Naveen Jindal School of Management

MIS 6330 — IT Security

Instructor:	Professor A. Lahiri	**Office:**	3.809
Mobile:	414-350-0855	**Email:**	atanu.lahiri@utdallas.edu
Office hours:	After class on Mon, or call my mobile phone any time for appointment[++]		
Course website:	On eLearning		
TA:	Toru Ghoshal	**Email:**	txg140830@utdallas.edu

Text

Computer Security: Principles and Practice (3/e) by Stallings and Brown. This book is required. It's available in the book store.

Course material

I have prepared an extensive set of course notes that I will use during the class. These notes will be posted on the class website. These lecture notes are not intended to substitute regular reading from the textbook; they are there to act as a summary of topics/issues/concepts discussed in class. These notes are meant to save you the time to take notes in class, so that you can make better use of that time by listening, asking question, and participating in class. In addition, all homeworks and solutions will be posted on the class website.

Course description

This course is intended to prepare students for jobs that require comprehensive understanding of security threats, technical approaches to prevention and countermeasures, and related management issues. Though it does not have pre-requisites, it assumes familiarity with concepts such as DBMS and TCP/IP, which I will also briefly revisit. We will cover these topics:

1. **Introduction:** challenges, the CIA triad, feature vs. assurance, security strategy.
2. **Cryptography:** symmetric encryption, public-key encryption, secure hash functions, message authentication, sender authentication, digital certificates and signatures.
3. **User Authentication:** password policies, hashing and use of password salts, offline dictionary and rainbow table attacks, remote authentication and replay attacks, challenge-response protocols, biometric systems.
4. **Database Security:** access control basics (centralized vs. decentralized), role-based security (plus SQL GRANT statement), statistical database security, inference and tracker attacks (plus query restrictions, perturbation, micro-aggregation, and other common countermeasures).
5. **Software Security:** buffer and stack overflow, SQL and code injection, cross site scripting, software security testing (input fuzzing, output testing)
6. **Intrusion:** review of TCP/IP, firewall types (packet filters, circuit-level gateways, application proxies) and topologies (location of bastions and host firewalls); time permitting, IDS and honeypots.
7. **Malware and DoS:** viruses and other malware, antivirus software evolution, botnets and FFSN, flooding attacks, Denial of Service, reflection and amplification attacks, contingency plans for DoS.

[++] Grade-related conversations can't be done over phone/e-mail, so you must see me in person.

Though our focus on management of technology and not technology per se, most of the lectures will be fairly technical. It is not possible to implement a security strategy unless you have a good understanding of the underlying technologies. I intend to maintain my focus common security problems and countermeasures. I encourage you to actively participate in every class.

Course motivation

We live in a very different world today than what our parents lived in. In the middle of the last decade, a small group of hackers in Turkey drained bank accounts of 11,000 customers of a Turkish bank. Even a large multinational like Sony has been hacked, and it has cost the company hundreds of millions in shareholder value, if not billions. Curiously, the Pentagon believes that the next 9/11 will not be about planes crashing into buildings; instead, it will be hackers crashing the US stock exchanges, power grids, large telecommunication networks, or nuclear plants.

While the threats have grown, so have technologies that are used to combat them. The security vendors have registered significant growth, even through the recent economic recession. Businesses have stepped up their defenses: after the attack on Sony, many businesses have decided to increase their investments in security solutions. I personally believe that there are excellent career opportunities for IT professionals who have sound understanding of security related threats, technonologies, countermeasures, and policies. I recommend that you attend all lectures, as well as leverage readings, assigned review questions, and homeworks as much as possible.

Classroom expectations

Please bring copies of all the posted lecture notes to every class. *Please display your nametag at each session.* Please turn off (or put in the silent mode) your cell phone during class time. You need not bring your laptop computer to class, but if you do, please restrict its use for class-related purpose only. Also, turn off your laptop's speakers before starting to use it.

Homework

I will post several short individual homeworks. Keep checking the class website regularly.

Exams

We will have both a midsem and a final exam. Both are closed book and notes, but one letter-sized cheat-sheet is allowed. Electronic devices are not allowed. The final exam is not cumulative.

