STATE UNIVERSITY OF NEW YORK
COLLEGE OF TECHNOLOGY
CANTON, NEW YORK

MASTER SYLLABUS

CITA305 – Hardware Security

For available course numbers, contact the Registrar's Office at registrar@canton.edu

CIP Code: 15.1203

For assistance determining CIP Code, please refer to this webpage
https://nces.ed.gov/ipeds/cipcode/browse.aspx?y=55
or reach out to Sarah Todd at todds@canton.edu

Created by: Stacia Smith

School: Canino School of Engineering
Department: Decision and Graphic Media Systems
Implementation Semester/Year: Fall 2026

A. TITLE: Introduction to Hardware Security

B. COURSE NUMBER: CITA305

C. CREDIT HOURS (Hours of Lecture, Laboratory, Recitation, Tutorial, Activity):

# Credit Hours per Week	**3**
# Lecture Hours per Week	**3**
# Lab Hours per Week	**0**
Other per Week	**0**

D. WRITING INTENSIVE COURSE:

Yes	
No	X

E. GER CATEGORY:

Does course satisfy a GER category(ies)? If so, please select all that apply.

[1-2] Communication	
[3] Diversity: Equity, Inclusion & Social Justice	
[4] Mathematics & Quantitative Reasoning	
[5] Natural Science & Scientific Reasoning	
[6] Humanities	
[7] Social Sciences	
[8] Arts	
[9] US History & Civic Engagement	
[10] World History & Global Awareness	
[11] World Languages	

F. SEMESTER(S) OFFERED:

Fall	
Spring	
Fall and Spring	X

G. COURSE DESCRIPTION:

This course introduces students to the essential concepts and techniques of hardware security, focusing on the design and protection of hardware systems against vulnerabilities and attacks. Students will explore the bottom three layers of the OSI model and learn how they can be exploited or compromised through physical attacks. Key topics include secure hardware design, secure boot processes, and the prevention of tampering and unauthorized access. Emphasis will be placed on understanding the physical layer of devices, security mechanisms, and methods for detecting hardware faults or failures that could lead to system manipulation.

H. PRE-REQUISITES: CITA220 Data Communications and Network Technology
CO-REQUISITES: N/A

I. STUDENT LEARNING OUTCOMES:

Course Student Learning Outcome [SLO]	Program Student Learning Outcome [PSLO]	GER	ISLO & Subsets
a. Discuss principles of secure hardware design and implementation	Documents & Information		2 [CA], 5
c. Discuss Tamper resistance and anti-counterfeit measures	Documents & Information		2 [CA], 5
d. Identify secure boot processes and trusted computing environments	Documents & Information		2 [CA], 5
e. Describe methods for detecting hardware faults and anomalies	Documents & Information		2 [CA], 5

KEY	**Institutional Student Learning Outcomes** **[ISLO 1 – 5]**
ISLO #	**ISLO & Subsets**
1	**Communication Skills** Oral [O], Written [W]
2	**Critical Thinking** *Critical Analysis [CA], Inquiry & Analysis [IA] , Problem Solving [PS]*
3	**Foundational Skills** *Information Management [IM], Quantitative Lit, /Reasoning [QTR]*
4	**Social Responsibility** *Ethical Reasoning [ER], Global Learning [GL],* *Intercultural Knowledge [IK], Teamwork [T]*
5	**Industry, Professional, Discipline Specific Knowledge and Skills**

J. APPLIED LEARNING COMPONENT:

Yes	X
No	

If yes, select [X] one or more of the following categories:

Non-Clinical Practicum	X	Community Service	
Internship		Civic Engagement	
Clinical Practicum		Creative Works/Senior Project	
Practicum		Research	
Service Learning		Entrepreneurship [program, class, project]	

K. TEXTS: Various online resources such as SUNY Canton Library Books24x7

L. REFERENCES: N/A

M. EQUIPMENT: Technology Enhanced Classroom

N. GRADING METHOD: A-F

O. SUGGESTED MEASUREMENT CRITERIA/METHODS:

P. DETAILED COURSE OUTLINE:

1. Introduction to Hardware Security
   - A. Overview of computer hardware systems
     - o Overview of network device hardware
   - B. Introduction to hardware security attacks and threats
     - o Historical incidents of hardware vulnerabilities
   - C. Security vs. reliability vs. performance trade-offs

2. Fundamentals of Hardware Design
   - A. Basics of digital circuits and components
   - B. Introduction to embedded systems and microcontrollers
   - C. Introduction to programmable hardware

3. Hardware Vulnerabilities and Threat Models
   - A. Threat analysis in hardware systems
   - B. Physical tampering and reverse engineering

4. Hardware Security Standards and Guidelines
   - A. Security Standards for hardware
   - B. Hardware security certification processes

5. Secure Hardware Design Principles & Countermeasures
   - A. Tamper-resistant and tamper-evident design
   - B. Hardware-based root of trust
   - C. Secure boot and trusted platform modules (TPM)

Q. LABORATORY OUTLINE: N/A