CSEC - 3757 - Critical Infrastructure, Wireless, and Mobile Security

05. UG New Course No Special Designation

Due Dates and Resources

If you have questions or need assistance in filling out this proposal form, you may contact the Office of Curriculum.

Deadlines for curriculum can be found:

- Curriculum SharePoint
- Curriculum Website
- Procedural Calendar
- On your Curriculog dashboard under 'My Upcoming Events'

Resources for curriculum can be found:

- Originator How-To Guide
- Curriculum SharePoint

In order to meet the deadline, this proposal must be on the *Substantive College/School Level Review* step on or before the listed due date.

Directions for Form

General Instructions and Information

You may collapse individual sections of this form by clicking the arrow or "V" icon to the right of the section title.
All fields that are marked with an asterisk (*) are required.
Each section may have additional directions attached. Please follow all instructions.

Note: Proposals that are incomplete or filled out incorrectly will be returned to the originator.

INSTRUCTIONS FOR CREATING A NEW COURSE

Fill out all of the below fields.
Launch the proposal.
Approve the proposal.

Use the checkmark icon on the right of the screen to approve the proposal.

This form **SHOULD** be used only for the following:

- Creating a new course without a special designation (General Studies, Service Learning, Ethnic Studies & Social Justice, or Senior Experience).

This form **SHOULD NOT** be used for the following:

- Creating a new course with a special designation (General Studies, Service Learning, Ethnic Studies & Social Justice, or Senior Experience).
- Converting an omnibus or individual variable topic course into a regular course. Please use form #4 to complete this request.
- Making modifications to any course
- Creating or modifying graduate courses.

Part I: Department and Originator Information

College/School:* College of Aerospace, Computing, Engineering, and Design

Department:* Department of Computer Sciences

Name of Proposal Originator:* Klaus Streicher

Email of Proposal Originator:* Nstreich@msudenver.edu

Part II: Curriculum Proposal Justification and Resource Implication

Justification and resource implication for proposed curriculum action:*

CSEC 3757 Critical Infrastructure, Wireless, & Mobile Security:

Wireless and mobile systems have become ubiquitous, and they can have significant impacts on system security and operation, especially due to the relative openness and erratic nature of the wireless environment. The dynamic and inconsistent connectivity of wireless requires unique approaches to networking in everything from user identification and authentication to message integrity and cipher synchronization.

Industrial Control Systems (ICSs) and Supervisory Control and Data Acquisition (SCADA) systems are at the core of many critical infrastructure sectors in the United States. These systems use common components and are frequently interconnected; vulnerabilities can cause significant problems to their owner operators. Many ICSs have critical national security impacts, such as the electrical power grid as well as dams and water treatment facilities. Cyber operators should have knowledge of the attack and defense of ICSs.

This course will serve as a core course and supports NSA CAE-CO & ABET learning outcomes for the proposed CSEC degree.

Related Curriculum Proposals:* https://msudenver.curriculog.com/proposal:11729/form

According to the Undergraduate Curriculum Manual, it is the responsibility of both the originator as well as each level of review to consider potential overlap and curriculum conflict. Any potential overlap or conflict with existing curriculum should be reviewed, and the impacted department(s) should be requested to provide a letter of notification or support, depending on the circumstances.

Attach documentation that supports affected Departments were notified and/or provided support of the proposed changes in the Proposal Toolbox by clicking on the paperclip icon on the right side of the form.

Please Confirm That:* ☑ I, the originator of this proposal, have completed the necessary due diligence to review this proposal for any potential overlap and/or conflict with existing curriculum. Any departments identified as having potential overlap and/or conflicts have been contacted and a letter of notification and/or a letter of support has been obtained.

Part III: Course Information

Is the identified course prefix a new course prefix? * ☑ Yes ☐ No

Prefix:* CSEC

Course Number:* 3757

Course Title:* Critical Infrastructure, Wireless, and Mobile Security

Transcript/Banner Course Title:* ICS, Wireless, & Mobile Sec

Course Type:* Computer Security

CIP Code: 11.1003

Please check all that apply from the selections below. You may select more than one option if applicable.

