

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

**Information Security
26:198:643**

Fall 2017

Tuesdays 10:00am - 12:50pm, 1 Washington Park, Room 118

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 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 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 5

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



Sept 12

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



Sept 19

Digital Signatures and Certificates



Sept 26

Identification and Authentication

Quiz 1

Research Paper Title and Abstract due



Oct 3

Internet Security

Research Paper Outline and Reference List due



Oct 10

Internet Security (continued)



Oct 17

Security Models



Oct 24

Mid-term examination (Topics covered until Oct 17)



Oct 31

Security Models (Continued)



Nov 7

Database Security



Nov 14

Cloud Security

Quiz 2

 **Nov 21**

No class - Thanksgiving

 **Nov 28**

Cloud Security (continued)

Research Paper Due

 **Dec 5**

Research Paper Presentations: Each group will have 20 minutes to present

 **Dec 12**

Research Paper Presentations: Each group will have 20 minutes to present

 **Dec 19**

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. Identity Management
 5. Role Mining
 6. Security for Smart Devices
 7. Security and Internet of Things
 8. Security for Social Networks
 9. Big Data Security
 10. Security for Digital Money
 11. Inference Control
 12. Security in WWW
 13. Security for Mobile Systems
 14. Security for Spatial/temporal Systems
 15. Intrusion Detection
 16. Security for Web services
 17. Biometrics
 18. Viruses
 19. Computer Ethics
 20. Spam and Phishing
 21. Identity theft
 22. Security Policy Management
 23. Human Aspects of Security
 24.
-