CSA 2372: Security & Info Assurance

Department of Computer Science

Semester Year (Fall 2025)

Faculty Information

Dr. Mainuddin Shaik
Email: shaik.mainuddin@sulross.edu
Office Hours: Mondays & Wednesdays, 2:00 PM - 4:00 PM (via Zoom or by appointment)

Course Description

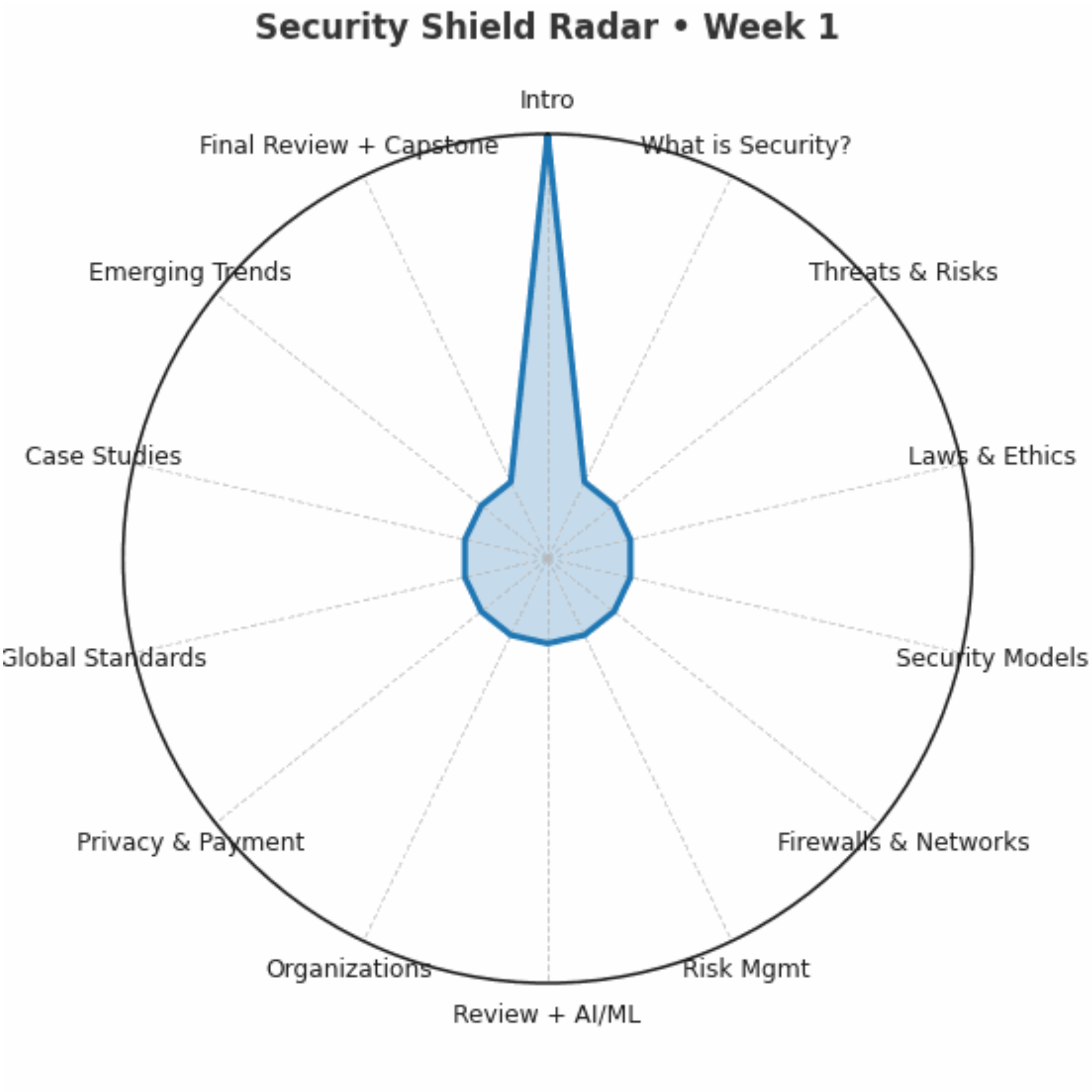
This course provides an accessible introduction to the fundamental principles of information security and assurance in today's digital world. Students will explore what security means, why it is essential for individuals and organizations, and the common risks that threaten information systems. The class emphasizes practical understanding, covering how organizations design strategies, policies, and safeguards to protect sensitive data. In addition, the course highlights how emerging technologies such as Artificial Intelligence (AI) and Machine Learning (ML) are transforming modern approaches to security design and threat detection. By the end of the semester, students will have a foundational understanding of key security concepts, an appreciation of ethical and legal considerations, and insight into the evolving role of intelligent technologies in protecting digital information.

