

Information Security
INF 350E (27880)/385T (28010) – Spring 2017
Friday 0900-1200

Lance Hayden
lhayden@ischool.utexas.edu

Course Overview

This class will be an overview of the field of information security, including security in information technology systems. It is meant to be an introduction to the topic, with a deliberate industry focus. The course will cover definitions, concepts, and goals that are commonly agreed upon by information security practitioners and industry and certification bodies.

In addition to diving into the lingo and professional activities of enterprise cyber security, the course will take a complementary and critical approach in which we will explore other and alternate conceptions of security and privacy, supplemental readings, and exploratory projects.

Course Objectives

The major areas of learning and course objectives for this class include:

1. Fundamentals of information and IT security
2. How businesses and governments approach enterprise security
3. How society adapts to security, risks, and threats
4. How security overlaps with other domains, including privacy, surveillance, identity, and national security

Assignments

Assignments will include reading and in-class discussions, exercises and lab work in a virtual lab environment, and projects and papers. Depending on the size and composition of the class, these assignments vary and we will discuss them in more detail during the first day we meet.

In general, assignments look like this:

Assigned Readings – We will read several required texts, including books and articles that are assigned during the semester (including by the students themselves.) I expect everyone to have completely read all assignments prior to class and be ready to discuss.

Discussions – Similarly, I expect everyone to participate in class. Actively. This is a graduate level class and that means any classes that turn into lectures by me represent a failure on both our parts. It is incumbent upon all of you to keep me from lecturing.

Practicals and Labs – We will apply a “hands on” approach to security through the use of labs and practical exercises designed to teach specific security-related skills as well as simulating what life is like in an enterprise security program.

Papers and Projects – In order to apply the readings and discussions, I’ll be asking you to undertake papers and projects over the course of the semester. There will be some choice and flexibility involved here. We’ll talk more about these assignments in class the first day and throughout the semester.

Grades

Given that the class only meets once a week, it is critical that you attend each scheduled class session. If you must miss a class you must let me know well ahead of time and arrange with one

of your colleagues to take notes for you or cover any assignments due. I reserve the right to impose grading penalties on students who miss class.

Class Participation – keeping up with the readings, resulting in regular and engaged participation in class discussions, is required and counts for 1/3 of your final grade.

Per University policy, the grading scale for this class is A, A-, B+, B, B-, C+, C, C-, D+, D, D-, and F.

Office Hours: By Appointment

Required Textbooks

- Donaldson, S., S. Siegel, C. Willams, & A. Aslam (2015). *Enterprise cybersecurity: How to build a successful cyberdefense program against advanced threats*. Apress.
- Kaplan, F. (2016). *Dark territory: The secret history of cyber war*. Simon & Schuster.
- Krebs, B. (2015). *Spam nation: The inside story of organized cybercrime - from global epidemic to your front door*. Sourcebooks.
- Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. W.W. Norton & Company.

Other supplemental readings will be assigned during the course of the semester. We will discuss these readings on the first day of class and throughout the Fall.

Policy on Scholastic Dishonesty

Students who violate University rules on scholastic dishonesty are subject to disciplinary penalties, including the possibility of failure in the course and/or dismissal from the University. Since such dishonesty harms the individual, all students, and the integrity of the University, policies on scholastic dishonesty will be strictly enforced. For further information please view the University catalog: <http://catalog.utexas.edu/general-information/the-university/#universitycodeofconduct>

Students with Disabilities

Students with disabilities may request appropriate academic accommodations from the Division of Diversity and Community Engagement, Services for Students with Disabilities, 471-6259.

Calendar:

<u>Class</u>	<u>Activity</u>	<u>Reading & Assignments</u>
Jan 20	Course Introduction Blog & News Assignments Discuss Labs & Simulation	<i>Syllabus</i>
Jan 27	Discuss: <ul style="list-style-type: none">• Readings• Blog posts• OTW Labs	<i>Dark Territory 1-8</i> Student blog posts (See Canvas) OTW Writeups (See Canvas)
Feb 3	Discuss: <ul style="list-style-type: none">• Readings• Blog posts• OTW Labs	<i>Dark Territory 9-15</i> Student blog posts (Canvas) OTW Writeups (Canvas)

Feb 10	Discuss: <ul style="list-style-type: none"> • Readings • Blog posts • OTW Labs 	<i>Spam Nation 1-7</i> Student blog posts (Canvas) OTW Writeups (Canvas)
Feb 17	Discuss: <ul style="list-style-type: none"> • Readings • Blog posts • OTW Labs 	<i>Spam Nation 8-12, Epilogue, A Conversation with Brian Krebs</i> Student blog posts (Canvas) OTW Writeups (Canvas)
Feb 24	OPEN	Film or Guest
Mar 3	Discuss: <ul style="list-style-type: none"> • Readings • Blog posts • OTW Labs 	<i>Data and Goliath 1-8</i> Student blog posts (Canvas) OTW Writeups (Canvas)
Mar 10	Discuss: <ul style="list-style-type: none"> • Readings • Blog posts • OTW Labs 	<i>Data and Goliath 9-16</i> Student blog posts (Canvas) OTW Writeups (Canvas)
Mar 17	<i>SPRING BREAK</i>	
Mar 24	Discuss Readings Discuss Assignments Kickoff Simulation Exercise	<i>Enterprise Cybersecurity 1-3, Apps A & B Supplemental Readings (Canvas)</i>
Mar 31	Discuss Readings Simulation Round One	<i>Enterprise Cybersecurity 4-7, App D Supplemental Readings (Canvas)</i> Security Policy Comparison Due
Apr 7	OPEN	Film or Guest
Apr 14	Discuss Readings Simulation Round Two	<i>Enterprise Cybersecurity 8-10, App E Supplemental Readings (Canvas)</i> Security Risk Assessment Due
Apr 21	OPEN	Film or Guest
Apr 28	Discuss Readings Simulation Round Three	<i>Enterprise Cybersecurity 14-15 Supplemental Readings (Canvas)</i> Incident Response Plan Due
May 5	Last Day Close things out	