CS361C: Spring 2015 Information Assurance and Security

Instructor: Dr. Bill Young; **Unique number:**51965
Class time: MWF 9-10am; **Location:** CLA 0.130
Office: GDC 7.810; **Office Hours:** MWF 10-noon and by appt.
Office Phone: 471-9782; **Email:** byoung at cs.utexas.edu
TA: Zhao Song; **Email:** zhaos at utexas.edu
TA Office Hours: Tuesdays 9am-noon, GDC 6.438F
TA: Cong Ding; **Email:** cong at cs.utexas.edu
TA Office Hours: Wednesday 1-4pm in GDC 6.438F
This website: www.cs.utexas.edu/users/byoung/cs361C /syllabus361C.html

x

Important Class Announcements:

Breaking news important to the class will be posted here. Consult this spot often.

On Friday, January 30, I'm attended some sessions of a conference on campus. We'll have class, but I won't hold my usual office hours from 10am-noon that day.

Your first assignment is here: Assignment 1. It assumes that we've made some progress on slideset 1.

If you're curious, here's an exam from a previous semester: Sample midterm

Here's a list of project topics from last Spring: Project Topics.

I have now created the groups for your class project. They were assigned randomly. Here's a list: Groups.

Feel free to email me (Send me an email message), but please put "CS361C" in the header. I'm teaching another class this semester and this helps me to understand the context of your question or comment.

Go to Slides section.
Go to Assignments section.
Go to Tests section.
Go to Interesting Links section.

Course Description:

Information Assurance is dedicated to keeping information safe from harm. This encompasses computer security, but also communications security, operations security, and physical security. That's a lot to study in one course. For example, NSA has an Information Assurance Directorate tasked with: "detecting, reporting, and responding to cyber threats; making encryption codes to securely pass information between systems; and embedding IA measures directly into the emerging Global Information Grid. It includes building secure audio and video communications equipment, making tamper protection products, and providing trusted microelectronics solutions. It entails testing the security of customers' systems, providing OPSEC assistance, and evaluating commercial software and hardware against nationally set standards, to better meet our nation's IA needs."

Our approach will be to cover selected topics from this very broad area of study with the goal of preparing the student to think critically about security from a wholistic perspective, rather than a purely technical perspective. Also, the topics covered will be those deemed necessary for the InfoSec Certification. Topics may include:

1. Introduction to Information Assurance
2. Metrics for Information Assurance
3. Networking and Cryptography
4. Information Assurance Planning and Deployment
5. Vulnerabilities and Protection
6. Identity and Trust Technologies
7. Verification and Evaluation
8. Incident Response
9. Human Factors
10. Legal, Ethical, and Social Implications

Students are expected to read assigned materials prior to the class meeting and to participate actively in the discussion. A significant portion of your grade will be based on your engagement in the class.

Notice that CS students at UT have the option of completing a number of security-related courses and receiving a government-sanctioned certification in security. See the following link for information: Infosec Certification.

Prerequisites:

You are expected to have taken and passed the following courses (or equivalent) with a grade of at least C-: Computer Science 311, 311H, 313H, or 313K; Computer Science 307, 314, 314H, 315, or 315H; Computer Science 310, 310H, 429, or 429H; and Mathematics 408C, 408K, or 408N. If you don't have the prerequisites, be sure to clear it with the CS department, or risk being dropped from the course.

Using Piazza:

We will be using Piazza for class discussion. The system is highly catered to getting you help fast and efficiently from classmates, the TAs, and myself. Rather than emailing questions to the teaching staff, I encourage you to post your questions on Piazza. If you have any problems or feedback for the developers, email team@piazza.com. Our class page will be set up shortly and announced here. Return to top of page.

Textbook and Slides:

There is no required text for the class this semester.

Handouts of all class slides will be made available over the course of the semester via links below. Slides din PDF format. The PDF files can be viewed with Acroread. If you print from Acroread, you can print 2 or 4 slides per page; I suggest that you do so to save paper.

Slide set 0: It's a Dangerous (Cyber) World (PDF)

Slide set 1: Intro to Information Assurance (PDF)

Return to top of page.

