Talent Generation for Vehicle Cyber Security

Jeremy Daily, Ph.D., P.E., Department of Mechanical Engineering, The University of Tulsa

Urban Jonson, Chief Technology Officer, National Motor Freight Traffic Association, Inc.

Rose Gamble, D.Sc., Tandy School of Computer Science, The University of Tulsa

1 Abstract

The cyber security of vehicle systems is a growing concern as market forces drive an explosion of connectivity within and around the cyber-physical systems comprising the vehicles on the road today. To keep pace with these market trends, the pool of qualified personnel to address the design and implementation challenges needs to be expanded. Acquiring the cross disciplinary skills involving mechanical engineering, electrical engineering, computer science, and security is challenging. It may require multiple majors, which can result in more than four years at a university, as well as include additional certifications, such as in cyber security. Federal investment in focusing educational efforts to create a pipeline of these professionals is in low supply. Private industry partnering with educational institutions is needed to foster initiatives that involve cross disciplinary curriculum strategies and investment in undergraduate and graduate research opportunities for training the next generation of professionals. A description of programs and concepts is presented to provide industry partners examples of actionable efforts in training the next generation of cyber security aware automotive engineers.

2 Introduction

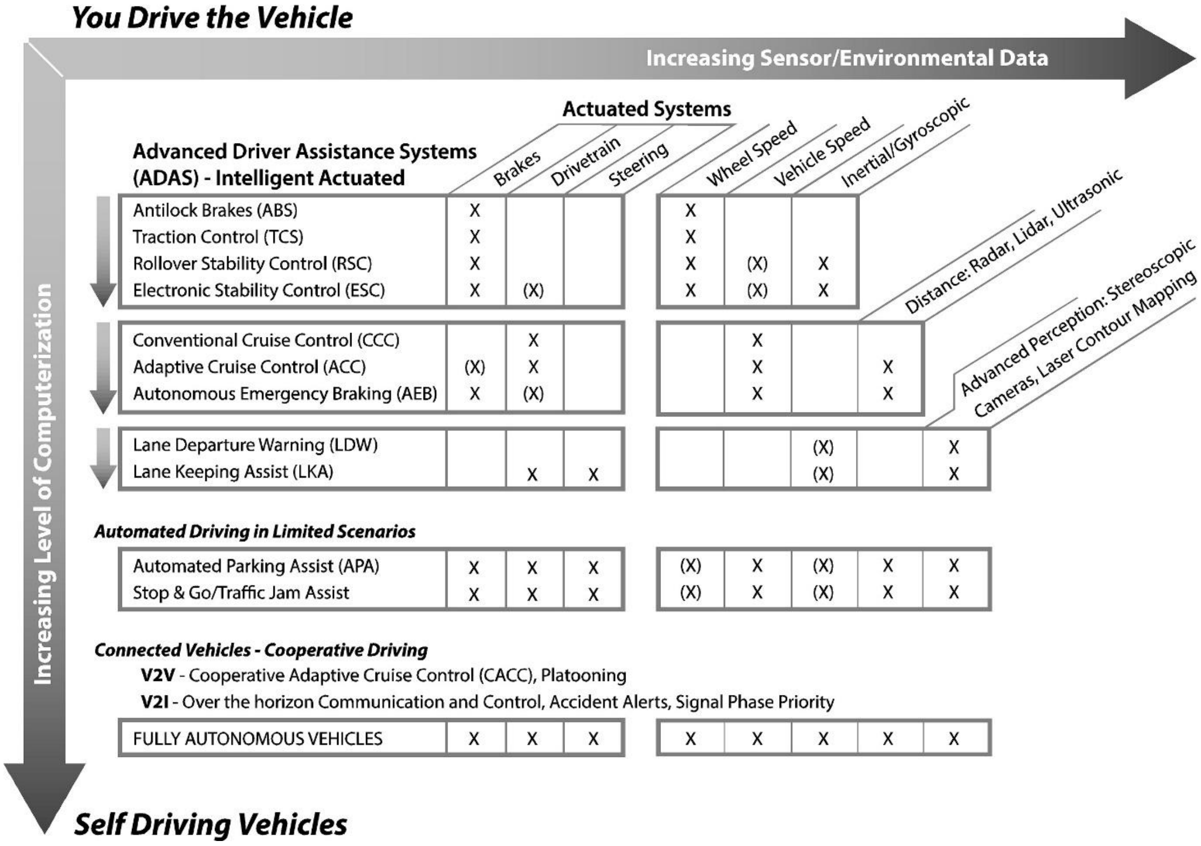
2.1 Motivation

In (Koscher et al., 2010) and (Checkoway et al., 2011) researchers shined the light on the idea that vehicles were vulnerable to cyber attacks. The evolvement of the industry in the past few years has been noticeable in its recognition of cyber security as a necessary component of vehicle and component design. SAE has published the J3061 guidebook to illustrate best practices in the design process. Technology companies are increasing efforts in developing and promoting cyber security solutions for automobiles. Conference attendance on automotive cyber security has grown, and patents related to vehicle cyber security have recent filing dates. However, the people needed to design, implement, and test the secure systems are rare, and the demand for such talent has outpaced the supply of qualified labor in the market. This paper outlines programs, initiatives, and strategies to help the transportation industry engage with universities to facilitate generating the skilled labor needed to address the growing need to solve cyber security related problems.

According to NHTSA reports, in 2013, there were approximately 10.6 million registered heavy vehicles in the US. Based on recent analysis by National Motor Freight Traffic Association, Inc. (NMFTA, 2015), it is estimated that the heaviest of vehicles, class 8 truck tractors, see a service life of 10 years. These trucks are key to maintaining the “just in time” inventory and industrial processes our society currently enjoys. Any major disruption in the flow of goods handled by heavy vehicles could have a significant impact on our daily lives (ATA, 2006). As such, it is critical to address cyber security talent generation for both passenger vehicles and commercial vehicles.

