

INFO 622
Network Security and Administration
Spring, 2009

INSTRUCTOR: Dr. Richard J. Coppins

TEXT: Cryptography **and Network Security**, Stallings,
Pearson Prentice-Hall, 4th Edition, 2006

References: **Network Security**, Kaufman, Perlman and Speciner,
Prentice-Hall, 2nd Edition, 2002
Security in Computing, Pfleeger and Pfleeger,
Prentice-Hall, 4th Edition, 2007
*(Neither of these is required, but I will draw material
from them.)*

OFFICE: B4113 Snead Hall

OFFICE HOURS: M 3:30 – 4:30, 6:00 – 7:00
T 2:30 – 4:30, 6:00 – 7:00

Others by appointment

OFFICE PHONE: 828-7114 (e-mail is much better; messages are not
checked daily)

E-MAIL: rcoppins@vcu.edu

DESCRIPTION:

This course studies the principles of network security and its application to real networks. In addition, trusted computing and best practices will be covered. Finally, the use of intrusion detection, intrusion prevention and other related tools also will be studied (time permitting).

Course Outline

This is a rather lengthy list of topics, which means we'll skim some of the material.

- I. Introduction
 - Security Policies
- II. Cryptography
 - Classical Encryption Techniques
 - Block Ciphers and DES
 - Complexity Theory and Basic Algebra
 - AES
 - Additional Topics in Symmetric Ciphers
 - Using Symmetric Encryption
- III. Public-Key Encryption and Hash Functions
 - Introduction to Number Theory
 - Public-Key Cryptography and RSA
 - Key Management; Other Public-Key Systems
 - Message Authentication and Hash Functions
 - Hash and MAC Algorithms
 - Digital Signatures and Authentication Protocols
- IV. Network Security Applications
 - Authentication
 - E-Mail Security
 - IP Security
 - Web Security
- V. System Security
 - Intruders
 - Malicious Software
 - Firewalls
 - Trusted Systems
 - Common Criteria
 - Forensics
- VI. Additional Topics
 - **Communications of the ACM**, Feb. 2006, "Risks of Live Digital Forensic Analysis," "Live Forensic Diagnosing," "Investigating Sophisticated Security Breaches," "Next-Generation Digital Forensics"
 - **Communications of the ACM**, April 2007, "Predicting Hostile Activity in Networks," "Hiding Data: Forensics and Anti-Forensics"
 - **IEEE Security and Privacy**, March/April 2005, "Online Banking Security,"

Notes:

- 1) This course requires the completion of a number of assignments. All work is due on the date specified at the beginning of class. **Late work will lose 5 points per day except in very unusual circumstances and only by previous arrangement with me.**
All assignments must be typed, or neatly handwritten. (If I can't read it I can't grade it.)
- 2) *Section 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990 require VCU to provide an 'academic adjustment' and/or 'a reasonable accommodation' to any individual who advises us of a physical or mental disability. Students seeking academic adjustments or accommodations must self-identify with the Coordinator of Services for Students with Disabilities on the West campus. After meeting with the Coordinator, students are encouraged to meet with instructors to discuss their needs, and if applicable, any laboratory safety concerns related to their disabilities. If you have a physical or mental limitation that requires an academic adjustment or accommodation, please arrange a meeting with me at your earliest convenience (but definitely by the end of the second week of class).*
- 3) This class will follow the guidelines of the new VCU Honor System as printed in the VCU Resource Guide. All tests and assignments will be done individually unless otherwise designated. Any violation of the standards of academic integrity will result in a grade of 'F' failure for the course and appropriate action under the academic integrity standards. The Division of Student Affairs maintains these policies that pertain to academic life. You may download an electronic version of the resource guide from the VCU web at <http://www.students.vcu.edu/rg/>. On the first page of the resource guide is a link to the honor code and all other policies.
- 4) If a class is canceled due to inclement weather, any assignment or test will be rescheduled for the next class automatically.
- 5) Messages also can be left with the department secretary; the department number is 828-1737.

Web Site:

All assignments (and the syllabus) will be available on the course web site. The URL is:

<http://www.isy.vcu.edu/~rcoppins/INFO622>

(Please note that the URL is case-sensitive. So, info622 will NOT work.) Now you can download any of the items you wish.

GRADING:

Homework will make up 65% of your grade; the other 35% will be based on a series of papers (to be assigned during the semester).

REFERENCES FOR THE END OF THE SEMESTER:

Communications of the ACM, Feb. 2006:

- “Risks of Live Digital Forensic Analysis,” pg. 56
- “Live Forensic Diagnosing,” pg. 63
- “Investigating Sophisticated Security Breaches,” pg. 48
- “Next Generation Digital Forensics,” pg. 76

Communications of the ACM, April 2007:

- “Predicting Hostile Activity in Networks,” pg. 63
- “Hiding Data: Forensics and Anti-Forensics,” pg. 15

IEEE Security and Privacy,

- March / April 2006 : “Online Banking Security,” pg. 14
- July / Aug. 2006: “When Applying Standards to Web Services Is Not Enough,” pg.
- Jan. / Feb. 2007: “How Not To Be Seen”
- Nov. / Dec. 2006: “Network Intrusion Detection”
- Jan. / Feb. 2006: “DRM, Spyware and Security”

Additional References:

These references are certainly not comprehensive, but they might be valuable.

Practical Cryptography, Ferguson and Schneier, Wiley, 2003. Approaches cryptography from an engineering point of view rather than as a set of mathematical concepts.

Designing Network Security, Kaeo, Cisco Press, 2nd edition, 2004.

Network Security Principles and Practices, Malik, Cisco Press, 2003.

Hackers Beware, Cole, New Riders Publishing, 2002. How hackers attack systems and how to defend against them.

Inside Network Perimeter Security, Northcutt, Zeltser, Winters, Kent and Ritchey, SANS Institute (SAMS Press), 2005. Intended for people who work with networks and must defend them.

The Code Book, Singh, Doubleday, 1999. A very readable discussion of cryptography from its beginnings to the future.

Network Security Essentials, Stallings, 2nd Edition, Prentice-Hall, 2003. Terse but lots of good information.

Introduction to Cryptography, Trappe and Washington, 2nd Edition, Prentice-Hall, 2006. Detailed discussion of the algorithms and the theory behind them.

Internet Security Glossary (RFC 2828). A glossary (191 pages of definitions and 13 pages of references) which provides abbreviations, explanations, and recommendations for use of information system security terminology.

ISO / IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management (a discussion of best practices for IT security)

Journals:

IEEE Security and Privacy
Journal of Information Systems Security
Information Security (a trade journal)
SC Magazine (a trade journal)

A Few URL's of interest:

Bruce Schneier's blog: www.schneier.com/blog/

IETF Security area: sec.ietf.org/

Peter Gutman's home page (all sorts of info on crypto):

www.cs.auckland.ac.nz/~%7epgut001/

Steganography: www.steganos.com

www.stegoarchive.com

www.sourceforge.net/projects/camerashy

William Stallings page for **Cryptography and Network Security** (many other useful links): williamstallings.com/Crypto/Crypto4e.html