Readings and Assignments:

I will occasionally assign readings from papers over the course of the semester. You are expected to have read the assigned material and also to have read the course slides before class. There may be pop quizzes on this material at any time.

There will be several projects assigned over the course of the semester. Each student should work on assignments individually unless I explicitly say that teams are allowed. The projects generally will not be programming projects, but will involve writing short reports on various aspects of security. This is not a writing course and your spelling and grammar skill will not be graded. Rather, the grade will depend on the amount of thought and (possibly) research you put into the assignment. However, you should strive to produce quality work that is grammatically correct and formatted nicely.

Standing assignment: Read over the class slides before we discuss them.

Assignment 1, due 2/6/15 at classtime

Semester project: In addition to the other assignments, teams of 5 students will become experts in some specialized security topic, write a paper on that topic, and make a presentation to the class. A partial list of possible topics will be offered. If a topic strikes your fancy, you can claim it by sending me an email. All topics must be distinct. Since there over 100 students in the class, it is infeasible for students to work alone on this. However, the fact that you are working as teams of 5 means that your product must be a high quality team effort.

An alternative to a class presentation is to produce a high quality video describing your work. It will be shown in class in lieu of your presentation. An excellent example from a previous semester is here: Drone Video

You will be provided very specific formatting instructions for the project paper. In particular, it will be done using LaTeX and following a format provided. This has two goals:

1. it eliminates the tendency to fudge the length of the paper by padding;
2. it teaches you a very useful technical skill if you ever plan to publish in a technical arena (or even if you don't).

Everything you need to know about LaTeX will be provided.

Quizzes:

Short in-class quizzes may be given at any time. These will cover material covered in previous classes and check whether you are keeping up with the reading. *There will be no makeups for quizzes you miss,* but any single quiz is only a tiny proportion of your final grade.

Return to top of page.

Tests:

There will be two major tests during the semester. Both tests will be given during the regular class-time. The first will be March 11; the second will be May 6. Here's a midterm exam from a previous semester: Sample midterm. Your best study strategy is to review the readings and class notes and ensure that you understand thoroughly the topics we covered in class. Tests are open book / open notes.

The **final test** will be held in class the last week of classes. A sample final test will be posted. There will be no final exam during the exam period.

No laptops:

Students are asked not to have their laptops or other electronic devices open during class. Copies of all slides will be provided. Please just listen, participate, and absorb the material.

Grading policies:

Class attendance is required and will be checked on a majority of class days. Excessive unexcused absences will result in a reduced grade. *If you don't plan to come to class regularly, don't register for this class.* Signing in for another student not present will be considered cheating by both students.

Grades are averaged using the weighting below, with the following proviso: *You will not receive passing credit for the course if you have unexcused absences for more than half of the scheduled class meetings at which attendance is taken.*

Also, this class largely consists of discussion. You *must* participate in the discussions. If you are either too shy or too lazy to participate, it will affect your grade negatively. Please discuss it with me if you have issues that keep you from speaking up in class.

Description	Percent
Attendance, Quizzes and Participation	10%
Paper and presentation	30%

Other Assignments	20%
Midterm Test	20%
Final Test	20%

Course grades are assigned on the scale: A = 90-100; B = 80-90; etc., except that I reserve the right to be more generous than this indicates. That is, I may enlarge any of these ranges; I will not shrink any range.

How to Succeed in this Class:

You succeed in this class by participating fully. It may be possible to coast through it, but you won't get a good grade.

1. Come to class regularly
2. Read the slides before class
3. Think carefully about the questions embedded in the slides (usually in purple)
4. Do any assigned readings on time
5. Participate in the class discussions
6. Take enough time and care with the assignments

Scholastic Dishonesty:

Academic dishonesty will not be tolerated. See http://www.cs.utexas.edu/academics/conduct for an excellent summary of expectations of a student in a CS class.

All work must be the student's own effort (with the exception of explicitly approved group effort on projects). No deviation from the standards of scholastic honesty or professional integrity will be tolerated. Scholastic dishonesty is a serious violation of UT policy; and will likely result in an automatic F in the course and may result in further penalties imposed by the department or by the university. Don't do it. If you are caught, you will regret it. And if you're not caught, you're still a cheater.

