MACOMB COMMUNITY COLLEGE
WAYNE STATE UNIVERSITY

Creation of a Cybersecurity Course for Automotive Technicians

HI-TEC

July 21-22, 2021

Nelson Kelly

Assistant Director

Center for Advanced Automotive Technology (CAAT)

Macomb Community College

14500 East 12 Mile Road

Warren, MI 48088-3896

Center for Advanced Automotive Technology
C · A · A · T

NSF

Macomb Community College
Education • Enrichment • Economic Development
Discover. Connect. Advance.

WAYNE STATE

Nelson Kelly
Assistant Director, Energy and Automotive Technology
Center for Advanced Automotive Technology (CAAT)
Macomb Community College, Warren MI

B. S. Chemistry
Miami University (Ohio)
Ph.D. Physical Chemistry
Pennsylvania State University
Research Scientist
General Motors R&D Center, Warren MI
Macomb Community College
Center for Advanced Automotive Technology, CAAT
Adjunct Instructor, Automotive Technology
Assistant Director, Energy and Automotive Technology

Background:

- 35-year career at the General Motors Research and Development Center
- Developed and taught three new courses for an Electric Vehicle Program, Macomb CC
- Responsible for developing new courses in emerging automotive technologies at CAAT

The Center for Advanced Automotive Technology (CAAT)

- Located at Macomb Community College, South Campus in Warren, MI
- Mission
  - Develop and disseminate advanced automotive technology curricula using seed funding
    - Connected, automated , intelligent vehicles
    - Light-weight materials for vehicles
    - Electric and hybrid vehicles and alternative fuels
  - Provide outreach activities to middle and high school students (STEM/STEAM)

Main Questions

- Why is an automotive cybersecurity course needed?
- How did CAAT create a new cybersecurity course?
- How did CAAT get input from outside experts in industry, government, and academia?
- How did CAAT get proposals for the course and choose one to fund?
- How does CAAT disseminate the new course?
- How did CAAT get the new course in Macomb Community College's Vehicle Engineering Technician, Associate of Applied Science Degree?

Automotive Cybersecurity is the Key to Protecting Vehicles from Hackers

Security Breaches Get Front Page Headlines!!!

- HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT
- **Report warns of possible mass casualties from automotive cyberattacks**
- GM TOOK 5 YEARS TO FIX A FULL-TAKEOVER HACK IN MILLIONS OF ONSTAR CARS
- **Vehicle Cyber Attacks Rise Six-Fold, Exposing Digital Weakness**

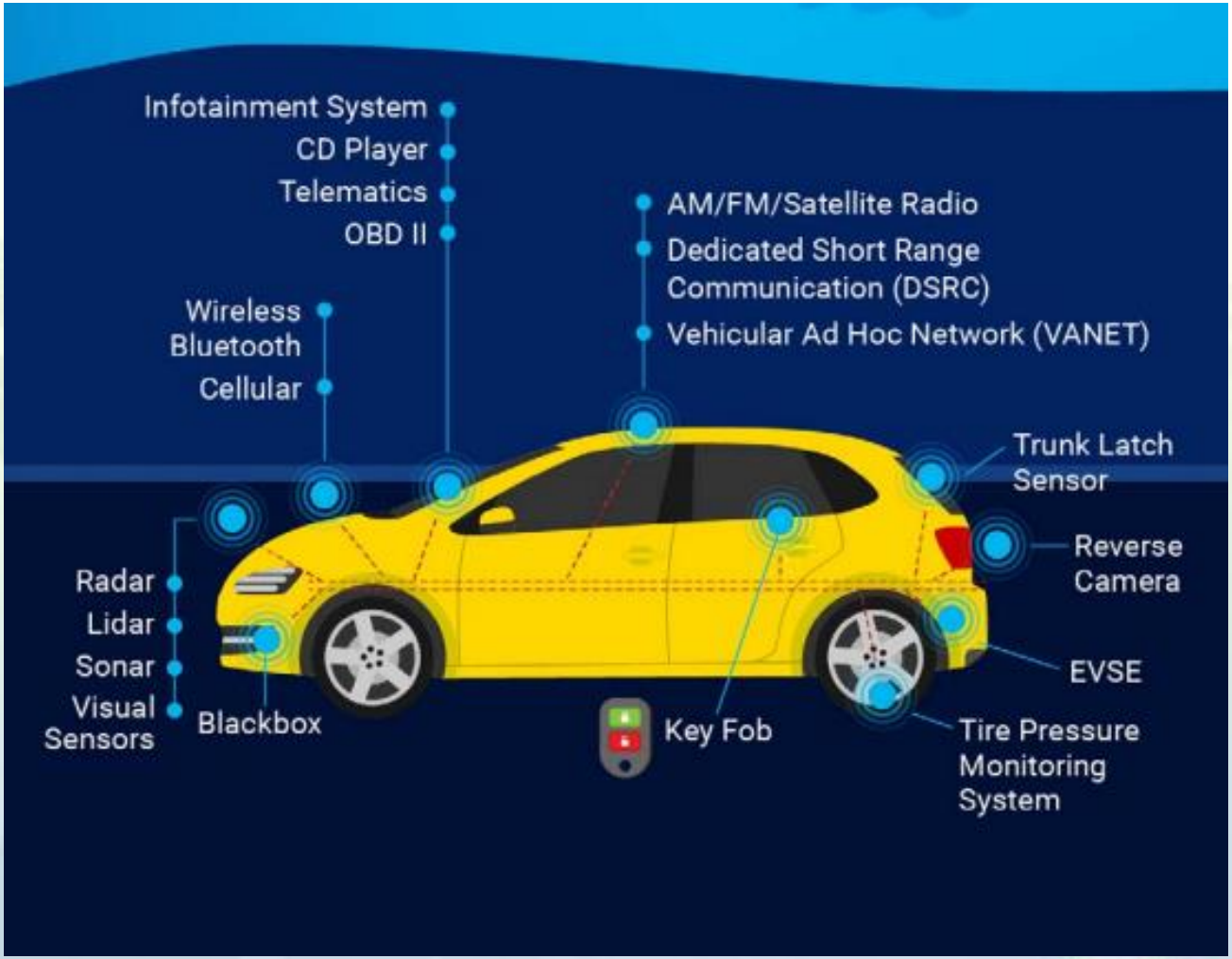
What is Automotive Cybersecurity?

