CyberTRUCK Challenge Sponsorship Information for 2018

www.CyberTRUCKchallenge.org

The CyberTRUCK Challenge Mission

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.

About the CyberTRUCK Challenge

Cybersecurity issues are closely guarded secrets today and discussions about cybersecurity posture or vulnerabilities rank in the core concerns of any organization. Yet, given the nature of our interconnected world and the ubiquity of processing power and storage power in even the most mundane of products (e.g. new toasters, refrigerators, door bells, and thermostats) understanding security posture, issues, and remediation are critical to our society.

While progress in data sharing is being made through the various ISACs (Information Sharing and Analytics Centers), too little is being done to energize and encourage discourse among the engineers, and too little is being done to help prepare and develop the next generation workforce – to develop their skills, provide them with a network of potential mentors, and excite their interest in transportation sector cybersecurity. The CyberTRUCK Challenge attempts to remedy this.

This event is committedly pro-industry, and all its actions, efforts, and outreach is to help industry understand and eventually conquer cybersecurity challenges. It is a resource for participants to draw on in terms of education, in terms of connections, in terms of understanding the needs and priorities and remedies of sister organizations, in terms of understanding the government perspective, and lastly as a recruitment resource for HR's arsenal of tools.

CyberTRUCK Challenge Vision Statement

Ubiquitous, reliable, safe, and cost effective transportation is key to our way of life and a prime ingredient of the American lifestyle. The CyberTRUCK Challenge, along with sponsors like the State of Michigan and the National Motor Freight Traffic Association, believes the cybersecurity of the transportation domain – whether cars or trucks or planes or heavy equipment – is at the core of an important new industry and discipline. Michigan is backing research, information exchange, fostering communities of interest, and engaging the imagination of today's students and tomorrow's cyber workforce in specifically highlighting vehicular cybersecurity and Michigan's central role in the future of connected and autonomous vehicles. The CyberTRUCK Challenge teaches techniques and understanding of this domain, and also helps facilitate collaboration among industry, academia, the research community, and government. This event will be strongly pro-industry and seek to provide understanding, tools, and highly useful resources to help OEMs and suppliers master the cybersecurity domain and create progressively superior products.

Sponsorship Levels

Running a world-class event, like the CyberTRUCK Challenge, requires resources. These include student travel subsidies, instructor compensation, catering, equipment and supplies, shipping, promotional materials, rentals, and event support. We seek tax-deductible contributions at the following levels:

Level	Benefits
Platinum $25,000	• Dedicated vendor booth space will be available for the sponsor • Large sponsor logos will be included prominently on the CyberTRUCK Challenge logo for this year • Large sponsor logos will be printed on banners, signs, T-shirts, name tags, and other promotional material • One of the catered meals will be attributed to the sponsor • Sponsor will be scheduled a short speaking slot to address the Challenge • Sponsor can bring any reasonable number of personnel to the event
Gold $10,000	• Dedicated vendor booth space will be available for the sponsor • Medium sponsor logos will be included prominently on the CyberTRUCK Challenge logo for this year's event • Medium sponsor logos will be printed on banners, signs, and T-shirts • Can bring up to 5 people to participate in the event
Silver $5000	• Dedicated vendor booth space will be available for the sponsor • Small sponsor logos will be included prominently on the CyberTRUCK Challenge logo for this year's event • Can bring up to 2 engineers to participate in the event.

In-Kind Donations

Companies that cannot sponsor with cash donations can still sponsor with useful in-kind donations to assist the event. This could be in the form of a truck, electronic control modules, tools, or human resources (i.e. send some engineers for the week). Written receipts will be provided for cash contributions only. Companies providing in-kind support will be responsible for their own record keeping. Logo and vendor booth space is not available for non-cash sponsors.

Premium Sponsor with Naming Rights

The Board of Directors of the CyberTRUCK Challenge will reserve the opportunity for one entity to be a premium named sponsor for the event. If you are interested in being a premium sponsor at a level significantly higher than the Platinum level, please contact one of the organizers.

