Rutgers The State University of New Jersey
Rutgers Business School, Newark and New Brunswick

Information Security
26:198:643

Fall 2018
Tuesdays 1:00pm - 3:50pm, 1 Washington Park, Room 226

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:

1. William Stallings and Lawrie Brown, Computer Security: Principles and Practice, 2/E ISBN-10: 0132775069 ISBN-13: 9780132775069 2012 Prentice Hall
2. Matthew Bishop, Introduction to Computer Security, Addison-Wesley
3. Charlie Kaufman, Radia Perlman and Mike Speciner, ``Network Security: Private Communication in a Public World," Prentice-Hall.
4. 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 and Privacy (DBSEC)
5. Annual Computer Security Applications Conference (ACSAC)
6. Computer Security Foundations Workshop
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 25%
Midterm Examination 25%
Final Examination 25%
Quizzes 25%

Tentative Schedule:

Sept 4
Basic Security Concepts, Introduction to Cryptography, Secret Key and Public Key Cryptography

Sept 11
Introduction to Cryptography, Secret Key and Public Key Cryptography (continued)

Sept 18
Digital Signatures and Certificates

Sept 25
Identification and Authentication
Quiz 1
Research Paper Title, Abstract and Reference List due

Oct 2
Internet Security

Oct 9
Internet Security (continued)
Research Paper Outline due

Oct 16
Security Models

Oct 23
Mid-term examination (Topics covered until Oct 16)

Oct 30
Security Models (Continued)

Nov 6
Database Security

Nov 13
Cloud Security
Quiz 2

Nov 20
No class - Thanksgiving
Nov 27
Crypto Currency
Dec 4
Research Paper Due
Research Paper Presentations: Each group will have 20 minutes to present
Dec 11
Research Paper Presentations: Each group will have 20 minutes to present
Dec 18
Final Examination

Topics for the Research paper include:

1. Best Source: The session topics in the conferences listed above
2. Security Models for New Application domains
3. Cloud Security
4. Identify Management
5. Role based access control
6. Attribute based access control
7. Security policy configuration, mining
8. Security for Smart Devices
9. Security and Internet of Things
10. Security for Social Networks
11. Big Data Security
12. Security for Digital Money
13. Inference Control
14. Security in WWW
15. Security for Mobile Systems
16. Security for Spatial/temporal Systems
17. Intrusion Detection
18. Security for Web services
19. Biometrics
20. Viruses
21. Computer Ethics
22. Spam and Phishing
23. Identity theft
24. Security Policy Management
25. Human Aspects of Security
26. Crypto currency
27. .....