

## IS2150/TEL2810: Introduction to Security

**Instructor:** James Joshi  
706A, IS Building, Tel:412-624-9982  
Email: [jjoshi@mail.sis.pitt.edu](mailto:jjoshi@mail.sis.pitt.edu)

Office Hours:  
Wednesday: 1.30 – 3:00 p.m., OR by appointments

**GSA:** Amirreza Masoumzadeh [amirreza@sis.pitt.edu](mailto:amirreza@sis.pitt.edu)  
TBD

### Course Description

This course covers fundamental issues and first principles of security and information assurance. The course will look at the security policies, models and mechanisms related to confidentiality, integrity, authentication, identification, and availability issues related to information and information systems. Other topics covered include basics of cryptography (e.g., digital signatures) and network security (e.g., intrusion detection and prevention), risk management, security assurance and secure design principles, as well as e-commerce security. Issues such as organizational security policy, legal and ethical issues in security, standards and methodologies for security evaluation and certification will also be covered.

**Special note:** The coverage of this course has been primarily guided by the requirements of some of the CNSS standards (about 85% of the content). In addition, the course also attempts to cater to students who are interested in taking a single course but would like to gain a broad understanding of issues in information security.

The overall goal of the course is to develop a broader understanding of the information security field, so that the student can

- *Recognize, analyze and evaluate* security problems and challenges in networks and systems.
- *Apply* their knowledge to *synthesize* possible approaches to solve the problems in an integrated way.

More specifically, the goals of the course are to develop the skills to:

- *Analyze and evaluate* the fundamentals of security policy models and mechanisms, and their need for different types of information systems and applications
- *Apply* the basics of Cryptographic techniques and network security for ensuring the basic security goals of security of information systems.
- *Recognize* the various security issues/terminologies related to software, networks and applications to show how they are interrelated and available techniques and approaches to solve/tackle security problems.
- *Describe/identify* the various social, legal and non-technical dimensions of security and its relation to technical counterparts.

### Prerequisites

- TEL2000 OR Equivalent Background; Instructor Permission

In essence, the following is expected of the students

- *Basic knowledge of:* operating systems, data structures, database systems and networks; Java.
- *Basic mathematics:* undergraduate mathematics, some knowledge about mathematical logic, set notation, etc. These issues will be reviewed in the course.

Students not sure about the required background should meet the instructor.

**Special note:**

- The course attempts to explore some theoretical issues for which the stated mathematical background is essential.
- The course will involve some Java programming.

Students are highly encouraged to use office hours (the Instructor's and/or the GSA's) and make special arrangements with the instructor, if additional help is needed.

---

**Textbook:**

**Introduction to Computer Security:** by Matt Bishop (ISBN: 0-201-44099-7), Addison-Wesley (**Required Text**) ([Available online](#) for Pitt Students)

*This is a simplified version of (some topics have been removed!)*

**Computer Security: Art and Science** by Matt Bishop (ISBN: 0-201-44099-7), Addison-Wesley. **So if you have a copy of this book, it is fine too** ([Available online](#) for Pitt Students)

**Other Reference Material**

[Security in Computing](#), 2nd Edition, Charles P. Pfleeger, Prentice Hall ([Online](#))

[Security Engineering: A Guide to Building Dependable Distributed Systems](#), Ross Anderson, Wiley, John & Sons, Incorporated, 2001 (there is newer version)

[Inside Java 2 Platform Security: Architecture, API Design, and Implementation](#) by Li Gong, Gary Ellison, Mary Dageforde

[Practical Unix and Internet Security](#), Simon Garfinkel and Gene Spafford ([Online](#))

A list of papers will be provided to supplement the book

---

**Course Outline**

Security Basics

- General overview and definitions
- Security models and policy issues

Basic Cryptography and Network security

- Introduction to cryptography and classical cryptosystem
- Authentication protocols and Key Management

- IPsec, VPNs, E-commerce issues

#### Systems Design Issues and Information assurance

- Design principles
- Security Mechanisms
- Auditing Systems
- Risk analysis
- System verification and evaluation

#### Intrusion Detection and Response

- Attack Classification and Vulnerability Analysis
- Detection, Containment and Response/Recovery

#### Legal, Ethical Issues

#### Overview of Miscellaneous Issues (Time permitting)

- Malicious code, Mobile code
- Digital Rights Management, Forensics
- Emerging issues: E/M-commerce security, Multi-domain Security Issues etc.

#### **Grading (Tentative)**

Lab + Homework/Quiz/Paper Review	45%
Two Exams	30%
Paper/Project	20%
Misc. (Seminar, Participation in class)	5%

---

**If you have a disability for which you are or may be requesting an accommodation, you are encouraged to contact both your instructor and Disability Resources and Services, 216 William Pitt Union, 412-648-7890 or 412-383-7355 (TTY) as early as possible in the term.**

**Disability Resources and Services will verify your disability and determine reasonable accommodations for this course.**

---