

## ***Illinois IDEA HS Course Outline***

**College/Division:** Northern Illinois University, Department of Computer Science

**Course Title:** Principles of Computer Security

**Course Designator/Number:** CSCI 650

**Credit Hours:** 3

**Instructor/Originator Name:** Shankar Hedge

**Catalog Description:** Survey of security considerations as they apply to computer and information systems. Topics include access control, security models and architecture, physical security, networking security, cryptography, disaster mitigation and recovery, and legal and ethical issues.

**Pre-requisites:** None

**Restrictions/Suggestions:** Course is available for graduate and undergraduate credit. Undergraduates need 90 hours and GPA > 3.0

**Rationale:** This course provides a foundation on a wide-range of computer and network security topics leaving the in-depth study on specific topics to subsequent courses. It will serve two purposes: (1) As a first course in computer security for the students and IT professionals with little background in the subject, and (2) IT managers who want to get a survey of security issues, protocols and tools at a high-level.

**Intended Audience:** Graduate students and upper level undergraduate students.

**Expected Student Outcomes:**

When students complete this course they should be able to

- Define and describe computer and network security problems, threats/ attacks/ vulnerabilities, basic access control methods, and simple steps to minimize possibility of an attack
- Describe widely used hashing and encryption algorithms, digital signatures, digital certificates (Public-Key Infrastructure), and associated standards and protocols
- Describe major tools and techniques used for securing the Internet communication, e-mail, wireless communication, and remote login authentication and authorization

- Explain basic operational aspects of security such as risk assessment, disaster recovery and business continuity plan, and legal aspects of security

**Text:** *Principles of Computer Security* by William Conklin, Gregory White, Chuck Cothren, Dwayne Williams, and Roger Davis, McGraw-Hill Technology Education, 2004, ISBN 0-07-225509-9

**Topical/Subject Matter:**

Vulnerabilities and Attacks, Access Control & Authentication, Security Models, Physical Security, Cryptography, Public Key Infrastructures

Firewalls/Proxy Servers, Intrusion Detection/Prevention Systems, Disaster Recovery and Business Continuity, Risk Management, Legal & Ethical issues

Functions of the following protocols/tools will be covered at a high-level:

Authentication (Kerberos, CHAP)

Security at the Application Layer (PGP, S/MIME, HTTPS, SFTP)

Security at the Transport Layer (SSL/TLS)

Security at the Network Layer (IPSec)

Remote Access AAA (RADIUS, TACACS+)

Wireless Security ( 802.11/WEP, WAP/WLTS)

Directory Service (LDAP)

**Course Activities:** Course delivered via NIU Blackboard Course Management System; Weekly chat sessions (or as needed); Discussion Board

**Evaluation/Assessment:**

- 7-8 on-line quizzes based on course modules. After completing the module, students have 24 hours to complete the quiz.
- 4-5 written homework, either hand-on activity (e.g. encrypted e-mail communication with instructor) or solve simple security problems based on course material.
- 2 Exams (Mid-term and Final)

**Bibliography/References:** *Principles of Computer Security* by William Conklin, Gregory White, Chuck Cothren, Dwayne Williams, and Roger Davis, McGraw-Hill Technology Education, 2004, ISBN 0-07-225509-9

Selected articles from computer security related Journals and Magazines (to be recommended during the course)