Opt-out of Named Recognition

By default, sponsors will be recognized by the CyberTRUCK Challenge and your company name and logo may be included ore referenced in promoting the Challenge. However, any sponsor can opt-out of named recognition. To opt-out, please send a written request to the organizers.

Mailing Address

Please send sponsorship checks to the following address. If banking transfers or credit card payments are desired, please contact us directly:

CyberTRUCK Challenge, Inc.
c/o Jeremy Daily, Mech. Engr.
800 S. Tucker Dr.
Tulsa, OK 74104
PH: (937) 238-4907
e-mail: jeremy-daily@utulsa.edu

Please make checks payable to "CyberTRUCK Challenge." An invoice can be issued upon request.

An example of the prominent display of logos at the CyberTRUCK Challenge.

All donations are tax deductible as the CyberTRUCK Challenge is a non-profit 503(c) designated educational organization.

Due Date

To receive full benefit of the sponsorship levels, we need commitment and resources by **May 1st, 2018**. Sponsors will need to supply high quality logos for inclusion in the promotional material by May 16th.

CyberTRUCK Challenge Participation

Participation at the CyberTRUCK Challenge is by invitation only and requires participants and visitors to sign a non-disclosure agreement. There are four categories of participants: 1) Students, 2) Industry, 3) Government, and 4) Security Research Mentors. (Speakers and Instructors are also participants.)

- Students must submit an application to attend the CyberTRUCK Challenge that will be reviewed and approved by the CyberTRUCK Challenge Board of Advisors. Faculty must recommend the student.
- Industry participants must demonstrate some level of sponsorship to attend as a participant.
- Government employees and contractors may participate provided they contribute to the mission of the CyberTRUCK Challenge.
- Security Researchers will be invited to attend and provide mentorship for students based on referrals and professional accomplishments. Please contact the organizers for more details.

All participants and visitors are responsible for their own travel expenses unless you are a student.

Benefits of Participation

The success of the inaugural CyberTRUCK Challenge demonstrates the following benefits:

- Establish relationships within the community and understand resources outside your company.
- Scout student talent that will build the capabilities of your engineering teams.
- Position your company at the forefront of the industry in addressing cyber-security issues.
- Help fill the talent gap of qualified engineers capable of addressing cyber-security challenges.

We encourage sponsor engineers to participate in the full week's activities. This maximizes the engagement opportunities and helps forge bonds with the students (future colleagues).

Media and Promotional Opportunities

No on-site media will be allowed (on-site being defined as the rooms for training and for assessments, we do not suggest we can prohibit media from the entire campus). However, some sponsors see the event as a potential media opportunity and the event respects their right and need to be able to share the fact of their participation, if not the details of it. To that end, the State of Michigan has retained McCann as a media representative, which will have staff ready to work on a coordinated message to develop a pro-industry "story" showing industry and government working proactively together to address a growth and technological advancement issue before it becomes a problem. These coordinated messages can help highlight the leadership and forward thinking of participating parties.

Protocols for Information Sharing and Protection

Information sharing protocols: the basic tenet is -

"What happens at the Challenge, remains at the Challenge"

Restrictions

Information **NOT** to be shared external to or after the CyberTRUCK Challenge:

- Data capture or logs remain with the OEM. After the Friday briefings, all logs and data capture will be transferred to the OEM providing the vehicle, and any copies or files on the lab computers will be erased. Staff will then format the hard drives for lab computers.
- Vehicles used during the Challenge will not be discussed or referenced in any identifying way. No manufacturer or model, etc. will be identified. Vehicles will be referenced as "Learning Platforms."
- Discoveries, approaches, scenarios, situations, narratives, stories, etc. and the like, regarding vehicle assessments will not be discussed.
- Names of individuals or organizations participating in the Challenge, except noted Sponsors (on the t-shirt, promotional material, etc.), those individuals or organizations appearing on the CyberTRUCK Challenge website. Any entity may also grant express written approval to any participating individual or organization to identify the granting entity (ONLY); this may be done post Challenge and may be an external communication.
- Identities of participants and their organizations; this includes students, guests, vehicle team members, instructors, presenters, etc. will not be shared.

