MS Program in Cyber Security

Fields of Specialization

1	Communications Security (CS)
2	Cyber Security Management (CSM)
3	Computer Systems Security (CSS)
4	Cyber Physical Systems Security (CPSS)

Semester-Wise Course Plan

FELLOWS

FR: Fellowship Requirement, **IR:** Institutional Requirement, **C**: Core, **O**: Optional

No.	Course Title	Cr. Hrs.	Course Status	Credit Hours
SPRING SEMESTER – YEAR 1				
1	Communication Skills	1	IR	**13**
2	Cryptography	3	C	
3	Network Security	3	C	
4	**Optional-1**	3	O	
5	**Optional-2**	3	O	
SUMMER SESSION – YEAR 1				
1	**Fellowship Requirement - I**	3	FR	**6**
2	**Fellowship Requirement - II**	3	FR	
FALL SEMESTER – YEAR 1				
1	**Optional-3**	3	O	**12**
2	**Optional-4**	3	O	
3	**Optional-5**	3	O	
4	**Optional-6**	3	O	
SPRING SEMESTER - YEAR 2				
1	Thesis Research	6	C	**6**
SUMMER SEMESTER - YEAR 2				
1	Thesis Research	6	C	**6**

*FR = Any repeated or specialized course based on basic degree, probable placement, future assignment, etc.

Total Credit Hours = 37+6

NON-FELLOWS

IR: Institutional Requirement, **C**: Core, **O**: Optional

No.	Course Title	Cr. Hrs.	Course Status	Credit Hours
SPRING SEMESTER – YEAR 1				
1	Communication Skills	1	IR	**13**
2	Cryptography	3	C	
3	Network Security	3	C	
4	**Optional-1**	3	O	
5	**Optional-2**	3	O	
FALL SEMESTER – YEAR 1				
1	**Optional-3**	3	O	**12**
2	**Optional-4**	3	O	
3	**Optional-5**	3	O	
4	**Optional-6**	3	O	
SPRING SEMESTER - YEAR 2				
1	Thesis Research	6	C	**6**
SUMMER SEMESTER - YEAR 2				
1	Thesis Research	6	C	**6**

Total Credit Hours = 37

List of Courses

COMMUNICATIONS SECURITY	CYBER SECURITY MANAGEMENT	COMPUTER SYSTEMS SECURITY	CYBER PHYSICAL SYSTEMS SECURITY
CIS-575 Wireless Network and Mobile Computing	CIS-574 Risk Management and Control	CIS-564 Computer System Security	EE-545 Systems Programming
CIS-662 Cryptanalysis	CIS-576 Formal Methods for Information Security	CIS-571 Digital Forensics	EE-546 Embedded Systems and Drivers Programming
CIS-664 Wireless System Security	CIS-577 Cyberspace Operations and Design	CIS-578 Advanced Data Science for Security Analysis	EE-547 Communication Engineering
CIS-667 Network Security Monitoring	CIS-581 Vulnerability Discovery and Exploit Development	CIS-580 Database Security	EE-548 Industrial Automation Systems
CIS-670 Ethical Hacking and Network Defense	CIS-582 Cyber Warfare	CIS-663 Secure Software Development	EE-645 Emissions Security
CIS-671 Social Network Analysis		CIS-668 Security and Privacy in Cloud Computing	EE-646 Secure Embedded System Design
CIS-673 Advanced Cryptography		CIS-672 Malware Analysis	EE-647 Cyber Security of Industrial Control Systems
			CIS-662 Cryptanalysis
			CIS-665 Embedded System Security
COMMON FOR ALL SPECIALIZATIONS			
CIS-562 Information Theory and Coding	CIS-573 Electronic Physical Access Control and Surveillance	CIS-579 Machine Learning in Cyber Security	CIS-565 Information System Security Management
CIS-550 Advanced Computer Architecture	CIS-551 Advanced Operating Systems	NE-501 Fundamentals of Nuclear Engineering	-

MS Cyber Security

Course Contents

CMS-501: Communication Skills

Status	Institutional Requirement
Credits	1
Prerequisites	NIL

Writing module: Preparation of a project proposal or technical report, writing letters, mission statements, office memos etc; Speaking module: Presentation of the project proposal or technical report; Listening module: Simulations of interviews, lectures and question-answer sessions; Reading module: Reading of a suitable fiction novel (approximately 30-50 pages a week) with the use of vocabulary support, completion of assigned tasks and discussions.

References

1. *Eric H. G., and Glendinning N., English for Electrical and Mechanical Engineering, Oxford University Press, 1995.*
2. *Huckin T. N., and Oslen L.A., Technical Writing and Professional Communication for Nonnative Speakers of English, 2nd Edition, McGraw Hill, 1991.*
3. *Swales J. M., and Feak C. B., Academic Writing for Graduate Students, A Course for Nonnative Speakers of English, 3rd Edition, Uni. of Michigan Press, 1994.*

CIS-550: Advanced Computer Architecture

Status	Core
Credits	3
Prerequisites	NIL

Overview of modern processor architectures; Processor Design; Memory Hierarchy: Cache and Cache Coherence; Bus Architecture; Types of parallel machine: Vector Pipeline Architectures, Replicated Architectures, SIMD/MIMD, Shared Memory and Distributed Memory; Connectivity; Clusters; Networks; Routing; Performance Comparison; Dataflow; Virtual Concurrency; Branch prediction; TLB; Emulated instruction sets; VLIW; Out of order execution; Latency hiding; Case Studies: iA64, Linux clusters and IBM SP; Microcontrollers: Intel, PIC; Real-time processors: TMS320.

References

1. *Hennessy J. L. and Patterson D. A., Computer Architecture -- A Quantitative Approach, 5th Ed., Morgan Kaufmann Publications, Elsevier, Inc., 2012.*
2. *Stallings W., Computer Organization and Architecture, 9th Ed., Pearson Education Ltd, 2012.*
3. *Murdocca M. J., Heuring V. P., Computer Architecture and Organization: An Integrated Approach, John Wiley & sons Inc, 2007.*
4. *Englander I., The Architecture of Computer Hardware and System Software: An Information Technology Approach, International Student Version, 4th Ed., John Wiley & sons Inc, 2010.*

CIS-551: Advanced Operating Systems

Status	Core
Credits	3
Prerequisites	NIL

Process Synchronization: Synchronization Mechanisms, Process Deadlocks; Distributed Operating Systems: Architectures, Mutual Exclusion, Deadlock Detection, Agreement Protocols; Distributed Resource Management: File

Systems, Share Memory, Scheduling; Failure Recovery and Fault Tolerance; Protection and Security: Resource Security and Protection, Data Security; Multiprocessor Operating Systems; Database Operating Systems.

References

1. *Singhal M., and Shivaratri N. G., Advanced Concepts in Operating Systems, McGraw-Hill Series in Computer Science, 2008.*
2. *Silberschatz A., Galvin, P. B., Gagne G., Operating System Concepts, 9th ed., John Wiley & Sons, 2013.*
3. *Stalling W., Operating Systems, 5th ed., Pearson Education, 2006.*
4. *Tanenbaum A. S., Modern Operating Systems, 3rd ed., Prentice Hall, 2007.*

CIS-562: Information Theory and Coding

Status	Optional
Credits	3
Prerequisites	NIL

Theory of information: Entropy, Mutual information, Source coding theorem; Lossless compression of data, Optimal lossless coding; Communication channels: Channel capacity, Noisy communication channels, Channel coding theorem, Source channel separation theorem, Multiple access channels, Broadcast channels, Gaussian noise, and time-varying channels; Huffman coding; Universal source coding; Differential entropy; Block codes and Convolutional codes; Error correction code; Reliable and efficient communication systems.