- National Highway Transportation Safety Administration (NHTSA)
  - Cybersecurity, within the context of road vehicles, is the protection of automotive electronic systems, communication networks, control algorithms, software, users, and underlying data from malicious attacks, damage, unauthorized access, or manipulation.

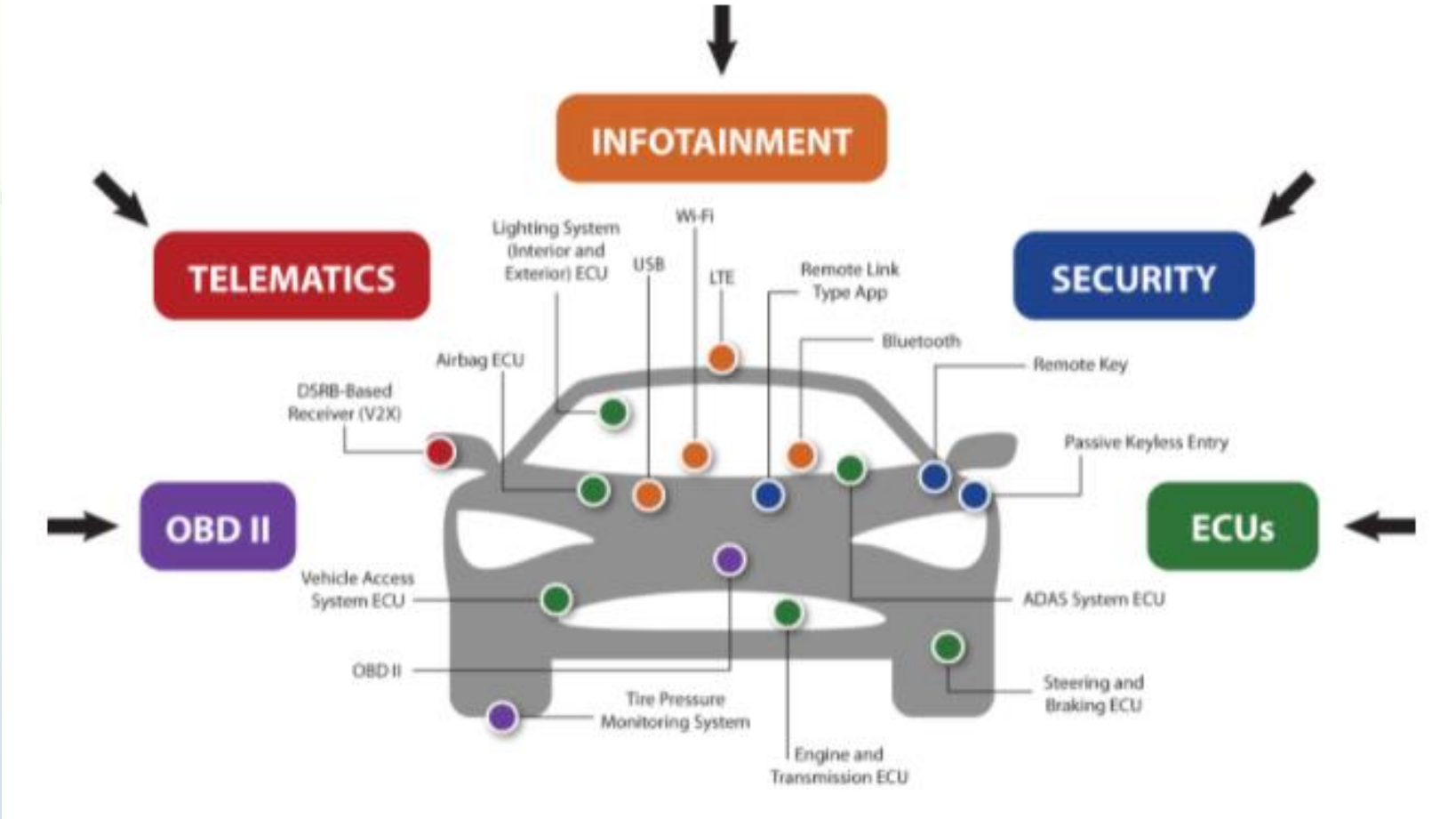
ADDITIONAL RESOURCES

- NHTSA AND VEHICLE CYBERSECURITY PDF, 196.08 KB
- AUTOMATED VEHICLES SYMPOSIUM 2016
- CYBERSECURITY BEST PRACTICES FOR MODERN VEHICLES PDF, 2.69 MB
- FEDERAL REGISTER NOTICE ON AUTOMOTIVE CONTROL SYSTEMS
- AUTOMOTIVE CYBERSECURITY TOPICS & PUBLICATIONS
- CRASH AVOIDANCE TECHNICAL PUBLICATIONS
- ELECTRONIC SYSTEMS PERFORMANCE IN PASSENGER MOTOR VEHICLES
- VEHICLE CYBERSECURITY ROUNDTABLE

