TEXAS A&M UNIVERSITY
SAN ANTONIO

CSEC 2325: Hardware Security

Instructor Information

Instructor: Dr. Robert Jones
Email/Text: rtjones@tamu.edu / +1 867-322-1700 *(this is a Canadian number; be advised)*
Class Meeting Time: Tuesdays/Thursdays 1100 - 1215
Location: Zoom
Link: https://tamusa.zoom.us/j/82145133686?pwd=9FmByeoehFnI68eryKtJInwBHSIDK1.1 (code Spring25!)
Office Hours: By appointment (physical or zoom available) SciTech/STEM 211U

Textbook/Materials

All textbook material for this class are being provided as OER and will be free. Students will want to set aside roughly $25 for this class to purchase materials for the “Hands-On Hardware Demo and Write-Up” due 3/27/25.

Grading Scale

A: 900-1000 points
B: 800-899 points
C: 700-799 points
D: 600-699 points
F: Below 600 points

Course Components

Assignment	Points	Proposed Due Date
Census Assignment	50	01/28/25
Threat Modeling Assignment	200	02/27/25
Midterm Exam	100	03/04/25
Hands-On Hardware Demo and Write-Up	250	03/27/25
Hardware Security Design Proposal	200	04/17/25
Final Exam	100	05/09/25
Pop Up Assignments/Quizzes	100	Ongoing

Learning Outcomes

By the end of this course, students should be able to:

- Analyze and evaluate potential security threats in hardware components, including System on Chip (SoC) and Printed Circuit Boards (PCBs), and recommend effective mitigation strategies.
- Demonstrate the ability to perform and interpret results from side-channel attacks, hardware malware analysis, and other physical attack methodologies.

- Design and implement basic secure hardware solutions, incorporating countermeasures such as Trusted Platform Modules (TPMs), tamper-proofing, and encryption techniques.
- Assess hardware security risks within the supply chain and propose strategies for verifying component authenticity and ensuring trust in manufacturing processes.
- Examine and articulate the ethical and legal implications of hardware security vulnerabilities and countermeasures, using real-world case studies to support analysis.

Weekly Schedule

Date	Day of Week	Topic
1/21/2025	T	Bad Weather Day
1/23/2025	R	Welcome, Syllabus Overview, Course Structure
1/28/2025	T	Introduction to Hardware Security and Challenges
1/30/2025	R	Basics of Hardware Components
2/4/2025	T	Cryptographic Hardware Fundamentals
2/6/2025	R	Security in SoC
2/11/2025	T	Case Studies in SoC Security
2/13/2025	R	Security in Printed Circuit Boards (PCBs)
2/18/2025	T	PCB Reverse Engineering
2/20/2025	R	Threat Models and Attack Surfaces
2/25/2025	T	Practical Threat Identification
2/27/2025	R	Hardware Malware
3/4/2025	T	Analysis of Hardware Malware
3/6/2025	R	Physical Attacks on Hardware
3/18/2025	T	Side-Channel Attack Demonstration
3/20/2025	R	Countermeasures Against Physical Attacks
3/25/2025	T	Implementing Countermeasures
3/27/2025	R	Secure Hardware Development
4/1/2025	T	Trusted Platform Modules (TPMs)
4/3/2025	R	Hardware/Practical Supply Chain Security
4/8/2025	T	Emerging Hardware Security Threats
4/10/2025	R	Quantum Computing and Hardware Security
4/15/2025	T	Trusted Execution Environments (TEEs)
4/17/2025	R	Attacking TEEs
4/22/2025	T	Hardware Forensics
4/24/2025	R	Forensic Tools and Techniques
4/29/2025	T	Ethics in Hardware Security
5/1/2025	R	Legal Frameworks in Hardware Security
5/5/2025	T	Course Wrap-Up and Next Steps
5/9/2025	F	Final Exam Due

Course Policies

Weekly Assignment Availability and Due Dates: You will receive a minimum of 1 week to complete all assignments. All assignments will be submitted in Blackboard. Due dates for assignments will be clearly indicated in Blackboard. Assignments, unless noted, should be submitted as ONE DOCUMENT in docx/pdf format unless otherwise noted.

Deadline/Late Policy: This assignment is to be completed and submitted through Blackboard no later than the deadline/due-date indicated on the Blackboard. Contact your Instructor immediately using the Blackboard Inbox or by email if you require any assistance. If for technical or personal reasons, you miss the deadline/due date, you may submit the assignment up until, but no later than, the late submission window. Assignments are not accepted for any reason after the late submission window and there are no makeup assignments. Missing assignments are recorded as a zero grade. If you miss the due date, even by a minute for technical or personal reasons you are late. Send your Instructor a message through Blackboard Inbox on or before the due/deadline if you need to get assistance so there is time to respond and for you to take the appropriate actions in order to complete and submit the assignment. Students are expected to continue to work diligently to complete any assignment while in communication with the Instructor.