References

1. Cover T. M, and Thomas J. A, Elements of Information Theory, 2nd Ed., John Wiley & Sons, 2006.
2. Wicker B. S., Error Control systems for Digital Communication and Storage, Prentice-Hall, 1994.
3. Gallagher R. G., Information Theory and Reliable Communication, Springer-Verlag, 1970.

CIS-564: Computer System Security

Status	Optional
Credits	3
Prerequisites	NIL

Software Flaws and Malwares: Viruses and their countermeasures, Worms, Trojan Horses, Bots, Rootkits; Buffer Overflow: Basics, Stack Buffer Overflow, Heap Overflow, Global Data Area Overflow; Compile Time and Runtime Defenses; Denial of service (DoS) attacks and defenses, Hostile Scripts: CGI Scripts, Web Scripts, Handling Script Security Miscellaneous, Spyware; Mobile Agent Security; Software-Based Attacks: Software Reverse Engineering, Software Tamper Resistance, Content Filtering; Digital Rights Management; Secure Software Development; Storage Security: Storage Media, Local file systems, Network File systems, RAID, Clustering, Backup Systems, File Integrity; Operating Systems and Security; Linux Security; Windows and Windows Vista Security; Processor security features ; Database Security; Securing Digital Contents.

References

1. *Stallings W., Brown L., Computer Security: Principles and Practice 2nd ed. Prentice Hall, 2012.*
2. *Kizza J. M., A Guide to Computer Network Security, Springer, 2009.*
3. *Robert C Newman, Computer Security: Protecting Digital Resources, Jones & Bartlett Learning, 2010.*
4. *Mike Harwood, Marcus Goncalves, Matthew Pemble, Security Strategies in Web Applications and Social Networking, Jones & Bartlett Learning, 2011.*
5. *Jason Albanese,Wes Sonnenreich, Network Security Illustrated, McGraw-Hill,2004.*

CIS-565: Information System Security Management

Status	Optional
Credits	3
Prerequisites	NIL

Elements of Information Protection, Difference between Information and Computer Security, Roles and Responsibilities, Common Threats, Policies and Procedures, Risk Management, Fraud and Theft, Malicious Hackers,

Denial-of-Service Attacks, Social Engineering, Information Security Architecture, Enterprise wide Security Program, Business Unit Responsibilities, Information Security Awareness Program, Information Security Program Infrastructure, Employment, Standards of Conduct, Conflict of Interest, Performance Management, Employee Discipline, Corporate Communications, Workplace Security, Business Continuity Plans (BCPs), Procurement and Contracts, Records Management, Asset Classification, Access control, Organization wide Policy Document Standards: ISO 27001/27002, COBIT, NIST FISMA, Legal Requirements, Physical Security, Security Technologies, Trusted Computing , Multilevel Security, Multilateral Security.

References

1. *Robert Johnson, Mark Merkow, Security Policies and Implementation Issues, Jones & Bartlett Learning, 2011.*
2. *Thomas R. Peltier et al., Information Security Fundamentals, Auerbach Publications, 2005.*
3. *Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed., John Wiley & Sons, 2008.*
4. *Tudor J. K., Information Security Architecture-An Integrated Approach to Security in the Organization, Auerbach Publications, 2001.*
5. *Steve Purser, A Practical Guide to Managing Information Security, Artech House, 2004.*

CIS-567: Cryptography

Status	Optional
Credits	3
Prerequisites	NIL

Definitions: Cryptography, cryptanalysis, steganography, encryption, decryption, plaintext, cipher text, etc; Mathematics of Cryptology: Number theory, Abstract algebra: groups, rings, fields; modular Arithmetic; Classical Cryptology: Simple Substitution ciphers, Transposition ciphers, ploy-alphabetic ciphers; Secret Key Cryptography: Modern Block Ciphers: Data Encryption Standard (DES), Advanced Encryption Standard (AES), Pseudorandom Number Generation and Stream ciphers: LFSR-based stream ciphers, RC4; Modes of Cipher operations: ECB, CBC, CFB, OFB, XTS-AES; Public Key Cryptography: Key agreement: Diffie-Hellman, Elgamal, Elliptic Curve Cryptography; RSA, Digital Signatures Integrity and authentication; Hash Functions: MD5, SHA-3; Message Authentication Codes : HMAC, DAA and CMAC, Authenticated Encryption using CCM and GCM.

References

1. *Stallings W., Cryptography and Network Security: Principles and Practice, 5th ed, Prentice Hall, 2011.*
2. *Jonathan Katz and Yehuda Lindell, Introduction to Modern Cryptography, CRC Press, 2007.*
3. *Niels Ferguson, Bruce Schneier, Tadayoshi Kohno, Cryptography Engineering. Wiley, 2010.*
4. *Christof Paar and Jan Pelzl, Understanding Cryptography, Springer, 2010.*

CIS-568: Network Security

Status	Optional
Credits	3+1
Prerequisites	NIL

Introduction to Network Security, User Authentication: Password-bases, token-based, biometric, remote authentication; Access Control: Principles, Discretionary and Role based; Key Management and Distribution, Security at the data link layer: MAC Flooding, ARP Spoofing, STP attacks, VLAN attacks; Security at the network layers: Attacks and Countermeasures for RIP, OSPF and BGP, IPSec and IKE, VPN, NAT, Secure Multicasting; Intrusion detection, Firewalls, IP spoofing prevention, Secure communication at the transport and application layers: SSL/TLS,HTTPS, Secure Shell; Email security: PGP, S/MIME, DKIM; Domain name server (DNS) security, Wireless networks security, Network Management Security.

References

1. *Stallings W., Network Security Essentials: Applications and Standards, 4th ed, Publisher: Prentice Hall, 2011.*
2. *Alan Yeung, Angus Wong, Network Infrastructure Security, Springer, 2009.*
3. *J. Michael Stewart, Network Security, Firewalls, and VPNs, Jones & Bartlett Learning, 2011.*

4. *Bill Ballad, Tricia Ballad, Erin Banks, Access Control, Authentication, and Public Key Infrastructure, Jones & Bartlett Learning, 2011*
5. *Bryan Burns et al., Security Power Tools, O'Reilly Media, 2007.*

CIS-571: Digital Forensics

Status	Optional
Credits	3
Prerequisites	NIL

The Evolution of Hacking, Footprinting the Environment, Scanning the Environment and Network, System Enumeration and System Hacking, Sniffers, Backtrack R3, System Forensics Fundamentals, Overview of Computer Crime, Challenges of System Forensics, Forensics Methods and Labs, System Forensics Technologies, Controlling a Forensic Investigation, Collecting, Seizing, and Protecting Evidence, Investigating Information-Hiding Techniques, Recovering Data, Investigating and Scrutinizing E-mail, Performing Network and Internet Analysis, Searching Memory in Real Time with Live Systems Forensics, Incident/Intrusion Response, Mobile System Forensics, Future Directions.