Attack Surfaces of a Modern Vehicle



Attack Surfaces of a Modern Vehicle



Conclusion: An Automotive Cybersecurity Course is Needed

- Connected Vehicles: vehicles are becoming nodes on the Internet of Things
  - Attack surfaces for hackers
    - Wireless sensors and systems
      - Tire-pressure monitoring system
      - Remote keyless entry
    - On-board diagnostics (OBD-2), Controller Area Network (CAN) bus
    - Global positioning system (GPS)
    - Infotainment system
    - Over the air (OTA) software updates for vehicle software
- Vehicle software is very complex
  - Over 100 million lines of code
  - Electronic control units (ECU) – microprocessors will make decisions based on software
- Cybersecurity needs to be considered in the initial system design, not added in near the end of the vehicle system development process
  - *Automotive technician training needs to include an automotive cybersecurity course*

CAAT Process for New Course Creation is Called Seed Funding

- CAAT seed funding model
  - Request for proposal, review, revision, contract with deliverables and dates, approval of resources, payment, free posting of materials in CAAT Resource Library
  - CAAT uses an on-line proposal template to standardize and simplify the application process
- CAAT has created courses and modules in emerging automotive technologies and posted the materials on the CAAT web site for free
  - Hybrid and Electric Vehicles
  - Connected and Automated Vehicles
  - Vehicle Lightweighting

CAAT Automotive Cybersecurity Course Solicitation and Development

- Step 1: CAAT prepares course outline
  - Research, webinars, meetings, books, journal articles
  - identify and solicit input from experts
- Step 2: Issue RFP on CAAT web site with instructions and a Proposal Template
  - Disseminate the RFP on the web site, via email, and at a meeting of connected vehicle experts

CAAT Proposal Template Posted on CAAT Seed Funding Web Site

- Organization Information
- Abstract
- Project Purpose, Outcomes, and Objectives
- Course Scope
- Target Audience
- Qualifications
- Project Plan and Deliverables
- Project Timeline
- Project Budget
- Project Reports

Expected proposal length is approximately 10 pages

CAAT Automotive Cybersecurity Course Development and Dissemination

- Step 3: Receive proposals and review them
- Step 4: Choose best proposal, solicit expert comments
- Step 5: Revise proposal with proposer and issue a contract
  - Deliverables, dates, payments
- Step 6: Review course materials, approve, and post for *free* use on CAAT Seed Funding Resource Library

CAAT Research on Automotive Cybersecurity Course Content

- Automotive electronics, ECUs, and CAN
  - Software and firmware
- Attacking (hacking) vehicles and connected/automated vehicles
  - History, Miller and Valesek Jeep hack, cybersecurity awareness
  - Attack vectors; types of threats and attacks
- SAE and ISO standards
  - J3061, ISO 21434, IEEE 1609
  - Safety and security from start to finish
- Protecting vehicles from attacks
  - Penetration testing
  - Security Credential Management System (SCMS)
- References
  - Cybersecurity for Commercial Vehicles (2019)
  - The Car Hackers Handbook (2016)
  - SAE Journal, “Transportation Cybersecurity and Privacy” (2018)

Request for Proposals on CAAT Seed Funding Web Site

November 7, 2018

Dear Funding Inquirer:

The Center for Advanced Automotive Technology (CAAT) is pleased to announce that funding is available for educational institutions to create a new course in automotive cybersecurity for automotive technicians. This course will be needed by future automotive technicians as vehicles become more cyber secure so that they can safely communicate with the outside world. The maximum amount that can be requested is $25,000.

In discussions with industry experts, CAAT has identified several key areas that proposers should consider in creating the new course:

- Automotive electronics, ECUs, and CAN
  - Software and firmware
- Attacking (hacking) vehicles and connected/automated vehicles
  - History, Miller and Valesek Jeep hack, cybersecurity awareness
  - Attack vectors; types of threats and attacks
- SAE and ISO standards
  - J3061, ISO 21434, IEEE 1609
  - Safety and security from start to finish
- Textbooks and reports
  - Cybersecurity for Commercial Vehicles (2019), The Car Hackers Handbook (2016)
  - SAE Journal, Transportation Cybersecurity and Privacy (2018)
- Protecting vehicles from attacks
  - Penetration testing
  - SCMS

We encourage proposers to review the results of a previous CAAT seed-funded course by downloading the course syllabi, lectures, and other materials. In particular the course titled "Connected, Automated, and Intelligent Vehicles" prepared by Professor Gary Mullett of Springfield Technical Community College is an excellent example of what is expected in the delivered course materials. A list of the Requirements for Delivery of Course Materials should also be downloaded from the CAAT web site for reference.

Please use the Proposal Template from the CAAT web site to apply for CAAT funding.

Your completed application should be no more than 10 pages (not including attachments for the budget and figures or charts). Submit your proposals electronically to kellyn@macomb.edu. Any questions may be directed to using the above email or call Nelson Kelly at 586-447-8619 (office).

We look forward to working with you and wish you every success with your proposal.

