

COMP 4580 - Computer Security

Calendar Description: Computer security and information management. This course will examine state-of-the-art knowledge about the issues relevant to data and computer security.

Lab Required

Prerequisites: COMP 3430 and COMP 3720

Outline

- 1) Introduction (1/2 week)
- 2) Access control matrix (1/2 week)
- 3) Foundational results - decidability (1/2 week)
- 4) Security policies (1/2 week)
- 5) Confidentiality policies (1/2 week)
- 6) Integrity policies (1/2 week)
- 7) Hybrid policies (1 week)
- 8) Basic Cryptography (1 week)
- 9) Cryptographic checksums, digital signatures (1/2 week)
- 10) Key management (2 weeks)
- 11) Cipher techniques - networks and cryptography (1 1/2 weeks)
- 12) Secure Applications (1/2 week)
- 13) Firewalls (1/2 week)
- 14) Malicious logic, (1/2 week)
- 15) Identity and anonymity in the Internet (1/2 week)
- 16) Intrusion detection (1/2 week)

Text: Mat Bishop, *Introduction to Computer Security*, Addison Wesley, 2005

Mat Bishop, *Computer Security: Art and Science*, Addison Wesley, 2004.

Reference Books: W. Stallings, *Network Security Essentials*, 2nd ed., Prentice-Hall, 2003.

B. Schneier, *Applied Cryptography, second edition, protocols, algorithms and source code in C*, John Wiley & Sons Ltd, 1996

C.P. Pfleeger and S. L. Pfleeger, *Security in computing*, 3rd edition, Prentice-Hall, 2003

Dieter Gollmann, *Computer Security*, John Wiley & Sons Ltd, 2001.

J. F. Kurose and K.W. Ross, *Computer Networking*, 3rd edition, Addison-Wesley, 2005