This seminar is focused on connecting talent with the heavy duty industry to keep vehicles secure by bringing awareness, excitement, and professional involvement to the heavy vehicle cyber domain. Karl leads the CyberTruck Challenge, an immersive experience in truck related cybersecurity. He will also discuss the growing industry participation and outcomes. We look forward to seeing you there!

**Wednesday, December 12th** from **12-1PM** | *Lunch will be provided!*

Location: Engineering Building Deans Conference Room, 3405

For more info please contact: Monique Viau @ viaumoni@egr.msu.edu
The Promise
The Danger(s)

Source: www.weeklystandard.com
The Danger(s)

Source: www.wired.com

Source: www.weeklystandard.com
Commercial Vehicles
Without Trucks...

**Day 1:**
- Medical supply delivery stops
- Fuel stations not resupplied – price hike
- Mail stops
- Just-in-time model breaks

**Day 2-3:**
- Food shortages & hoarding
- Bottled water, milk - gone
- ATMs / Cash – gone
- Fuel stations – gone
- Garbage collection – stops
- Rail & Port operations affected

**Day 7:**
- Car travel stops (no fuel)
- Hospitals run out of oxygen

**Day 14:**
- Clean water almost gone

**Day 30:**
- Clean water gone

**Day 60:**
- ……………
Day 60
Perspective

If man were meant to fly, he would have wings!
Perspective

If man were meant to fly, he would have wings!
Perspective

If man were meant to fly, he would have wings!
How?

- Education (K-12)
- Advanced education
- Engineering practices
- Certification
- Proven methodology
- Standards
- Dawn of a new discipline
Michigan Leadership and Initiatives

- Walsh College – first in the nation to offer a series of specific automotive cybersecurity courses leading to certification
- Other universities building cyber programs at undergraduate and graduate level – at least 5 Michigan colleges are now involved in this domain
- Macomb Community College offering new Automotive Cybersecurity class
- The CyberAuto Challenge
- The CyberTruck Challenge
- New Square One initiatives to focus on educating and exciting HS students for the automotive cybersecurity domain
CYBERAUTO CHALLENGE
JULY 22-27, 2018
DETROIT, MICHIGAN, USA
SAE.ORG/EVENTS/CYBERAUTO
CyberAuto Challenge – What is it?

• Immersive, hands-on event
• 3 days of training, followed by 1+ day of assessments
• Great opportunity for mentorship
• Great hiring opportunity
• Brings the best of students, industry, and research community
• Focused on “breaking”
• Competitive selection
Workforce Development – CyberAuto Challenge

Goal #1: Educate and excite the next generation workforce for a career in automotive cybersecurity

Goal #2: Forge and foster a community of interest from industry, government, and academia focused on responsible and constructive automotive cybersecurity

Notoriety:

- Specifically cited by the automakers in response to Congressional inquiry
- Only named event called out in NHTSA’s Cybersecurity Best Practices document (2016)
- State participation (MSP, TARDEC)
- Fed participation (DOD, DHS, DOT, DOE)
CyberAuto Challenge

- Michigan = 32
- Maryland = 13
- NJ / SC = 5 each
- PA = 4
- CO / IL / OH = 3 each
- KS = 2
- AZ/CA/VA/NY/TX/IA/MO = 1
Selection Process

Recommendation (Professor, teacher, coach)

Review of “goodness of fit” (have 3rd party look at social media feeds, ask for character references)

“Pre-work”
- ~7 week on-line environment
- Teaches basics
- Tests aptitude and motivation

- Linux
- CANBUS Basics
- SDLC
- Cryptography
- Secure Programming

Selection
## The Schedule

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0700-0730</td>
<td>Welcome &amp; Inprocessing</td>
<td>Breakfast</td>
<td>Breakfast</td>
<td>Breakfast</td>
<td>Breakfast</td>
<td>Breakfast</td>
</tr>
<tr>
<td>0730-0800</td>
<td>Breakfast</td>
<td>Welcome</td>
<td>Legal &amp; Ethics</td>
<td>Advanced Wireless</td>
<td>Side-Channels</td>
<td>Charging Station</td>
</tr>
<tr>
<td>0800-0830</td>
<td>Software RE</td>
<td>CANBUS Part 1</td>
<td>CANBUS Park 2</td>
<td>Advanced Wireless</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>0830-0900</td>
<td>Wireless Intro</td>
<td>Advanced Wireless</td>
<td>Socket CAN</td>
<td>Arsenal Talks</td>
<td>Charging Station</td>
<td>How to Hack</td>
</tr>
<tr>
<td>0900-0930</td>
<td>Hardware RE</td>
<td>Hardware RE</td>
<td>Socket CAN</td>
<td>Advanced Wireless</td>
<td>Side-Channels</td>
<td>Charging Station</td>
</tr>
<tr>
<td>0930-1000</td>
<td>CANBUS Part 1</td>
<td>CANBUS Part 1</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1000-1030</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1030-1100</td>
<td>Wireless Intro</td>
<td>Wireless Intro</td>
<td>Wireless Intro</td>
<td>Wireless Intro</td>
<td>Wireless Intro</td>
<td>Wireless Intro</td>
</tr>
<tr>
<td>1100-1130</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1130-1200</td>
<td>Software RE</td>
<td>Software RE</td>
<td>Software RE</td>
<td>Software RE</td>
<td>Software RE</td>
<td>Software RE</td>
</tr>
<tr>
<td>1200-1230</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch</td>
<td>Lunch &amp; Graduation</td>
</tr>
<tr>
<td>1230-1300</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1300-1330</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1330-1400</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1400-1430</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1430-1500</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1500-1530</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1530-1600</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1600-1630</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1630-1700</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1700-1730</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1730-1800</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1800-1830</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1830-1900</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1900-1930</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>1930-2000</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>2000-2030</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>2030-2100</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>2100-2130</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>2130-2400</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
<tr>
<td>0000-0630 next day</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
<td>CANBUS Park 2</td>
</tr>
</tbody>
</table>