In recent years, there has been significant interest generated in the cyber security of passenger cars due some high-profile research and news. While heavy vehicles are substantially similar in architecture to light vehicles, there exists little research published on this class of vehicles. Heavy vehicles are typically just as computerized as passenger vehicles. More importantly, they have been more pervasively “connected” for telematics, fleet management, and engine management using both satellite and cellular communication technologies for quite some time. Rather than using proprietary communication protocols, which need to be reverse engineered, heavy vehicles utilize the SAE J1939 standard to ensure interoperability between suppliers.

As vehicles are becoming increasingly connected and automated, more and more functions come under the control of electronic control units (ECUs), which utilize actuators or drive-by-wire to control such things as braking, acceleration, steering, etc. This progression is illustrated in the diagram below.



You Drive the Vehicle
Increasing Sensor/Environmental Data
Increasing Level of Computerization
Self Driving Vehicles

Advanced Driver Assistance Systems (ADAS) - Intelligent Actuated	Actuated Systems: Brakes	Drivetrain	Steering	Wheel Speed	Vehicle Speed	Inertial/Gyroscopic	Distance: Radar, Lidar, Ultrasonic	Advanced Perception: Stereoscopic Cameras, Laser Contour Mapping
Antilock Brakes (ABS)	X			X				
Traction Control (TCS)	X			X				
Rollover Stability Control (RSC)	X			X	(X)	X		
Electronic Stability Control (ESC)	X	(X)		X	(X)	X		
Conventional Cruise Control (CCC)		X			X			
Adaptive Cruise Control (ACC)	(X)	X			X		X	
Autonomous Emergency Braking (AEB)	X	(X)			X		X	
Lane Departure Warning (LDW)						(X)		X
Lane Keeping Assist (LKA)		X	X			(X)		X
Automated Driving in Limited Scenarios								
Automated Parking Assist (APA)	X	X	X	(X)	X	(X)	X	X
Stop & Go/Traffic Jam Assist	X	X	X	(X)	X	(X)	X	X
Connected Vehicles - Cooperative Driving								
V2V - Cooperative Adaptive Cruise Control (CACC), Platooning								
V2I - Over the horizon Communication and Control, Accident Alerts, Signal Phase Priority								
FULLY AUTONOMOUS VEHICLES	X	X	X	X	X	X	X	X

Figure 1: The computerization of the heavy vehicle taken from (NMFTA, 2015).

Unfortunately, heavy vehicles are harder to study than passenger cars due to the sheer size and expense of the vehicles. As such, there has been a significant gap in research, though some funded efforts have recently emerged (Daily et al., 2016) and (Burakova et al., 2016). Additionally, the industry did not have sufficient technical resources internally to fully address the issues facing the industry. There were no academic programs designed to equip students with the knowledge required to work in this highly specialized field, especially for the heavy duty sector.

