

GSLIS 385T.6 – Introduction to Information and Network Security
Spring 2002

Lance Hayden
512.378.1072
lhayden@gslis.utexas.edu
lhayden@cisco.com

Introduction

The goal of this class is to provide a detailed discussion of the basic terminology and concepts of Information and Network Security. I assume that you have taken the class because the subject interests you and that you don't have a great deal of experience in it. Therefore my job becomes one of showing you the basics, stimulating your interest, and perhaps even starting you down the road to becoming a professional in the security field. Even if you aren't looking for a job in security, what you take away from this class can help you in the schools, libraries, and not-for-profit worlds as well. The fact is that the world is becoming increasingly networked, down to the "last mile" to your home computer and various personal computing devices. The more you know about security the more you can make educated decisions regarding these technologies.

This class is designed to be flexible. I don't like rules and I prefer to leave the decisions regarding what you get out of the class up to you to every extent possible. That being said, there are assignments but I encourage you to get outside your traditional academic and personal zip-codes and explore new possibilities. If you have an interesting idea for an assignment please let me know and we can discuss it. Traditional papers are fine, but some of my favorite assignments have been fairly quirky (the product reviews done as a Flash presentation and as a Shakespearean 1-act play, respectively, come immediately to mind). The point is that I get bored as quickly as you do (more quickly in all likelihood – just look at my resume), so entertaining yourself and me is definitely encouraged.

I like to go into this class with two basic expectations:

1. That you are interested in this topic and looking to learn as much as you can about it, either generally or on specific topics.
2. That you'll learn more when you have "skin in the game" and are not simply being spoon-fed material and then spitting it back out.

As such, this class will be challenging. I want it to be challenging. It will also be very straightforward. I have built flexibility in the grading system as well and anyone that really wants an A should get one. But no one is guaranteed an A nor do I expect everyone to earn one. I believe that a B is a strong, respectable grade and that even a C is

nothing to be ashamed of, especially if a student is balancing other factors and may not have as much time as others to devote to the course.

My hope is that the coursework will allow everyone to achieve a certain level of knowledge, rewarding those who choose to go above and beyond the norm without penalizing those whose academic or professional goals may be different, or those students juggling other priorities in addition to this class. I would also encourage you again to think outside the box. Take risks. As you will see from the grading scale, everyone in the class can afford to screw up at least one assignment. I don't want you to be afraid to explore and you shouldn't be penalized for it. Additionally, should you have any special interests or ideas for papers, do not hesitate to approach me. I am willing to consider alternative assignments on a case-by-case basis.

Textbooks

I've chosen two books for the class this semester. I will also supplement the texts with readings and research from the Net.

Maximum Security, 3rd Ed.

Anonymous

SAMS, 2001

ISBN: 0672318717

Secrets & Lies – Digital Security in a Networked World

Bruce Schneier

John Wiley & Sons, 2000

ISBN: 0471253111

Reading Assignments

Readings will be from the textbooks with supplementary readings from the Net, which I will assign no later than one class period prior to the due date. **I expect all assignments to be read and that you are ready to discuss them in class.** I know every instructor everywhere says that, but I am serious. I like interactive classrooms and as much as I enjoy hearing myself talk (you'll find that out as the semester progresses) I hate to be the only one in the conversation. And I make this commitment to you - I will read everything that I assign prior to class myself. If I don't read it, then I won't hold you responsible for it. I have listed all textbook readings and as many supplemental readings as I can on the syllabus. There is no penalty for reading ahead, and some weeks have a lot of readings assigned so plan accordingly. If I assign it and I read it, then you will have no excuses if you come to class unprepared. While I despise grading for participation I do reserve the right to take away credit for lack of participation based upon blowing off the assignment. However, I am confident that all of you are in this class because you choose to be and that you are **excited** about all the readings...

Opening Discussions

To facilitate interactivity around the class and readings we will start each week by going over a couple of points from the text that I will choose from the assignments. This will set the tone for the lecture and allow you to voice any questions from the readings. I expect everyone to be prepared and participate (upon threat of actually grading on it – “*Hey – don’t make me come back there...*”)

Office Hours

Call or email me for an appointment.

LISTSERV

I will set up a LISTSERV mailing list for the class and notify you of the list name. I find the mailing list to be the best way to communicate and keep in touch. Most of my admin messages will be sent out via the list, so it pays to subscribe. I also hope everyone uses the list to collaborate and share info. You can find instructions for UT LISTSERV services at <http://www.utexas.edu/cc/maillinglists/index.html>.

Class Schedule

I have included a planned class schedule below. **This schedule is tentative.** I try to make every class and work my travel schedule for Cisco around the course, but at times I have to leave town unavoidably. I have built a number of flex days into the schedule to accommodate these unexpected situations, as well as for guest lectures and topics that may come up over the course of the semester. I will keep you updated of any changes to the schedule as the semester progresses.

