CyberTruck Challenge
2025

Call for Instructors

Overview

The core courses offered for the 2025 CyberTruck Challenge in Battle Creek Michigan from 9-13 June 2025 are as follows:

1. Heavy Vehicle Systems
2. In-Vehicle Networking for Heavy Vehicles
3. Diagnostic Systems for Heavy Vehicles
4. Heavy Vehicle Fleet Data and Services in the Cloud
5. Hardware Reverse Engineering
6. Firmware Reverse Engineering
7. Patching Embedded Systems on Heavy Vehicles
8. Wireless Systems for Heavy Vehicles
9. Command Lines and Scripting (1 hour)
10. Open-source intelligence (1 hour)

This call for instructors is to request proposals for a course that will fit within a 2-hour block (unless otherwise noted above) that emphasizes hands-on experience for the students.

Each course must articulate the student learning objectives. These learning objectives should be either “knowledge of” or “how to” statement where “how to” objectives correspond to demonstrated student hands on experiences an “knowledge of” objectives bring awareness to the students. Good classes will have about 5-7 objectives. The CyberTruck Challenge organizer have initial learning objectives for instructors to start with. These are available upon request.

For example, in a class on Automotive Ethernet, an objective may be “Knowledge of message encapsulation,” where the lesson content describes how messages are encapsulated with headers and footers

Misson Statement

1. Help develop the next generation workforce by bringing awareness, excitement, professional involvement, and practicum-based training to the heavy vehicle cyber domain.

2. Help establish a community of interest for heavy vehicle cybersecurity that transcends individual companies or departments and reaches across disciplines and organizations to make a more universal and experienced base of engineers and managers.

based on the different RFCs published. Another objective may be "How to read messages using Wireshark," where students work through a hands-on exercise to capture real traffic from an ethernet-based system on a truck. Good course content and objectives will heavily favor practical experiences that are not available by any other means. In other words, if a student can watch a video or ask ChatGPT to get the content, then it is not worth spending too much time on it. Likewise, if there are activities that can only be done with real vehicles or vehicle systems, these should be favored in the course. The goal of the hands-on training is to equip students with skills and tools to enable them to make meaningful assessments on the heavy vehicle assets supplied by the sponsors.

Dates

- Call for Instructors Release: 20 November 2024
- Instructor Proposal Due Date: 31 December 2024
- Instructor Selection and Notification: 1 February 2025
- Course Content (slides and exercise) Draft: 1 April 2025
- Final slides and requirements for software, files, materials, and supplies: 15 May 2025
- CyberTruck Challenge teaching event: 9-13 June 2025

Why Teach for the CyberTruck Challenge?

Marketing. The CyberTruck Challenge is the premier event for you to demonstrate your ability to explain the complex nature of cybersecurity directly to potential customers. The industry sponsors with the technical background necessary to evaluate security needs will be there. Typically, all major OEMs making heavy vehicles for on-highway use are sponsors for the event. Also, major suppliers responsible for many of the electronics on the vehicle are also present. Finally, the community of interest in cybersecurity of heavy vehicles, including some carriers, are present. This collection of potential customers and community members related to cybersecurity is unique.

Requested Deliverables

Coversheet:

1. Instructor Name(s)
2. Organization Name
3. Point of Contact: email and phone number
4. Title of Class
5. Five to Seven Student Learning Objectives (like the ones in the descriptions below).
6. Concerns, requirements, or restrictions regarding the dissemination of course materials.

Note: all participants are required to enter into a non-disclosure agreement. Copyrights on the course content are retained by the authors. Proposed learning objectives may be incorporated into the overall list of objectives for the CyberTruck Challenge. This means instructors should consider their proposed learning objectives as open source.

Description of the Use Cases:

Describe the scenarios and activities that refine the learning objectives. In other words, explain why and how the proposed learning objectives will be beneficial to the students during the security assessment conducted at the CyberTruck Challenge.

Description of the Activities for the students:

What will the students do during the class?

- Please outline 2-3 main activities for them to accomplish.

What will the students need to successfully complete the assigned tasks?

- What equipment or supplies will the students work with?
- How do the activities interface with the trucks available at the CyberTruck Challenge?

What are the prerequisites the students need to be successful?

- What should a freshman in college teach themselves before coming to the CyberTruck Challenge?
- Is there any read-ahead materials that will be useful?

Assessments:

How will instructors assess the students' performance against the learning objectives?

How can the CyberTruck Challenge organizers evaluate the efficacy of the class?

