Identity Security

Identity and Security: Managing, Protecting, and Assuring Sensitive Information Assets

Instructors:

Craig Blaha
Phone: (512) 633-9745
Email: craig.blaha@utexas.edu

Office Hours: By Appointment
TA: TBD
Office Hours: TBD

Course Location and Meeting Times: UTA 1.204

8:00 AM – 12:00 PM
Weekend 1, September 6-7
Weekend 2, October 4-5
Weekend 3, October 25-26
Weekend 4, November 15-16
Weekend 5, December 6-7

I. Recommended (NOT required) Reading List

1. *Cryptography and Network Security*, 6th ed., Stallings, W. Pearson, 2013.
2. *Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats*, Donaldson, S., Siegel, S., et. al. Apress, 2015.

Due to the dynamic nature of information security, this course will utilize extensive supplemental readings in current cybersecurity and identity topics, including journal articles, news reports, blogs, and industry publications. These readings will be selected and assigned closer to the actual course dates and throughout the semester.

II. Course Aims and Objectives:

Aims:

This course aims to prepare students for leadership roles in identity related, network and information technology firms. Students will understand common information security architecture, tools, concepts, and terminology

This course provides students in the MSIMS program a foundational understanding of the theory, concepts, and practical applications of information security and its relationship to identity management. Focused on the people, processes, and technologies that support today's organizational cybersecurity programs, this course prepares students for leadership roles in the protection of sensitive information assets. Students will leave this course with a solid understanding of the history of information security; the threats and challenges that cybersecurity programs face today; methods, tools, and architectures used to create successful cybersecurity programs in industry, government, and not-for-profit organizations; and the skills and techniques for governing a strategic enterprise information security program. Students completing the course will be well prepared for careers in identity management, network security operations, enterprise security program management, and enterprise information

technology risk management. This course combines theoretical with practical readings and exercises, and includes explanations of both technical and non-technical security concepts and practices.

Specific Learning Objectives:

By the end of this course, students will:

1. Understand how information is communicated via the Internet, the operation of its essential components, the operation of its security services, and how those services are implemented.
2. Be able to manage an organization wide risk assessment, including managing security related network scans.
3. Understand the general historical development of information security as a discipline, with specific focus on the evolution of information security in the context of computing, networking, and the Internet.
4. Understand how information is stored and processed in computer systems, and the security implications of these activities
5. Understand how information is transmitted and managed over networks, including the Internet, and how the essential components of these networks operate
6. Understand the theoretical components of information security, particularly *confidentiality*, *integrity*, and *availability*, and how these components are incorporated into security technologies and management programs
7. Understand the structure and functions of an enterprise cybersecurity program, including:
    a. Security Program Management
    b. Security Risks and Threats
    c. Security Controls and Technologies
    d. Security Program Monitoring and Evaluation
8. Apply the concepts and techniques of information security to a variety of cases, scenarios, and exercises, demonstrating knowledge through class discussion, papers and presentations, and the completion of technical security lab exercises.

III. Course Topics

Information security is a dynamic field, which changes frequently as new threats and countermeasures are incorporated into our information environment. That being said, one may identify general category topics that continuously remain relevant for information security professionals, even as their details change with time. These include:

a. Security governance, leadership, and strategy – management, at an executive level, of an organization's information security program
b. Security policies and standards – bureaucratic and organizational architectures designed to standardize information security program practices
c. Compliance and audit – external and internal review of organizational activities against defined frameworks and regimes for standardized behavior
d. Security risk and threat management – the identification and analysis of how security problems or failures may impact the organization
e. People-centric security – the process of training and managing people to ensure proper security behaviors and culture, and maximizing the value of human capital in support of protecting information assets
f. Security in endpoints and devices – how security functions at the level of information technology, including servers, personal computers, network devices, and mobile devices
g. Network security – how security functions as information flows between devices in a networked infrastructure such as the Internet