Course Materials

The recommended textbook:

Whitman, M. E., & Mattord, H. J. *Principles of Information Security*.

Additional readings, handouts, and multimedia resources may be provided throughout the semester to supplement the textbook and support classroom discussions.



Important Dates

- **Aug 25** – First Day (Introductions only)
- **Sep 1** – Classes start (Week 2)
- **Nov 27–28** – Thanksgiving Break (No Class)
- **Dec 3** – Last Day to Submit All Work
- **Dec 10** – Last Day of Class (No new work, grading only)

Program Student Learning Outcomes

Upon completion of students will be able to:

1. **Define and explain** fundamental concepts of information security and assurance, including threats, risks, and basic security models.
2. **Identify and evaluate** common vulnerabilities and risks in digital systems, along with organizational methods for mitigating them.
3. **Recognize the role of policy, ethics, and law** in shaping information security practices at local, national, and global levels.
4. **Demonstrate awareness** of how emerging technologies, such as Artificial Intelligence (AI) and Machine Learning (ML), are transforming approaches to threat detection and security design.
5. **Apply critical thinking** to simple case studies and scenarios involving security challenges and solutions.

Course Student Learning Outcomes

Upon successful completion of this course, students will be able to:

1. **Explain** the fundamental principles of information security and assurance in a clear and practical manner.
2. **Describe** common types of threats, risks, and vulnerabilities that affect digital information systems.
3. **Discuss** the importance of legal, ethical, and policy frameworks in shaping security practices.
4. **Illustrate** how core security models, controls, and design strategies protect sensitive data and support organizational resilience.
5. **Examine** real-world examples of security architectures such as firewalls, networks, and secure system design.
6. **Analyze** case studies to understand how organizations respond to risks and compliance requirements.
7. **Evaluate** the impact of emerging technologies—including Artificial Intelligence (AI) and Machine Learning (ML)—on modern security approaches.
8. **Integrate** knowledge from weekly assignments into a final capstone project that demonstrates a holistic understanding of information assurance.

Marketable Skills

Students can expect to develop the following skills in the **Fundamental Security Design and Information Assurance** course:

1. **Critical Thinking & Problem-Solving** – Ability to identify, evaluate, and propose solutions for common digital security risks.

2. **Communication Skills** – Capacity to explain security concepts in clear, accessible language suitable for both technical and non-technical audiences.
3. **Ethical & Legal Awareness** – Understanding the role of policies, regulations, and ethical standards in protecting digital information.
4. **Analytical Skills** – Competence in examining case studies, assessing vulnerabilities, and exploring organizational responses to threats.
5. **Adaptability with Emerging Technologies** – Awareness of how new technologies, including Artificial Intelligence (AI) and Machine Learning (ML), influence modern security practices.
6. **Foundational Technical Literacy** – Basic familiarity with security models, access controls, and network defense strategies that support further study or entry-level applications.

Course Quiz, Assignments and Grading

Assignment Type	% of Final Grade	Description
Weekly Quizzes	30%	Short, low-stakes quizzes to reinforce key concepts from readings and class.
Weekly Assignments	50%	Applied exercises that build week-to-week, introducing case studies and design ideas.
Final Capstone Assignment	20%	Comprehensive project integrating all course topics; demonstrates overall understanding.
Total	**100%**	

Late Assignment Statement:

Assignments are due by 11:59 pm on the posted due date. Late submissions will be accepted up to 48 hours past the deadline with a 10 % deduction per day. Work submitted more than 48 hours after the due date will not be accepted unless prior arrangements have been made with the instructor for extenuating circumstances. Participation in discussions must follow module timelines; late posts may not receive credit.