Sincerely,

Nelson Kelly, Assistant Director
Center for Advanced Automotive Technology
Macomb Community College
14500 E. 12 Mile Road
Warren, MI 48088-3896

(586)-447-8619

Note: some of these links are no longer active on our web site because we are not presently soliciting proposals

Email to Experts on Automotive Cybersecurity Identified By CAAT Research

Hello,

I work at an NSF-funded Advanced Technological Education Center at Macomb Community College called the Center for Advanced Automotive Technology (CAAT). One thing we do at CAAT is fund course development in emerging automotive technologies. We are considering funding the development of a new course on automotive cybersecurity. The first step in that process is to develop an outline of the major topics to be covered. I am contacting experts such as you for suggestions on course content. Once I have completed this research phase, I'll post a request for proposals on our web site at:
http://autocaat.org/Educators/Seed_Funding/

A good example of the result of the course development process via seed funding is a course on Connected, Automated, and Intelligent Vehicles developed by Gary Mullett of Springfield Technical Community College. The syllabus, lectures, and other materials are available for download (for free) at:
http://autocaat.org/webforms/ResourceDetail.aspx?id=4551

If you have suggestions for course content or for organizations who might be interested in creating the course, please email me at kellyn@macomb.edu

Best regards,

CAAT Solicited Input from Industry, Academia, and Government

- Michigan Connected and Automated Vehicle Working Group
  - CAAT presented a talk "***Creation of a Cybersecurity Course for Automotive Technicians***" at the October 25, 2018 meeting with an initial course outline
    - Based on input at the meeting, CAAT added the Security Credential Management System (SCMS) bullet
    - SCMS is a set of "keys" to verify the authenticity of information coming into the vehicle ECUs
  - Input from the meeting: the automotive cybersecurity foundational skills/knowledge that industry would like to see in a new technician hire is covered in CAATs outline

Results of RFP Solicitation

- RFP period was November 7 to December 31, 2018
- Received eight proposals
- All were good; any one of them would have been satisfactory
- Ranked proposals based on four categories
  - Learning outcomes linked to course outline
  - Laboratory activities linked to vehicle systems
  - Timing of delivery of materials
  - Cost

Proposal by Professors from Kettering University was Chosen for Funding

- Kettering University, Principal Investigators
  - Mehrdad Zadeh, Professor of Electrical and Computer Engineering
  - Crag Hoff, Dean, College of Engineering
- Contract duration, 15 weeks
  - Start: March 4, 2019
  - Finish: June 17, 2019
- Deliverables
  - Comprehensive syllabus, outline, learning outcomes
  - Lectures (ppt)
  - Homework, tests, quizzes, projects

Course Materials

All Materials Available for ***free*** download at CAAT Seed Funding web Site Under Funded Programs

- Comprehensive syllabus
- Seven Lectures
- Homework for each topic
- Quizzes for each topic
- Experiments
- Projects

Automotive Cybersecurity Course Outline

- Topic 1: Understanding Threat Models: Identify areas with the highest risk components
  - Threat Modeling
  - Threat Identification
  - Threat Rating Systems

- Topic 2: Bus Protocols & Vehicle Communication
  - CAN bus and diagnostic link connector (DLC)
  - CAN Bus Packet Layout
  - Media Oriented Systems Transport (MOST)
  - SocketCAN interface
  - Diagnostics/Logging, CAN Security, ISO-TP protocol
  - SAE J1698 Standard

Automotive Cybersecurity Course Outline

- Topic 3: Automotive electronics and ECUs
  - Introduction to ECUs, software, and firmware
  - Attacking vehicles: ECU Hacking

- Topic 4: Attacking vehicles
  - Classes of attack vectors
  - SAE J2534 & tools
  - In-vehicle infotainment (IVI) system & remote attacking

- Topic 5: Defining Frameworks for Cybersecurity in Vehicles
  - J3061
  - ISO 21434

Automotive Cybersecurity Course Outline

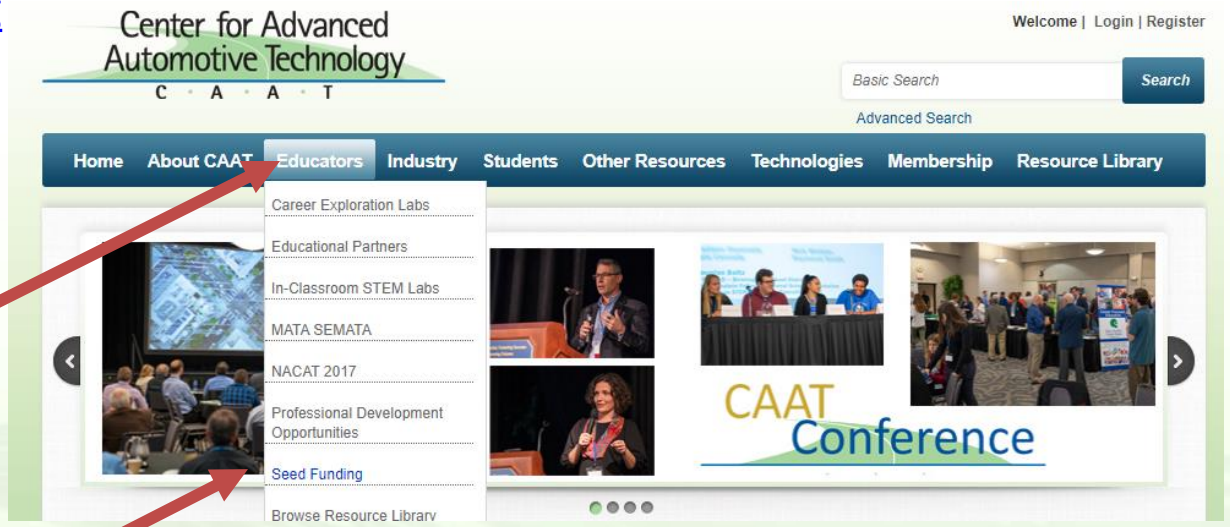
- Topic 6: Attacking Connected/automated vehicles
  - V2V and V2I communication
  - IEEE 1609 & Wireless Access in Vehicular Environments (WAVE)
  - Attacking Wireless Systems
- Topic 7: Protecting Vehicles from Attacks
  - Cybersecurity protection Methods
  - Penetration testing
  - Security Credentials Management System (SCMS)

