision Trees: CART, C4.5, ID3. Random Forests.

Bayes decision rule, Error probability, Error rate, Minimum distance classifier, Mahalanobis distance; K-NN Classifier, Linear discriminant functions and Non-linear decision boundaries.

Parametric Techniques Generative Methods grounded in Bayesian Decision Theory, Maximum Likelihood Estimation, Bayesian Parameter Estimation, Sufficient Statistics

Non-Parametric Techniques: Kernel Density Estimators, Parzen Window, Nearest Neighbor Methods

Single and Multilayer perceptron, training set and test sets, standardization and normalization.

Unsupervised Methods: Component Analysis and Dimension Reduction, The Curse of Dimensionality, Principal Component Analysis, Fisher Linear Discriminant

Clustering: Different distance functions and similarity measures, Minimum within cluster distance criterion, K-means clustering, single linkage and complete linkage clustering, MST, medoids, DBSCAN, Visualization of datasets, existence of unique clusters or no clusters.

Feature selection: Problem statement and Uses, Probabilistic separability based criterion functions, interclass distance based criterion functions, Branch and bound algorithm, sequential forward/backward selection algorithms, (l,r) algorithm.

Feature Extraction: PCA, Kernel PCA.

Recent advances in PR: Structural PR, SVMs, FCM

References

1. Richard O. Duda, David G.Stork,Peter E. Hart, Pattern Classification, Wiley 2007
2. Bishop, C. M. Pattern Recognition and Machine Learning. Springer. 2007.
3. Dougherty, Pattern Recognition and Classification, Springer 2011.
4. Theodoridis, S. and Koutroumbas, K. Pattern Recognition. Edition 4. Academic Press, 2008.

5. Russell, S. and Norvig, N. Artificial Intelligence: A Modern Approach. Prentice Hall Series in Artificial Intelligence. 2003.
6. Bishop, C. M. Neural Networks for Pattern Recognition. Oxford University Press. 1995.
7. Andrew R. Webb, Kith D. Copsey, Statistical Pattern Recognition, Wiley 2011

CST740 Security Analysis of Protocols (3-0-0)

Cryptographic background; Authentication; Key establishment and IP security; Denial of service; Anonymity and MIX networks; Fairness and contract signing; Privacy and protection of individual information; Wireless security (mobile phones, WiFi);

Protocol analysis tools: Finite-state checking; Infinite-state symbolic analysis; Probabilistic model checking; Game-based verification; Process algebras (spi-calculus and applied pi-calculus); Protocol logics (BAN, DDMP, Isabelle); Introduction to Probabilistic polynomial-time calculus; Relating cryptographic and formal models;

References:

1. Latest reputed conference and journal articles as chosen by the instructor.
2. Maximum Security, 2nd Edition, SAMS Books by Anonymous, 1998, ISBN: 0-672-31341-3.

   Maximum Linux Security, SAMS Books by Anonymous, 2000, ISBN: 0-672-31670-6.
3. The Cuckoo's Egg : Tracking a Spy Through the Maze of Computer Espionage; by Clifford Stoll; Pocket Books; ISBN 0671726889
4. It's no secret: Measuring the security and reliability of authentication via 'secret' questions, by Schechter, Brush, and Egelman
5. 10 Risks of PKI: What You're not Being Told about Public Key Infrastructure, by Ellison and Schneier
6. Computer Networks, a Systems Approach (3rd edition), by Peterson and Davie.
7. *Network Security: Private Communication in a Public World" (2nd edition),* by Kaufman, Perlman, and Speciner

CST742 Biometrics (3-0-0)

Introduction of Biometric traits and its aim, image processing basics, basic image operations, filtering, enhancement, sharpening, edge detection, smoothening, enhancement, thresholding, localization. Fourier Series, DFT, inverse of DFT. Biometric system, identification and verification. FAR/FRR, system design issues. Positive/negative identification. Biometric system security, authentication protocols, matching score distribution, ROC curve, DET curve, FAR/FRR curve. Expected overall error, EER, biometric myths and misrepresentations. Selection of suitable biometric. Biometric attributes, Zephyr charts, types of multi biometrics. Verification on multimodel system, normalization strategy, Fusion methods, Multimodel identification. Biometric system security, Biometric system vulnerabilities, circumvention, covert acquisition, quality control, template generation, interoperability, data storage. Leading technologies : Finger-scan –

Facial-scan – Iris-scan – Voice-scan – Hand Scan, Retina Scan - components, working principles, competing technologies, strengths and weaknesses. Recognition systems: Face,Signature, Fingerprint,Ear, Iris etc. Assessing the Privacy Risks of Biometrics – Designing Privacy-Sympathetic Biometric Systems – Need for standards – different biometric standards.