Grading Rubrics

Quizzes (13 total, 30% of grade)

- Short, multiple-choice/true-false format based on weekly readings and lectures.
- **Grading:** Automatic, based on correct answers.

Assignments (12 total, 50% of grade)

Rubric for Each Assignment (5% each):

Criteria	Excellent (90–100)	Good (80–89)	Developing (70–79)	Needs Improvement (<70)
Understanding of Concept	Shows clear and accurate understanding of the week's topic; applies ideas thoughtfully.	Mostly correct with minor gaps.	Partial understanding; some confusion or missing key details.	Misunderstood the main concept; incomplete or inaccurate.
Application & Examples	Provides relevant, clear, and realistic examples/scenarios.	Examples given but may lack depth.	Minimal examples or loosely related.	No examples, or examples are incorrect.
Clarity & Organization	Well-organized, easy to follow, clear writing/diagram.	Generally organized, a few unclear points.	Hard to follow at times; ideas not fully connected.	Disorganized, unclear, difficult to read.
Completion	Fully meets assignment requirements (length, diagrams, reflections).	Meets most requirements; minor omissions.	Missing some required parts.	Incomplete; large portions missing.

Capstone Project (20% of grade)

Rubric for Capstone (20%):

Criteria	Excellent (90–100)	Good (80–89)	Developing (70–79)	Needs Improvement (<70)
Integration of Course Content	Effectively integrates concepts from all prior assignments (1–12); shows a full "security shield."	Integrates most assignments; minor gaps.	Partial integration; only some assignments reflected.	Little to no integration of course content.
Depth & Insight	Provides thoughtful, creative insights into how security concepts connect.	Solid analysis, but less depth or originality.	Limited insight; mostly restating facts.	Lacks depth; superficial or incomplete.
Practical Application	Shows how concepts apply in real-world contexts (e.g., schools, workplaces, personal security).	Some application to real-world; may lack detail.	Minimal real-world application.	No clear application.

Criteria	Excellent (90–100)	Good (80–89)	Developing (70–79)	Needs Improvement (<70)
Clarity & Professionalism	Report/Slides are clear, organized, visually neat, and professional.	Mostly clear; a few formatting or clarity issues.	Somewhat difficult to follow or unpolished.	Disorganized and unclear presentation.

Course Schedule

Module	Dates	Key Topics & Assignments	Readings
1	Aug 25 – Aug 31	**Introductions** – Welcome, course overview, expectations. **Due Aug 31:** Discussion/IDA: Introduce Yourself	–
2	Sept 1 – Sept 7 (Sept 1 Labor Day – no class)	**What is Security?** – Foundations of information security, the CIA triad, why security matters. **Due Sept 7:** • Quiz 1 • **Assignment 1:** Reflection – What does “security” mean and why is it important?	Ch. 1: Introduction to Information Security
3	Sept 8 – Sept 14	**Threats & Risks** – Common threats, vulnerabilities, and risk concepts. **Due Sept 14:** • Quiz 2 • **Assignment 2:** Threats table – Identify three threats, their impacts, and relevance.	Ch. 2: The Need for Security
4	Sept 15 – Sept 21	**Laws & Ethics** – Policy, legal, and ethical frameworks in security. **Due Sept 21:** • Quiz 3 • **Assignment 3:** Write a short scenario on an ethical/legal issue and reflect on it.	Ch. 3: Legal, Ethical, and Professional Issues
5	Sept 22 – Sept 28	**Security Models** – Access controls, trust models, and secure design. **Due Sept 28:** • Quiz 4 • **Assignment 4:** Create a simple diagram/model for protecting a personal device or home Wi-Fi.	Ch. 4: Security Policy & Planning Ch. 5: Security Models