It is important to point out that the ideas and concepts in this paper are intended to show a technique to help fill the talent pipeline for future engineers and security professionals to work in the automotive and heavy vehicle cyber security fields. The programs described herein may not directly produce a cyber security expert, but the programs do provide some important training and opportunities from which future security experts would arise.

2.2 Engineering Education

Education for specific tasks in the industry is often achieved through trade schools, community colleges, or continuing adult education. Students attending four-year universities can obtain degrees in computer science and engineering fields to help them satisfy the base requirement for working in the automotive or heavy duty industry. This education alone is typically insufficient to address growing concerns related to cyber security in the transportation industry. Additional programs are needed to augment the traditional degree path, as well as provide opportunities for non-traditional students.

In traditional engineering design classes, students may learn to perform functional decomposition by studying the flow of material, energy, and information in and out of systems (Ullman, 1996). However, the security of a system needs to address the permissions of a process. In other words, who is allowed to perform such functions? Additionally, vehicles now contain more and more personally identifiable information, requiring data privacy protection and access control. These factors impact the design process and requirements for which a security solutions are implemented. Based on a functional decomposition and an establishment of requirements, a design process using guidance like SAE J3061 can be used.

While the approach for the design method using industry guidance is good, students seeing the process for the first time are just beginning to understand how the cyber-physical systems work. As such, they often do not possess the technical skills to build solutions that satisfy the functional requirements. This means the learning objectives need to introduce students to the technology that is fielded and available in the automotive industry.

A central concept of the educational process is to instill a certain level of professional curiosity into the students working on these programs. This “hacker” mentality reflects the desire to explore how things are put together, how they work, and how they might be modified, which can be malicious, but not always. A simple example would be someone looking at small device and asking “hey, what are all those blinking lights about and what makes them shine?”, “where does that wire go, what does it do, and what happens when I plug it in someplace else?” or “maybe I could hack this to make it better?” Hacks can also be described as non-traditional fixes that are not really intended to be permanent, as in “that’s not a solution, it’s a hack”. Overall, the hacker mindset is a way to explore a problem space with new and interesting techniques and viewpoints without being constrained to only traditional approaches and methods. This non-malicious but non-traditional engagement is a critical state of mind and skill set for students studying cyber security and is a real asset to future employers.

The key to attracting and retaining students with the right mindset for cyber-security work is to give them engaging and flexible research projects which do not fall into the traditional lab model which simply reinforces the “known results” already unveiled in the students text book. A balance between learning the theoretical foundations and solidifying understanding through practical implementations tends to produce the most capable students. It is the freedom to explore new and creative ways to solve real world problems that motivate and excite students. A workbench with proper tools, faculty and university support, and interesting problems to solve provide great teaching tools, increase student motivation, and attract excellent students. It is important that students within such a program be given individual and group projects, which allow him or her to explore practical technology applications in a collaborative atmosphere.

The types of students that fit this description abound, but they need guidance and technical skills to achieve the goal of being effective in solving industry cyber security problems in the transportation sector. In this section, we discuss specific strategies and institutional approaches to attract and train students.

2.3 Approaches to Cyber Security Education

There are few examples of programs dedicated to developing both automotive engineering and cyber security talent in their graduates. Some schools have recognized the need for focusing on cyber security education. Swain (2014) shares an approach to cyber security education that makes the case for having many different approaches to achieve the outcome of graduating student with competence in cyber security. However, his approach was limited to traditional computer science students.

To broaden the awareness of cyber security in education, some programs have emerged that address knowledge gaps for the general student. The program described by Hoffman et al. (Hoffman et al., 2016), discuss the policy and management perspectives of cyber security, which while generally applicable does little for the solving specific problems using technology in the transportation sector. A similar generalized approach was implemented at Iowa State as described in (Idziorek et al., 2011). Again, this approach was broad and focused on awareness of cyber security issues more than their direct application.