References

1. *Sean-Philip Oriyano, Michael Gregg, Hacker Techniques, Tools, and Incident Handling, Jones & Bartlett Learning Publication, 2011.*
2. *John R. Vacca, K Rudolph, System Forensics, Investigation, and Response, Jones & Bartlett Learning Publication, 2011.*
3. *Nelson B., Phillips A., Steuart C., Guide to Computer Forensics and Investigations, 4th ed., Cengage Learning, 2010.*
4. *Albert J. Marcella, Jr. Doug Menendez, Cyber Forensics-a Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd ed., Auerbach Publications, 2008.*
5. *Altheide C., and Carvey H., Digital Forensics with Open Source Tools, Elsevier, 2011.*

CIS-573: Electronic Physical Access Control and Surveillance

Status	Optional
Credits	3
Prerequisites	NIL

Fundamental concepts of Electronic Physical security, Fundamental concepts of Electronic Access Control, Fundamental concepts of image processing, Introduction to Biometric Systems for access control, Fingerprint based biometrics, Facial Recognition, Iris based person identification, hand and palmprint based identification, Voice/Speech biometrics, Soft biometrics, Design issues in biometrics, multimodal biometrics, anti-spoofing and liveness detection techniques, Multimodal biometrics, Closed Circuit Television and Internet Protocol (IP) Cameras, Automated Video Understanding and activity recognition, Motion sensing mechanisms, Physical access restriction systems. Student project involving implementation of an EPACS System.

References

1. *Yang, Jucheng, ed. New Trends and Developments in Biometrics. InTech, 2012.*
2. *Jain, Anil, Patrick Flynn, and Arun A. Ross, eds. Handbook of Biometrics. Softcover reprint of hardcover 1st ed. 2008 edition. New York: Springer, 2010.*
3. *Norman, Thomas L. Electronic Access Control. Waltham, MA: Butterworth-Heinemann, 2011.*
4. *Romanowich, John, Danny Chin, and Thomas V. Lento. Smart Video Security Handbook: A Practical Guide for Catching Intruders Before They Act. 1 edition. Video Valley Press, 2015.*
5. *Fu, Yun. Human Activity Recognition and Prediction. Springer, 2015.*

CIS-574: Risk Management and Control

Status	Optional
Credits	3
Prerequisites	NIL

Auditing: Principles, Standards and Frameworks, Tools and Techniques, Planning Audit for Compliance, Audit Reports; Goal-Based Security Controls, Implementation-Based Security Controls, Security Control Formulation and Development Process, Security Architecture Design; Risk Management: Fundamentals, Threats, Vulnerabilities, Exploits, Maintaining Compliance, Developing a Risk Management Plan, Risk Assessment Approaches, Risk Assessment: Assets Identification, Activities to be Protected, Identifying Risk Mitigation: Security Controls, Planning throughout the Organization, turning assessment into a plan, Business Impact Analysis, with a Business Continuity Plan, with a Disaster Recovery Plan, Computer Incident Response Team Plan.

References

1. *Chris Jackson, Network Security Auditing Tools and Techniques, Cisco Press, 2010.*
2. *Kohnke, Anne, Dan Shoemaker, and Ken E. Sigler. The Complete Guide to Cybersecurity Risks and Controls. CRC Press, 2016.*
3. *Darril Gibson, Managing Risk in Information Systems, Jones & Bartlett Learning, 2011.*
4. *Andy Jones, Debi Ashenden, Risk Management for Computer Security- Protecting Your Network and Information Assets, Elsevier, 2005.*

CIS-575: Wireless Network and Mobile Computing

Status	Optional
Credits	3
Prerequisites	NIL

Introduction to Wireless Networks, Definition of Mobile and Wireless, Components of Wireless Environment, Challenges, Foundations of Mobile and Ubiquitous Computing, Introduction to MANET, MAC layer and 802.11 networks. Wireless LAN : Infra red Vs radio transmission, Infrastructure and Ad-hoc Network, MANET MAC layer, MAC layer issues, Routing in MANET , Unicast, Multicast routing in MANETs, Example of MANETs, D2D networks, DTN, Wireless inter- networking, WSN, QoS in MANET, Self-organizing networks; Introduction, formation, SON in cellular networks, SON in WLAN. , Mobility Management; Mobility management, routing area in UMTS networks, tracking area in LTE, introduction to hand-off.

References

1. *Stallings, William. Wireless communications & networks. Pearson Education, 2009.*
2. *Olenewa, Jorge. Guide to wireless communications. Cengage Learning, 2013.*
3. *Theodore S. Rappaport, Wireless Communications: Principles and Practice, 2nd Ed, Prentice Hall, 2008.*
4. *Gast, Matthew. 802.11 wireless networks: the definitive guide. O Reilly Media, Inc.", 2005.*
5. *Adelstein, Frank, et al. Fundamentals of mobile and pervasive computing, McGraw-Hill, 2005.*

CIS-576: Formal Methods for Information Security

Status	Optional
Credits	3
Prerequisites	NIL

Basics of formal methods for security (principles and techniques), modeling, design and verification of security protocols and systems, access control and security models, information flow control, secure public-key infrastructures, probabilistic methods, security in distributed systems/secure middleware. Formal Verification Tools.

References

1. *Matt Bishop: Computer Security, Pearson Education, 2003.*
2. *Cremers, Cas, and Sjouke Mauw. Operational semantics and verification of security protocols. Springer Science & Business Media, 2012.*
3. *Giampaolo Bella, Formal Verification of Security Protocols, Springer, 2007.*
4. *Colin Boyd and Anish Mathuria, Protocols for Authentication and Key Establishment, Springer, 2003.*
5. *Peter Ryan, Steve Schneider, und M. H. Goldsmith: Modeling and Analysis of Security Protocols, Addision-Wesley, 2000.*

CIS-577: Cyberspace Operations and Design

Status	Optional
Credits	3
Prerequisites	NIL

Cyberspace Environment and Design: Characteristics, design approach, planning for operation; Cyberspace Operational Approaches: Foundational approaches that utilize cyberspace capabilities to support organizational missions, The pros and cons of the different approaches; Cyberspace Operations: Network Operations (NETOPS), Defensive Cyberspace Operations (DCO), Offensive Cyberspace Operations (OCO), Defense and Diversity of Depth network design, Operational methodologies to conduct cyberspace operations; Cyberspace Integration: Design a cyberspace operation and integrate it with a Joint Operations plan, Practice the presented methodologies in a practical application exercise; Building Cyber Warriors and Warrior Corps: The warrior and warrior corps concept as applied to cyber organizations, The challenges of training and developing a cyber-workforce from senior leadership to the technical workforce Designing Cyber Related Commands: Mission statements, Essential tasks, Organizational structures, Tables of organizations; Training and Readiness for Cyber Related Commands: Mission Essential Tasks (METs), Developing the cyber workforce, Plan your own training programs within your organization.

