

COURSE DESCRIPTION

Department and Course Number: COMP 6370

Course Title: Computer and Network Security

Total Credits: 3

Required: No

Prerequisites: COMP 3270

Class meetings per week: 3 hours

Lab meetings per week: 0 hours

Course Coordinator: Dr. Drew Hamilton

Date Prepared: February 13, 2004

Current Catalog Description:

Survey of computer network attack and defense techniques, viruses and other malware and operating system vulnerabilities and safeguards.

Textbooks:

None.

References:

Selected articles from journals and conferences; selected resources from NIST, NSA, U.S. DoD.

Course Objectives:

1. Recognize potential risks and threats to computer operations and communications.
2. Understand Federal rules and regulations affecting computer security, including legal ramifications, FOIA, and policies.
3. Understand security issues unique to wireless communications.
4. Have a working knowledge of relevant cryptographic techniques.
5. Have a critical understanding of computer security with an emphasis on “end-to-end” vulnerabilities.

Prerequisites by Topic:

1. Familiarity with topics covered in an undergraduate algorithms course

Topics Covered: (specify number of hours on each)

1. Introduction (2 hours)
2. Internet standards & RFCs (3 hours)
3. Conventional encryption (3 hours)
4. Public key cryptography (3 hours)
5. OS security vulnerabilities (3 hours)
6. Network security administration (3 hours)
7. Malicious software (4 hours)
8. Network authentication (4 hours)
9. Email security (3 hours)
10. Software vulnerability (4 hours)

11. Web security (4 hours)
12. Java security (3 hours)
13. IPSEC (1 hour)
14. IPSEC/VPNs (1 hour)
15. Firewalls (2 hours)
16. Designated approving authority and information systems security officer (1 hour)
17. Exams (1 hour)

Laboratory Projects: (specify number of weeks on each)

None.

Oral and Written Communications:

Each student is required to complete a ten-page research paper on a topic relevant to the course.

Social and Ethical Issues:

Although not a formal part of the course, social and ethical implications of network security (e.g., privacy) are discussed as part of course lectures.

Theoretical Content:

Computational complexity is addressed in cryptography and public key instruction and then applied as appropriate throughout the course.

Problem Analysis and Solution Design:

All students apply fundamental software engineering practices to analyze, design, implement, test, and document solutions to all programming assignments.