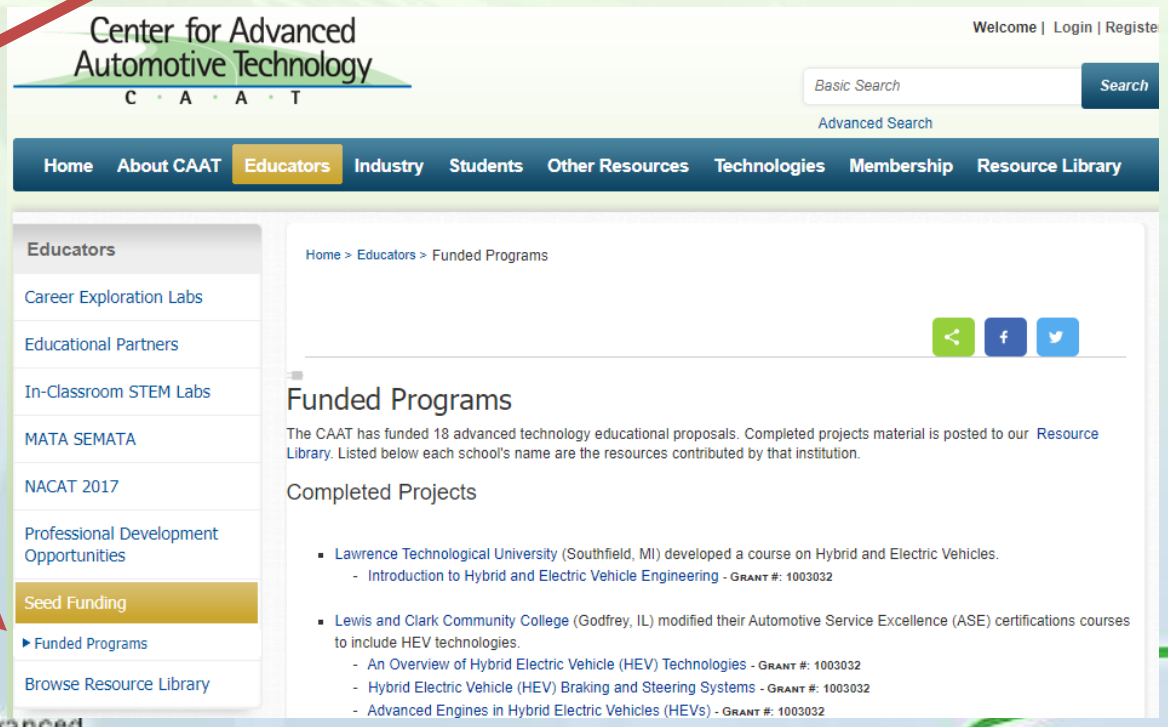
Download the Automotive Cybersecurity Course Materials for *Free* from CAAT

- Step 1, go to autocaat.org
- Step 2, click on Educators
- Step 3, scroll down to Seed Funding
- Step 4, click on Funded Programs
- Step 5, choose Kettering, and the Automotive Cybersecurity course

- Kettering University (Flint, MI) developed courses on aluminum, composite, and dissimilar materials for automotive lightweighting. Emphasis is given to engineering design, manufacturing processes, design guidelines, and drafting notation. Developed a course on the basics of cybersecurity threat models, high risk attack areas of vehicles, classes of attacks, and protecting vehicles from attacks.
  - Design with Composite Materials Course - GRANT #: 1400593
  - Design with Aluminum Course - GRANT #: 1400593
  - Joining Aluminum and Dissimilar Materials Course - GRANT #: 1400593
  - New Course Development and Assessment Tools in Automotive Lightweighting - GRANT #: 1400593
  - Automotive Cybersecurity for Automotive Technicians - GRANT #: 1801150