*Groups are indicated by color:* **Group 1** (blue), **Group 2** (green), **Group 3** (red).
Save the Date – CyberAuto Challenge 2019

The CyberAuto Challenge will be held from 21-26 July 2019

For information, to nominate a student, or to participate email: karl.heimer@outlook.com
The CyberTruck Challenge
Mission & Purpose

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

• Help **establish community of interest for heavy vehicle cyber** that transcends individual companies or departments and reaches across disciplines and organizations to make a more universal and experienced base of engineers and managers.
CyberTruck Challenge – What is it?

• Immersive experience in truck related cybersecurity
• Heavily practicum based
• Team based event
• Engaged industry, government, and academia to work along-side students in teams taught by industry experts – provides access to some of the best trainers and security teams in the world
• Provides “hacking” or assessment environment on real trucks and real components for about ½ of the event time
• Seeks to foster mentor-protégé relationship building between students and the professional team members
• College (graduate and undergraduate) focused
Who Attends?

- University Students
- Security Researchers (Ethical Hackers)
- Government
  - Dept. of Defense
  - Dept. of Transportation
  - Others
- Industry
  - OEMs
  - Suppliers
  - Fleets
  - Technicians

Rarely do these groups get a chance to meet, learn and do research together.

2017 Participant Composition

- Students 35%
- Industry 18%
- Government 32%
- Researchers 15%
Details

• Annual event held in June
• Location: Macomb CC Sports & Expo Center
• Students: graduate and undergraduate
• Teams: students, industry engineers, supplier engineers, government engineers, hackers
• Format: practicum

100% Increase in universities attending
## Schedule & Curriculum

<table>
<thead>
<tr>
<th>Time</th>
<th>Sunday, 10 June</th>
<th>Monday, 11 June</th>
<th>Tuesday, 12 June</th>
<th>Wednesday, 13 June</th>
<th>Thursday, 14 June</th>
<th>Friday, 15 June</th>
</tr>
</thead>
<tbody>
<tr>
<td>0700-0800</td>
<td>Site Closed</td>
<td>Site Closed</td>
<td>Hardware</td>
<td>Conducting Assessments*</td>
<td>Assessment</td>
<td>Assessment</td>
</tr>
<tr>
<td>0800-0900</td>
<td>Breakfast/Registration</td>
<td>Breakfast</td>
<td>Breakfast</td>
<td>Breakfast</td>
<td>Breakfast</td>
<td>Breakfast</td>
</tr>
<tr>
<td>0900-1000</td>
<td>Welcome and NDA</td>
<td>Truck Systems</td>
<td>Cryptography</td>
<td>Assessment</td>
<td>Assessment</td>
<td>Assessment</td>
</tr>
<tr>
<td>1000-1100</td>
<td>Engines</td>
<td>Lunch</td>
<td>Software</td>
<td></td>
<td></td>
<td>Site Closed</td>
</tr>
<tr>
<td>1100-1200</td>
<td>Lunch</td>
<td>Lunch</td>
<td></td>
<td></td>
<td></td>
<td>Student Team Briefs</td>
</tr>
<tr>
<td>1200-1300</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Review*</td>
</tr>
<tr>
<td>1300-1400</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td>1400-1500</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td>1500-1600</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td>1600-1700</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td>1700-1800</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Lunch</td>
</tr>
<tr>
<td>1800-1900</td>
<td>Informal Welcome Reception (offsite)</td>
<td>Dinner</td>
<td>Dinner</td>
<td>Dinner</td>
<td>Dinner</td>
<td>dinner</td>
</tr>
<tr>
<td>1900-2000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Restaurant</td>
</tr>
<tr>
<td>2000-2100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Restaurant</td>
</tr>
<tr>
<td>2100-2200</td>
<td>Site Closed</td>
<td>Site Closed</td>
<td>Site Closed</td>
<td>Site Closed</td>
<td>Site Closed</td>
<td>Site Closed</td>
</tr>
<tr>
<td>After 2200</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Site Closed</td>
</tr>
</tbody>
</table>
Outcomes

Has attending made you MORE likely to enter this industry?