Use of AI:

Will your course utilize ChatGPT or other Ais in your class? If so, how will you protect the intellectual property of the sponsors?

Other Details:

Please provide any additional information that may help the organizers understand and advocate for your proposal. Also, please provide a statement regarding your financial and travel needs for conducting the training at the CyberTruck Challenge.

Submission:

On or before the due date, please submit your proposal in PDF format (slides or written document) to info@cybertruckchallenge.org.
Please also CC Jeremy.Daily@colostate.edu, ujonson@serjon.com, and Ben.L.Gardiner@gmail.com with your proposal.

Detailed Course Descriptions

Heavy Vehicle Systems

1. Differentiate between different protocols on the CAN busses in a truck.
2. Understand the purpose of different electronic control modules on a truck.
3. Organize heavy vehicle systems into functional groups based on subsystem purpose.

4. How to determine engineering values from network traffic using PGNs and SPNs in J1939.
5. Knowledge of the functions for proprietary messages.
6. Knowledge of different networks found in trucks
    a. J1708
    b. PLC4TRUCKS
    c. J1939
    d. Automotive Ethernet
7. Knowledge of message encapsulation
8. Understand differences between automotive ethernet and others.
9. Knowledge of MACSec
10. Knowledge of public attacks causing de-rates

In-Vehicle Networking for Heavy Vehicles

11. How to setup read messages using Wireshark
12. How to capture vehicle network traffic.
    a. How to use Python to RX
    b. How to use SocketCAN to RX
    c. Wireshark
13. RP1210 and pyhvnetwork
14. How to passively enumerate controller applications from logs of network traffic.
15. How to actively enumerate controller applications.
16. How to send network traffic onto the vehicle network.
    a. How to use Python to TX
    b. How to use SocketCAN to TX
17. Knowledge of the purpose of the vehicle network gateway and ideal filtering rules
18. Knowledge of specific protocol attacks for trucks.
    a. Address Claim Attack
    b. Transport Protocol Attacks

Diagnostic Systems for Heavy Vehicles

19. Knowledge of vehicle diagnostic software
20. Compare Diagnostics over IP (DoIP) to Unified Diagnostics Services over CAN
21. How to reuse existing vehicle scanner code
22. How to bisect network replays to search for desired traffic
23. How to Shim RP1210 DLLs to intercept and manipulate diagnostics traffic
24. How to extract diagnostics data from captured traffic
25. Knowledge of Seed-Key exchange and attacks

Hardware Reverse Engineering

26. How to Passive analysis based on pictures of the PCB
27. Knowledge of PCB debug interfaces
28. How to do UART Snooping
29. How to dump firmware via JTAG

30. How to dump firmware using FlashROM for SPI flash
31. How to dump firmware using SWD/OCD

Firmware Reverse Engineering

32. Knowledge of Linux-based firmware images (conventional, exemplary)
33. Knowledge of checksums, and signing
34. How to identify a checksum (from binary/disassembly, from size)
35. How to survey a binary as preparation for reverse engineering (e.g. binwalk)
36. How to use the "strings" command
37. How to reverse engineer binaries for function comprehension

Patching Embedded Systems on Heavy Vehicles

38. How to modify and repack large firmware
39. How to patch binaries
40. How to write firmware via JTAG
41. How to write firmware using SWD/OCD
42. How to write firmware using FlashROM

Wireless Systems for Heavy Vehicles

Wireless systems include terrestrial HD radio (AM/FM/DAB), Satellite Radio (Sirius XM), Bluetooth, Wi-Fi, mesh networks (802.15), Cellular, RFID, NFC, and GPS. Please do not try to include all wireless technologies in the class; instead focus on some practical and engaging activities for the event using a Software Defined Radio (SDR).

43. Knowledge of wireless connection types
44. Knowledge of connection types
45. How to setup a wireless transceiver station
46. How to capture target devices on a wireless network
47. How to capture and crack wireless handshakes
48. How to broadcast with a software defined radio

Command Lines and Scripting (1 hr)

49. How to use the command-line Windows
50. How to use the command-line Linux
51. How to use Python with CAN
52. How to use AI to generate code

OSINT (1 hr)

53. Knowledge of Open source Intelligence Sources and methods
54. How to use Google Dorks
55. How to use Shodan Search Engine
56. How to understand and use Body Builder Manuals
57. How to discover and use firmware from the Internet

Out of Scope: Chip Off reading and writing, confirming device control at scale, GPS jamming (things that will put you in jail).