Tentative Course Outline

(version September 7, 1995)

September

Thu	7	Administrivia. Overview of course. Discussion of security objectives. Ethics.
Tue	12	Physical Security. Discussion of risks. Physical protection. Tamperproof devices and chips. Copy protection. Backup; disaster planning; cold sites.
Thu	14	Communications Security and Risk Analysis. Phone System security. Wireless phones. Risk Analysis. Problem Set 1 out.
Tue	19	Classical Cryptography. One-time pad. DES. RC5. Pay-TV.
Thu	21	Public-Key Cryptography I. Diffie-Hellman. Digital Signatures. Hash Functions. Certificates. Secret-Sharing. Key Escrow. Problem Set 1 due. Problem Set 2 out.
Tue	26	Public-Key Cryptography II. Hash Functions (MD5). Modular Arithmetic. Public-Key RSA, DSS (El Gamal).
Thu	28	Crypto Protocols. Key Management. Oblivious Transfer. Commitment. Zero-knowledge. Problem Set 2 due. Problem Set 3 out.

October

Tue	3	Authentication and Identification I. Logic of Authentication.
Thu	5	Authentication and Identification II. Passwords. Password management. Password crackers. Password aging. Password stealing: Login spoofs; ethernet or X-window snooping. Variable passwords: S/Key. Tokens: Datakey, SecurID. Biometrics. Problem Set 3 due. Problem Set 4 out.
Tue	10	NO CLASS.
Thu	12	Intrusion Detection. Auditing. Problem Set 4 due. Problem Set 5 out.
Tue	17	Access Control. Access Control Lists. Subject/Objects. Reference Monitor. Capabilities. Revocation. Groups.

Thu	19	Viruses. Morris Virus (Worm.) Virus Detection. Trojan horses. Tripwire. Problem Set 5 due. Problem Set 6 out.
Tue	24	Information Flow Models I. Bell-LaPadula model. Harrison-Ruzzo model.
Thu	26	Information Flow Models II. Integrity and Denial of Service. Problem Set 6 due. Take–home Midterm Quiz out.
Tue	31	Secure Operating Systems. Protection of Memory. Secure Kernels. Confinement. Certification of Operating Systems. Covert Channels. Midterm Quiz due.

November

Thu	2	Smart Cards. Secure Co-Processors. Term Project proposal due. Problem Set 7 out.
Tue	7	Intellectual Property Protection. Software Protection. Site Licensing. Fingerprinting. Encrypted distribution channels.
Thu	9	Introduction to network protocols. TCP/IP, HTTP, Ethernet, OSI models. Problem Set 7 due. Problem Set 8 out.
Tue	14	IP security. Firewalls.
Thu	16	Distributed Secure Systems. Kerberos. Problem Set 8 due. Problem Set 9 out.
Tue	21	Email Security. PGP. PEM.
Thu	23	NO CLASS
Tue	28	WWW Security. SSL ans SHTTP. Problem Set 9 due.
Thu	30	Electronic Commerce I. Payment Protocols (iKP.)

December

Tue	5	Electronic Commerce II. Electronic Cash.
Thu	7	Electronic Elections. Term Project due.
Tue	12	Legal Infrastructure. Public-key Certificates. Digital Notaries.