Check All that Apply:*
- ☑ Required for Major
- ☐ Required for Minor
- ☐ Required for Concentration
- ☐ Required for Certificate
- ☑ Elective
- ☐ Specified Elective

To receive Title IV financial aid funds, all institutions of higher education must comply with the federal definition of a credit hour. The Higher Learning Commission requires institutions to maintain policies and procedures for verifying compliance with this definition.

Federal Credit Hour Definition: *A credit hour is an amount of work represented in intended learning outcomes and verified by evidence of student achievement that is an institutionally-established equivalency that reasonably approximates not less than:*
(1) one hour of classroom or direct faculty instruction and a minimum of two hours of out-of- class student work each week for approximately fifteen weeks for one semester or trimester hour of credit, or ten to twelve weeks for one quarter hour of credit, or the equivalent amount of work over a different amount of time; or (2) at least an equivalent amount of work as required in paragraph (1) of this definition for other activities as established by an institution, including laboratory work, internships, practica, studio work, and other academic work leading toward to the award of credit hours. 34CFR 600.2 (11/1/2010)

Credits:* 4

Distribution of Credits:* 4 + 0

Schedule Type(s):* Lecture

Grade Mode(s):* Letter

Face-to-Face or Equivalent Hours per course

Consult Appendix B and C of the Curriculum Manual to determine the hours for the course

Lecture:	50	**Lab:**	
Internship:		**Practicum:**	
Other Hours:		**Additional Student Work Hours:**	120

Please answer yes or no to the below questions. If you answer yes to any of the questions, please fill out the related field on the right.

A specified repeatable course is a course that allows a student to repeat the course either in its entirety or for a certain identified total number of credit hours. If you decide to make your course repeatable, please specify either how many times a student can repeat the course for credit, or for the total number of credits they can receive.

Is this course a specified repeatable course?* (•) No ( ) Yes

If yes, indicate specified repeatable number of credits and/or repeats allowed:

Is this course a variable topics umbrella course?* (•) No ( ) Yes

If yes, indicate variable topic number of credits and/or repeats available:

A crosslisting is when a course is made available under additional prefixes for students in other programs.

An equivalency is when two courses are coded in Banner to be equal to each other.

Generally equivalencies are used when an old, archived course is needed to be equal to a new course. Crosslistings are used for all active courses. Supporting documentation should be included to demonstrate approval for crosslistings.

Are there course equivalencies?* (•) No ( ) Yes

If yes, list all equivalent courses in alphabetical order:

Will this course be requesting a crosslisting with any other prefix(es)?* (•) No ( ) Yes

If yes, list all crosslistings in alphabetical order:

Registration Restrictions

Program:

Major:

Level: Undergraduate

Class:

Student Attribute:

The following fields will allow you to attach prerequisites, corequisites, or prerequisites or corequisites to your course. Please specify if you want and of these prerequisites, corequisites, or prerequisites or corequisites Banner enforced.

Banner enforcement means that the requirement will be enforced when the student attempts to register for a course. If you do not Banner enforce the requirement, the system will not check the student's record for the requirement to be met.

Please also indicate the minimum passing grade.

Prerequisite(s):	CS 3700
Banner Enforced Prerequisite(s):	CS 3700
Minimum Passing Grade for Banner Enforced Prerequisite(s):	C- or T
Corequisite(s):	
Banner Enforced Corequisite(s):	
Prerequisite(s) or Corequisite(s):	
Banner Enforced Prerequisite(s) or Corequisite(s):	
Minimum Passing Grade for Banner Enforced Prerequisite(s) or Corequisite(s):	

Part III: Course Information, continued

Catalog Course Description:* Students address the security challenges of three key areas: wireless protocols, mobile devices, and industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems from a critical infrastructure perspective. They explore vulnerabilities and security mechanisms in wireless networks, assess the risks associated with mobile devices, and examine the unique requirements for securing ICS and SCADA systems. Through theoretical study and practical application, students practice implementing effective security strategies across these diverse and dynamic environments.