As industries assess and deal with cyber security issues, specific industry related approaches have emerged. For example, Foreman et al. (2015) describe how Purdue University has approached teaching cyber security principles for industrial control systems for critical infrastructure. Heavy vehicles are part of the US critical infrastructure. Thus, the general security protections needed for critical infrastructure are highlighted by the fact that cyber attacks on these cyber-physical systems can often lead to physical harm. The Purdue faculty correctly point out that there is a separation of engineering and traditional IT at the corporate, industrial and even educational organizations. Similar organizational issues are likely engrained in the heavy vehicle and automotive sectors as well. While a trend exists in the motor freight carrier and transportation industries, it is only in early stages and not apparent at most companies. Breaking down these artificial barriers can effectively start in college using multi-disciplinary approaches to cyber security problems. Another key point made by Foreman et al. (2015) is the use of hands-on approaches to solve security problems with industrial control systems. A similar hands-on approach is advocated in this paper.

To introduce cross disciplinary topics such as cyber security with respect to critical infrastructure, one approach is to craft modules that can be inserted into computer science and engineering curriculums (Mishra, et al. 2016). The modules developed by Mishra et al. (2016) are self-contained to allow an instructor to insert one or more of them with minimal changes, while still achieving the learning outcomes of the course. Some modules depend on others, but a full introduction to critical infrastructure security can be taught with no prerequisites. In addition, assessment rubrics are associated with each module. We see this concept as addressing multiple issues. For instance, team teaching courses that cross disciplinary boundaries, such as those related to critical infrastructure protection and heavy vehicle cyber security, would no longer be necessary. This collaborative effort is problematic when determining an instructor's teaching load for the semester and, more often than not, leads to an overload. Another issue addressed is curriculum dependency, in which the same modules can be inserted into different curriculum paths. Thus, a computer science student does not have to take the prerequisites for the mechanical engineering course to get the needed information for a dependent module, but only has to take the computer science course that contains the module that is the prerequisite.

Students at Walsh College have an opportunity to explore vehicle cybersecurity in a course based on the Car Hacker's Handbook (Smith, 2015). The course, entitled Foundations of Automotive Cybersecurity, uses the student research challenges as an experience for credit (Brennan, 2017). The availability of a course text and structured classes for credit are a step in the right direction. It is important for those types of offerings to grow and become available at more institutions. Furthermore, this course leverages the work of industry leaders and captures the benefits of the student cyber challenge programs (SAE, 2017).

2.4 Traditional vs Non-traditional Students

Traditional workforce development for Science, Technology, Engineering, and Mathematics (STEM) starts with exposing K-12 students to the various disciplines with the hope that they attend college and pick a STEM major. Undergraduates then acquire the knowledge, skills, and resources to pursue meaningful employment in industry or continue their academic careers as graduate students. Upon successful completion of graduate studies, a researcher can continue in the university setting as a post-doc or faculty member. This traditional approach is illustrated in the graphics shown in Figure 3. The triangle in the figure shows the decreasing number of personnel participating at the different levels. At any level, personnel can transition to the industry, but if they transition without sufficient education, the industry must invest resources to bring the talent up to speed as the scope of the problems they address evolves.

Often a working professional may recognize the need for additional knowledge and skills to remain competitive and effective in their career. In fact, it is a central tenet of the engineering profession to engage in continuing professional development. Often 3 to 5 day continuing education courses are an attractive option for busy working professionals to enhance their skills or cross train into other disciplines. For example, the Continuing Education for Science and Engineering (CESE) department at University of Tulsa offers a course entitled Hands-On Heavy Duty Communications Protocols that is focuses on teaching professionals how to understand and work with J1939 and J1708/J1587 networks by programming a series of exercises that demonstrate different aspects of the protocols. Another class on the digital forensics of heavy vehicle event data recorders is also taught. The flexibility of CESE to match industry needs to available teaching talent makes offering short courses an efficient means to satisfy immediate demands for training.

Beyond the short course offered by continuing education, longer certificate programs in cyber security have emerged. However, there are few, if any, certificate programs for cyber-physical systems security for automotive and heavy vehicle systems. Another attractive approach for working professionals is to pursue a Master's degree in cyber security using distance learning technologies. A challenge remains in determining the best way to conduct effective training in this matter.