References

1. *Paulo Shakarian et al. "Introduction of Cyber Warfare: A Multidisciplinary Approach", Elsevier, 2013.*
2. *Jeffery carr et al, "Inside Cyber Warfare: Mapping the Cyber Underworld," O'Reilly Publication, 2012.*
3. *Jason Andress et al. "Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners" , Elsevier 2013.*
4. *R. A. Clarke, Robert Knake "Cyber War: The Next Threat to National Security and What to Do About It" Haper Collins Publisher 2010.*

CIS-578: Advanced Data Science for Security Analysis

Status	Optional
Credits	3
Prerequisites	NIL

Handling Streaming Data - In-memory Analytics using Spark, Introduction to Redis, Using Redis in Spark for In-mem analytics, Message Brokers (MQTT, Kafka, Active MQ), CMS, HLL algorithms, Social media Analytics, Streaming Sensor Data Analytics, Introduction to Streaming Algorithms, Advanced Hadoop& MR, Implementing complex algorithms using MR, Analytics HDFS data in Spark (in-memory) using Shark and Spark SQL, Implementing Slowly changing dimensions in Hadoop based Data warehouses. Big Data Warehouse - Hadoop Ecosystem, HBase, Pig & Pig Latin, Sqoop, ZooKeeper, Hue, Hive,Flume,Oozie Security Concerns in Big data, Visualization techniques in Big Data Analytics, Case Study & Implementation.

References

1. *A. Rajaraman and J. D. Ullman, Mining of Massive Datasets, Cambridge University Press, 2012.*
2. *N. Burlingame, The Little Book of Big Data, New Street Communications, 2012.*

CIS-579: Machine Learning in Cyber Security

Status	Optional
Credits	3
Prerequisites	NIL

Introduction to machine Learning(ML), ML examples, supervised, semi-supervised, and unsupervised learning, Regression, Clustering, generative vs. discriminative learning; Classification: linear and nonlinear classifiers, perceptron, MLP, kNN, Naïve Bayes Classifier, Decision Tree, SVM, SOM, Deep Neural Networks, Ensemble Classifiers; multiple linear regression, Generalized Linear regression; Preprocessing: data balancing, SMOTE; cross-validation, ROC and PR curves; Feature Space, Feature Selection; Feature Reduction: PCA, ICA, and LDA; Bias

Variance Dilemma, No-free lunch; Learning-based Intrusion Detection, Semi-supervised and unsupervised Malware Analysis, Pattern-based Vulnerability Discovery, Privacy Attacks using Machine Learning.

References

1. *Dua, Sumeet, and Xian Du. Data mining and machine learning in cybersecurity. CRC press, 2016.*
2. *Sergios Theodoridis Sergios Theodoridis Konstantinos Koutroumbas, Pattern Recognition, 4th Ed, Elsevier, 2008.*
3. *Alpaydin, Ethem. Introduction to machine learning. MIT press, 2014.*
4. *Witten, Ian H., et al. Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann, 2016.*
5. *Di Pietro, Roberto, and Luigi V. Mancini, Intrusion detection systems. Springer, 2008.*
6. *Ghorbani, Ali A., Wei Lu, and Mahbod Tavallaee. Network intrusion detection and prevention: concepts and techniques. Springer, 2009.*

CIS-580: Database Security

Status	Optional
Credits	3
Prerequisites	NIL

Database security concepts, importance in industrial, civilian and government domains, database secrecy, integrity, availability, security architecture, identify assets, risks and vulnerabilities, role players, operating system security, privileges, passwords, roles, access control models, discretionary access control and role based access control, mandatory access control, database application security models, securing dbms, policies, profiles and roles, user creation and administration, database intrusion prevention, fault tolerance and recovery, database detection and forensic security controls, log management, sql injection, defensive programming, database encryption and masking, virtual private databases, database auditing models, application data auditing, multilevel secure relational model, covert channels and inference channels, watermarking relational databases, security in distributed databases, security and privacy issues of data mining.

References

1. *Ron Ben Natan, Implementing Database Security and Auditing, Elsevier, 2005*
2. *Alfred Basta, Database Security, Cengage Learning, 2011*
3. *Gertz, Michael, Jajodia, Sushil, The Handbook of Database Security: Applications & Trends, Springer, 2008*
4. *Patricia Huey, Oracle Security Guide 11g Release 2 (11.2), Oracle, 2015*
5. *Database Security Guideline, Database Security Consortium, 2009*
6. *Eduardo B. Fernandez, Database Security and Integrity, Addison-Wesley,1981*

CIS-581: Vulnerability Discovery and Exploit Development

Status	Optional
Credits	3
Prerequisites	NIL

Background- Vulnerability Discovery Methodologies, What is Fuzzing, Fuzzing Methods and Fuzzer Types, Data Representation and Analysis, Requirements for Effective Fuzzing Targets and Automation- Automation and Data Generation, Environment Variable and Argument Fuzzing, Environment Variable and Argument Fuzzing: Automation, Web Application and Server Fuzzing, Web Application and Server Fuzzing: Automation, File Format Fuzzing, File Format Fuzzing: Automation on UNIX, File Format Fuzzing: Automation on Windows, Network Protocol Fuzzing, Network Protocol Fuzzing: Automation on UNIX, Network Protocol Fuzzing: Automation on Windows, Web Browser Fuzzing, Web Browser Fuzzing: Automation, In-Memory Fuzzing, In-Memory Fuzzing: Automation Advanced Fuzzy Technologies- Fuzzing Frameworks, Automated Protocol Dissection, Fuzzer Tracking, Intelligent Fault Detection. Advanced Linux Exploitation-Linux heap management, constructs, and environment, Navigating the heap, Abusing macros such as unlink() and frontlink(), Function pointer overwrites, Format string exploitation, Abusing custom doubly-linked lists, Defeating Linux exploit mitigation controls, Using IDA for Linux application exploitation, Patch Diffing, one day Exploits and Return Oriented Shellcode, The Microsoft patch

management process and Patch Tuesday, Obtaining patches and patch extraction, Binary diffing with BinDiff, patchdiff2, turbodiff, and darungrim, Visualizing code changes and identifying fixes, Reversing 32-bit and 64-bit applications and modules, Triggering patched vulnerabilities, Writing one-day exploits, Handling modern exploit mitigation controls. Windows Kernel Debugging and Exploitation- Understanding the Windows Kernel, Navigating the Windows Kernel, Modern Kernel protections, Debugging the Windows Kernel, WinDbg, Analysing Kernel vulnerabilities and Kernel vulnerability types, Kernel exploitation techniques. Windows Heap Overflows and Client-Side Exploitation- Windows heap management, constructs, and environment, Browser-based and client-side exploitation, Remedial heap spraying, Understanding C++, vftable/vtable behavior, Modern heap spraying to determine address predictability, Use-After-Free attacks and dangling pointers, Determining exploitability, Defeating ASLR, DEP, and other common exploit mitigation controls Android Exploitation- Android Basics, Android Security Model, Introduction to ARM, Android Development Tools, Engage with Application Security, Android Security Assessment Tools, Exploiting Applications, Protecting Applications, Secure Networking, Native Exploitation and Analysis. iOS exploitation-Introduction to iOS hacking, iOS User Space Exploitation, iOS Kernel Debugging and Exploitation.

