Course Title:	CS-881, Computer Security Architecture
Credit Hours:	3+0
Pre-requisites:	▪ Information Assurance
Course Description:	This course is aimed at graduate students with a strong interest in security. It covers architectural and foundational aspects of security and demands both practical and theoretical abilities. Topics include foundations of access control, security policies, non-interference, key management, identities and anonymity, access control mechanisms, information flow, confinement, formal specifications and verification of security policies and protocols, vulnerability analysis, intrusion detection, and program security.
Tools and Technologies:	▪ Formal Security Assessment Methods (Promela/Spin) ▪ SELinux
Learning Outcomes:	On successful completion of this course students will be able to: 1. Understand the tools used by information and cyber security experts and how they conduct 'red-team' audits of large systems such as Banks and large corporations 2. Engage in active research at the forefront of these areas.
Tentative MS Thesis:	▪ Automatic Security Logic Analyzers ▪ Rule Language for Web Application Firewalls
Text Books:	▪ Matt Bishop (2003): Computer Security Art and Science, Pearson Education.
Reference Books:	▪ Computer Security Principles and Practice, William Stallings and Lawrie Brown. Pearson Education 2008
Course Contents:	▪ Access Control Techniques o UNIX Access Control, Windows ACL, o ACL Distinctions, ACL Scaling o Practical Object Access Control, Capability List o Capabilities and Propagation, Revoking

	Capabilities ○ Protection Rings, Data Access Rules ○ Data Control Transfers, Stack Switching, ○ Hardware Rings ▪ Confidentiality Policy ○ MAC vs DAC ○ Multi-Level Security Models, Bell-LaPadula Model ○ No-reads up, *-Property and No-writes down ○ Basic Security Theorem, Levels and Lattices ○ Total Order, Multi-Level Directory and Object Labels ○ Principle of Tranquility ▪ Integrity Policies ○ Biba Integrity Model, Intuition for Integrity Levels ○ Information Transfer Path, Low-Water-Mark Policy ○ Ring Policy, Strict Integrity Policy, Execute Clarification ○ LOCUS and Biba, Clark-Wilson Integrity Model ○ CDI Arrangement ▪ Database Security ○ Database Model and Relational Models ○ Access Control in System Design ○ Access Control in the SQL Model ○ SQL Grant and Creating Views ○ Row Level Access Control ○ Delegating Policy Authority ○ SQL Revoke, Data Consistency ○ ACID Transactions, Two Phase Update or Commit ▪ Common Criterion and System Evaluation ○ Orange Book and Rainbow Series ○ Trusted Computer System Evaluation Criterion ○ Reference Monitor, Trusted Computing Base

	(TCB) o FIPS-140, Protection Profile, Capability Maturity Levels ▪ Design Principles o Economy of mechanism o Fail-safe defaults o Complete mediation o Open design o Separation of Privilege o Least Privilege o Least Common Mechanisms o Psychological Acceptability ▪ System Assurance o Trust, Problems from lack of assurance o Types of assurance, Life cycle and assurance o Waterfall life cycle model, Other life cycle models ▪ Malware o Trojans, Virus, Worms, etc. o Exploitable Code Issues o Configuration Management o Buffer Overview, Format String, Input Checking o Time-of-use to Time-of-check, Ethical hacking ▪ Network Threats and Networking Review o OSI Reference Model, Switches o Physical Denial of Service, IPv4 and Address Spoofing o ARP cache Poisoning o Routing Example and Dynamic Routing Protocols o Smurf Attack, Reconnaissance ▪ Advance Network Threats and Networking Review 2 o Datagram Transport, UDP Header and DHCP o TCP Header and Three way handshake o SYN Flood and SYN Flood Constrainer

	○ Session Hijacking, Domain Name System DNS ○ DNS Problems, Transactions and Communications ○ Kaminsky's Observation, DNSSEC ▪ Network Security Controls and Architecture ○ Segmentation, Wireless, Security Domains ○ VPN, Firewall Technology, Address Translation ○ Denial of Service attacks, Intrusion Detection ○ Teardrop Attack, Address Hiding (NAPT), Honey Pots ▪ Law and Security ○ Intellectual Property, Copyright, Patents, Trade Secret ○ Wire Tapping, International Law ○ SOX General IT Controls ▪ IPSec and SSL ○ SSL Sessions ○ Structure of SSL ○ SSL Record Layer ○ SSL Mac Computation ○ Ephemeral D-H: Cipher, MAC Algorithms ○ SSL Alert Protocol ○ IPSec Tunnel and Transport Modes ○ ESP and Integrity ○ AH Protocol