

# Security of software Systems

Ehud Gudes

Dept. of Computer Science

Ben-Gurion University, Beer-Sheva

Telephon: 08-6461626, email: ehud@cs.bgu.ac.il

The topic of Data security and Integrity is becoming increasingly important, especially with the spread of the Internet and World-wide Web applications. Preserving the integrity of data on the one hand, and preventing the unauthorized disclosure or modification of information on the other hand, is critical to any organization which uses computer based systems.

In this course we'll study the basic concepts, models and techniques for providing Security in Information and Computer systems. The emphasis of the course is on the basic system software components such as: Operating systems and Database systems, and it is not intended to cover Cryptography and Network security in the greatest detail.

## **Preliminary list of topics:**

1. Motivation and examples for data security problems. Organizational issues. The Privacy problem. Data Integrity.
2. Security policies and Security models (Discretionary and Multi-level))
3. Encryption Algorithms (both classic and Public key) Encryption protocols. Authentication.
4. Basic models for OS security Advanced models: ACLs, Capabilities, Trusted systems. Security in Unix and in Windows-NT.
5. Program and programming language security. Viruses and worms. Entropy and information flow in programs
6. Database security - Relational <sup>1</sup>database security. Authorization models. Security in statistical databases.
7. Security in Networks, Internet and the Web.

There are several **books** which I use in this course:

1. *Stallings W and L. Brown* Computer security - Principles and Practice the book I rely on most!
2. *Pfleeger C. P.* Security in Computing - the book I used in previous years
3. *Gudes E* Security in Software systems - Training Guide (Hovereth) - Open University - will be on reserve in the library.
4. *Summers R.* Secure computing - another general good book.
5. *Schneier B.* Applied Cryptography - a "bible" of modern cryptographic protocols.
6. *Stallings W.* Cryptography and Network security - a good book on this subject
7. *Oppliger R.* Security technologies for the world Wide web - one of the few good books on internet and Web security.

In addition, I will put on the site a set of papers which should be read.

The course requirements include:

1. three theoretical exercises, one programming exercise - 40% of the grade
2. A midterm exam - 30%
3. A final project or a review paper - 30% of the grade. For those doing a review paper, the programming exercise is a must. For those doing a project, in exceptional cases the project may include the programming exercise for 40% of the grade.
4. Presence - must be present in at least 70% of the classes

*Pre-requisites:* Introductory courses in Operating systems and in Database systems or in Parallel.