References

1. *Hack I.T. - Security Through Penetration Testing, T. J. Klevinsky, Scott Laliberte and Ajay Gupta, Addison-Wesley, ISBN: 0-201-71956-8*
2. *Metasploit: The Penetration Tester's Guide, David Kennedy, Jim O'Gorman, Devon Kearns, Mati Aharoni*
3. *Professional Penetration Testing: Creating and Operating a Formal Hacking Lab, Thomas Wilhelm.*

CIS-582: Cyber Warfare

Status	Optional
Credits	3
Prerequisites	NIL

Unconventional War Around the World: Stop Georgia Project, Estonia, Russian Information War, Gaza War, Operation Cast Lead, Stuxnet, China the Cyber Super Power; Legal Status of Cyber War: Nuclear Nonproliferation Treaties, UNCLOS, MALT, Is This an Act of Cyber War, Cyber: The Chaotic Domain; Response to International Cyber Attack as Act of War: The Legal Dilemma, Law of War, Non State Actors, Analyzing Cyber Attacks, Active Defense; Intelligence Component to Cyber War: Korean DDoS Attack, RU-GE War aftermath, Ingushetia Conflict, Predictive Role of Intelligence; Non State Hacker and Social Web: Case studies from around the world: Russia, China, Pakistan & Indian Cyber Attacks; Organized Crime in Cyberspace: Atrivo/Intercage, ESTDomains, McColo: Bullet proof hosting for world largest BotNet, Kremlin, Investigating Attribute; Weapon zing Malware: A New Threat Landscape: StopGerigia.ru Malware Discussion, Twitter as Dos Command Post Against Iran, Social Engineering, Channel Consolidation, An Adversary Look at Linkedin, BIOS base Rootkit, Malware for Hire, Targeted Attack Against Military Brass and Government Executive; The Role of Cyber in Military Doctrine: The Russian Federation, Chine Military Doctrine, US Military Doctrine, Israel Military Doctrine, Cyber Early Warning Model, The Challenge We Face, Early Warning Networks, Build Tactical Network for Early Warning, Lear Lessons from Cyber Wars and Atttacks, Defense Readiness Condition for Cyberspace; Advice of Policy Makers: Scenarios and Options to Response, Whole of Nations Cyber Security, How Things are Done in Other Part of the World: US, China, India, Israel, Iran.

References

1. *Carr, Jeffrey. Inside cyber warfare: Mapping the cyber underworld. " O'Reilly Media, Inc.", 2011.*
2. *Arquilla, John. "Strategic Warfare in Cyberspace by Gregory J. Rattray." Political Science Quarterly 117.2 (2002): 319-321.*
3. *Kramer, Franklin D., Stuart H. Starr, and Larry K. Wentz. Cyberpower and national security. Potomac Books, Inc., 2009.*
4. *Adams, James. The next world war: Computers are the weapons and the front line is everywhere. Simon and Schuster, 2001.*
5. *Buckley, John, and George Kassimeris, eds. The Ashgate research companion to modern warfare. Routledge, 2016.*

CIS-590: Special Topics I

Status	Optional
Credits	3
Prerequisites	Nil

This course may be used for advanced topics not already covered in the syllabus. The special paper may be conducted as a lecture course or as an independent study course. The faculty must approve the topic and contents of the course.

CIS-662: Cryptanalysis

Status	Optional
Credits	3
Prerequisites	CIS-567

Cryptanalysis of Classical Cryptosystems; Cryptanalysis of Block Ciphers: Hellman's Time Memory trade-off attack, Linear Cryptanalysis, The Piling-up Lemma, Linear Approximations of S-boxes, A Linear Attack on an SPN, Differential Cryptanalysis, Differential Cryptanalysis of DES, Slide Attack, Related Key attacks Introduction to Side Channel attacks; Cryptanalysis of Stream Ciphers: Correlation attack and fast correlation attack, Algebraic attack, distinguishing attacks, Fast Walsh Transform, Correlation Immunity and Algebraic Immunity of Boolean functions; Cryptanalysis of Asymmetric Cryptosystems: Factoring Algorithms, The Pollard p1 Algorithm, The Pollard Rho Algorithm, Dixon's Random Squares Algorithm, Security of the Rabin Cryptosystem, Semantic Security of RSA, Factoring Algorithms: Pollard's p-1 , Pollard Rho, Dicson Randomized Square Root, Pomerance Quadratic Sieve for factor bases , Wiener's Low Decryption Exponent, Continued Fraction, Quadratic Sieve, Elliptic curve factorization method, Algorithms to attack Discrete Log Problem on Finite Fields: The Silver-Pohling-Hellman, The Index-Calculus, Attacks on basic key exchange and key transport protocols;

References

1. *Richard A. Mollin, . An introduction to Cryptography, 2nd ed., Chapman and Hall/CRC,2006*
2. *Mark Stamp, Richard M. Low, Applied Cryptanalysis- Breaking Ciphers in the real world, Wiley-IEEE, 2007.*
3. *Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC, 1996.*

CIS-663: Secure Software Development

Status	Optional
Credits	3
Prerequisites	CIS-564

Secure software attributes, Requirements engineering for secure software, Software engineering of secure application, Security-aware SDLC, System complexity drivers and security, Threat Modeling, Least privilege coding, privilege hierarchy, Least common mechanism, Code analysis, Fail-safe defaults in coding, Vulnerability cycles, Integration of application with Security architecture, Secure data structure design, Secure database services, Secure transport protocols, Penetration Testing and Application Security Testing, Constrained data access models, Secure procedure design, Development of security focused test cases, Security Mechanism and Protocols, Implementation of Security Mechanism, Secure Programming in: C /C++, Java & Microsoft.NET.

References

1. *Robert C. Seacord, Secure Coding in C and C++, 2nd ed., Addison-Wesley, 2013*
2. *Mark G. Graff, Kenneth R. van Wyk, Secure Coding: Principles and Practices, O'Reilly, 2003.*
3. *Messier M., Viega J., Secure Programming Cookbook for C and C++, O'Reilly, 2003.*
4. *Alan Cooper et al., "About Face 3: The Essentials of Interaction Design", John Wiley & Sons, 2007.*

CIS-664: Wireless System Security

Status	Optional
Credits	3
Prerequisites	CIS-575

Security in Wireless Networks and Devices: Cellular Wireless Communication, Wireless LANs, Wireless Application Protocol; Bluetooth Security: Introduction, Technology, Architecture, Weaknesses and Countermeasures; Mobile Telecom Networks: GPRS, UMTS, Architectures; Security in Mobile Ad Hoc Networks (MANETs): Introduction, Routing Protocols, Vulnerabilities, Preventing Attacks, Cryptographic Tools; Wireless Sensor Networks: Introduction, Sensor Devices, Sensor Network Security, Mitigating the threat of stolen devices, Security analysis of iOS 7, Android 4.4, End-to-end mobile security, Mobile Malware, Mobile Security Design and Management;

References

1. *Douligeris C., and Serpanos D. N., Network Security Current Status and Future Directions, John Wiley & Sons, 2007.*
2. *Ronald L. Krutz, Securing SCADA Systems, Wiley Publishing, 2006.*
3. *Sutton R. J., Secure Communications Applications and Management, John Wiley & Sons, 2002.*
4. *Tara M. , and Elden C. R., Wireless Security and Privacy: Best Practices and Design Techniques, Addison Wesley, 2002.*
5. *Peter van de Put, Professional iOS Programming, John Wiley, 2014.*

CIS-665: Embedded System Security

Status	Optional
Credits	3
Prerequisites	CIS-550

Embedded System Security: Trends, Policies and Threats; Systems Software Considerations: Operating System Role and Requirements, Multiple Independent Levels of Security, Access Control and Capabilities; Secure Embedded Software Development: Principles of High-Assurance Software Engineering, Minimal Implementation, Component Architecture, Independent Expert Validation; Embedded system Cryptography; Data Protection Protocols for Embedded Systems : Data-in-Motion Protocols, Data-at-Rest Protocols, Emerging Applications; Secure Rabbit Processor; FPGA Security, Secure Processors: IBM 4758, AEGIS, ARM Trust zone; SCADA System: Security Issues, SCADA Protocols, Vulnerabilities and Attacks, Security Methods and Techniques.