The note field DOES show up in the course listing in the university catalog. A note should be made in specific instances where additional information about a course needs to be conveyed to students. The most common reasons for adding a note are:

The course is crosslisted Example: ***(Note: Credit will be granted for only one prefix.)***
Variable credit courses Example: ***(Note: Variable Credit)***
A course is repeatable Example: ***(Note: This course may be repeated up to 3 times under different topics)*** **OR** ***(Note: This course is repeatable for a maximum of six semester hours)***
If a student cannot take two courses and earn credit for both Example: ***(Note: Students cannot earn credit for XXX1234 and XXX2345)***

Note:

Lab Fees: **Field Trips:**

Part III: Course Information, continued

The following section is the course content. You must adhere to the following format for each section:

Required reading: **Please list materials in preferred citation style (eg. MLA, APA, etc.).**

List each material in this format. If there are multiple materials please format them in a bullet or list style

Specific Measurable Student Behavioral Learning Objectives: **Please list the SBLOs in your preferred numbering or bulleting style. Start section with: Upon completion of this course, the student should be able to:.**
Detailed Outline of Course Content or Outline of Field Experience/Internship: **Please list the course outline in your preferred numbering or bulleting style. It is recommended that you use a numbering format for this field.**
Evaluation of Student Performance: **Please list the evaluation of student performance in your preferred numbering or bulleting style.**

You must use the numbering list feature within the toolbar above each field. Right click on a number in the list and select "Numbered List Properties" to change the numbering style. Please maintain consistency in the selected numbering or bulleting styles.

Required reading and other materials will be equivalent to:*

- Simpson, P. J. (2021). *Practical Industrial Cybersecurity: ICS, SCADA, and PLC Cybersecurity*. IT Governance Publishing.
- Kukushkin, A. 2018. *Introduction to Mobile Network Engineering: GSM, 3G-WCDMA, LTE and the Road to 5G*. John Wiley & Sons.
- James Forshaw. 2017. *Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation*. No Starch Press, San Francisco, CA, 336 pages. ISBN: 978-1-59327-750-5.

Specific, Measurable Student Behavioral Learning Objectives:*

Upon completion of this course, students should be able to:

1. Describe unique security and operational attributes in the wireless environment and their effects on network communication guarantees and protections.
2. Demonstrate knowledge of common vulnerabilities and use of available tools.
3. Describe effective (and ineffective) mechanisms for protecting commonly deployed wireless and mobile networks and corresponding protocols that are employed in these systems, including wireless link and infrastructure components.
4. Describe the components of ICS systems and how they are programmed.
5. Describe the different network protocols used in the operation of ICS and SCADA systems and their security vulnerabilities.
6. Use industry standard software tools to aid in analysis of ICS systems at a compliance level.

Detailed Outline of Course Content (Major Topics and Subtopics) or Outline of Field Experience/Internship *