References:

1. Introduction to Biometrics, Jain, Ross, Nandakumar, Springer 2011
2. Guide to Biometrics, Ruud M.Bolle,Sharath Pankanti, Nalini K. Ratha,Andrew W. Senior, Jonathan H. Connell,Springer 2009
3. Biometrics – Identity Verification in a Networked World, Samir Nanavati, Michael Thieme, Raj Nanavati, Wiley-dreamtech India Pvt Ltd, New Delhi, 2003
4. Biometric Technologies and Verification Systems, John R Vacca, Elsevier Inc, 2007
6. Digital Image Processing using MATLAB,By: Rafael C. Gonzalez, Richard Eugene Woods, 2nd Edition, Tata McGraw-Hill Education 2010

CST744 Digital Forensics (3-0-0)

PRE-REQUISITES: Computer Networks, Network Security

COURSE OUTCOMES:

6. Describe what digital investigation is, the sources of evidence, and the limitations of forensics.
7. Describe the legal requirements for use of seized data, data collection, and storage
8. Reconstruct application history from application artifacts and replay of attack
9. Capture and interpret network traffic, analyze mobile devices, and inspect for presence of malware
10. Apply forensics tools to investigate security breaches and identify anti-forensic methods.

COURSE OUTLINE:

Foundations: Basic Principles and methodologies for digital forensics, Design systems with forensic needs in mind
Evidence Collection: Rules of Evidence, Jurisdictions, Chain of Custody; Search and Seizure of evidence: legal and procedural requirements; Digital Evidence methods and standards, Techniques and standards for Preservation of Data
Evidence Analysis: OS / File System Forensics, Application Forensics, Web Forensics, Network Forensics, Mobile Device Forensics
Investigation: Computer / Network / System attacks, Attack detection and investigation, Anti-forensics

TEXT BOOKS:

1. Thomas J Holt , Adam M Bossler, Kathryn C Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction, Routledge, 2015
2. Eoghan Casey, Handbook of Digital Forensics and Investigation, Academic Press**,** 2009
3. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, III Edition, 2011
4. Angus McKenzie Marshall, Digital Forensics: Digital Evidence in Criminal Investigations, Wiley-Blackwell, 2008

CST746 Intrusion Detection (3-0-0)

Overview of computer security solutions, Vulnerability assessment, firewalls, VPN’s
Review of Network protocol
Vulnerabilities: buffer overflow, packet fragmentation, out-of-spec packets
Overview of Intrusion Detection and Intrusion Prevention: Network and Host based IDS
Classes of attacks: Network layer (scans, denial of service, penetration), Application layer (software exploits, code injection), Identity theft, root access, etc.
Threats: Malware detection, Drones, Worms, Viruses, Botnets, Email/IM issues, Insider Threat issues
IDS and IPS – Architecture and internals, tcpdump.
Malicious and non-malicious traffic, IP headers, TDP, UPD and ICMP protocols and header formats, Header information to detect intrusion, logs and their analysis,
Signature based Solutions, Snort, Snort rules
Anomaly Detection Systems and Algorithms: Network Behavior Based Anomaly Detectors (rate based), Host based Anomaly Detectors, Attack trees and Correlation of alerts
Collaborative Security

Text & References:

1. Matt Fearnow, Stephen Northcutt, Karen Frederick, and Mark Cooper. *Intrusion Signatures and Analysis*, SAMS.
2. Carl Endorf, Gene Schultz, Jim Mellander, *Intrusion Detection and Prevention*, McGraw Hill.
3. Stephen Northcutt and Judy Novak. *Network Intrusion Detection*, SAMS.
4. Paul E. Proctor. *The Practical Intrusion Detection Handbook*, Prentice Hall.
5. Rebecca Gurley Bace: *Intrusion Detection*,

CST748 Internet of Things (3-0-0)

Introduction: Internet of Things and Connected Products, IoT paradigm, Smart objects, Goal orientation, Convergence of technologies; Business Aspects of the Internet of Things.

Internet and “Things”: Layers, Protocols, Packets, Services, Performance parameters of a packet network and applications: Web, Peer-to-peer, Sensor networks, and Multimedia.

Hardware and Software: Hardware components, Microcontrollers and Software; Operating Systems.

Protocols and Platforms: IoT Communication Protocols, Transport Protocols, Application Protocols; Cloud computing for IoT.

Services and Attributes: Data creation, Data gathering and Data dependency; Robustness, Scaling, Privacy, Security, Trust.

Application: Implications for the society, IoT case study.

Text and References:

1. The Internet of Things: Key Applications and Protocols, David Boswarthick, Olivier Hersent, and Omar Elloumi, Wiley
2. Building the Internet of Things with IPv6 and MIPv6, Daniel Minoli, Wiley.
3. Latest research articles.

