CmpE 526 Operating System and Network Security, Spring 2016

Instructor :	Dr. M. Ufuk Çağlayan, ETA 45, Tel. 359 6698, caglayan@boun.edu.tr
Class Meetings :	Thursdays, 14:00-16:50, ETA A5
Textbook :	- W. Stallings, Cryptography and Network Security, Prentice-Hall, 2011, 5th Ed.
Reading Material :	- Matt Bishop, Introduction to Computer Security, Addison Wesley, 2005 - Matt Bishop, Computer Security: Art and Science, Addison Wesley, 2003 - Additional list of textbooks and selected papers to be distributed

Grading :	Term paper	100	
	Term paper presentations	100	
	Projects 1 and 2	250=100+150	
	Midterm	250	
	Final Exam	300	Total Exams : 55%
	Total	1000	

Subjects possibly to be covered in Lectures (some by my PhD students):

1. Introduction and course organization.
2. Overview of operating system and computer network security issues : Computer security basics, risk analysis, security policies (template), trusted computers and networks, Orange Book, UNIX security, TCP/IP security, organizations (CERT, CSRC), standards.
3. Symmetric Ciphers: Classical techniques, terminology, conventional cryptosystem model, substitution, transposition, cryptanalysis, various conventional encryption techniques (Playfair, Vigenere, rotor machines, etc). Modern techniques, Simple DES, block cipher principals, DES and its details. AES and its details. Other modern techniques such as IDEA, BLOWFISH, CAST, RC2, RC5, etc. Use of conventional cryptology and confidentialty issues, key distribution problem, random numbers as keys.
4. Number Theory : Prime numbers, modular arithmetic, Fermat's and Euler's theorems, primality testing, Euclid's algorithm, Chinese remainder theorem, discrete logarithms. Mostly reading and/or presentations
5. Public Key Cryptography : Diffie-Hellman approach, public key cryptosystem model, principles of public key cryptology, RSA scheme, key management, Diffie-Hellman key exchange. Number theory issues, elliptic key cryptography.
6. Authentication and Digital Signatures : Requirements and functions, message authentication codes, hash functions, algorithms such as MD5, SHA, RIPEMD, HMAC. RSA digital signatures and DSS. Authentication protocols.
7. UNIX/LINUX Security Issues: User accounts and the login process, password file entries, passwd command, passwords and password selection, password encryption and aging, initialization/startup files and directories, root account and superuser, su command, file protection: ownership and access rights, owners, group owners, user and group ids, read, write, execute rights on files and directories, access rights and permissions of new files, file encryption, set user id and set group id properties, effective user and group ids, chown, chgrp, chmod and related commands, system files and directories and their access control, process accounting, log files, break-ins, hidden files
8. Security Issues of Other Operating Systems : Windows, Solaris, Android, IOS.
9. Authentication Applications : Kerberos (algorithms and v4/v5 software). X.509, certificates, performance, problems, certification authorities, certificate software.
10. TCP/IP security: IP security, IPsec. DNS security, FTP/Telnet security, NIS/NFS security, SNMP security
11. Electronic Mail Security : PGP, S/MIME, PEM, SMTP and Sendmail.
12. Web security: HTTP, SSL, JAVA security.
13. System Security: Concepts, packet filtering. Intruders, intrusion detection, malicious software, viruses, worms, hacker tools, firewalls. Example commercial and public domain software. OS/Network Security Tools: Example commercial and public domain software tools.
14. Security of Digital Money and Payment Systems : Principles, SET protocol and other protocols.
15. Formal Methods, Modeling, Model Checking, Theorem Proving,Verification and Related Software Tools in Security
16. Exact topics and the schedule of PhD student lectures will be distributed later.

Additional Notes :

1. You should take this course only if you have successfully taken (grades C or above) an Operating Systems course and a Computer Networks course, at undergraduate and/or graduate level.
2. Your attendance is required and checked in all lectures and presentations. Presentations are evaluated/graded by the classroom participants. **Absence in at most 3 class meetings will result in grade F.**
3. You can not miss your presentations (of course with the exception of health reasons). Drop the course if you would not be able make it.
4. Midterm and final exam are TBA
5. Email list is cmpe526@listeci.cmpe.boun.edu.tr.
6. Term paper presentations, each 40 minutes including 5-10 minutes of questions and answers, 4 presentations/week.