1. Stream and Block Ciphers and Security Protocols in Wireless Networks
    1. Overview of Stream Ciphers (e.g., RC4, A5/1)
    2. Overview of Block Ciphers (e.g., AES, DES)
    3. Key Properties: Confidentiality, Integrity, Authentication, Non-repudiation
    4. Wireless Security Protocols: WEP, WPA/WPA2/WPA3, 802.1X, EAP
    5. Known Limitations and Vulnerabilities: Weak Key Management, Replay Attacks, Key Reinstallation Attacks (KRACK)
    6. Comparative Analysis of Ciphers and Protocols in Different Wireless Context
2. Security Implementations in Different Wireless Systems
    1. GSM Security: A5/1, A5/2, A5/3 Ciphers, SIM Authentication
    2. LTE Security: EPS-AKA Protocol, NAS and AS Layer Security, IPsec
    3. WiFi Security: WPA2-Personal, WPA2-Enterprise, WPA3, WPS Vulnerabilities
    4. Bluetooth Security: Secure Simple Pairing, BLE Security, KNOB Attack Vulnerabilities
    5. RFID Security: Cryptographic Protocols, Physical Layer Attacks (e.g., Eavesdropping, Skimming)
3. Mobile Identifiers and Registration, Device/User Tracking, and Anti-Tracking Measures
    1. Types of Mobile Identifiers: IMSI, IMEI, MSISDN, MAC Address
    2. Registration Procedures in Mobile Networks (GSM, LTE, 5G)
    3. Device and User Tracking Techniques: Passive Monitoring, Active Probing
    4. Anti-Tracking Measures: IMSI Catcher Detection, Randomization of MAC Addresses, Signal Obfuscation
    5. Privacy Enhancements in 5G: Subscriber Privacy, SUPI and SUCI
4. Availability Issues in Wireless Networks
    1. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks in Wireless Networks
    2. Jamming Attacks: Types (Spot, Sweep, Barrage), Detection, and Mitigation
    3. Interference Issues: Co-Channel and Adjacent Channel Interference, Mitigation Techniques
    4. Network Congestion and Overload Scenarios
    5. Failover and Redundancy Mechanisms in Wireless Networks
5. Programmable Logic Controllers (PLCs)

1. Introduction to PLCs: Architecture and Functionality
2. Common PLC Programming Languages (e.g., Ladder Logic, Function Block Diagram)
3. Security Challenges: Unauthorized Access, Code Injection, PLC Rootkits
4. Best Practices for Securing PLCs: Access Control, Regular Patching, Network Segmentation

6. Supervisory Control and Data Acquisition (SCADA) Systems
    1. SCADA System Components: RTUs, HMIs, Communication Networks
    2. Common SCADA Architectures: Centralized vs. Distributed
    3. Security Challenges: Remote Access Vulnerabilities, Lack of Encryption, Insider Threats
    4. Security Controls for SCADA Systems: Firewalls, VPNs, Anomaly Detection
    5. Incident Response and Recovery in SCADA Environments
7. Distributed Control System (DCS)
    1. DCS Overview: Architecture and Operational Models
    2. Comparison with SCADA Systems: Key Differences and Use Cases
    3. Security Issues in DCS: Network Segmentation, Insider Threats, Vulnerable Protocols
    4. Strategies for Securing DCS: Access Control, Secure Protocols, Regular Auditing
8. ICS Communication Protocols
    1. Common ICS Protocols: Modbus, DNP3, IEC 60870-5-104, OPC UA, BACnet
    2. Protocol Vulnerabilities: Lack of Encryption, Replay Attacks, Man-in-the-Middle Attacks
    3. Secure Protocol Implementation: Using TLS/SSL, Role-Based Access Control
    4. Monitoring and Anomaly Detection in ICS Networks
9. US Critical Infrastructure Sectors and Regulations by Sector
    1. Overview of US Critical Infrastructure Sectors: Energy, Water, Transportation, Healthcare, Financial Services, etc.
    2. Key Regulations and Standards: NERC CIP, NIST SP 800-82, DHS CISA Guidelines
    3. Sector-Specific Cybersecurity Requirements and Challenges
    4. Risk Management and Compliance Frameworks

Evaluation of Student Performance:* Student evaluations can include asessments of the following types:

1. Homework assignments
2. Projects
3. Quizzes and/or exams
4. Active participation

CAEPD and Registrar's Office Use Only

Notes Curriculum and Catalog Specialist replaced ampersand in the course title to ensure it meets catalog standards.

This new course will be effective for the University 2025-2026 Undergraduate Catalog via the Summer 2025 Catalog Addendum and will be available in Banner beginning in Spring 2026.

Form Revised July 2024