h. Cryptography – the practice of protecting and verifying information using encryption systems and algorithms
i. Information asset management and classification – the practice of understanding and managing the value of an organization's information, and protecting sensitive assets from loss or damage
j. Identity and access management – the means by which people and systems are allowed to use or control specific information assets
k. Physical security – the protection of physical and environmental infrastructures from threats and risks
l. Malware – the challenges of malicious code, including viruses, worms, spyware, and other software-based threats
m. Security monitoring and logging – visibility into an organization's digital environment for the purposes of managing information use and detecting attacks and other failures
n. Security vulnerability management – the practice of identifying and managing weaknesses in an infrastructure that may be exploited by an attacker
o. Security incident response – the practice of managing and recovering from a security failure, including data loss, damage, or theft
p. Business continuity and disaster recovery – the ability of an organization to maintain and continue operations in the wake of a disaster or other incident that degrades or destroys organizational capabilities
q. Legal implications of information security – the practice of understanding and managing information security at a policy and regulatory level, as well as the legal implications of security decisions and activities

IV. Course Schedule:

Meeting #	Main Topic(s)	Instructor or Guest Lecturer
1 – Sept 6	**Introduction** Course Introduction and Structure Discussion of Enterprise Security part 1 In class exercise	**Blaha**
2 – Sept 7	**Information Security Overview** Kobayashi Maru Discussion of Enterprise Security part 2 In class exercise Homework – read one book, follow one blog, progress on OTW For 10/5, prepare case study #1	**Blaha**
3 – Oct 4	**Systems Administration** Overview, security implications, tools and techniques In class exercises/tasks	**Burns**
4 – Oct 5	**ID, Authn, Authz, and Access Management** CIA, PPT, GRC Student Case Study Presentations Case study in class exercise Homework – PPT, GRC Due 12/6, blog, book, OTW	**Blaha**

5 – Oct 25	**Data Networking** IP addressing, public and private IP address concepts. IP addressing is foundational for understanding how two or more hosts communicate, which is a necessary basis to understanding how computer hacks/breaches occur. Ports and protocols - Hacks/breaches typically use and exploit common protocols (SMB, RDP, FTP, etc.) to accomplish data exfiltration. We'll cover a variety of protocols and how they're employed by bad actors to steal data from organizations. Threat detection and prevention - We'll cover the purpose of firewalls, intrusion prevention systems, endpoint protection, SIEM (security incident and event management, full packet capture, NetFlow, etc). to explore how these technologies are employed to detect threats. These technologies are employed to perform post-breach investigation to confirm the timeline and extent of breaches.	**Reyes**
6 – Oct 26	**Threat Vectors** Hosts/networks become compromised through many variations or combinations of vectors (phish email, software vulnerability, system misconfiguration, etc.) Breach Detection Case Study - Students will dissect and analyze a fictitious data breach. Assignment deliverables include a write-up, a diagram showing the breach sequence of events and a short video briefing (uploaded to Canvas) that addresses the C-suite. Homework: blog, book, OTW	**Reyes**
7 – Nov 15	**Applied Encryption** Diffie Hellman/El Gamal, Back doors, internet of things, spoofing	**Riley**
8 – Nov 16	**Applied Encryption 2** RSA, and Elliptical Curve Cryptography Physical Security, and Biometrics Homework: blog, book, OTW – reminder, Case GRC and PPT due 12/6	**Riley**
9 – Dec 6	**ID, Authn, Authz, and Access Management** Case study presentations Model Diplomacy Tabletop exercise In class exercise	**Blaha**
10 – Dec 7	**Course Wrap-up** Model Diplomacy Session II In class exercise	

V. Grading Procedures: Grades will be based on:

(a) (20%) Participation
(b) (20%) Weekly reading
(c) (20%) 4 case studies (write-ups & presentations)
(d) (20%) 1 lab journal kept throughout the class (Canvas)
(e) (10%) MD Tabletop Exercise write-ups (individuals or groups)
(f) (10%) Breach Detection Exercise