- Yes: 89%
- No: 5%
- Maybe: 6%
- No Response: 0%

Have you found a mentor?

- Yes: 87%
- No: 0%
- Maybe: 13%
- No Response: 0%
Workforce Development – CyberTruck Challenge

“The biggest benefit for me was probably talking with all the professionals in industry. Talking to them about what they did just affirmed that I want to work in the same field.”
-- John Maag, Class of 2019 (EE)

“This experience is amazing. I would never get an opportunity to work with an actual vehicle if it wasn’t for the CyberTruck Challenge.”
-- Subhojeet Mukherjee, Ph.D. Candidate (CS)
Plans over next 1-5 years

1.) Pre-work and selection
2.) College program tie-in
3.) CTF component
4.) NSF Workshops

1.) EV-EVSE attack vectors (electrical vehicle infrastructure
2.) “Smart City” attack vectors
3.) Crypto update pending advances in quantum cryptography

1.) Metrics Framework
2.) Tools and vuln checkers
3.) Security product targets
Sponsors

300% Increase in sponsored trucks

80% Increase in security companies

A special thank you to our sponsors

for supporting the 2nd Annual Cybertruck Challenge, June 11-15 2018.
The CyberTruck Challenge will be held from 23-29 June 2019 at the Macomb Community College.

For information, to nominate a student, or to participate email: karl.heimer@outlook.com
Your Participation

• What additional new topics should we consider?
• Are any of the topics superfluous?
• What kinds of subsystems are most important?
• What sorts of services (hiring contacts, etc.) would be helpful?
• What additional universities should we contact?
• What do you need to see or hear for your organization to sponsor and/or participate?

• What else?
Secure is a verb
Discussion

Karl Heimer
+248.270.0117
karl.heimer@outlook.com
Thank you

Presentation to the NMFTA; November 2018
Karl Heimer
karl.heimer@outlook.com
+1.248.270.0117
Backup

Karl Heimer
+248.270.0117
karl.heimer@outlook.com
Carmakers now integrate some of the most complex code on Earth.
Consequences: Vulnerabilities and Code Size

- **Vulnerabilities** probable per shipped car
  - Standard Release Errors
  - Clean Room Dev
  - Vulnerabilities
Attacker Methodology

Hacker Protocol

- Reconnaissance
- Target Selection
- Attack & Toehold
- Privilege Escalation
- Infiltration
- Exfiltration
- Persist | Clean
Cyber-informed Design: Layered Security

- Firewall
- IDS
- SSL Certs
- 2-Factor Authentication
- Code Obfuscation
- Encryption System
- Anti-Spam
- Secure Browsing
- Remote Access Authentication
- Red/Black Separation
- Integrity Checks
- Gateway
- Application Whitelisting
- Encrypted Network Storage
- Auditing Procedures
- Malware Scanner
- Removable Media Encryption
- OTA
- 2-Factor Authentication
- Code Obfuscation
Cyber-informed Design: Defense in Depth

- Layered Security
- Threat Analysis
- Vulnerability checks & understanding
- Reconnaissance
- Forensics
- Response
- Reconstitution
Cyber-informed design: Resiliency

- Assume and Prevent an Enemy root
- In-service V&V and Update
- Fail safe or “de-automate”
- Continuity of Critical Functions
- Architecture Assumes Compromise
- Use Segmented Architecture
- Onboard & Remote Analytics to Understand State
Instruction and Seminars

Topics related to heavy vehicle protocols, like J1939 and J1708 communications were discussed.

The CyberTruck Challenge was modeled after the successful SAE Battelle Cyber Auto Challenge. There were a few Cyber Auto graduates at the inaugural event.
Assessment Period

Mitch, a security researcher, explains key software features for students as they assess the heavy vehicle systems.

Matt acts as a mentor for a Virginia Tech student during the assessment period.
Meet the Division of Engineering Research
Division of Engineering Research (DER)

DER is located in the Engineering Building Room 2527

https://www.egr.msu.edu/der/  Proposals@egr.msu.edu

Kelli Martin, Director
kelli@egr.msu.edu (517) 353-9492

Andy Hazel, Research Administrator II
andyh@egr.msu.edu (517) 353-5473

Rebecca Baynai, Research Administrator II
rebaynai@egr.msu.edu (517) 355-7435

Robert Nelsen, Research Administrator II
rnelsen@egr.msu.edu (517) 355-5103

David Palme, Research Administrator I
dpalme@egr.msu.edu (517) 432-0875

Ziba Banafsheha, Research Administrator I
Ziba@egr.msu.edu (517) 355-5104

Jacque Shoppell, Assistant Director
shoppell@egr.msu.edu (517) 353-5084

Students:
• Junhui Xiao xiaojunh@egr.msu.edu
• Emily Kemp kempemil@egr.msu.edu
• Monique Viau viaumoni@egr.msu.edu
• Jeremy Webb webbjer2@egr.msu.edu