Course Title:	**CS-882, Advanced Information Security**
Credit Hours:	3+0
Pre-requisites:	▪ Information Assurance
Course Description:	This course is aimed at preparing students for research in computer security and includes advanced security topics such as TPMs, VoIP Security, remote attestation, cloud computing security, computer forensics, SPAM and anonymous/onion routing.
Tools and Technologies:	▪ jTSS, jTPM ▪ Tor
Learning Outcomes:	On successful completion of this course students will be able to: 1. Understand state of the art in security research 2. Engage in active research at the forefront of these areas.
Tentative MS Thesis:	▪ Distributed Intrusion Detection using Map Reduce ▪ SEECS Private Cloud Security Architecture ▪ TPM Attestation for Private Clouds
Text Books:	▪ Schneier, Bruce; Applied Cryptography
Reference Books:	▪ Peltier, Thomas; Information Security Risk Analysis
Course Contents:	▪ Physical security and forensics o Forensics/Spying, Disks, Paper, Phones o Emissions Security (EMSEC), TEMPEST ▪ SPAM o SPAM Origins o SPAM Categories o How Email Works, Identity Concealing: Bot Networks o Open Proxies, Open Mail Relays o Empirical Analysis of SPAM, Conversion Pipeline o Black Listing Countermeasures

	o Payment Based Countermeasures ▪ DKIM o Email Ranking, Bayesian Spam Filtering o Apache Spam Assassin ▪ Digital Rights Management o Software Reverse Engineering (SRE) o Digital Rights Management (DRM) Enforcement o Rights Expression Languages (RELs) o Anti-Disassembly, Anti-Debugging, Tamper Resistance o Code Obfuscation, Software Cloning o MetaMorphic Software o Case studies: METSRights, ODRL, MPEG -21 ▪ Remote Attestation o Hardware TTP ▪ TPM Interconnection o Linux Integrity Measurement o Policy-Reduced Integrity Measurement Architecture o Case study: Xen Hypervisor o Intel Trusted Execution Technology o ARM TrustZone, Terra Architecture, Trusted Quake o Windows BitLocker ▪ Security Issues in VoIP o VoIP Standard Suites ▪ Session Initiation Protocol (SIP) o VoIP Security Vulnerabilities (Protocol Issues) o Security Measures (Signaling) and (Media) o Skype Issues ▪ Policies o Chinese Wall, Role-Based Access Control o Take-Grant Model, Discretionary Access Control

	o Mandatory Access Control, Bell-LaPadula o Clark-Wilson Integrity Model o Certification and Enforcement Rules o Separation of Duty in Model o Attribute based Access Control o Case Study: Shibboleth Properties ▪ Encrypting with Identities and Attributes o Public-Key Encryption o Why Don't People Use Encrypted Email? o Identity-Based Encryption (IBE) o IBE Usage and Security o Case study: Checkpoint o Attribute-Based Messaging o Ciphertext-Policy ABE (CP-ABE) o Cryptographic Concern: Collusion in CP-ABE o KP-ABE Application: Cable TV in the Tivo Age o Example Application: KP-ABE as Delegation Mechanism ▪ Wireless Security o Sensor Networks, Secure Bootstrapping Problem o Capture attacks, Evaluation Metrics, q-composite keys o Multi-path Key Reinforcement o Random-pairwise key scheme ▪ Jamming o Constant Jammer, Deceptive Jammer o Random Jammer, Reactive Jammer o Defense against Jamming o Coordinated Channel Switching o Synchronous Spectral Multiplexing o Asynchronous Spectral Multiplexing o ZigBee, SKKE, Cognitive Radio o Dynamic Spectrum Allocation

	o Transmitter Verification Scheme o Detecting Primary Beacons o Introduction, Name services and the DNS ▪ Information Flow o Non-interference models and analysis techniques o Confinement and covert channels o State Automation, Capability System, Projection o Non-Interference, Security Policies and MLS o Isolation and Channel Control, Entropy o Conservative Automated Analysis of Flow o Compiler-based Mechanisms, Chroot and Sandboxes o Timing Channels and Noise, Analysis using SRM o Case Study: Channels found in Xenix o Covert Flow Trees