

CSEC - 3756 - Software Reverse Engineering

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.

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 3756 Software Reverse Engineering:

The ability to understand software for which source code is unavailable is a critical skill within the cyber operations field. Use cases include malware analysis and auditing of closed source software.

This course will serve as a core course and supports NSA CAE-CO & ABET learning outcomes for the proposed Computer Security 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: * 3756

Course Title:* Software Reverse Engineering

Transcript/Banner Course Title:* Software Reverse Engineering

Course Type:*

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 the award of credit hours. 34CFR 600.2 (11/1/2010)

Credits:* 4

Distribution of Credits:* 4 + 0

Schedule Type(s):*

Grade Mode(s):*

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 120
Work Hours:

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 3600

Banner Enforced Prerequisite(s): CS 3600

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 develop essential skills in understanding and analyzing software without access to its source code, a critical capability in cybersecurity. Through hands-on labs and theoretical study, students reverse engineer software of unknown origin, including malware, and document their findings. The course covers techniques for modifying software functionality, recognizing common programming constructs in assembly language, and analyzing network traffic to uncover custom communication protocols. Students explore methods for identifying software vulnerabilities using a range of analysis techniques. Students apply these skills in real-world scenarios, contributing to tasks such as malware analysis and auditing of closed-source software.

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:*

Michael Sikorski and Andrew Honig. 2012. *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software* (1st. ed.). No Starch Press, USA.

Eagle, C. and Nance, K. 2020. *The Ghidra Book: The Definitive Guide*. No Starch Press.

Kyle Cucci. 2024. *Evasive Malware: A Field Guide to Detecting, Analyzing, and Defeating Advanced Threats*. No Starch Press, San Francisco, CA, 488 pages. ISBN: 978-1-7185-0326-7.

Specific, Measurable Student Behavioral Learning Objectives:*

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

1. Safely reverse engineer and document software of unknown origin and malware.
2. Safely and directly patch software to modify its functionality.
3. Recognize common C programming constructs in assembly language.
4. Reverse engineer network traffic to document custom communication protocols.
5. Identify vulnerabilities in software using fuzzing, static analysis, and dynamic analysis.

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

1. Reverse Engineering Techniques

1. Static vs. Dynamic Analysis
2. Disassembly and Decompilation
3. Binary Analysis Techniques
4. Control Flow Graph Analysis
5. Data Flow Analysis
6. Code Injection and Instrumentation Techniques

2. Reverse Engineering Tools

1. Disassemblers (e.g., IDA, Ghidra)
2. Debuggers (e.g., GDB, OllyDbg, WinDbg)
3. Hex Editors (e.g., HxD)
4. Binary Analysis Tools (e.g., Binary Ninja, Radare2)
5. Network Analyzers (e.g., Wireshark)
6. Dynamic Analysis Sandboxes (e.g., Cuckoo Sandbox)
7. **Obfuscation Detection Tools**

3. **Reverse Engineering for Software Specification Recovery**

1. **Identifying Software Functionality and Purpose**
2. Extracting Data Structures and Algorithms
3. API Mapping and Call Flow Analysis
4. Protocol and File Format Analysis
5. Identifying Key Components and Code Paths

4. Reverse Engineering for Malware Analysis

1. Analyzing Malware Behavior (Static and Dynamic)
2. Detecting and Extracting Embedded Malware Payloads
3. Unpacking and Unpacking Techniques
4. Analyzing Malware Communication Channels (C2)
5. Signature Generation for Malware Detection
6. **Behavior-Based Detection Techniques**

5. **Patching Software**

1. **Identifying Vulnerabilities in Binary Code**
2. Crafting and Applying Binary Patches
3. Code Modification and Injection Techniques
4. Patch Validation and Testing
5. Bypassing Anti-Tampering Mechanisms

6. Deobfuscation of Obfuscated Code

1. Identifying and Understanding Obfuscation Techniques
2. Deobfuscation Methods (e.g., Decryption, Decompression)

3. Reversing Packing and Encryption
4. Analyzing Control Flow Flattening and Opaque Predicates

5. Automated Deobfuscation Tools and Techniques

7. Protocol Reverse Engineering

1. Identifying Protocol Types and Structures
2. Capturing and Analyzing Network Traffic
3. Message Format Analysis (e.g., Headers, Payloads)
4. State Machine Reconstruction
5. Creating Protocol Parsers and Decoders

8. Software Analysis

1. Automated Software Analysis Techniques
2. Static vs. Dynamic Analysis in Software Security
3. Fuzzing and Input Validation Techniques
4. Source Code Analysis and Vulnerability Detection
5. Analyzing Software Dependencies and Libraries

Evaluation of Student Performance:*

Student evaluations can include assessments 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

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