Communications Guide and Vision for the 2018 CyberTruck Challenge

Version 2: 20180131/kh

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.

This document describes the vision of the event, describes the media opportunities at the event, and poses some model questions and answers.

This is a "living" document – please send comments so we can have a reference for a common voice to any external questions.

VISION: Ubiquitous, reliable, safe, and cost effective transportation is key to our way of life and a prime ingredient of the American lifestyle. The State of Michigan believes that 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.

MEDIA 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.

Q & A:

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 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 is TARDEC and the 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.