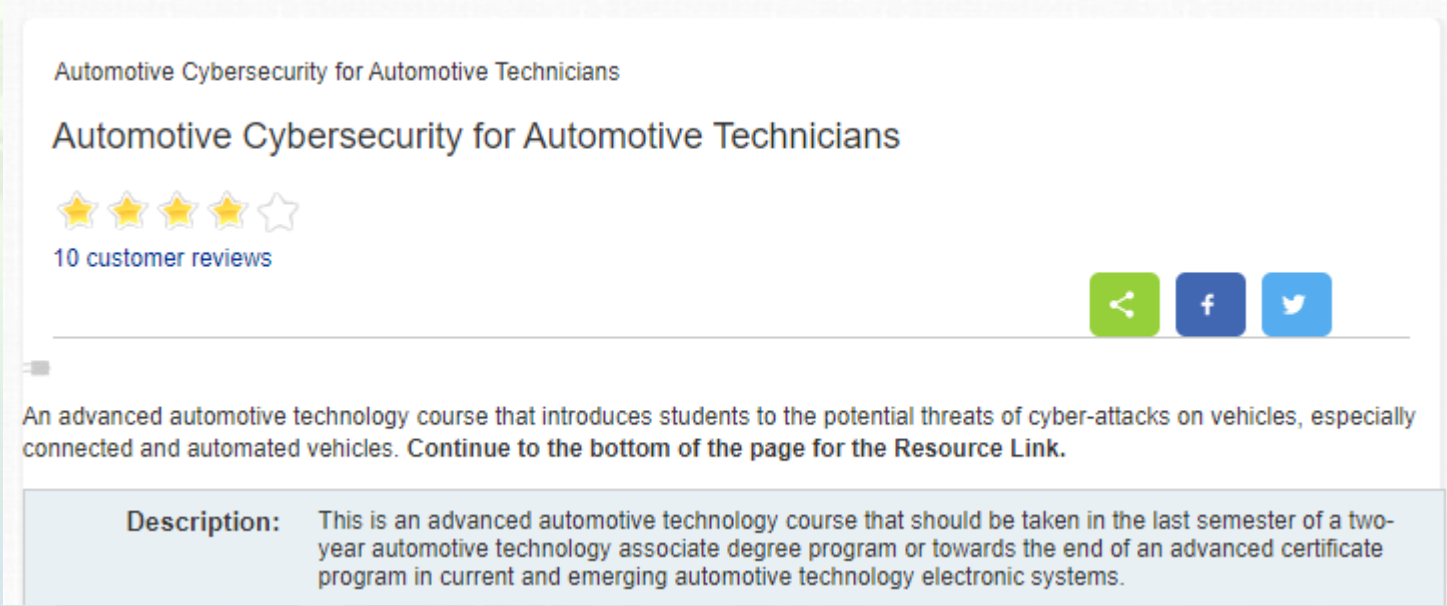
autocaat.org





Final Steps to Download and View CAAT Seed Funding Courses

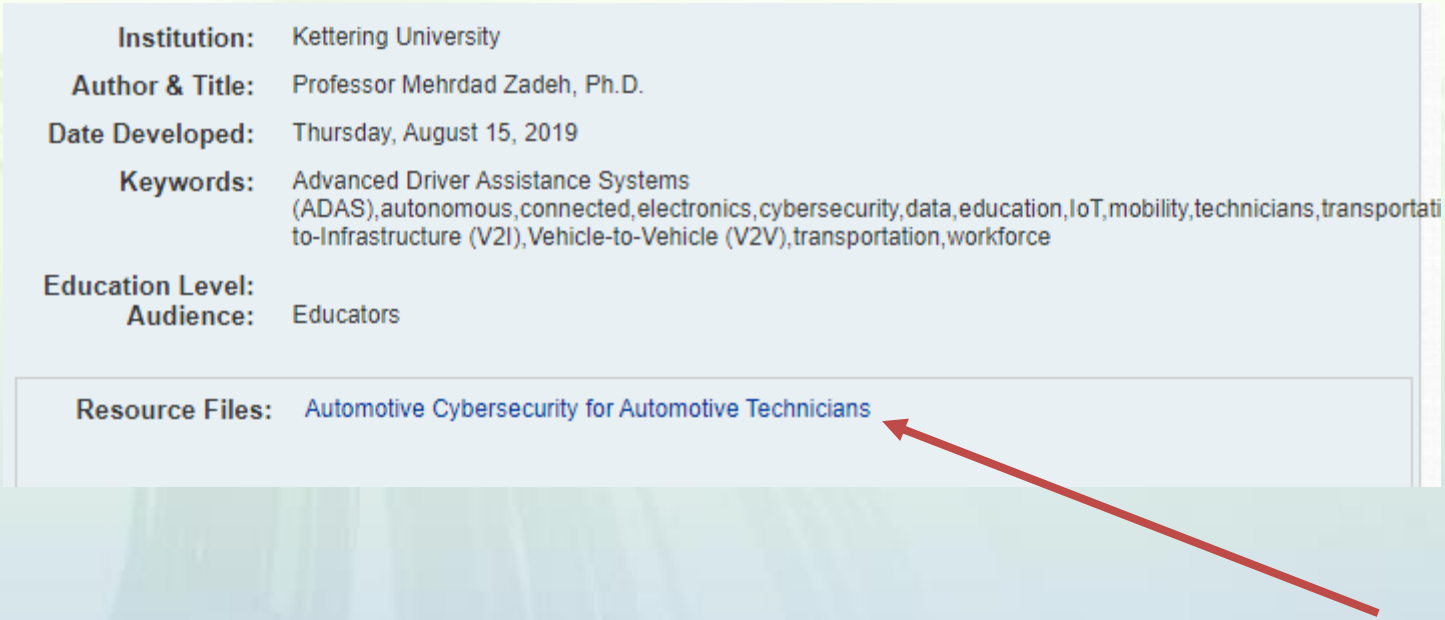
- After you complete Step 5 and click on the course, you will see the course title, description, authors, etc.



- Go to the bottom of the page to “Resource Files”

