SPRINGFIELD TECHNICAL COMMUNITY COLLEGE

ACADEMIC AFFAIRS

Course Number: PROG-450 Department: INFT

Course Title: Internet/Network Security II Semester: Fall Year: 2003

Course Objective	Competencies
1. To teach students how to protect data and systems 2. Use a firewall product in a very in-depth manner 3. To utilize some encryption/decryption techniques 4. To use an intrusion detection system in a very in-depth manner 5. To be able to secure data on a windows and Linux operating system platform 6. To write a security and procedures document 7. To have the student assess computer and network vulnerabilities and to be able to implement the tools to stop these vulnerabilities	Define and understand the following: • Biometric hardware/software used in conjunction with access control systems • Passwords (e.g., cracking/defensive cracking, guidelines for good password) • Access control list/Access control matrix • Multilevel security • Audit logs • Wireless technology • E-mail servers, routers, remote system access • Protocols: TCP/IP, Secure Sockets Layer, Secure Electronic Transaction • Telephony & Private Branch Exchange (PBX) security • Threats: (e.g., eavesdropping/wiretapping, traffic analysis, replay attacks, electromagnetic radiation interception, scanners, sniffers, Domain Name Server attacks, IP spoofing, Denial of Service/Distributed Denial of Service attacks Terminology (e.g., plaintext, ciphertext, cryptanalysis, key, algorithm, block cipher, stream cipher) • Symmetric cipher systems (e.g., Data Encryption Standard, Advanced Encryption Standard)

Course Objective	Competencies
	• Asymmetric cipher systems (e.g., RSA algorithm, Diffie-Hellman) • E-mail encryption (e.g., Pretty Good Privacy) • Digital signatures • Digital certificates • Public Key Infrastructure (PKI) • Memory (e.g., random access memory, read only memory, cache, proxy cache) • Evaluation criteria (e.g., Trusted Computer System Evaluation Criteria, Common Criteria) • Availability • Object classification levels • Controls (prevent, detect, recover) • Separation of duties • Least privilege • Social engineering • Malicious code: Trojan Horses, Viruses (e.g., boot sector, program [file], macro), Bombs, (e.g., logic, time), Trapdoors, Worms, Controls (e.g., prevention/inoculation, anti-virus policy/software, backups) • Security policies & procedures development (evaluate, develop, document, communicate & implement) • Risk Analysis/Risk Assessment • Auditing (e.g., policies, guidelines, procedures) • Security monitoring, testing & evaluation • Security reviews & spot monitoring

Course Objective	Competencies
	• Security maintenance • Security education and awareness • Physical Security (e.g., fire suppression; guards; locks; alarms; disposal of sensitive media) • Understanding of security goals (confidentiality, integrity, availability, authentication, non repudiation) • Knowledge of system security tools & applications • NT Administration (e.g., setting registry keys, setting up a safe file system, secure account policies, backups, auditing, monitoring and responding to incidents)