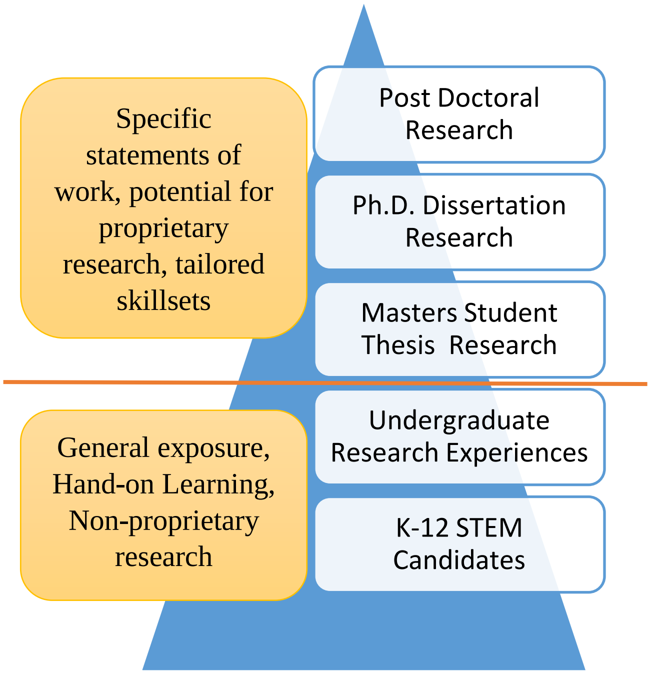

Specific statements of work, potential for proprietary research, tailored skillsets
General exposure, Hand-on Learning, Non-proprietary research
Post Doctoral Research
Ph.D. Dissertation Research
Masters Student Thesis Research
Undergraduate Research Experiences
K-12 STEM Candidates

Figure 2: Traditional progression of university research talent.

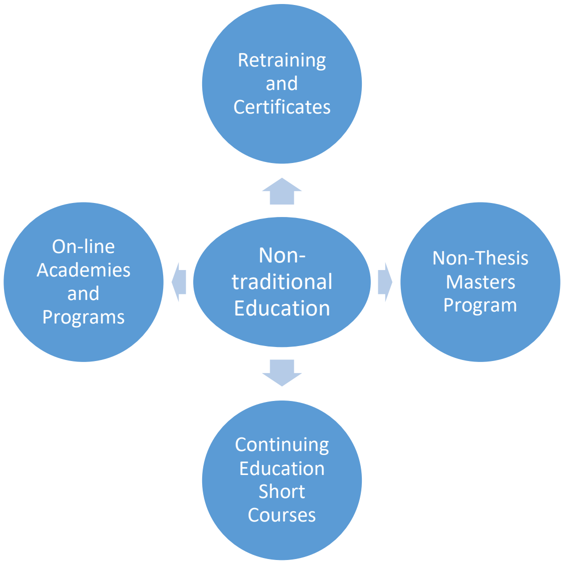

Retraining and Certificates
On-line Academies and Programs
Non-traditional Education
Non-Thesis Masters Program
Continuing Education Short Courses

Figure 3: A few options for non-traditional educational opportunities.

A recent commentary by Martin (2017) points to the need for universities to equip a broader group of students with cyber security skills. For instance, the University of Tulsa has recently instituted Minor in Cyber Security. Though it is served by the Tandy School of Computer Science, it is open to students majoring in any engineering field or majoring in business. The key aspect of the instruction is to teach programming-on-demand, advocating broad training in cyber security with respect to understanding malware, privacy, data analysis, and defending against attacks. In addition, the Tandy School of Computer Science instituted a Master of Science degree in Cyber Security starting the Fall 2015. This degree provides leveling classes for students with no prior experience in cyber security, and targets students from multiple disciplines. It provides an in-depth understanding of information assurance, network security, security economics, and security engineering. Those with prior experience, such as computer science majors, engineering majors, or cyber security minors, can apply their acquired skills as part of the project-based classes. Internships are advocated during the summer with faculty actively placing students in local companies or working with partners, such as NMFTA, where the students stay on campus to perform applied research.

2.5 Technical Skills for Cyber Security Engineering

To enhance critical thinking, educational efforts need to impart knowledge and understanding for the disciplines, provide analysis skills, foster creativity to come up with solutions, and enhance the ability to evaluate the best path forward. These skills need to be translated into application-oriented topics for instruction. There may be many options for specific implementations requiring only a few core concepts. For example, encryption as a tool is a concept, but there may be many options for implementations and its association with an application. Some technical student learning outcomes that range in abstraction can be communicated as a taxonomy in the following evolving table.