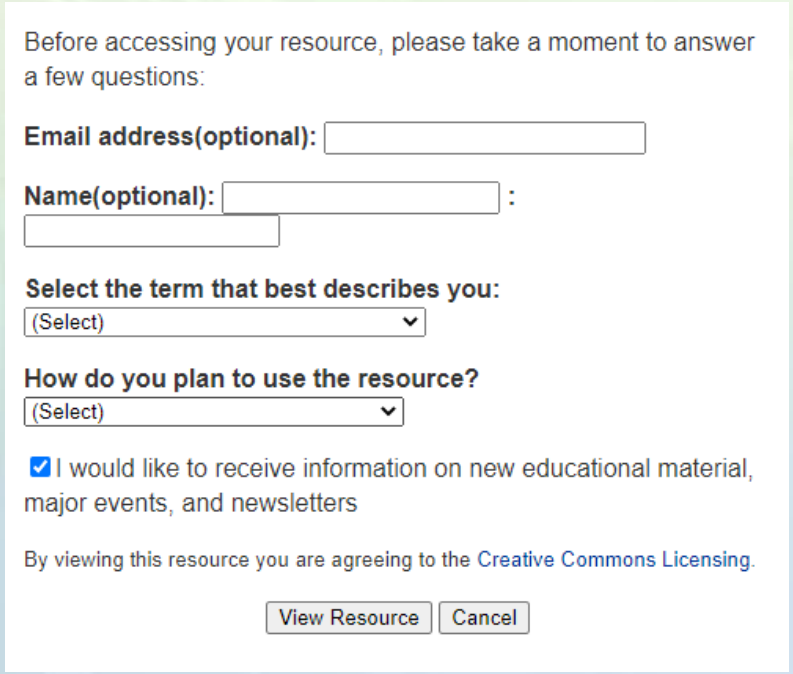
Final Steps to Download and View CAAT Seed Funding Courses

- Click on the course title next to “Resource Files”



Final Steps to Download and View CAAT Seed Funding Courses

- You must answer two questions to proceed with the download of materials. This is to help CAAT understand our audience and their needs, and how well we are disseminating the resources. If you check the box (optional) you will receive news on CAAT events and our Newsletter.
- Click on “View Resource” and the course download will proceed



Macomb Community College Adopted the Automotive Cybersecurity Course as Developed by CAAT and Kettering University as a New Course in 2021

- Curriculum Committee proposal for new AUTO course
- MCC Automotive Technology supported proposal
  - Result: accepted for listing in 2021 e-catalog
  - AUTO 2600, “Automotive Cybersecurity”
- On-line syllabus (CAAT/Kettering syllabus provided the basis)
- AUTO 2600 added as a requirement for the Macomb Associate of Applied Science, Vehicle Engineering Technician Degree by Curriculum Committee

AUTO 2600 - Automotive Cybersecurity

Credit Hours: 3.00

Prerequisites: None

The goal of the course is to introduce students to the potential threats of cyber-attacks on vehicles, especially connected and automated vehicles. The basics of cybersecurity threat models, high-risk attack areas of vehicles, classes of attacks, and protecting vehicles from attacks are introduced. Standards and protocols related to automotive cybersecurity will be covered. Cybersecurity methods and penetration testing for vehicles will also be presented.

Automotive Cybersecurity
Macomb Community College
Official Course Syllabus

AUTO 2600 - Automotive Cybersecurity

Credit Hours: 3.00

Prerequisites: None

The goal of the course is to introduce students to the potential threats of cyber-attacks on vehicles, especially connected and automated vehicles.

The basics of cybersecurity threat models, high-risk attack areas of vehicles, classes of attacks, and protecting vehicles from attacks are introduced.

Standards and protocols related to automotive cybersecurity will be covered. Cybersecurity methods and penetration testing for vehicles will also be presented.

OUTCOMES AND OBJECTIVES

- Outcome 1: Upon completion of this course, students will be able to explain the importance of using cybersecurity threat models in designing automotive systems
  - Objectives:
    - 1. Identify which automotive systems have the highest risk components
    - 2. Explain threat modeling rating systems (ISO 26262 ASIL and DREAD)
    - 3. Apply a scoring system to rank and categorize potential cybersecurity risks
    - 4. Identify a task list to address high-priority hacking and component failure risks for automotive control systems
    - 5. Identify countermeasures to mitigate risks of attacks

- Outcome 2: Upon completion of this course, students will be able to compare different bus protocols and vehicle communications
  - Objectives:
    - 1. Analyze CAN bus, diagnostic link connector (DLC) - OBD2, SAE J1698, J1850, and J2534
    - 2. Analyze Media Oriented Systems Transport (MOST), LIN, FlexRay, and automotive Ethernet
    - 3. Identify the strengths and weaknesses of each protocol
    - 4. Explain Diagnostics/logging CAN data and ISO-TP protocol
    - 5. Set up a CAN virtual network using SocketCAN and can-utils
    - 6. Explain different aspects of bus protocols and vehicle communications

OUTCOMES AND OBJECTIVES

- Outcome 3: Upon completion of this course, students will compare methods of attacking vehicles
  - Objectives:
    - 1. Analyze vehicle-to-vehicle (V2V) and vehicle to infrastructure (V2I) communication
    - 2. Explain IEEE 1609 and Wireless Access in Vehicular Environments (WAVE)
    - 3. Analyze methods to attack wireless systems
    - 4. Explain how to access, retrieve, and disassemble data from an automotive ECU
    - 5. Explain how different sensors measure physical variables and covert the information to an electronic signal
- Outcome 4: Upon completion of this course, students will explain frameworks for cybersecurity in vehicles
  - Objectives:
    - 1. Analyze SAE J3061
    - 2. Analyze ISO 21434
    - 3. Compare the different types of attacks (front door vs. back door attacks)
    - 3. Give real-world examples of recent vehicle hacking attacks
- Outcome 5: Upon completion of this course, students will be able to explain methods for protecting vehicles from attacks
  - Objectives:
    - 1. Analyze cybersecurity protection methods
    - 2. Interpret the role of penetration testing and exploit vulnerabilities using C-code
    - 3. Explain the role of the Security Credential Management System

Summary

- Detailed description of the creation of an Automotive Cybersecurity Course using CAAT seed funding from start to finish
  - Identify need for the course in automotive technician education
  - CAAT research to generate a course outline
  - Input from industry, academia, government
    - Meetings, CAAT web site, email
  - CAAT creates final course outline for Request for Proposals (RFP) posting
  - Receive RFPs, evaluate, select the best one, issue contract to proposer
  - Receive and review materials and offer feedback to proposer
  - Final review and acceptance of course materials by CAAT
  - Course materials posted for free download on CAAT web site along with those from other CAAT seed funded courses and course modules
  - Adoption of a new course, AUTO 2600 "Automotive Cybersecurity" by Macomb Community College Curriculum Committee, listing in Macomb's e-catalog, and addition as a requirement for Macomb's Associate of Applied Science in Automotive Technology, Vehicle Engineering Technician Degree

But Wait, There's Much More….

