Information Security
26:198:643
Spring 2016
Wednesdays 10:00am - 12:50pm, 1 Washington Park, Room 308

Instructor: Prof. Vijay Atluri
Office: 1082, 1 Washington Park, Newark
Office Hours: Wednesdays 1:30 - 3:30pm and by appointment
Telephone: 973-353-1642
Fax: 973-353-5003
E-mail: atluri@rutgers.edu
Homepage: http://cimic.rutgers.edu/~atluri

Official University/Campus closings due to inclement weather:
Call 973-353-1766 or 732-932-1766, Newark Campus Information

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, emerging applications and smart devices; Identity theft; Control and prevention of viruses and other rogue programs.

Text Book: There is no prescribed text.

Reference Books:

2. Matthew Bishop, Introduction to Computer Security, Addison-Wesley
4. Plus selected readings

Other sources:

1. The DBLP Bibliography 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 WG 11.3 Working Conference on Data and Application Security and Privacy (DBSEC)
5. Annual Computer Security Applications Conference (ACSAC)
7. ACM Conference on Data and Application Security and Privacy (CODASPY)
8. ACM Transactions on Information Systems Security (TISSEC)
9. IEEE Transactions on Dependable and Secure Systems (TDSC)
10. Journal of Computer Security
11. Computers & Security

Expected Work:

Research Paper and Presentation 30%
Mid term Examination 25%
Final Examination 25%
Homeworks 20%

Tentative Schedule:

Jan 20
Basic Security Concepts, Introduction to Cryptography, Secret Key and Public Key Cryptography

Jan 27
Introduction to Cryptography, Secret Key and Public Key Cryptography (continued)

Feb 3
Digital Signatures and Certificates
Research Paper Title and Outline due
Homework 1 posted

Feb 10
No Class

Feb 17
Identification and Authentication
Homework 1 Due

Feb 24
Internet Security
http://www.symantec.com/connect/articles/ip-spoofing-introduction

Mar 2
Security Models

Mar 9
Mid-term examination (Topics covered until March 2)

Mar 23
Security Models (Continued)
Homework 2 posted

Mar 30
Database Security
Homework 2 Due

Apr 6
Intrusion Detection Systems
Research Paper Due

Apr 13
Research Paper Presentations: Each student will have 20 minutes to present

Apr 20
Research Paper Presentations: Each student will have 20 minutes to present

Apr 27
Research Paper Presentations: Each student will have 20 minutes to present

May 4
Makeup Class
Research Paper Presentations: Each student will have 20 minutes to present

May 11
Final Examination

Topics for the Research paper include:

1. Best Source: The session topics in the conferences listed above
3. Identify Management
4. Role Mining
5. Security for Smart Devices
6. Security for Social Networks
7. Big Data Security
8. Security for Digital Money
9. Inference Control
10. Security in Electronic Commerce
11. Security in WWW
12. Security for Mobile Systems
14. Intrusion Detection
15. Security for Web services
16. Biometrics
17. Security of Statistical Databases
18. Viruses
19. Computer Ethics
20. Spam and Phishing
21. Identity theft
22. .....