Late work will be penalized 10% per day and will not be accepted after 5 days.

If you miss more than 2 total assignment due dates entirely without contacting the instructor prior to the closing of the late window for the second assignment, the instructor reserves the right to drop you from the course.

When Work Will be Graded: Work will be graded within 1 week after it is due and the majority of students have completed the assignment. Even if you turn in something the day it is assigned, do not expect a grade before the assignment is actually due. During certain circumstances such as midterm grade posting or other similar events, the instructor may grade work ahead of this schedule to improve student visibility to grades during key periods.

Grades: Check your Grades often in Blackboard. Each student is expected to review his or her graded assignments promptly each week. Changes to a student's grade will only be made upon request made through Blackboard Inbox within 1 week after an assignment is graded, and only if the individual student provides clear evidence that is accepted by the Instructor as to why their answer should be accepted and the grade changed. Discussing grades or other academic concerns on discussion boards or group messages in this course is not permitted.

Drop Grade for Course Evaluation: If you complete a course evaluation in the class you may drop any one assignment, past or future, from the course. The total amount of points that you will be graded on changes from 1000 to whatever is left, and your grade will be calculated based on the percentage of points you have compared to your revised, lower total after a grade drop. You may initiate this grade drop when the course evaluation period opens and the instructor posts a special 0 point assignment.

Incomplete Grades: There are very few situations in which I will ever consider giving out an incomplete grade. One exception is military deployment and another is life threatening illness. You must be passing at the time of requesting an incomplete grade. If you feel that your situation warrants this consideration, contact me as soon as possible.

Student responsibility to contact instructor: There is always a lot going on in the world and I am here to help you, but please help me help you! Keep me posted if you need additional assistance, resources, or have something going on that will factor into you being successful in this class. I would rather hear from you more often than not often enough.

University Wide - IMPORTANT POLICIES AND RESOURCES

Academic Accommodations for Individuals with Disabilities: Texas A&M University-San Antonio is committed to providing all students with reasonable access to learning opportunities and accommodations in accordance with The Americans with Disabilities Act, as amended, and Section 504 of the Rehabilitation Act. If you experience barriers to your education due to a disability or think you may have a disability, Disability Support Services is located in the Central Academic Building, Suite 210. You can also contact us via phone at (210) 784-1335, visit us https://www.tamusa.edu/Disability-Support-Services/index.html or email us

at **dss@tamusa.edu**. Disabilities may include, but are not limited to, attentional, learning, mental health, sensory, physical, or chronic health conditions. All students are encouraged to discuss their disability-related needs with Disability Support Services and their instructors as soon as possible.

Academic Learning Center: The Academic Learning Center provides free course-based tutoring to all currently enrolled students at Texas A&M University-San Antonio. Students wishing to work with a tutor can make appointments through the Brainfuse online tutoring platform. Brainfuse can be accessed in the *Tools* section of Blackboard. You can contact the Academic Learning Center by emailing tutoring@tamusa.edu, calling (210) 784-1307, or visiting the Central Academic Building, room 202.

Counseling/Mental Health Resources: As a college student, there may be times when personal stressors interfere with your academic performance and negatively impact your daily functioning. If you are experiencing emotional difficulties or mental health concerns, support is available to you through the Student Counseling Center (SCC). To schedule an appointment, call 210-784-1331 or visit Madla 120.

All mental health services provided by the SCC are free and confidential (as the law allows). The Student Counseling Center provides brief individual and group therapy, crisis intervention, consultation, case management, and prevention services. For more information on SCC services visit tamusa.edu/studentcounseling

Crisis support is available 24/7 by calling the SCC at 210-784-1331 (after-hours select option '2').

Additionally, the TELUS Student Support App provides a variety of mental health resources to including support for in the moment distress, an anonymous peer to peer support network, mental health screenings, podcasts, and articles to improve your mental wellbeing.

Emergency Preparedness: JagE Alert is Texas A&M University-San Antonio's mass notification. In the event of an emergency, such as inclement weather, students, staff and faculty, who are registered, will have the option to receive a text message, email with instructions and updates. To register or update your information visit: https://tamusa.bbcportal.com/.