VI. Assignments

1. Participation
    a. Your active and positive participation in the class will count as 20% of your grade.
2. Weekly Reading
    a. As an information security professional, you will need to develop a habit of reading as much as possible in order to be aware of the latest threats and vulnerabilities. Your homework for this class, therefor, includes reading one book of your choice and following one blog of your choice between sessions, and offering a brief discussion about each on Canvas and in class.
3. Technical presentations
    a. Students will be asked to offer a few brief (3-5 minute) technical presentation on a variety of different technical topics. This assignment is structured in the following way:
        i. 9/7 – You will be assigned a technical topic, given 10 minutes to prepare, and asked to
        ii. 10/5 – choose one technical topic you are interested in, be prepared to present on that topic at the beginning of class
        iii. The technical presentations are worth 10% of your grade.
4. Student Lab Journal
    a. Your write up of the in-class labs and exercises will count as 15% of your grade.
5. Four Case Studies
    a. Your write up and presentation of the four case studies over the course of the semester, using the various lenses we discuss in class, is worth 20% of your grade
6. Model Diplomacy Tabletop exercise
    a. The written components of the MD Tabeltop exercise, conducted over the course of the semester, will count as 20% of your grade.
7. Kobayashi Maru test
    a. An in-class test designed to encourage you to think like a hacker.

VII. Course Policies

Class attendance and participation policy: Students are expected to attend all class sessions and complete all assignments on-time. Exceptions will be made on a case-by-case basis. If attending remotely, students will be expected to be visually present and engaged with the class.

VIII. Academic Integrity

University of Texas Honor Code
The core values of The University of Texas at Austin are learning, discovery, freedom, leadership, individual opportunity, and responsibility. Each member of the university is expected to uphold these values through integrity, honesty, trust, fairness, and respect toward peers and community.

IX. Other University Notices and Policies

Use of E-mail for Official Correspondence to Students

- All students should become familiar with the University's official e-mail student notification policy. It is the student's responsibility to keep the University informed as to changes in his or her e-mail address. Students are expected to check e-mail on a frequent and regular basis in order to stay current with University-related communications, recognizing that certain communications may be time-critical. It is recommended that e-mail be checked daily, but at a minimum, twice per week. The complete text of this policy and instructions for updating your e-mail address are available at **http://www.utexas.edu/its/help/utmail/1564 .**

Documented Disability Statement

Any student with a documented disability who requires academic accommodations should contact Services for Students with Disabilities (SSD) at (512) 471-6259 (voice) or 1-866-329-3986 (video phone). Faculty are not required to provide accommodations without an official accommodation letter from SSD. *(Note to Faculty: Details of a student's disability are confidential. Faculty should not ask questions related to a student's condition or diagnosis when receiving an official accommodation letter.)*

- Please notify me as quickly as possible if the material being presented in class is not accessible (e.g., instructional videos need captioning, course packets are not readable for proper alternative text conversion, etc.).

- Please notify me as early in the semester as possible if disability-related accommodations for field trips are required. Advanced notice will permit the arrangement of accommodations on the given day (e.g., transportation, site accessibility, etc.).

- Contact Services for Students with Disabilities at 471-6259 (voice) or 1-866-329-3986 (video phone) or reference SSD's website for more disability-related information: http://www.utexas.edu/diversity/ddce/ssd/for_cstudents.php

Behavior Concerns Advice Line (BCAL)

If you are worried about someone who is acting differently, you may use the Behavior Concerns Advice Line to discuss by phone your concerns about another individual's behavior. This service is provided through a partnership among the Office of the Dean of Students, the Counseling and Mental Health Center (CMHC), the Employee Assistance Program (EAP), and The University of Texas Police Department (UTPD). Call 512-232-5050 or visit http://www.utexas.edu/safety/bcal.

Emergency Evacuation Policy

Occupants of buildings on the UT Austin campus are required to evacuate and assemble outside when a fire alarm is activated or an announcement is made. Please be aware of the following policies regarding evacuation:

- Familiarize yourself with all exit doors of the classroom and the building. Remember that the nearest exit door may not be the one you used when you entered the building.
- If you require assistance to evacuate, inform me in writing during the first week of class.
- In the event of an evacuation, follow my instructions or those of class instructors.

Do not re-enter a building unless you're given instructions by the Austin Fire Department, the UT Austin Police Department, or the Fire Prevention Services office.