E4180: Network Security

Henning Schulzrinne
Columbia University, New York
schulzrinne@cs.columbia.edu

Columbia University, Fall 2000

Last modified September 5, 2000

Course Outline

- course mechanics
- threats
- secret-key crypto
- hashes & message digests
- public key algorithms
- number theory
- operating system vulnerabilities
- intrusion detection
- authentication systems
- Kerberos
- email security (PGP, S/MIME)
- firewalls
- IP security (IPsec)
- SSL, TLS
- WWW security

The Course Alphabet Soup

- DES, IDEA, Blowfish, AES, RSA
- SSL, TLS, OTP
- IPsec, AH, ESP
- CHAP, PAP, RADIUS, AAA
- PGP, S/MIME, ssh

Course Goals

- descriptive: what's out there
- skill-oriented ➠ programming assignments
- critical: what's wrong with…, how else can we do this?
- interactive: discussion, questions encouraged (and considered in grade…)
- work-in-progress… ➠ web site, mailing list, newsgroup

Am I in the Right Room?

This course does *not* address:

- "How do I break into the CIA webserver?"
- "Should cryptography be exported to Transylvania?"
- "Are Galois fields isomorphic?"
- "How do I apply artificial intelligence to encryption?"

You should know (➠ self-assessment test)...

- general networking concepts (packets, CL vs. CO, ...)
- TCP vs. UDP
- HTML vs. HTTP
- C or C++; Java may be used where possible

Course Mechanics

WWW page: http://www.cs.columbia.edu/security/

Mailing list: `cs4180@cs.columbia.edu` for announcements, a web board for discussion

Assignments: 5, with questions + small programming problems

Slides: PostScript and PDF on web page; use `psnup` to create 2 slides/page

Grading: Assignments 30%, midterm 30%, final 35%, class participation (in person or by email) 5%

Course Policies

- see web page!
- Zero tolerance for cheating: you cheat, you visit Dean of Students.
- May discuss homework problems with fellow students, but solve *individually*.
- Declared collaboration: points / N
- Nondeclared collaboration ➠ 0, cheating.
- Auditing: must get 50% of homework credit to pass.

Course Text

Course texts:

- Charlie Kaufman, Radia Perlman and Mike Speciner, *Network Security - Private Communication in a Public World*, Prentice Hall, Englewood Cliffs, New Jersey, 1995. ISBN 0-13-061466-1
- Bruce Schneier, *Applied Cryptography* (2nd ed.), John Wiley, 1996. ISBN 0-471-11709-9. **(optional)**

Reference Books

- William R. Cheswick and Steven M. Bellovin, *Firewalls and Internet Security*, Addison Wesley, 1994. ISBN 0-201-63357-4
- James F. Kurose and Keith W. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, Addison Wesley, 2000. ISBN 0-471-11709-9.
- D. E. Comer, *Internetworking with TCP/IP*, vol. 1. Englewood Cliffs, New Jersey: Prentice Hall, 3rd ed., 1995.