More information about Emergency Operations Plan and the Emergency Action Plan can be found here: https://www.tamusa.edu/about-us/emergency-management/.

Download the SafeZone App (https://safezoneapp.com/) for emergencies or call (210) 784-1911. Non-Emergency (210) 784-1900.

Financial Aid and Verification of Attendance: According to the following federal regulation, 34 CFR 668.21:

U.S. Department of Education (DoE) Title IV regulation, a student can only receive Title IV funds based on Title IV eligibility criteria which include class attendance. If Title IV funds are disbursed to ineligible students (including students who fail to begin attendance), the institution must return these funds to the U.S. DoE within 30 days of becoming aware that the student will not or has not begun attendance. Any student receiving federal financial aid who does not attend by the census date will have their financial aid terminated and returned to the DoE. Please note that any student who stops attending at any time during the semester, a Care report will be submitted, and you will possibly be dropped from the class. Your financial aid may have to be recalculated and a portion of your federal aid may have to be returned to the DoE.

Writing, Language, and Digital Composing Center: The Writing, Language, and Digital Composing Center supports graduate and undergraduate students in all three colleges as well as faculty and staff. Tutors work with students to develop reading skills, prepare oral presentations, and plan, draft, and revise their written assignments. Our language tutors support students enrolled in Spanish courses and students composing in Spanish for any assignment. Our digital studio tutors support students working on digital projects such as eportfolios, class presentations, or other digital multimedia projects. Students can schedule appointments through JagWire under the Student Services tab. Click on "Writing, Language, and Digital Composing Center" to make your appointment. The Center offers face-to-face, synchronous online, and asynchronous digital appointments. More information about what services we offer, how to make an appointment, and how to access your appointment can be found on our website at https://www.tamusa.edu/academics/.

Meeting Basic Needs: Any student who has difficulty affording groceries or accessing sufficient food to eat every day or who lacks a safe and stable place to live, and believes this may affect their performance in the course, is urged to submit a CARE referral (https://www.tamusa.edu/university-policies/Student-Rights-and-Responsibilities/file-a-report.html) for support. Furthermore, please notify the professor if you are comfortable in doing so. This will enable them to direct you to available resources.

Military Affairs: Veterans and active-duty military personnel are welcomed and encouraged to visit the Office of Military Affairs for any question involving federal or state VA Education Benefits. Visit the Patriots' Casa building, room 202, or to contact the Office of Military Affairs with any questions at military.va@tamusa.edu or (210)784-1397.

Religious Observances: Texas A&M University-San Antonio recognizes the diversity of faiths represented among the campus community and protects the rights of students, faculty, and staff to observe religious holidays according to their tradition. Under the policy, students are provided an opportunity to make up any examination, study, or course work requirements that may be missed due to a religious observance provided they notify their instructors before the end of the second week of classes for regular session classes.

The Six-Drop Rule: Students are subject to the requirements of Senate Bill (SB) 1231 passed by the Texas Legislature in 2007. SB 1231 limits students to a maximum of six (6) non-punitive course drops (i.e., courses a student chooses to drop) during their undergraduate careers. A non-punitive drop does not affect the student's GPA. However, course drops that exceed the maximum allowed by SB 1231 will be treated as "F" grades and will impact the student's GPA.

Statement of Harassment and Discrimination: Texas A&M University-San Antonio is committed to the fundamental principles of academic freedom, equal opportunity, and human dignity. To fulfill its multiple missions as an institution of higher learning, A&M-San Antonio encourages a climate that values and nurtures collegiality and the uniqueness of the individual within our state, nation, and world. All decisions and actions involving students and employees should be based on applicable law and individual merit. Texas A&M University-San Antonio, in accordance with applicable federal and state law, prohibits discrimination, including

harassment, on the basis of race, color, sex, religion, national origin, age, disability, genetic information, veteran status, sexual orientation, gender identity, gender expression, or pregnancy/parenting status.

Individuals who believe they have experienced harassment or discrimination prohibited by this statement are encouraged to contact the appropriate offices within their respective units.

Texas A&M University-San Antonio faculty are committed to providing a safe learning environment for all students and for the university as a whole. If you have experienced any form of sex- or gender-based discrimination or harassment, including sexual assault, sexual harassment, domestic or dating violence, or stalking, know that help and support are available. A&M-San Antonio's Title IX Coordinator can support those impacted by such conduct in navigating campus life, accessing health and counseling services, providing academic and housing accommodations, and more. The university strongly encourages all students to report any such incidents to the Title IX Coordinator. Please be aware that all A&M-San Antonio employees (other than those designated as confidential resources such as counselors and trained victim advocates) are required to report information about such discrimination and harassment to the university. This means that if you tell a faculty member about a situation of sexual harassment, sexual violence, or other related misconduct, the faculty member must share that information with the university's Title IX Coordinator (titleix@tamusa.edu, 210-784-2061, CAB 439K). If you wish to speak to a confidential employee who does not have this reporting requirement, you can contact the Student Counseling Center at (210) 784-1331 or visit them in Madla 120.