- CAAT seed funding materials in emerging automotive technologies over the last ten years
  - (see next slide for summary)

  - See CAAT web site for downloading ***free*** course and module materials

- CAAT monthly newsletters (CAAT Tracks) from 2014 to the present
  - Archived on CAAT web site
  - Sign up to receive newsletters automatically

CAAT's 19 Seed Funding Partners and their Contributions to New Course Materials in Emerging Automotive Technologies

	Institution	Hybrid or Electric Vehicles	Light Weighting	Connected Automated Vehicles	Completion Date
1	Lawrence Technological University	X			2011
2	Lewis and Clark CC	X			2011
3	Grand Rapids CC	X			2012
4	Lansing CC	X			2012
5	Grand Valley State University & Muskegon Community College	X			2013
6	Ivy Tech CC	X			2014
7	Kent Intermediate School District	STEM			2014
8	Utica Community Schools	STEM			2014
9	Wayne State University	X			2015
10	University of Alabama at Birmingham	X			2015
11	Jackson State University			X	2016
12	Kettering University		X		2016
13	Roane State Community College		X		2017
14	Kettering University		X		2016
15	Springfield Technical Community College			X	2017
16	Kettering University		X		2016
17	University of Alabama Birmingham			Experimental Testing	2017
18	Kettering University			Cybersecurity	2019
19	Macomb Community College			C Programming	2021

CAAT Courses and Course Modules

- To date CAAT has developed 17 courses and 13 modules through seed funding partnerships with the educational institutions on the previous slide

Topic	Courses	Course Modules
Electric and Hybrid Vehicles	3	11
Connected and Automated Vehicles	3	1
Material Lightweighting	7	
STEM	1	1
Experimental Testing	1	
Automotive Cybersecurity	1	
Embedded C Programming for Automotive (in progress)	1	

Macomb CC Added Four CAAT Seed Funding Courses to the Vehicle Engineering Technician Degree

	Macomb Community College - Vehicle Engineering Technician Program 2021					
	Course	Course Title	Semester 1	Semester 2	Semester 3	Semester 4
			Fall 2021	Winter 2022	Fall 2022	Winter 2023
	AUTO-1000	Automotive Systems	3			
	TMTH-1150	RCL Analysis	4			
	ELEC-1161	Electronics Technology 1	3			
	ELEC-1171	Electronics Technology 2	3			
	AAS/ABA	Gen Ed - English or Composition, Group I.A	3			
	AUTO-1040	Automotive Electrical 1		3		
CAAT	AUTO-2600	Automotive Cybersecurity		3		
	ELEC-1211	Digital Electronics Basics		3		
	ITNT-1500	Principles of Networking		4		
	PHSA-150	Gen Ed - Physical Science 1050, Group II		4		
	ELEC-2150	LabVIEW Basics			3	
	ITCS-1140	Intro to Programing Design & Development			4	
CAAT	ITCS - 1300	Embedded C Programming for Automotive Systems			4	
	PRDE-1250	Basic Blueprint Reading			2	
	AAS/ABA	Gen Ed - Economics or Sociology, Group III			3	
	AUTO 2060	Automotive Electrical 3				3
CAAT	AUTO-2000	Connected, Automated & Intelligent Vehicles				3
CAAT	ELEC-2310	Vehicle Experimental Testing				4
	AAS/ABA	Gen Ed - Creative Writing, Group IV				3
	AAS/ABA	Gen Ed, need 15 credit hours, Group I, II, III, IV				2
			16	17	16	15
					Total Credits	64

References

1. Automotive Cybersecurity. National Highway Transportation Safety Administration.
2. Cybersecurity Guidebook for Cyber-Physical Systems, SAE International J3061, January 2016.
3. Road Vehicles – Cybersecurity Engineering, ISO/SAE 21434.
4. Cybersecurity for Commercial Vehicles, SAE International, Gloria D'Anna, editor, 2019.
5. The Car Hackers Handbook: A Guide for the Penetration Tester, Craig Smith, 2016.
6. NREL, 2019 "Vehicle Cybersecurity Threats and Mitigation Approaches "National Renewable Energy Laboratory. NREL/TP-5400-74247.
7. Connected and Automated Vehicles, Professor Gary Mullett, Springfield Technical and Community College, free course on CAAT seed funding web site.
8. Cybersecurity for Automotive Technicians, Professors Mehrdad Zadeh and Craig Hoff, Kettering University, free course on CAAT seed funding web site:

For Questions and/or More Information

Contact Information

Nelson A. Kelly
Assistant Director, Energy and Automotive Technology
Center for Advanced Automotive Technology (CAAT)
Macomb Community College
14500 East 12 Mile Road
Warren, MI 48088-3896

Phone: 586-447-8619

Email: kellyn@macomb.edu

CAAT web site: autocaat.org

- **Acknowledgement**: This material is based upon work supported by the National Science Foundation under Grant No. 1801150.
- **Disclaimer**: Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.