CST750 Ethical Hacking (3-0-0)

PRE-REQUISITES: Computer Networks, Network Security

COURSE OUTCOMES:

1. To know about hacking concept and apply it in ethical manner.
2. To provide awareness of security policies in defense field.
3. To learn about the tools and methods for hacking servers and Operating System.

COURSE OUTLINE:

Introduction & Overview: Ethical Hacking Terminology, Types, Different stages and phases in Ethical Hacking, Gaining Access, Hactivism, Footprinting and Social Engineering, E-Mail Tracking, Common Types of Attacks, Identity Theft, Phishing Attack, Online Scams, URL obfuscation.

Scanning and Enumeration: Scanning, types of scanning, Ping Sweep Techniques, Proxy Servers, HTTP Tunneling Techniques, IP Spoofing Techniques, Enumeration, Null Session, SNMP Enumeration, System Hacking: Understanding Password Cracking Techniques, Understanding the LanManager, Hash Cracking Windows passwords, Redirecting the SMB logon to Attacker.

Attacks: Trojans, Backdoors, viruses, worms, sniffers, Denial of Service and Session Hijacking

Hacking: Hacking Web Servers, Web Application Vulnerabilities and Web-Based Password Cracking Techniques, SQL Injection and buffer overflows.

Penetration Testing: Penetration testing methodology, Steps of penetration testing, Legal Framework, Penetration Testing Tools: Manual and Automated Tools, Penetration Testing Deliverables.

Text Books:

1. Hands-On Ethical Hacking and Network Defense – By Michael T. Simpson, Kent Backman, James Corley
2. Official Certified Ethical Hacker Review Guide – By Steven DeFino, Barry Kaufman, Nick Valenteen.
3. CEH Official Certified Ethical Hacking Review Guide, Wiley India Edition.
4. Certified Ethical Hacker: Michael Gregg, Pearson Education.
5. Certified Ethical Hacker: Matt Walker, TMH.
6. The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy (Syngress Basics Series)
7. Allen Harper, Shon Harris, Jonathan Ness, Chris Eagle, Gideon Lenkey, Terron Williams, Gray Hat Hacking: The Ethical Hackers Handbook, 3rd Edition.

CST752 Parallel and Distributed Systems (3-0-0)

Parallel and Distributed Computing: Concepts and issues in parallel and distributed computing. Multi-core and GP GPU computing, Distributed Systems models and enabling technologies, computer clusters for scalable parallel computing, Virtual machines and Virtualization. Grid Computing systems and resource management, Cloud computing and related issues.

Reference Book

1. Distributed and Cloud computing, Kai Hawang, Geoffrey C. Fox and Jack J. Dongarra, Morgan Kaufmann Publishers, 2012.

CST754 Cyber Laws and IPR (3-0-0)

Understanding Copy Right in Information Technology: Understanding the technology of Software software-copyright vs Patent debate Authorship , Assignment issues Commissioned work, Work for hire Idea/Expression dichotomy, Copy right in internet, Legal Issues in internet and Software Copyright Jurisdiction Issues, Copyright Infringe Remedies of Infringement Multimedia, Copyright issues Software Piracy, Patents understanding; **Cyber Crimes:** Understanding Cyber Crimes in context of Internet, Indian Penal Law & Cyber Crimes Fraud Hacking Mischief, International law, Obscenity and Pornography Internet, Potential of Obscenity Indian Law On Obscenity & Pornography Technical, Legal solutions International efforts Changes in Indian Laws, Ecommerce & Taxation, Security and Evidence in E-Commerce Dual Key encryption Digital signatures security issues, UNCITRAL model law of E- Commerce, Indian Legal Position on E-Commerce IT Act 2000/Indian Evidence Act/Draft law on E-Commerce

Procedures and security Polices, Risk assessment methodologies, Risk management, DRP/BCP-Business impact analysis, Asset classification, process level strategy, information classification organization, Crisis management plan, Resources recovery strategy, Framework, audits benchmarks, compliance, communications; **Data protection for system designers**: Evaluation criteria and security testing, International standards, Analysis and Logging, Recovery and data backs, Security policy development; **Security Models**: Frameworks, Standards, Security Certification ISO 17799/ ISO 27001, System Security Engineering Capacity Maturity Model, Laws and Legal Framework for Information Security, Recovery and risk analysis, Operating system and application specific auditing.

Text Book:

1. V. D. Dudeja ,”*Cyber Crime and Law Enforcement*”, Commonwealth Publishers, 2003

2. C. Davis,”*IT Auditing: Using Controls to protect Information Assets*”, TMH, 2011