Module	Dates	Key Topics & Assignments	Readings
6	Sept 29 – Oct 5	**Firewalls & Networks** – Basic network defense, firewalls, and secure architectures. **Due Oct 5:** • Quiz 5 • **Assignment 5:** Sketch a small network with a firewall and explain how it works.	Ch. 6: Security Technologies Ch. 7: Cryptography Basics
7	Oct 6 – Oct 12	**Risk Management** – Strategies for managing risk and building resilience. **Due Oct 12:** • Quiz 6 • **Assignment 6:** Conduct a mini risk assessment of a real-world example (e.g., phone loss, email hack).	Ch. 8: Risk Management
8	Oct 13 – Oct 19	**Review + AI/ML in Security** – Midpoint review and how AI/ML is reshaping security practices. **Due Oct 19:** • Quiz 7 • **Assignment 7:** Reflection – How is AI/ML used in security today? One benefit, one concern.	Instructor-provided article/whitepaper
9	Oct 20 – Oct 26	**Security in Organizations** – Administrative and organizational security functions. **Due Oct 26:** •Quiz 8 • **Assignment 8:** Case note – How can an organization (school, hospital, company) organize its security?	Ch. 9: Physical and Infrastructure Security Ch. 10: Information Security in Organizations
10	Oct 27 – Nov 2	**Privacy & Payment Security** – Protecting personal data, payment systems, HIPAA/FERPA/PCI. **Due Nov 2:** • Quiz 9 • **Assignment 9:** Write a short summary of one privacy/payment regulation (HIPAA, FERPA, PCI DSS).	Ch. 11: Law, Privacy, and Compliance
11	Nov 3 – Nov 9	**Global Security Standards** – U.S., state, and international standards (NIST, ISO, GDPR). **Due Nov 9:** • Quiz 10	Ch. 12: Security Standards & Practices

Module	Dates	Key Topics & Assignments	Readings
		• **Assignment 10:** Comparison chart – Compare two standards (e.g., NIST vs. ISO 27001).	
12	Nov 10 – Nov 16	**Case Studies** – Real-world examples of security breaches and responses. **Due Nov 16:** • Quiz 11 • **Assignment 11:** Case study analysis – What happened, what went wrong, lessons learned.	Instructor-selected case studies; Ch. 13 review
13	Nov 17 – Nov 23	**Emerging Trends** – AI, ML, IoT, biometrics, blockchain, and future directions. **Due Nov 23:** • Quiz 12 • **Assignment 12:** Choose one emerging trend and explain its impact and risks.	Supplemental Readings (Instructor-provided)
14	Nov 24 – Nov 30 (Nov 27 Thanksgiving – no class)	**Final Review + Capstone** – Bringing it all together. **Due Dec 3:** • Quiz 13 • **Capstone Assignment:** Comprehensive security plan integrating all prior assignments.	Review: Ch. 1–13
15	Dec 1 – Dec 3	**All Work Due** – Final submissions accepted until **Dec 3.**	–
16	Dec 4 – Dec 10	**No New Work** – Instructor grading period only.	–

ADA Statement

SRSU Accessibility Services. Sul Ross State University (SRSU) is committed to equal access in compliance with the Americans with Disabilities Act of 1973. It is SRSU policy to provide reasonable accommodations to students with documented disabilities. It is the student's responsibility to initiate a request each semester for each class. Students seeking accessibility/accommodations services must contact Mrs. Mary Schwartze Grisham, LPC, SRSU's Accessibility Services Director or Ronnie Harris, LPC, Counselor, at 432-837-8203 or email mschwartze@sulross.edu or ronnie.harris@sulross.edu. RGC students can also contact Alejandra Valdez, at 830-758-5006 or email alejandra.valdez@sulross.edu. Our office is located on the first floor of Ferguson Hall, room 112, and our mailing address is P.O. Box C122, Sul Ross State University, Alpine. Texas, 79832.