References

1. *David Kleidermacher, Mike Kleidermacher, Embedded Systems Security- Practical Methods for Safe and Secure Software and Systems Development, Elsevier, 2012.*
2. *Stapko T., Practical Embedded Security: Building Secure Resource-Constrained Systems, Elsevier, 2008.*
3. *Gebotyes C.H., Security in Embedded Devices, Springer, 2006.*
4. *F. Rodriguez-Henriquez, N. A. Saqib, A. Diaz-Perez, C. K. Koc , Cryptographic Algorithms on Reconfigurable Hardware, Springer, 2006.*

CIS-667: Security and Privacy in Cloud Computing

Status	Optional
Credits	3
Prerequisites	NIL

Cloud Computing Models, Secure Data Outsourcing, Secure Computation Outsourcing, Proof of Data Possession / Retrieveability, Virtual Machine Security, Trusted Computing Technology and Clouds, Cloud-Centric Regulatory Compliance Issues And Mechanisms, Business and Security Risk Models, Applications of Secure Cloud Computing.

References

1. *Winkler Vic JR, Securing the Cloud: Cloud computer Security techniques and tactics, Elsevier, 2011.*
2. *Pearson Siani and George Yee., Privacy and security for cloud computing, Springer, 2012.*
3. *Krutz Ronald L. and Russell Dean Vines, Cloud security: A comprehensive guide to secure cloud computing, John Wiley & Sons, 2010.*
4. *Halpert, Ben, Auditing cloud computing: A security and privacy guide, John Wiley & Sons, 2011.*
5. *Alliance C., Security guidance for critical areas of focus in cloud computing v3. 0., Cloud Security Alliance, 2011.*

CIS-668: Network Security Monitoring

Status	Optional
Credits	3
Prerequisites	CIS-568

Network Security Monitoring (NSM) Cycle, Planning Data Collection, Sensor Platforms, Detection Mechanisms, Indicators of Compromise and Signatures, Reputation-Based Detection, Signature-Based Detection, Anomaly-Based Detection with Statistical Data, Packet Analysis, Threat Intelligence, Analysis Process, Analysis Tools.

References

1. *Sanders Chris, and Jason Smith, Applied Network Security Monitoring: Collection, Detection, and Analysis, Elsevier, 2013.*
2. *Bejtlich Richard, The Practice of Network Security Monitoring: Understanding Incident Detection and Response, No Starch Press, 2013.*
3. *Blask, Chris, et al. Security Information and Event Management (SIEM) Implementation, McGraw-Hill, 2011.*
4. *Marty Raffael, Applied security visualization, Upper Saddle River: Addison-Wesley, 2009.*

CIS-670: Ethical Hacking and Network Defense

Status	Optional
Credits	3
Prerequisites	CIS-568

Certified ethical hackers, Network and computer attacks: Malicious software - Protection against malware - Intruder attacks on networks and computers -Addressing physical security, Ethical hacking plan and Hacking methodology. Footprinting And Social Engineering: Footprinting tools, Conducting competitive intelligence, DNS zone transfers, Social engineering: Introduction - Performing attacks – Countermeasures; Port Scanning: Overview, Types, Tools, Conducting ping sweeps, Shell scripting, Enumeration: Introduction – Enumerating Windows - Symbian - Java OS - Android – NetWare; Hacking Networks: Hacking web servers: Web application and its vulnerabilities, Tools for web attackers and security testers, Hacking wireless network: Technology - Standards - Authentication - Wardriving - Wireless hacking, Protecting networks with security devices; Hacking Operating Systems: Windows: Vulnerabilities - Choosing tools - Information gathering - RPC - Null sessions - Share permissions - Hardcore vulnerability exploitation, Linux: Vulnerabilities - Information gathering - Unconnected services -.rhosts and hosts equivalent files - NFS - File permissions - Buffer overflow; Hacking Applications: Messaging systems, Web applications, Mobile applications, Databases, Reporting results

References

1. *Michael T. Simpson, Kent Backman and James Corley, "Ethical Hacking and Network Defense", Cengage Learning, 2013.*
2. *Kevin Beaver, "Hacking for Dummies", Wiley Publication, 2010.*
3. *Ankit Fadia, "Unofficial Guide to Ethical Hacking", Macmillan Company, 2006.*
4. *Ankit Fadia and Manu Zacharia, "Network Intrusion Alert: An Ethical Hacking Guide to Intrusion Detection", Thomson Course Technology, 2010.*
5. *EC-Council, "Ethical Hacking and Countermeasures: Threats and Defense Mechanisms", Cengage Learning, 2010.*

CIS-671: Social Network Analysis

Status	Optional
Credits	3
Prerequisites	NIL

Networks- Concepts: nodes, edges, adjacency matrix, one and two-mode networks, node degree Random network models: Erdos-Renyi and Barabasi-Albert- Concepts: connected components, giant component, average shortest path, diameter, breadth-first search, preferential attachment Network centrality- Concepts: Betweenness, closeness, eigenvector centrality (+ PageRank), network centralization Community- Concepts: clustering, community structure, modularity, overlapping communities Small world network models, optimization, strategic network formation and search- Concepts: small worlds, geographic networks, decentralized search Contagion, opinion formation, coordination and cooperation- Concepts: simple contagion, threshold models, opinion formation, unusual applications of SNA SNA and online social networks- Concepts: how services such as Facebook, LinkedIn, Twitter, Couch Surfing, etc. are using SNA to understand their users and improve their functionality.

References

1. *John Scott, Social Network Analysis, 3rd Edition, SAGE, 2012.*
2. *Wouter de Nooy, Andrej Mrvar, Vladimir Batagelj, Exploratory Social Network Analysis with Pajek, 2nd Revised Edition, Cambridge University Press, 2011.*
3. *Patrick Doreian, Frans Stokman, Evolution of Social Networks, Routledge, 2013.*
4. *David Easley and Jon Kleinberg, Networks, Crowds, and Markets: Reasoning About a Highly Connected World, Cambridge University Press, 2010.*

CIS-672: Malware Analysis

Status	Optional
Credits	3
Prerequisites	CIS-565

Malware history and classification; Analysis of threat reports by prominent security companies; Infection Vectors (Buffer flows, Drive-by Downloads, Social Engineering), Botnets (Definition and Components, Architecture, Active and passive detection techniques) , Code obfuscation (executables and data obfuscation); Malware Analysis (Basics, static and dynamic), Software Reverse Engineering, Software Tamper Resistance, Virtualization Technology and Applications: Virtualization Taxonomy, Security Applications, Virtual Machine Introspection; Online fraud cycle, Underground economy & market and Digital currency

