RUTGERS
Rutgers Business School
Newark and New Brunswick

Computer Science
COURSE NUMBER: 26:198:643
COURSE TITLE: Information System Security

COURSE DESCRIPTION

Recent years have witnessed widespread use of computers and their interconnecting networks. This demands additional computer security measures to protect the information and relevant systems. This course prepares the students to meet the new challenges in the world of increasing threats to computer security by providing them with an understanding of the various threats and countermeasures. Specifically, students will learn the theoretical advancements in information security, state-of-the-art techniques, standards and best practices. In particular, the topics covered in this course include: Study of security policies, models and mechanisms for secrecy, integrity and availability; Operating system models and mechanisms for mandatory and discretionary controls; Data models, concepts and mechanisms for database security. Basic cryptology and its applications; Security in computer networks and distributed systems; Identity threat; Control and prevention of viruses and other rogue programs.

COURSE MATERIALS

Text Book:

1. Matthew Bishop, Introduction to Computer Security, Addison-Wesley 2004

Reference Books:

1. Charlie Kaufman, Radia Perlman and Mike Speciner, ``Network Security: Private Communication in a Public World," Prentice-Hall, 1995.
2. Silvana Castano, Mariagrazia Fugini, Giancarlo Martella, and Pierangela Samarati, ``Database Security," Addison-Wesley, Reading, MA, 1994.
3. Plus selected readings

Other sources:

1. The DBLP Bibiliography An Excellent source for the Research materials in the Database area

2. Google Scholar

Related Journals and Conferences:

1. ACM Conference on Computer and Communications Security (CCS)
2. IEEE Symposium on Security and Privacy (S&P)
3. ACM Symposium on Access Control Models and Technologies (SACMAT)
4. IFIP WG11.3 Working Conference on Data and Application Security (DBSEC)
5. Annual Computer Security Applications Conference
6. Computer Security Foundations Workshop (ACSAC)
7. ACM Transactions on Information Systems Security
8. IEEE Transactions on Secure and Dependable Systems
9. Journal of Computer Security

10. Computers and Security

FINAL GRADE ASSIGMENT

Research Paper and Presentation	50%
Midterm Examination	25%
Final Examination	25%

Computer Science **(26:198:643)**

COURSE SCHEDULE

Jan 25
Basic Security Concepts

- Lecture Notes z Chapter 1
- ITPRC.COM The Information Technology Professional's Resource Center z Security Tutorials Online
- CERT

Feb 1
Introduction to Cryptography, Secret Key and Public Key Cryptography

- Lecture Notes z Chapters 8 and 9 z Chapter 4, and chapters 2,3 and 5 from reference book 1.
- Cryptography FAQ z Introduction to Cryptography - 2 z Demonstration for RSA Cryptography using JavaApplet. z AES: The New encryption standard selected by the US govt

Feb 8
Digital Signatures and Certificates

- Research Paper Title and Outline due z Chapter 10 z Lecture Notes
- A nice introduction to digital signatures z Article on Elliptic Curve Cryptography z Identification and Authentication z Chapters 11 z Lecture Notes
- Article on Biometrics z Article on Kerberos

Feb 15, 22
Internet Security

- Lecture Notes
- TCP SYN Flooding and IP Spoofing
- You will find more information on the attacks at CERT z Research paper discussions

Mar 2, 9

Securiy Models

- Chapters 2,3,4

z Lecture Notes 1

z Lecture Notes 2

- "M.A. Harrison, W.L. Ruzzo, and J.D. Ullman: Protection in Operating Systems. CACM, August 1976.

z Access Control: Principles and Practice, Ravi Sandhu & P. Samarati, IEEE Communications, Volume 32, Number 9 /September 1994 z Lattice-Based Access Control Models,Ravi Sandhu, IEEE Computer, Volume 26, Number 11

(Cover Article) November 1993 z "D.F.C. Brewer and M.J. Nash: "The Chinese Wall Security Policy", in IEEE Symposium on

Security and Privacy '1989 z Role-Based Access Control Models, "R.S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E.

Youman. IEEE Computer, 29(2):38--47, February 1996. z "D. Ferraiolo, R. Sandhu, S. Gavrila, D. Kuhn, and R. Chandramouli. Proposed NIST standard for role-based access control. ACM Transactions on Information Systems Security, 2001.

Mar 23

- Database Security z Chapters 14,15

z Lecture Notes

- Database Security -- Concepts, Approaches, and Challenges Elisa Bertino and Ravi Sandhu, IEEE Transactions on Dependable and Secure Computing, Vol. 2, NO. 1, January-March 2005 z A chapter from "Multilevel secure transaction processing," Kluwer Academic Publishers, by

V.Atluri, S. Jajodia and B. George z

Research Paper Due

Mar 30 z Mid-term

examination

Apr 5 The Role Mining Problem, Guest Lecture by Haibing

Lu

Apr 12 z Security and Privacy in Spatial and Mobile Data, Guest Lecture by Heechang Shin (May

need to advance the meeting time)

Apr 19 z Research Paper

Presentations

Apr 26 z Research Paper

Presentations

May 3 z Research Paper

Presentations

May 10 z Final

Examination

Topics for the Research paper include:

1. Best Source: The session topics in the conferences listed above
2. Authorization Models for New Application domains
3. Role-based Access Control
4. Inference Control
5. Security in Electronic Commerce
6. Security in WWW
7. Security for Mobile Systems
8. Intrusion Detection
9. Security for Web services
10. Biometrics
11. Privacy
12. Privacy preseving data sharing and mining
13. Security of Statistical Databases
14. Viruses
15. Computer Ethics

16. Spam and Phishing
17. 17. Identity theft
18. …….