Permissions

Information ALLOWED to be shared:

- Approved CyberTRUCK Challenge messages as placed on the website.
- Approved promotional information - brochures, posters, announcements, press releases, etc. distributed during recruitment and/or posted to CyberTRUCK Challenge website.
- Messages describing the goal of the event as a workforce development exercise as the primary objective and mission of the CyberTRUCK Challenge:
    a. Workforce development efforts by Challenge Sponsors and the industry
    b. The Challenge is an example of the industry's continued commitment to continuous improvement in vehicle designs and cyber capabilities
    c. The Challenge helps to develop the next generation cyber engineer for heavy vehicles
    d. The Challenge seeks to inspire youths to choose science, technology, engineering and math

- The Challenge seeks to attract the brightest minds to the industry; attract students to choose careers in the automotive industry.
- The Challenge demonstrates the high tech and cyber nature of heavy truck industry using real world vehicles and systems. Vehicles will be referenced as "Learning Platforms." The learning platform is a modern, fully featured, vehicle.
- The Challenge helps to improve the skills and knowledge of the current workforce in cybersecurity.
- When in doubt, please verify external statements through the CyberTRUCK Challenge staff (listed on the CyberTRUCK Challenge websites).

Social Media

- No posting, blogging, tweeting information that describes the specific details of the Challenge on social media such as Facebook, Twitter, Instagram, Pinterest, etc. is allowed.

Photography

- Participants may not take photographs, video recordings or capture images during the Challenge.

  NOTE The event itself maintains an "EVENT CAMERA" and the staff will take pictures with it. These pictures will be appropriately "cleared" and can then be used by organizations and individuals, possibly with use restrictions. If anyone wants a particular photo – contact the staff and ask them to take it with the event camera – we will then verify it can be released, and if so release it with any special use instructions.
- All individuals will sign a release allowing the CyberTRUCK Challenge and/or Michigan Defense Center to use their likeness or image in promotional materials.

Non-disclosure agreements: Terms of Participation

- Individuals agree to sign a Terms of Participation/NDA agreement upon arrival (advance copy available for review). Sponsoring organizations commit their representative(s) to the information sharing protocols via their Sponsorship and/or Contributor Contract.
- The Michigan Defense Center and the CyberTRUCK Challenge will hold all Terms of Participation, Sponsor and Contributor Contract and will bear responsibility for oversight.
- A packet of Terms of Participation identifying the names of individuals and organizations covered under the agreement for the event will be available two weeks after the event's conclusion, upon request.

Legal Briefing Attendance

- All participants for the week are required to attend legal briefing on 1st day (Monday) and concluding day (Friday).
- All visitors/observers must sign the NDA and will receive a legal briefing.

Frequently Asked Questions

1.) Q: Who comes to this event?

A: Industry, both the OEMs and the supplier community, government engineers and managers, college students, academic researchers, and hackers.

2.) Q: Hackers? You mean you actually have people try to hack the systems?

A: Yes. There are many ways to use the term "hackers" – and not all of them are the "bad guys" – as a society we use researchers and ethical hackers to evaluate banks, hospitals, government organizations, large corporations, the power grid, and almost everything else. In today's world it is increasingly difficult to find any "thing" that doesn't have communications with something else and which doesn't have a computer in it. It is normal to have specialists who review the security of systems and components to look at this system, too. Here at the CyberTRUCK Challenge we used ethical hackers from major companies and some well-known within academia to provide the perspective and model the actions that a "bad guy" hacker would when faced with assessing the systems.

3.) Q: But, aren't you worried that they will find something?