References

1. *Sikorski, Michael, and Andrew Honig. Practical malware analysis: the hands-on guide to dissecting malicious software. no starch press, 2012.*
2. *Ligh, Michael Hale, et al. The art of memory forensics: detecting malware and threats in Windows, Linux, and Mac memory. John Wiley & Sons, 2014.*
3. *Dang, Bruce, Alexandre Gazet, and Elias Bachaalany. Practical reverse engineering: x86, x64, ARM, Windows kernel, reversing tools, and obfuscation. John Wiley & Sons, 2014.*

CIS-673: Advanced Cryptography

Status	Optional
Credits	3
Prerequisites	CIS-567

Advanced Mathematics for Cryptography: Quadratic residues, and quadratic reciprocity, Legendre Symbol, Jacobi symbol, Cyclic groups, Cosets, Field extensions, Finite fields, Factorization of polynomials, irreducible polynomials, Polynomial ring over R, Polynomial Ring over F, Primitive Polynomials over Finite Fields, Elliptic Curves, Lattices; Block Ciphers or Stream Ciphers: Evaluation Criteria of Block and stream ciphers, Correlations and Walsh Transforms, Boolean Functions and S Boxes, Cryptographic Criteria: Propagation Characteristics, Nonlinearity and Resiliency, Correlation Immunity, Indistinguishability, Next bit predicators, one way functions, Authenticated Modes of Encryption, GCM, Security Criteria of Authentication -Un-forgeability, Strong un-forgeability; Public Key: Elliptic Curve Cryptography, ECDSA, Lattice Based Cryptography; Miscellaneous Topics of Modern Cryptography: PRNGs based on Hard problems, Cryptographic Protocols analysis techniques, Key Management Cycle, Secret sharing schemes, Zero knowledge protocols, Cryptography based on Bilinear Mapping, Mutiparty Computation, Introduction to Quantum Cryptography.

References

1. *Anderson, Ross. Security engineering. John Wiley & Sons, 2008.*
2. *Boyd, Colin, and Anish Mathuria. Protocols for authentication and key establishment. Springer Science & Business Media, 2013.*
3. *Blahut, Richard E. Cryptography and secure communication. Cambridge University Press, 2014.*
4. *Katz, Jonathan, and Yehuda Lindell. Introduction to modern cryptography. CRC press, 2014.*
5. *Research Papers*

CIS-690: Special Topics II

Status	Optional
Credits	3
Prerequisites	Nil

This course may be used for advanced topics not already covered in the syllabus. The special paper may be conducted as a lecture course or as an independent study course. The faculty must approve the topic and contents of the course.

EE-545: Systems Programming

Status	Optional
Credits	3
Prerequisites	NIL

Introduction, Lab & Software Setup, Windows Driver Model Overview, Windows Basic Device Driver Implementation (IRQL, Memory Pool), Debugging Kernel mode driver and Windows/Linux/OSX Boot Process With WinDbg and KD IDApro, IOCTL implementation, File System/Network/Keyboard Filter Driver, TDI/Winsock driver Implementation, NDIS 6.1 TCP/IP Stack Implementation, Introduction to Display Drivers, Drivers for Enumerating File/Process/Port/Registry (Assuagement for hiding), File System Implementation, Bus/DMA Driver, Linux Driver Introduction, Enumeration of Process file and registry and port, MAC/OSX Driver Introduction, Enumeration of Process file and registry and port.

References

1. *R. Love, Linux System Programming: Talking Directly to the Kernel and C Library. O'Reilly, 2013.*
2. *Russinovich, Solomon, "Windows Internals". Microsoft Press, 4th Ed, 2012.*
3. *N. Wilt, The CUDA Handbook: A Comprehensive Guide to GPU Programming, Addison-Wesley, 2013.*
4. *M. Barr and A. Massa, Programming Embedded Systems: With C and GNU Development Tools, 2nd Ed , O'Reilly, 2006.*

EE-546: Embedded Systems and Drivers Programming

Status	Core
Credits	3
Prerequisites	NIL

Introduction to embedded systems; introduction to ARM Cortex-M processor, ARM Cortex-M architecture, registers, memory organization, operating modes; Assembly and C language programing, Memory and I/O interfacing techniques and programing; Peripherals (Timer, Interrupts) interfacing and programing; debugging architecture and components; Synchronous serial communication and industry standard protocols (i.e. SPI, I2C) using ISR(interrupt service routines); Introduction to RTOS; Windows Driver Model Overview, Windows Basic Device Driver Implementation (IRQL, Memory Pool), Debugging Kernel mode driver and Windows/Linux/OSX Boot Process With WinDbg and KD IDApro.

References

1. *Jonathan W. Valvano, Introduction to Embedded Systems: Introduction to ARM CORTEX-M Microcontrollers, CreateSpace , 4th Edition, 2012.*
2. *Joseph Yiu, The Definitive Guide to ARM Cortex-M3 and Cortex-M4 Processors, Newnes, 3rd Edition, 2013.*

3. *M. A. Mazidi, Shujen Chen, S. Naimi, TI ARM Peripherals Programming and interfacing. Using C language for ARM cortex, 1st Edition, 2014.R. Love, Linux System Programming: Talking Directly to the Kernel and C Library. O'Reilly, 2013.*
4. *Russinovich, Solomon, "Windows Internals". Microsoft Press, 4th Ed, 2012.*
5. *M. Barr and A. Massa, Programming Embedded Systems: With C and GNU Development Tools, 2nd Ed , O'Reilly, 2006.*

EE-547: Communication Engineering

Status	Optional
Credits	3
Prerequisites	NIL

Introduction to Analog modulation ; Amplitude modulation, Angle modulation Pulse modulation, PAM, PCM and DPCM and other forms of pulse modulation; Digital bandpass modulation; Detection of signals in Gaussian noise; Coherent Detection; Non-coherent detection; Error performance of Binary systems; Communication Link Analysis; Characterization of bandlimited channels, Signal Design for band limited channels; Radio wave propagation; Transmit and Receive signal models; Ray tracing models, Empirical path loss models; Statistical Description of a wireless channel; Narrow band fading models; Wideband fading models; Discrete time models; Space-time Channel models; Capacity in AWGN; Capacity of flat-fading and frequency selective fading channels; Diversity principle; Micro and Macro diversity; Multiple channel and Advanced Transceiver Schemes; Frequency and Time Division Multiple Access Systems; Principle of Cellular Networks; Spread Spectrum Systems; Orthogonal Frequency Division Multiplexing; Overview of standardized Wireless Systems; GSM IS-95, CDMA 2000, WCDMA/UMTS, 3GPP Long-Term Evolution, WiMAX and WLAN.

