Overview

For this part of the undergraduate course, students will break up into groups up to 4 members and learn about a subject related to security that will not be covered in class. The team will write a 6-8 page report summarizing the key aspects of their topic.

The reports will be graded on how well they

- Motivate the subject;
- Introduce the fundamental knowledge needed to understand the subject;
- Explain the solutions used to address the subject/problem;
- Write and explain the above issues (quality of exposition will be important).

(Note: Students should make a strong effort to describe material in their own words.) Students should provide a bibliography with their report.

The reports will be due on May 5th, 2005 by 5pm. Since this is after the last day of class, and occurs during the exam period, the reports should be handed into me at my office in Core 523. Only one copy of the report should be turned in. The names of all team members should be on the report.

Suggested Topics

Below are some suggested topics for investigating. Please contact me to let me know who your team consists of, and what topic you would like to investigate. If it hasn't been selected already, then I will sign you up for that topic. If you would like to discuss a different topic than those provided, please see me. (Note: You are responsible for finding and forming a team. Everyone must be on a team!)

- Twofish
- Password Techniques for Unix
- RC6
- SERPENT
- Shor’s Algorithm for Factorization
- ENIGMA
- Linear Cryptanalysis
- MD5 and RIPEMD-160
- Data Compression (ZIP, etc)
- Firewalls
- Intruder Detection
- Smart Cards
- Video Scrambling in Cable TV
- Biometric Security (Fingerprint Scanners, etc)
- Denial of Service Countermeasures
- Digital Rights Management Solutions
- AdHoc Network Security
- Traffic Analysis Countermeasures
- DNA Computers
- Quantum Computers
- Jamming and Anti-Jamming Techniques
- Entropy and Perfect Secrecy
- Twinkle
- Number Field Sieve Factoring
- Security issues for RFID
- Buffer Overflow Attacks
- Secure Localization
- Wiretapping
- Administering Security
- Legal and Social Issues in Security