CSC 316
Computer Security and their Data
Fall 2007

The purpose of the term paper is to demonstrate some in-depth knowledge of a topic related or not to the class subject material. You can work on the term paper at most in a group of two.

After you choose a topic, and give the **proposal** (which must be printed on a printer of some sort, not handwritten!) to the instructor, you should wait for the acceptance/denial within 2 days. Receiving the ok, prepare one- or two- pages **abstrac**t describing what you propose to do in your term paper. This should include a description of the topic, what areas you will cover in it and of the main references (at least 3) that you will use.

The timetable for the deliverables is:

Choosing the topic (proposal)	***Monday December 3.***
Abstract	***Monday December 17***
Term paper (soft and hard copy)	***Monday January 21.***

Each paper will include at least seven appropriate citations to appropriate literature. By appropriate literature I mean recent and relevant publication (scientific journal, reliable sites on the Internet).

Your paper should be in proper style, use proper grammar and be carefully researched and phrased. In twelve points double-spaced type, with one inch margins, your paper should be at least ten pages long, not containing the references pages or diagrams (a cover page containing the title and your name, page i an abstract of your term paper, page ii an outline and then page 1 to n (where n is around 10), your term paper, page n+1 the references.

Note that your paper must be in your own words. If you copy text or pictures from another paper or book, or have someone else write it for you, this will be viewed as plagiarism. It will result in a grade of zero.

N.B: Your paper should be submitted both in hard copy, and soft copy (PDF). The soft copy should be submitted on the digital drop box with your full name and id as a title.

Just to itemize the most important point I will be looking for to evaluate your paper:

1. A **good** paper.
2. **Clearly** written and technically **sound**.
3. Nice presentation and critical in evaluating your idea.
4. Your paper should not look like an enumeration of facts.
5. Your paper should not look like a table of contents for another paper!
6. Your paper should not be a short version of another paper. (You should not take another paper, keep the structure, and just shorten the paragraphs.)

7. The paper needs to "say something" or "make a point" (have your friends read it, if they don't "get it", you need to make your point clearer).
8. Demonstration that you have read and understood your references.
9. Your paper should not spend much time on topics that have been extensively covered in the lectures.
10. You must give citations clearly.
11. You must not plagiarize.

Possible topics include:

Secure Operating Systems
Virtual machines for security
Privilege Separation
Information retrieval for audit logs
Authentication
- Authentication Protocols (Kerberos)
- Biometric Identification Devices
- S/KEY One-time Password System
- Digital Certificates
- Public Key Infrastructure (PKI)

Key Escrow
Random number generators
Database Security
- Sea Views SDBMS, Hospital DBMS (Privacy issues)
- Inference Control Mechanisms for Stastical Databases

Confidentiality and Privacy in medical databases
Security in Banking
Smart Card
- Implementations
- Zero-Knowledge Proofs

Convert Channel Analysis
- Information flow Tools

Intrusion Detection
- EMERALD, NetRanger, RealSecure,…

Hacking Industry
HTML filtering
Phishing and anti-phishing
Network Security
- Firewalls
- Firewall Protection
- Security of the World Wide web, Web Server Security
- Ways To Prevent Cyber Crime
- TCP/IP security
- Netscape Security Problems
- Java Applets, Java sacript, ActiveX
- Network Sniffers (Offense and Defense)
- Trusted File Servers
- Security of Mobile Code Systems
- Wireless Security

    - Virtual Private Networks (VPN)
    - Keyed Hashing
  - CORBA security
  - Authentication in distributed environments
- Network survivability
- Tools for vulnerability detection
- Virus and Worms
  - Internet Viruses
- Analysis of Encryption Protocols
  - Different Approaches
  - Timing Attacks
- Techniques and algorithms for high speed cryptography
- Electronic Election Protocols
- Public Protection of Software
  - Fingerprinting, Watermarking
- Electronic Commerce
  - Payment Protocols, Electronic Cash
  - Computer Protection In Business
- Privacy issues
- Ethics-University/Government/Private Sector
- Computer Security Law
  - Computer Security Law in Lebanon
- Penetration Studies
- Voice Mail Security
- Security Models
  - Integrity Models, Commercial Models and Policies,
- Access control models beyond MAC/DAC
- Digital steganography
- New Attacks
- Security auditing
- Tools for vulnerability detection
- Timing attacks on encrypted telnet sessions
- Encrypted databases
- Formal modeling of security systems
- Passive OS fingerprinting
- Secure coding
- Sandboxing untrusted code
- Information retrieval for audit logs
- Virtual machines for security