

Information Security

CS 6324: "Information 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. UNIX, Windows and Java security. Conventional encryption. Hash functions and data integrity. Public-key encryption (RSA, Elliptic-Curve). Digital signature. Watermarking for multimedia. Security standards and applications. Building secure software and systems. Legal and ethical issues in computer security.

Textbooks:

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

Professor in Charge: Edwin Sha

Prerequisites: Basic knowledge in operating systems

Important Dates:

- Term Project Presentations: April 24 and 26, 2012.
- We have in class quizzes. You must attend the class.
- Final test s held in CLASS on May 1, 2012, Tuesday. I will tell you how to prepare it.
- Term Project Report Due: 11am, April 27, 2012 Friday.
- Spring Break: March 11- 17, 2012.

Course Policy:

- Programming projects can be done by a team of two students.
- 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 fairly punished. Do not even try. I have seen cases where students were evicted from school The bad record might be permanently stored.

- The only allowable reason that you cannot attend the exam is that your body is physically unable to move due to an illness. A job interview or your own wedding 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 or projects will be given; after 5 days of delay, the homework or project will get 0 point.
- After the final grade is given, a student should not come to “negotiate” a better grade. I am 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 Information Security	1
Common Security Attacks	
Malicious Software	1
Real Examples	1
Operating systems security	3
Information Security Basics	
Access Control	1
Security Models	1
Conventional Cryptography	
Classical Encryption Techniques	1
Block Ciphers and DES	3
Introduction to Finite Fields	2
Advanced Encryption Standard	1
Public-Key Encryption	
Introduction to Number Theory	4
RSA cryptography	1
Key Management & Other Cryptosystems	1
Hash Functions & Data Integrity	2
Digital Signature	1
Security Applications	1
Secure Programming	
Buffer Overflow	2
Security in UNIX, Windows NT, Java, Database	2

Computer Usage: Homeworks will involve computer programming.

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 Guideto System and Network Security Practice*, Addison Wesley, 2001.
13. W. Kruse II and J. Heiser, *Computer Forensics*, Addison Wesley, 2002.

Grading: (Might be changed)

Homework & Programming Projects& Quizes	55%
Final test:	25%
Term Project and Presentation:	20%

Special Consideration:

The term projects can be an extensive survey, theoretical study or an implementation relevant to the theme of the course.