Student Responsibilities Statement

All full-time and part-time students are responsible for familiarizing themselves with the Student Handbook and the Undergraduate & Graduate Catalog and for abiding by the University rules and regulations. Additionally, students are responsible for checking their Sul Ross email as an official form of communication from the university. Every student is expected to obey all federal, state and local laws and is expected to familiarize themselves with the requirements of such laws.

SRSU Distance Education Statement

Students enrolled in distance education courses have equal access to the university's academic support services, such as library resources, online databases, and instructional technology support. For more information about accessing these resources, visit the SRSU website.

Students should correspond using Sul Ross email accounts and submit online assignments through Blackboard, which requires a secure login. Students enrolled in distance education courses at Sul Ross are expected to adhere to all policies pertaining to academic honesty and appropriate student conduct, as described in the student handbook. Students in web-based courses must maintain appropriate equipment and software, according to the needs and requirements of the course, as outlined on the SRSU website. Directions for filing a student complaint are located in the student handbook.

Counseling

Sul Ross has partnered with TimelyCare where all SR students will have access to nine free counseling sessions. You can learn more about this 24/7/365 support by visiting Timelycare/SRSU. The SR Counseling and Accessibility Services office will continue to offer in-person counseling in Ferguson Hall room 112 (Alpine campus), and telehealth Zoom sessions for remote students and RGC students.

Libraries

The Bryan Wildenthal Memorial Library and Archives of the Big Bend in Alpine offer FREE resources and services to the entire SRSU community. Access and borrow books, articles, and more by visiting the library's website, library.sulross.edu/. Off-campus access requires logging in with your LoboID and password. Librarians are a tremendous resource for your coursework and can be reached in person, by email (srsulibrary@sulross.edu), or by phone (432-837-8123).

No matter where you are based, public libraries and many academic and special libraries welcome the general public into their spaces for study. SRSU TexShare Cardholders can access additional services and resources at various libraries across Texas. Learn more about the TexShare program by visiting library.sulross.edu/find-and-borrow/texshare/ or ask a librarian by emailing srsulibrary@sulross.edu.

Mike Fernandez, SRSU Librarian, is based in Eagle Pass (Building D-129) to offer specialized library services to students, faculty, and staff. Utilize free services such as InterLibrary Loan (ILL), ScanIt, and Direct Mail to get materials delivered to you at home or via email.

Academic Integrity

Students in this class are expected to demonstrate scholarly behavior and academic honesty in the use of intellectual property. Students should submit work that is their own and avoid the temptation to engage in behaviors that violate academic integrity, such as turning in work as original that was used in whole or part for another course and/or professor; turning in another person's work as one's own; copying from professional works or internet sites without citation; collaborating on a course assignment, examination, or quiz when collaboration is forbidden. Students should also avoid using open AI sources ***unless permission is expressly given*** for an assignment or course. Violations of academic integrity can result in failing assignments, failing a class, and/or more serious university consequences. These behaviors also erode the value of college degrees and higher education overall.

Classroom Climate of Respect

Importantly, this class will foster free expression, critical investigation, and the open discussion of ideas. This means that all of us must help create and sustain an atmosphere of tolerance, civility, and respect for the viewpoints of others. Similarly, we must all learn how to probe, oppose and disagree without resorting to tactics of intimidation, harassment, or personal attack. No one is entitled to harass, belittle, or discriminate against another on the basis of race, religion, ethnicity, age, gender, national origin, or sexual preference. Still, we will not be silenced by the difficulty of fruitfully discussing politically sensitive issues.

Supportive Statement

I aim to create a learning environment for my students that supports various perspectives and experiences. I understand that the recent pandemic, economic disparity, and health concerns, or even unexpected life events may impact the conditions necessary for you to succeed. My commitment is to be there for you and help you meet the learning objectives of this course. I do this to demonstrate my commitment to you and to the mission of Sul Ross State University to create a supportive environment and care for the whole student as part of the Sul Ross Familia. If you feel like your performance in the class is being impacted by your experiences outside of class, please don't hesitate to come and talk with me. I want to be a resource for you.