References

1. *Lathi. B. P., Modern Analog and Digital Communications Systems, Oxford University Press, 3rd Edition, 1998.*
2. *S. Haykin, Communication Systems, Wiley, 4th Edition, 2000.*
3. *L. W. Couch, Digital & Analog Communication Systems, Prentice Hall, 7th edition, 2007.*
4. *J. G. Proakis and M. Salehi, Fundamentals of Communication Systems, Prentice Hall, 2005.*

EE-548: Industrial Automation Systems

Status	Optional
Credits	3
Prerequisites	NIL

Architecture of industrial automation systems; Programmable logic controllers; Distributed control systems; SCADA systems; Industrial networks; Serial communication, HART communication; PROFIBUS communication; Foundation fieldbus communication; Introduction to process control; Introduction to cyber security issues in

References

1. *B. R. Mehta and Y. J. Reddy, Industrial automation systems: Design and Implementation, Butterworth-Heinemann, 225 Wyman Street, Waltham, MA 02451, USA, 2015.*
2. *Frank Lamb, Industrial automation Hands-on, McGraw-Hill Education, USA, 2013.*
3. *Richard L. Shell and Ernest L. Hall (editors), Handbook of industrial automation, Marcel Dekker, Inc., 270 Madison Avenue, New York, NY 10016, USA, 2000.*
4. *B. Sklar, Digital Communications; Fundamentals and Applications, Prentice Hall, 2nd Edition.*
5. *Goldmith, Wireless Communications, Cambridge University Press, 2005*

EE-645: Emissions Security

Status	Optional
Credits	3
Prerequisites	EE-547

Electromagnetic Field and Wave Theory, Time varying fields and Maxwell's Equations, Uniform Plane Wave, Wave Propagation, Fundamentals of RFI, EMI and EMC, Common EMC units, Skin Effect, Characteristic Impedance, Electromagnetic Radiation and Antennas, Antenna Characterization and Transmit-Receive Operation, Basic Waveguide Operation, Basic Communications Theory, Basic EMC Requirements for Electronic Systems, Nature of Emissions, Conducted Emissions and Susceptibility, Radiated Emissions and Susceptibility, Typical Emissions Security (EMSEC) Attacks, Passive Attacks, Active Attacks, RedlBlack Engineering, Signal Spectra & Analysis, Requirements for Emissions Detection, Emissions Testing Methodology, Commercial & Military EMCITEMPEST Standards (FCC, CISPR, NSA 94-106, MIL-STD-461 F/G) , Considerations for Emissions Security Limits, Study of Conventional Countermeasure Schemes, Emission Suppression Techniques, Emission Controlled Design, Modulation & Isotropic Radiators, TEMPEST Design and Engineering.

References

1. *W. Hayt, J. Buck, Engineering Electromagnetics, McGraw-Hili, 2010*
2. *Clayton R. Paul, Introduction to Electromagnetic Compatibility, John Wiley & Sons, 2006*
3. *Henry W. Ott, Electromagnetic Compatibility Engineering, John Wiley & Sons, 2009*
4. *Bruce Gabrielson, TEMPEST Engineering and Hardware Design*
5. *Markus G. Kuhn, Compromising emanations: eavesdropping risks of computer Displays (Technical Report), University of Cambridge Computer Laboratory, 2003*
6. *Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems*
7. *MIL-STD-461 F/G: Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, U.S. Department of Defense, 2007.*

EE-646: Secure Embedded System Design

Status	Optional
Credits	3
Prerequisites	EE-548

Cryptographic processor and processing overhead, Cache Attacks on Ciphers , Physical and invasive attacks, Side-channel attacks, Hardware-based security primitives (PUFs, RNGs), watermarking of IPs, FPGA and system-on-chip (SoC) security; Hardware IP trust (watermarking, passive and active metering for prevention of piracy, trust verification), access control, hardware-based secure program execution, emerging threats and technologies; Supply chain risks mitigation including counterfeit detection and avoidance, Hardware tampering attacks and protection, Hardware Trojans; Secure Processors: Rabbit Processor, IBM 4758, AEGIS, ARM Trust zone.

References

1. *Tehranipoor, Mohammad, and Cliff Wang. Introduction to hardware security and trust. Springer Science & Business Media, 2011.*
2. *David Kleidermacher, Mike Kleidermacher, Embedded Systems Security- Practical Methods for Safe and Secure Software and Systems Development, Elsevier, 2012.*
3. *Stapko T., Practical Embedded Security: Building Secure Resource-Constrained Systems, Elsevier, 2008.*
4. *Gebotyes C.H., Security in Embedded Devices, Springer, 2006.*
5. *F. Rodriguez-Henriquez, N. A. Saqib, A. Diaz-Perez, C. K. Koc , Cryptographic Algorithms on Reconfigurable Hardware, Springer, 2006 .*
6. *Mukhopadhyay, Debdeep, and Rajat Subhra Chakraborty. Hardware security: Design, threats, and safeguards. CRC Press, 2014.*

EE-647: Cyber Security of Industrial Control Systems

Status	Optional
Credits	3
Prerequisites	EE-548

ICS security vs IT security, Critical infrastructure sectors, ICS security architecture, Distinct ICS security requirements, Major threats to ICS, Threats treatment in ICS and IT, ICS vulnerabilities: managerial, operational and technical, Purdue Enterprise Reference Architecture, Contemporary ICS security techniques: National institute of standards and technology, Department of homeland security, INL National SCADA testbed program, CCSP cyber security evaluation tool (CSET), ICS and IoT, IPv6 and ICS security.

References

7. *Tyson Macaulay and Bryan Singer, Cyber security for industrial control systems: SCADA, DCS, PLC, HMI and SIS, CRC Press, Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suit 300, Boca Raton, FL 33487-2742, 2011.*
8. *Joseph Weiss, Protecting industrial control systems from electronic threats, Momentum Press, 222 East 46th Stree, New York, N. Y. 10017, 2010.*
9. *Ronald L. Krutz, Securing SCADA systems, Wiley Publishing, Inc., 10475 Crosspoint Boulevard, Indianapolis, IN 46256, 2006.*
10. *Eric D. Knapp and Joel Thomas Langill, Industrial network security: Securing critical infrastructure neworks for Smart Grid, SCADA, and other industrial control systems, 2nd edition, Syngress, 225 Wyman Street, Waltham, MA 02451, USA, 2015.*

NE-501: Fundamentals of Nuclear Engineering

Status	Institutional Requirement
Credits	3
Prerequisites	NIL

Role and importance of nuclear energy; Nuclear cross-sections; Reaction rates; Nuclear fission and chain reaction; Criticality conditions; Conversion and breeding, Reactor components and their characteristics; Classification and design features of research, production, and power reactors, Introduction to fast and fusion reactor systems; Different types of fuel cycles; Core and feed-material preparations; Uranium enrichment; Fabrication of fuel; Reprocessing of irradiated fuel; Process waste disposal; Reactor fuel requirements; Burnup studies of nuclear fuels; Fuel cycle performance of commercially available reactors; In-core fuel management and fuel management strategies.

References:

1. *Lamarsh, J. R, Introduction to Nuclear Engineering, Addison-Wesley, 1983.*
2. *Glasstone, S. and A. Sesonske, Nuclear Reactor Engineering, D Van Nostrand, 1981.*
3. *Rahman, I. U. and Sheikh P. S., Introduction to Nuclear Engineering, Krieger, 1981.*
4. *Graves H. W. Jr., Nuclear Fuel Management, John Wiley, 1979.*

CIS-698: MS Thesis Research

Status	C
Credits	6+6
Prerequisites	Relevant courses in previous semester

Under this title, student will conduct research based project on some Computer Science related problem. He/She may take part in the on-going research or may introduce a novel approach in a specific field in consultation with his/her supervisor.

Under CIS-698 a proposal for Thesis Research should be developed for the project to be taken, being offered by the faculty member within the institute or outside and full time Thesis Research should be carried out based on the Thesis Research Proposal developed. The nature of the project may be research, development or design and may involve experimental or computational work or combination of both. Student performance in these activities will also be counted towards the overall evaluation.