- I would encourage you to arrange weekly meetings with your classmates to discuss the lectures and readings. Studying in small groups can help. At the same time, because the homeworks are NOT team homeworks, you should not collaborate on them.

Grading

Homework	*20%*
Midterm Exam	*40%*
Final Exam	*40%*

Your grade will depend on your performance vis-à-vis your classmates'.

Graded work, feedback, and solutions

Graded work (midterm exam) and feedback will be returned promptly to you. Solutions will be posted on the class website. If you want anything regraded, please write a separate memo (not email) describing your concerns and hand it to me along with the exam or homework that you want regraded. Please do not write anything on the graded exam or homework, if you want it regarded.

Schedule (Note: no classes on 9/5, 11/14, and 11/21)

Date	Topic	Reading	Homework
Session 1 Monday, 8/22, 4 PM to 5-15 PM	Introduction	Mod. 1, Ch. 1	
Session 2 Monday, 8/22, 5-30 PM to 6-45 PM	Introduction	Mod. 1, Ch. 1	
Session 3 Monday, 8/29, 4 PM to 5-30 PM	Introduction	Mod. 1, Ch. 1	
Session 4 Monday, 8/29, 5-30 PM to 6-45 PM	Cryptography	Mod. 2, Ch. 2	
Session 5 Monday, 9/12, 4 PM to 5-30 PM	Cryptography	Mod. 2, Ch. 2	Submit HW1
Session 6 Monday, 9/12, 5-30 PM to 6-45 PM	Cryptography	Mod. 2, Ch. 2	
Session 7 Monday, 9/19, 4 PM to 5-15 PM	User Authentication	Mod. 3, Ch. 3	Submit HW2
Session 8 Monday, 9/19, 5-30 PM to 6-45 PM	User Authentication	Mod. 3, Ch. 3	
Session 9 Monday, 9/26, 4 PM to 5-15 PM	Database Security	Mod. 4, Ch. 4 & 5	Submit HW3
Session 10 Monday, 9/26, 5-30 PM to 6-45 PM	Database Security	Mod. 4, Ch. 4 & 5	
Session 11 Monday, 10/3, 4 PM to 5-15 PM	Database Security	Mod. 4, Ch. 4 & 5	Submit HW4
Session 12 Monday, 10/3, 5-30 PM to 6-45 PM	Midterm Review		
Sessions 13 & 14 **Monday, 10/10, 4 PM to 5-30 PM**	**Exam-1**		
Session 15 Monday, 10/17, 4 PM to 5-15 PM	Software Security	Mod. 5, Ch. 10 & 11	
Session 16 Monday, 10/17, 5-30 PM to 6-45 PM	Software Security	Mod. 5, Ch. 10 & 11	
Session 17 Monday, 10/24, 4 PM to 5-15 PM	Software Security	Mod. 5, Ch. 10 & 11	Submit HW5
Session 18 Monday, 10/24, 5-30 PM to 6-45 PM	Intrusion & Firewall	Mod. 6, Ch. 9	
Session 19 Monday, 10/31, 4 PM to 5-15 PM	Intrusion & Firewall	Mod. 6, Ch. 9	Submit HW6
Session 20 Monday, 10/31, 5-30 PM to 6-45 PM	Intrusion & Firewall	Mod. 6, Ch. 9	

Session 21 Monday, 11/7, 4 PM to 5-15 PM	Malware & DoS	Mod. 7, Ch. 6 & 7	Submit HW7
Session 22 Monday, 11/7, 5-30 PM to 6-45 PM	Malware & DoS	Mod. 7, Ch. 6 & 7	
Session 23 Monday, 11/28, 4 PM to 5-15 PM	Malware & DoS	Mod. 7, Ch. 6 & 7	Submit HW8
Session 24 Monday, 11/28, 5-30 PM to 6-45 PM	Final Review		
Sessions 25 & 26 **Monday, 12/5, 4 PM to 5-30 PM**	**Exam-2 (Not comprehensive)**		

UT Dallas Syllabus Policies and Procedures

The information contained in the following link constitutes the University's policies and procedures segment of the course syllabus.

Please go to http://go.utdallas.edu/syllabus-policies for these policies.

The descriptions and timelines contained in this syllabus are subject to change at the discretion of the Professor.