Pregnant/Parenting Students: Texas A&M-San Antonio does not require a pregnant or parenting student, solely because of that status or issues related to that status, to (1) take a leave of absence or withdraw from their degree or certificate program; (2) limit the student's studies; (3) participate in an alternative program; (4) change the student's major, degree, or certificate program; or (5) refrain from joining or cease participating in any course, activity, or program at the University. The university will provide such reasonable accommodations to pregnant students as would be provided to a student with a temporary medical condition that are related to the health and safety of the student and the student's unborn child. These could include maintaining a safe distance from substances, areas, and activities known to be hazardous to pregnant individuals and their unborn child; excused absences because of illness or medical appointments; modified due dates for assignments; rescheduled tests/exams; taking a leave of absence; and being provided access to instructional materials and video recordings of lectures for excused absences, if these would be provided to any other student with an excused absence. Pregnant/parenting students are encouraged to contact the Title IX Coordinator with any questions or concerns related to their status (titleix@tamusa.edu; 210-784-2061; CAB 439K).

Texas A&M-San Antonio has also designated the Title IX Coordinator as the liaison officer for current or incoming students who are the parent or guardian of a child younger than 18 years of age. The Title IX Coordinator can provide students with information regarding support services and other resources.

Students' Rights and Responsibilities: The following statement of students' rights and responsibilities is intended to reflect the philosophical base upon which University Student Rules are built. This philosophy acknowledges the existence of both rights and responsibilities, which is inherent to an individual not only as a student at Texas A&M University-San Antonio but also as a citizen of this country.

Students' Rights

A student shall have the right to participate in a free exchange of ideas, and there shall be no University rule or administrative rule that in any way abridges the rights of freedom of speech, expression, petition and peaceful assembly as set forth in the U.S. Constitution.

Each student shall have the right to participate in all areas and activities of the University, free from any form of discrimination, including harassment, on the basis of race, color, national or ethnic origin, religion, sex,

disability, age, sexual orientation, gender identity, gender expression, and pregnancy/parenting or veteran status in accordance with applicable federal and state laws.

A student has the right to personal privacy except as otherwise provided by law, and this will be observed by students and University authorities alike.

Each student subject to disciplinary action arising from violations of university student rules shall be assured a fundamentally fair process.

Students' Responsibilities

A student has the responsibility to respect the rights and property of others, including other students, the faculty, and administration.

A student has the responsibility to be fully acquainted with the published University Student Rules found in the Student Handbook, Student Code of Conduct, on our website, and University Catalog, and to comply with them, as well as with federal, state, and local laws.

A student has the responsibility to recognize that student actions reflect upon the individuals involved and upon the entire University community.

A student has the responsibility to recognize the University's obligation to provide a safe environment for learning.

A student has the responsibility to check their university email for any updates or official university notifications.

We expect that students will behave in a manner that is dignified, respectful, and courteous to all people, regardless of sex, ethnic/racial origin, religious background, sexual orientation, or disability. Conduct that infringes on the rights of another individual will not be tolerated.

Students are expected to exhibit a high level of honesty and integrity in their pursuit of higher education. Students engaging in an act that violates the standards of academic integrity will find themselves facingacademic and/or disciplinary sanctions. Academic misconduct is any act, or attempt, which gives an unfair advantage to the student. Additionally, any behavior specifically prohibited by a faculty member in the course syllabus or class discussion may be considered as academic misconduct. For more information on academic misconduct policies and procedures please review the Student Code of Conduct (https://www.tamusa.edu/university-policies/student-rights-and-responsibilities/documents/Student-Handbook-2022-23.pdf) or visit the resources available in the OSRR website (https://www.tamusa.edu/university-policies/student-rights-and-responsibilities/academic-integrity.html).

Use of artificial intelligence (AI) tools, including ChatGPT, is permitted in this course for students who wish to use them. To adhere to our scholarly values, students must cite any AI-generated material that informed their work (this includes in-text citations and/or use of quotations, and in your reference list). Using an AI tool to generate content without proper attribution qualifies as academic dishonesty and violates Texas A&M-San Antonio's standards of academic integrity.