The University of Texas at Austin
Master of Science in Identity Management and Security
*School of Information and Center for Identity*

# Identity Security

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


Instructors:

**Bill Bard**
**Craig Blaha**
**Lance Hayden**


Office Hours: By Appointment

TA: TBD
Office Hours: TBD

Course Location and Meeting Times:

---

## I. 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.
3. 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. Develop and present an organization wide:
    a. Security Policy
    b. Business Continuity and Disaster Recovery Plan
    c. Incident Response Plan
3. Be able to manage an organization wide risk assessment, including managing security related network scans.

1. 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.
2. Understand how information is stored and processed in computer systems, and the security implications of these activities
3. Understand how information is transmitted and managed over networks, including the Internet, and how the essential components of these networks operate
4. Understand the theoretical components of information security, particularly *confidentiality*, *integrity*, and *availability*, and how these components are incorporated into security technologies and management programs
5. 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
6. 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

Describe the topics to be covered in the course. Please provide straightforward descriptions of the topics that speak to the value for the student (i.e. why are these topics important to know?)

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 – Jan 20** | **Introduction**<br>Course Introduction and Structure<br>Evolution of Attack and Defense<br>Discussion of Enterprise Security | **Blaha** |
| **2 – Jan 21** | **Practicals**<br>**Hour 1:** Introduce Practicals (Labs and Wargame)<br>**Hour 2:** *Over the Wire* Security Labs Introduction<br>**Hour 3:** Presentation – Building a Security Culture (Lance)<br>**Hour 4:** *ACME/HACKME* Wargame Introduction & Roles | **Hayden** |
| **3 – Feb 10** | **Networking**<br>**Hour 1:** The Layered Internet from the Bottom Up | **Bard** |

| | | |
|---|---|---|
| | Why layering? PHY and MAC as examples<br>**Hour 2:** What is a NETWORK?<br>The OS, addresses, routing<br>**Hour 3:** What is a SESSION?<br>More OS, ports, multi/demultiplexing, control<br>**Hour 4:** APPLICATIONS<br>The Web, mail, and some tools that make them work | |
| **4 – Feb 11** | **Encryption**<br>**Hour 1:** What are the basic cryptographic tools?<br>Characteristics, performance, limitations.<br>**Hour 2:** How can tools be combined to provide security services? Confidentiality, Integrity, Availability.<br>**Hour 3:** Essential Internet security protocols<br>WPA, IPSec, SSL/TLS<br>**Hour 4:** What about S/MIME?<br>An example of what should be available to protect electronic identity. | **Bard** |
| **5 – Mar 3** | **Networking and Identify Management**<br>Methods of Attack and Network Hardening<br>Wireless<br>ID, Authn, Authz, and Access Management | **Blaha** |
| **6 – Mar 4** | **PRACTICALS**<br>**Hour 1:** Recap and Discussion from Last Time<br>**Hour 2:** Student Lab Papers/Presentations<br>**Hour 3:** Presentation: Security Metrics (Lance)<br>**Hour 4:** *ACME/HACKME* Round One<br><br>**RESEARCH PAPER TOPICS/OUTLINES/SOURCES DUE** | **Hayden** |
| **7 – Mar 31** | **Application, Mobile, OpSec**<br>Application Security<br>Mobile Device Security<br>Operations and Op Sec | **Blaha** |
| **8 – Apr 1** | **PRACTICALS**<br>**Hour 1:** Recap and Discussion from Last Time<br>**Hour 2:** Student Lab Papers/Presentations<br>**Hour 3:** Presentation: Advanced Risk Models (Lance)<br>**Hour 4:** *ACME/HACKME* Round Two<br><br>**RESEARCH PAPER FIRST DRAFT DUE** | **Hayden** |
| **9 – Apr 28** | **Asset, Policy, and Engineering**<br>Asset Management and Supply Chain<br>Policy, Audit, E-Discovery<br>Security Engineering | **Blaha** |

| | | |
|---|---|---|
| **10 – Apr 29** | **PRACTICALS**<br>**Hour 1:** Recap and Discussion from Last Time<br>**Hour 2:** Student Lab Papers/Presentations<br>**Hour 3:** Presentation: Security Career Development (Lance)<br>**Hour 4:** *ACME/HACKME* Round Three and Close<br><br>**FINAL RESEARCH PAPERS DUE** | **Hayden** |

## V. Grading Procedures: Grades will be based on:

**(a)** (30%) Participation (Lecture and Practicals sessions)
**(b)** (30%) Security Research "Thesis" Paper
**(c)** (10%) An in-class quiz of approximately 20 minutes (Lecture)
**(d)** (15%) Student Labs (Practicals)
**(e)** (15%) Wargame (Practicals)

## VI. Assignments

1. Participation
    a. Your active and positive participation in the class will count as 30% of your grade.
2. Security Research "Thesis" Paper
    a. Students are expected to submit a unique research paper of publishable quality. Students will work with the instructors to determine a topic that is of interest to the student and relates to the topics of identity and information security. This paper does not need to be published in order to receive credit.
    b. The assignment is broken down as follows:
        i. **5 points:** Paper topic and resources – describe the topic or question you plan to write about and include a bibliography of 10 or more sources you plan to use to write your paper.
        ii. **10 points:** First draft of research paper.
        iii. **15 points:** Final draft of research paper.
    c. The research paper will count as 30% of your grade.
3. In Class Quiz
    a. During the second set of class meetings you will take an in-class quiz covering the networking and encryption discussion led by Professor Bard. The quiz will count as 10% of your grade.
4. Student Labs
    a. Your write up of the Over the Wire labs will count as 15% of your grade.
5. Wargame
    a. The written components of the wargame, conducted over the course of the semester, will count as 15% of your grade.

## 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.