A: Succinctly, no. Code evaluations and security evaluations are now mainstream in most industries. We have NDAs and legal protection in place, and all the "hackers" are from professional security firms with significant experience and who are accustomed to provide confidentiality regarding their work. Should anything be found, it would be protected information and would go to the equipment manufacturer who could then take appropriate action with respect to patching or development cycle changes.

4.) Q: Why are you doing this – or at least why now?

A: Now is the perfect time to do this. Now gives us a chance to address the immense technological changes coming to the industry and proactively plan for how to implement them and secure them. We think it is best to look down the road and be ready for changes rather than responding to them. By helping develop the next generation workforce – running this event for college students – and talking about real and intended technological changes we are creating the underlying capability to do something about potential future vulnerabilities. We believe this is a much better approach than waiting until an urgent response is needed for an unplanned and possibly surprising event.

5.) Q: Can you describe the training involved in this event?

A: There are several classes over a two-day period including hardware reverse engineering, software reverse engineering, systems reverse engineering, component analysis, fundamentals of CAN (Controller Area Network), fundamentals of the communications protocols used by these systems, and then some shorter demos and classes. We also spend time up front and at the course conclusion talking about the NDA and their legal, ethical, and moral responsibilities. After the two days of classes, we have a two-day guided assessment exercise in which the teams get to know the system they are assigned.

6.) Q: The coursework sounds very attack focused. Is this, then, primarily an attack-centered event?

A: It is intended to introduce how an attacker thinks and acts. Hackers tend to think differently than developers. Developers tend to ask themselves "how can I make this work". Hackers tend to ask themselves "how can I break this" or "how can I make this perform in an unintended way"? This means the minds engaged in cybersecurity tend to look at the world differently from and function differently from standard developers. There is real value to industry in this approach and making it accessible. Think of a football team – if you only practice defense, you might not understand how the offence will work and you might not cover the same spots on the field as you would if you had skirmishes with an offensive line (and the converse is also true). This provides a different point of view to take into account during the development and life-cycle maintenance activities.

7.) Q: You mention teams – what do the teams look like?

A: Teams are composed of college students, industry professionals (primarily engineers from OEM and suppliers, but perhaps an occasional technical manager, too), technicians, government (both engineers and some technical managers), and hackers.

8.) Q: Why is the Michigan Economic Development Corporation (MEDC) sponsoring this event?

A: Software development, maintenance, and validation is currently a major growth area in the transportation sector. Cybersecurity will be a near-term follower. It is inconceivable for a car company, a truck company, or a supplier to not have a strong software team today. This will be true of cybersecurity tomorrow. By being a thought leader in the space and being aggressively involved in building this business domain and showcasing the unique qualities of and opportunities in Michigan, we intend to attract both highly gifted professionals, and tech-savvy companies to do this important work right here in Michigan – which is newly numbered among the most proactive and advanced states with respect to cybersecurity. It also helps our existing industries by attracting a talent pool to them and by allowing them to make their products and competencies more broadly known.

9.) Q: Why are defense vehicles and commercial vehicles in the same event?

A: If you look at the general concept of transportation cybersecurity, many different organizations are affected by it and can share in learning about it and attracting talent and developing products to help remediate or even solve some of the cybersecurity risks. Michigan has been hosting a similar automotive sector event for years, and this is a great opportunity to bring larger vehicles together for a similar venue, and to help attract and train the future engineers for these systems. While there will certainly be differences among these different vehicles, we believe that by sharing knowledge, concerns, and threat information between the private and public sector we can have better appreciate of both the threat landscape and the most viable and effective ways to address and minimize risks.

10.) Q: This sounds like a great program – how can I participate?

A: Contact
Karl Heimer (+1.248.270.0117 // karl.heimer@outlook.com) or
Jeremy Daily (+1.937.238.4907 // jeremy-daily@utulsa.edu)

11.) Q: How do you know this event is a good idea?

A: It is modeled after and designed by the same people who founded the SAE-Battelle CyberAuto Challenge (www.sae.org/cyberauto) which is strongly supported by Industry as an educational and recruitment asset.