

Computer and Networks Security

CS 4393: "Computer and Networks Security"

A comprehensive study of security vulnerabilities in information systems and the basic techniques for developing secure applications and practicing safe computing. Topics including Common attacking techniques such as buffer overflow, Trojan, virus, etc. Operating Systems security. Conventional encryption. Hash functions and data integrity. Public-key encryption. Digital signature. Security standards and applications. Building secure software and systems.

Textbooks:

- Cryptography and Network Security, Third Edition or Fourth Edition, by William Stallings, Prentice Hall.
- Related Web Sites and Class Handouts.

Professor in Charge: Edwin Sha

Prerequisites: Only one: CS4348 OS. I will cover the required networking knowledge in class.

Important Dates:

- Final Exam: IN CLASS on May 1, 2012. 10am - 11:15am.
- Spring break: March 11 to March 17, 2012

Course Policy:

- Class participation is important. For your own sake, you should not miss any of the classes. There will be several pop-up quizzes in class. If you miss any, you get 0 point for that pop-up quiz.
- If you cheat in any exam or homework, you will be reported to the school and fairly punished. Do not even try. I have seen cases where students were evicted from school. The bad record would be permanently stored.
- You MUST take the Final Exam in the last class. A job interview is not an allowable excuse.
- I have been spending a lot of time preparing the course and would like to give you the best that a good student at UTD deserves to have. I am very serious in good teaching. If you are not serious in learning, please do not take this course.
- A penalty of 10% deduction each day for late submission of homework will be given and after 5 days, 0 point will be given.

- After the final grade is given, a student should not come to “negotiate” a better grade. I am very fair. In my whole teaching career, I have never changed a student grade after it is given.

<i>Topics:</i>	<i>Lectures</i>
Overview of Security	1
Security in OS	2
Review of TCP/IP	2
Common Security Attacks	
Malicious Software	2
Real Examples	1
Information Security Basics	
Access Control	1
Security Models	1
Conventional Cryptography	
Classical Encryption Techniques	3
Block Ciphers and DES	2
Introduction to Finite Fields	1
Advanced Encryption Standard	1
Public-Key Encryption	
Introduction to Number Theory	3
RSA cryptography	2
Key Management & Other Cryptosystems	1
Hash Functions & Data Integrity	1
Digital Signature	1
Security Practice in Email, Web	1
Secure Programming	
Buffer Overflow	1
Programming with Cryptography	1

Computer Usage: Homeworks will involve computer programming in UNIX systems.

References:

1. John Viega and Gary McGraw, *Building Secure Software*, Addison-Wesley, 2002.
2. Matt Bishop, *Computer Security: Art and Science*, Addison Wesley, 2003.
3. John Chirillo, *Hack Attacks Revealed: A Complete Reference for UNIX, Windows, and Linux with Custom Security Toolkit*, Second Edition, Wiley, 2002.
4. I. Cox, M. Miller and J. Bloom, *Digital Watermarking*, Morgan Kaufmann, 2002.
5. Peter Wayner, *Disappearing Cryptography*, Second Edition, Morgan Kaufmann, 2002.
6. Dieter Gollmann, *Computer Security*, John Wiley & Son Ltd., 1999.

7. Douglas R. Stinson, *Cryptography: Theory and Practice (Discrete Mathematics and Its Applications)*, 2nd edition, 2002.
8. A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996. Available on line: <http://www.cacr.math.uwaterloo.ca/hac/>
9. Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition*, 2002.
10. Charles Pfleeger and Shari Pfleeger, *Security in Computing*, Third Edition, Prentice Hall, 2003.
11. Michael Welschenbach, *Cryptography in C and C++*, Apress, 2001.
12. Julia Allen, *The CERT Guide to System and Network Security Practice*, Addison Wesley, 2001.
13. W. Kruse II and J. Heiser, *Computer Forensics*, Addison Wesley, 2002.

Grading: Not final yet, subject to change

Homework & Programming (3 or 4) & Quiz	65%
Final Exam:	35%