Submitting Assignments

Because of my limited visits to the GSLIS office, I prefer to receive the assignments soft copy. You can hand in a disk in class (I will accept standard floppies, zip disks, and CDs, depending on the assignment, or email me the assignment (provided it is of a reasonable size, say 500K or below. Send all assignments to my Cisco email address listed above. Please do not send documents to my GSLIS address and please **do not** send me a document that you have not checked with a **current** virus scanner. I will be quite annoyed if I get a virus from a soft-copy assignment and will take off points right off the bat. Hey, this is a **security class**, right?

Grading

My grading system is as follows:

Topic Papers (6 total)	25 points each
Final Project	60 points
Final Project - Presentation	20 points

Total Points Available 230 points

180 - 200 points	A
160 - 179 points	B
140 - 159 points	C
120 - 139 points	D
0 - 120 points	F

Papers and Final Project

You have the option of submitting up to 6 topic papers during the semester (the topics are tentatively listed below) and you will prepare a final project and a presentation at the end of the semester. The papers will be on a variety of network security related topics and I will provide guidance on them prior to the first deadline. As you can see above, there is a fudge factor of about one paper on the point scale. You are welcome to do all six, but only required to do three to ensure you a C (assuming you do well on each...). The final project and presentation are required of all students. You decide how much work to do to get the grade you want.

Each paper has a deadline date. After this date I will no longer be accepting papers for that topic. Please plan accordingly, as I will only make exceptions in extreme cases (and my definition of extreme may be far different from yours).

Paper Guidelines (Tentative)

Topic Paper One –	Security Incidents
Topic Paper Two –	Network Vulnerabilities
Topic Paper Three –	“Passive” Security Technologies
Topic Paper Four –	“Active” Security Technologies
Topic Paper Five –	Code Security Issues (Offensive or Defensive)
Topic Paper Six –	Security or Privacy Standards/Legislation
Final Project –	Security Survey Project and Presentation

Class Schedule

The following is the planned schedule for classes:

January 17

Hour 1

Intro to Class

Hour 2

Intro to Assignments

Hour 3

Summary Lecture

Readings:

January 24

Hour 1

Intro to Network Security

Hour 2

Intro to Network Security

Hour 3

TCP/IP Overview

Readings:

MS: 1, 2, 3, App B

SL: Part 1

January 31

Hour 1

TCP/IP

Hour 2

TCP/IP

Hour 3

TCP/IP

Readings:

MS: 4

February 7 – Topic Paper 1 Due

Hour 1

Hackers and Threats

Hour 2

Hackers and Threats

Hour 3

Hackers and Threats

Readings:

MS: 5, 6

February 14 - Pen Test Demo

Hour 1

Attacks and Vulnerabilities

Hour 2

Attacks and Vulnerabilities

Hour 3

Attacks and Vulnerabilities

Readings:

MS: 7, 8, 9

February 21 – Topic Paper 2 Due

Hour 1

LANCE @ RSA CONFERENCE

Hour 2

Guest Lecture – Michelle Desilets

Hour 3

Readings:

February 28

Hour 1

Hour 2

Hour 3

Readings:

“Passive” Defenses

“Passive” Defenses

“Passive” Defenses

MS: 10, 12, 13

SL: Part 2

March 7 – Hands On: PGP

Topic Paper 3 Due

Hour 1

Hour 2

Hour 3

Readings:

“Active” Defenses

“Active” Defenses

Cryptography

MS: 11, 14, 15

March 14

Spring Break

March 21 – Topic Paper 4 Due

Hour 1

Hour 2

Hour 3

Readings:

Virtual WMD and Malware

Virtual WMD and Malware

Virtual WMD and Malware

MS: 16, 17, 18

March 28

Hour 1

Hour 2

Hour 3

Readings:

Platforms

Platforms

Platforms

MS: 19, 20, 21, 22, 23, 24

April 4 – Hands On: Trinix

Topic Paper 5 Due

Hour 1

Hour 2

Hour 3

Readings:

The Security Program

The Security Program

The Security Program

MS: 25, 26, 27, 28, 29(opt)

SL: Part 3

April 11

Hour 1

Hour 2

Hour 3

Readings:

Privacy and Identity Theft

Security Consultants

Training and Certification

April 18 - Topic Paper 6 Due

Hour 1

Hour 2

Hour 3

Readings:

Open

April 25

Hour 1

Hour 2

Hour 3

Readings:

Open

May 3 – Final Paper/Presentation

Hour 1

Hour 2

Hour 3

Readings:

Final Presentations

Final Presentations

Final Presentations