Some Interesting Links:

When I find interesting articles relating to the course matter, I post them here. Some of these are pretty old, but interesting. The more recent articles are near the top. You are encouraged to read these, but they are not a required part of the course, unless I specifically require you to read selected ones.

Live Map of Cyber attacks
Selling Vulnerabilities
Vulnerabilities Persist
Cyberwarriors Needed
Cyberattacks and Jobs
Great time to start a cybersecurity career
CS Enrollments Rocket
Panetta on Cyber Risk
Military Networks Not Hardened Enough
Attacks on Electric Grid
IETF and security
Detecting Counterfeit Electronics
NSA Strategy for Cyberattacks
Cyberwar on Syria?
New Vulnerability in Apple Machines
That's Just Creepy
US Cyber Target List
Cyberwar on Business
New White House Security Plan and The Plan Itself
Facebook Flaw
Iran's Leader Urges Learning Cyberwar Skills
Cyberwar Hyped?
Cyber Combat: Act of War
Snowden vs. the NSA
The People vs. Winter
Crypto Breakthrough
Rootkit in a PLC
Did the US Almost Kill the Internet
Tor Exit Nodes Spy on Traffic
Acoustical Side Channel Attack
Most popular passwords
NSA Spying on Offline Computers1
NSA Spying on Offline Computers2
Obama on NSA spying
Biggest breaches of 2013
Accenture "ad"
NSA vs. Tech Companies
NSA spying unconstitutional
Drone Video
Feds Hiring Cyberexperts
Acoustical hacking

Cybersecurity jobs
Security jobs hot
Attracting security pros
Hacking Airplanes
Human side of cybercrime
Wow!
Cyberattacks that Destroy
Recruiting hackers
Tallinn Manual on Cyberwarfare
Highest Paying Tech Degrees
Demand for CyberSecurity Jobs Strong
Growth in CS Jobs
Cyberjobs Hot
Govt wants hackers
Cybersecurity skills hot
Beefing up Asymmetric Encryption
Better Password Encryption
Cyberthreats from Russia and China
Call for CyberSecurity Standards
Password Stealing
UK IT Skills Shortage and Cyber Threats
Sandia looks for bad guys in cyberspace
President's power in Cyberstrike
China Hack the New York Times
Shift in How US Wages War
Smartphone Sensors and Security
Pentagon to boost cybersecurity force
Internet vs. Sex
Cyber Attacks
Cyber Attacks
How vulnerable is the U.S.
Covert Channel between VMs
Anti-Virus Failures
Info on AES mixColumns
Peter Neumann
Experts needed
Women, minorities in Security
How Much Risk is Too Much?
Hotel locks hacked
Counterfeit chips
Counterfeit chips 2
Landing a cybersecurity job
DNS attack
security in the cloud
Education about the Internet
Cyberwar Rules

Cyber Attack
Value of the Internet
Attacks on RSA
Flaw in symmetric encryption
Could the Internet be Destroyed
Hackers in the Boardroom
CS Hot Major
Carelessness on the cloud
Sneakey
Malware in Electronics
Grads and security
Immune System Model
Dilbert on ISO 9000
Need to See Ahead
Hacking a Car
Cyberweapon that could bring down the Internet
Tool to Spot Vulnerabilities
Cyberwar Rules of Engagement
Security Game Changer
Power Grid Issues
Policy toward Iran
Bacteria as data storage
Internet Kill Switch
LM as Big Brother
Stuxnet from U.S. and Israel
DSS Trends report
War in Fifth Domain
Protecting Utilities
Google attack
Password changes
Google vs. China
Cyberattacks Existential Threat
Cyber Warriors
War Games
China and Cyber Attacks
Google Hack
CyberWarfare
Attack Certain
Need for a Cybersecurity Agenda
Information Operations Roadmap
Call for Cyber Treaty
Fear of Cyberattacks
Rainbow series
Bad Passwords
Computer Network Terrorism
Cyber Ninjas wanted

Exponential World Video