Course Information and Syllabus

This course concerns security issues in multi-user information systems and computer networks. It will cover fundamental techniques, in particular cryptography, for security and their applications in practical areas such as electronic commerce.

Instructors

Yeali S. Sun (孫雅麗), Room 909, Management II, 3366-1195, `sunny@im.ntu.edu.tw`
Anthony J.T. Lee (李瑞庭), Room 705, Management II, 3366-1188, `jtlee@im.ntu.edu.tw`
Yeong-Sung Lin (林永松), Room 808, Management II, 3366-1191, `yslin@im.ntu.edu.tw`
Yih-Kuen Tsay (蔡益坤), Room 1108, Management II, 3366-1189, `tsay@im.ntu.edu.tw`

Lectures

Tuesday 2:20–5:20PM, Conference Room 2, College of Management, Building I (level 4)

Prerequisites

Operating Systems and Computer Networks

Textbook

Cryptography and Network Security: Principles and Practices, 4th Edition, W. Stallings, Prentice Hall, 2006. (Note: **be sure to check out the errata list on the Web site of the book!**)
Supplementary readings.

Syllabus/Schedule

We will study the design and underlying principles of **automated tools for protecting information**, including software and data, *stored on computers or communicated over networks*. The main focus will be on the fundamentals and applications of **cryptographic technology**.

- Overview: basic concepts, architecture, model, etc. (.5 week: 09/16a)
- Symmetric Cryptography: classical techniques, block ciphers, DES, finite fields, AES, stream ciphers, applications, etc. (3.5 weeks: 09/16b, 09/23, 09/30, 10/07)
- Public-Key (Asymmetric) Cryptography: number theory, RSA, key management, ECC, etc. (4 weeks: 10/14, 10/21, 10/28, 11/04)
- **Midterm** (**2008/11/11**)
- Authentication, Hash Algorithms, and Digital Signatures (3 weeks: 11/18, 11/25, 12/02)
- Network Security: IPsec, virtual private networks (VPNs), IP traceback, firewalls, denial of service, etc. (2 weeks: 12/09, 12/16)
- Field Trip to the Acer eDC (2008/12/23)
- Network Security (continued) (2 weeks: 12/30, 01/06)
- **Final** (**2009/01/13**)

FTP Site

`ftp://140.112.106.6 to 15/` (must have an account at im.ntu.edu.tw; a guest account may be requested)

Grading

Midterm 35%, Final 35%, Homework 10%, Term Project 20%.

References

[1] *Cryptography and Network Security: Principles and Practices, 4th Edition*, W. Stallings, Prentice Hall, 2006. (Note: textbook of this course.)

[2] *Introduction to Cryptography, 2nd Edition*, J.A. Buchmann, Springer, 2004. (Note: an introductory book self-contained with a succinct coverage of mathematical foundations.)

[3] *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition*, B. Schneier, John Wiley & Sons, 1996. (Note: a very comprehensive book on cryptography and its applications.)

[4] *Network Security: Private Communication in a Public World, 2nd Edition*, C. Kaufman, R. Perlman, M. Speciner, Prentice Hall, 2002. (Note: very similar to [1] in scope and in technical depth.)

[5] *Security in Computing, 4th Edition*, C.P. Pfleeger and S.L. Pfleeger, Prentice Hall PTR, 2006. (Note: similar to [1] in scope and in technical depth. It covers fewer encryption algorithms, but is more comprehensive in system/program security. It also has chapters on data base security, security management, and legal and ethical issues.)

[6] *Network Security Essentials: Applications and Standards, 3rd Edition*, W. Stallings, Prentice Hall, 2006. (Note: a scaled-down version of [1], with light treatment of cryptography but more current information on other topics and more coverage on email security.)

[7] *Security in Distributed Computing: Did You Lock the Door?*, G. Bruce and R. Dempsey, Prentice Hall, 1997. (Note: covers a broader scope than [1], but with less technical depth.)

[8] *Computer Security, 2nd Edition*, D. Gollmann, John Wiley & Sons, 2006. (Note: similar to [7].)

[9] *Firewalls and Intranet Security: Repelling the Wily Hacker, 2nd Edition*, W.R. Cheswick, S.M. Bellovin, and A.D. Rubin, Addison-Wesley, 2003.

[10] *Building and Managing Virtual Private Networks*, D. Kosiur, John Wiley & Sons, 1998.

[11] *Building SET Application for Secure Transactions*, M.S. Merkow, J. Breithaupt, and K. Wheeler, John Wiley & Sons, 1998.

[12] *Practical UNIX and Internet Security, 3rd Edition*, S. Garfinkel, G. Spafford, and A. Schwartz, O'Reilly & Associates, 2003.

[13] *Operating System Concepts, 8th Edition* (Chapters 14 and 15), A. Silberschatz, P.B. Galvin, and G. Gagne, Wiley, 2008.

[14] *Computer Networks, 4th Edition* (Chapter 8), A.S. Tanenbaum, Prentice Hall, 2002.

[15] *Distributed Systems: Concepts and Design, 4th Edition* (Chapter 7), G. Coulouris, J. Dollimore, and T. Kindberg, Addison-Wesley, 2005.