Washtenaw Community College Comprehensive Report

CSS 285 Essentials of Automotive Penetration Testing
Effective Term: Fall 2020

Course Cover

Division: Business and Computer Technologies
Department: Computer Science & Information Technology
Discipline: Computer Systems Security
Course Number: 285
Org Number: 13400
Full Course Title: Essentials of Automotive Penetration Testing
Transcript Title: Auto Penetration Testing
Is Consultation with other department(s) required: No
Publish in the Following: College Catalog , Time Schedule , Web Page
Reason for Submission: New Course
Change Information:
Rationale: Today there are over 100 million lines of code in the average modern high end vehicle with multiple entry points for bad actors. As the threat of nation state hackers is on the rise, securing our critical infrastructure in the area of mobility has never been more important. Automotive companies have expanded their hiring needs to include Automotive Cyber Security Technicians and Engineers. These individuals will not only understand cyber security but be able to think like a hacker in order to make vehicles and the connected infrastructure safe from attacks
Proposed Start Semester: Winter 2021
Course Description: In this course, students will gain an understanding of the automotive cybersecurity threat-landscape. Automotive attack surfaces will be highlighted, with a focus on attack techniques to provide insight into creating secure automotive systems. Students will complete hands-on exercises including reverse engineering in a lab environment. Emphasis will be placed on offensive methodologies with a follow-up on defensive strategies.

Course Credit Hours

Variable hours: No
Credits: 4
Lecture Hours: Instructor: 60 **Student:** 60
Lab: Instructor: 0 **Student:** 0
Clinical: Instructor: 0 **Student:** 0

Total Contact Hours: Instructor: 60 **Student:** 60
Repeatable for Credit: NO
Grading Methods: Letter Grades
Audit
Are lectures, labs, or clinicals offered as separate sections?: NO (same sections)

College-Level Reading and Writing

College-level Reading & Writing

College-Level Math

No Level Required

Requisites

Prerequisite
ASV 131 minimum grade "C"
and
Prerequisite
CST 185 minimum grade "C"

General Education

Request Course Transfer

Proposed For:

Student Learning Outcomes

1. Identify and use appropriate processes and procedures for testing the security of a vehicle's information network.
   Assessment 1
   Assessment Tool: Outcome-related questions on the departmentally-developed final exam
   Assessment Date: Fall 2024
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of students assessed will score 70% or higher
   Who will score and analyze the data: Department faculty
   Assessment 2
   Assessment Tool: Departmentally-developed skills exam
   Assessment Date: Fall 2024
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: Random sample of 50% of all students with a minimum of one full section
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of students will score 70% or higher.
   Who will score and analyze the data: Department faculty

2. Describe the components and protocols surrounding vehicle security.
   Assessment 1
   Assessment Tool: Outcome-related questions on the departmentally-developed final exam
   Assessment Date: Fall 2024
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of students assessed will score 70% or higher
   Who will score and analyze the data: Department faculty

3. Test the security of a vehicle network in order to find vulnerabilities.
   Assessment 1
   Assessment Tool: Departmentally-developed skills exam
   Assessment Date: Fall 2024
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections

Number students to be assessed: Random sample of 50% of all students with a minimum of one full section
How the assessment will be scored: Departmentally-developed rubric
Standard of success to be used for this assessment: 70% of students will score 70% or higher.
Who will score and analyze the data: Department faculty

4. Identify regulatory and compliance issues to connected automobiles.
   Assessment 1
   Assessment Tool: Outcome-related questions on the departmentally-developed final exam
   Assessment Date: Fall 2024
   Assessment Cycle: Every Three Years
   Course section(s)/other population: All sections
   Number students to be assessed: All students
   How the assessment will be scored: Departmentally-developed rubric
   Standard of success to be used for this assessment: 70% of students assessed will score 70% or higher
   Who will score and analyze the data: Department faculty

Course Objectives

1. Build threat models to assess a vehicle's risk.
2. Identify areas of the vehicle with the highest risk components.
3. Develop a pre-engagement plan for testing to identify components in scope and provide guidelines for legal and ethical practices.
4. Utilize the results from testing to document and report findings for securing a vehicle's network systems.
5. Identify and explain the various bus protocols.
6. Translate engine codes using the Unified Diagnostic Services and the ISO-TP (an international standard for sending data packets over a CAN-Bus) Protocol.
7. Explain how the different module services work and their common weaknesses.
8. Identify the information that is logged about the driver and where that is stored.
9. Analyze Electronic Control Unit (ECU) firmware data for testing and exploitation.
10. Translate wiring diagrams to data networks.
11. Describe how infotainment systems work.
12. Describe how telematics systems work.
13. Explain how vehicle-to-vehicle networks are designed to work.
14. Differentiate among the various forms of V2X communications.
15. Identify implication and use of cryptography within a vehicle.
16. Conduct an audit of the wiring, voltages and protocols of each network bus on the vehicle.
17. Utilize the socketCAN interface to integrate CAN hardware tools for use in testing.
18. Analyze the CAN network by reverse engineering the CAN bus.
19. Use CAN security-related tools.
20. Access and modify ECU firmware to test security.
21. Simulate attacks on ECUs and other embedded systems to determine system weakness.
22. Use open source systems to access and exploit in-vehicle infotainment centers.

New Resources for Course

Course Textbooks/Resources

Textbooks
Manuals
Periodicals
Software

Equipment/Facilities

Level III classroom

Computer workstations/lab
Other: Cybersecurity Lab with access to test benches

Reviewer	Action	Date
Faculty Preparer:		
Cyndi Millns	*Faculty Preparer*	*Feb 04, 2020*
Department Chair/Area Director:		
Khaled Mansour	*Recommend Approval*	*Feb 04, 2020*
Dean:		
Eva Samulski	*Recommend Approval*	*Feb 07, 2020*
Curriculum Committee Chair:		
Lisa Veasey	*Recommend Approval*	*May 12, 2020*
Assessment Committee Chair:		
Shawn Deron	*Recommend Approval*	*May 14, 2020*
Vice President for Instruction:		
Kimberly Hurns	*Approve*	*May 16, 2020*