	Abstraction level		
Technical Concepts	**Conceptual**	**Fielded Systems**	**Specific Implementations**
Networking	Reliable Delivery Latency Bandwidth Layered Models	Ethernet Controller Area Networks FlexRay	J1939 on a heavy truck. UDS, LIN, IP networks
Encryption	Public Key Cryptography, Private Key Cryptography, Secure Hashing	AES, RSA, Blowfish, MD5, SHA, Random Number Generators	Send encrypted messages using hardware encryption modules built into microprocessors.
Programming	Data-structures, logic, numerical representation, communications, streaming, object oriented programming, functional programming.	Python, C, Arduino, Haskell, Assembly	Interfacing with Linux SocketCAN using Python. Programming an Arduino to read CAN messages
Electronics Design	Sensing and actuation, Printed circuit board design, Ohms law, reading data sheets.	FR4 PCBs, Electronics Design Software, FlexPCBs, evaluation modules. Component selection.	Altium Designer, Digi-Key, Mouser, PCB Assembly, Gerber Files
Transportation Systems	Logistical modeling, congestion, fuel consumption	Telematics units, Maintenance terminals, trucks and trailers	Truck-in-a-box systems, provisioned telematics units

This table is by no means exhaustive or complete. Rather, it expresses how to introduce an abstract concept and then drill down to specific implementations to give students experiences that help them improve their skill sets. Active industry participation in university programs helps keep relevant topics in front of students.

3 Student Research Experiences

The student research experience program at the University of Tulsa provides an excellent opportunity for both industry and the university to reap significant rewards. This section describes this program for student researchers to study solutions and strategies related to heavy vehicle cyber security. The first cohort of students came into the program with no background in cyber security.

The students are provided with summer employment, at competitive pay, working on real research projects learning applied skills and techniques relating to heavy vehicle cyber security. The students participate not only in research at the university but also partake in field trips to OEMs, motor freight carriers, and NMFTA for additional industry education and perspective. This type of program creates a significant draw for the university for talented students as well as the potential for university owned intellectual property. The industry benefits from open source results from real research being conducted at low cost as well as obtaining access to a pool of prospective employees with the real-world skills for heavy vehicle cyber security.

A typical student project is to build a benchtop truck system that has a heavy vehicle engine control module (ECM), instrument cluster and diagnostics port. Based on this hardware setup, the students learn how to read and interpreted the J1939 and J1708 networks using their custom-built hardware and software. The current approach is to use a Teensy USB based development board that is built on a Freescale 32-bit ARM Cortex M4 processor that is compatible with the Arduino programming environment. During this process, the students often discover the ability to execute a denial of service attack on a CAN bus by inadvertently flooding the network with CAN traffic because they forgot to set up a transmitting schedule.

After seeing how easy the denial of service attack was implemented, a student proposed a solution to mitigate that threat from propagating through a network. The idea was to set up two CAN controllers and transceivers with the Arduino microprocessor in the middle. One side of the network will be protected and the other will be "in the wild." Messages received on the unprotected network were examined for their content and schedule. If the message was safe to pass, it would do so. The solution was dubbed the "CAN Conditioner" and was implemented and demonstrated at the NMFTA meeting in the fall of 2016. While commercial CAN gateways exist, this student project was encouraging because it took an aspiring student with no background in embedded systems and cyber security less than a year to develop a functional prototype that could actually prevent some types of cyber attacks on trucks.

After the successes from the first year of the program, NMFTA and the University of Tulsa have expanded the project to include industrial partners. The commitments were structured to support larger numbers of students for the full calendar year. This way students remain active in the project year-round and not just in the summer. With firm commitments in place, recruiting, mentoring, and research activity definitions are being pursued to start the first round of students at the beginning of the 2017 summer session.

It is important to note that this program is primarily focused on undergraduate engineering and computer science students that work together and share information. The statement of work is worded in such a way that suggested topics will be explored, but the decision of the tasks and focus remains with the faculty director for the program. This means the system is not conducive to performing proprietary research. Written reports and student presentations are deliverables for the project. The students also have the opportunity to meet industry professionals and learn about motor carrier operations, which are experiences beyond the classroom that improve their ability to be effective in solving problems sooner. The results and outcomes of the student research will be shared among all the participating organizations. Sponsors are afforded the opportunity to review any publications before being released to ensure that the content being disseminated does not harm the industry. While the final decision to publish remains with the university, suggested edits will not be unreasonably withheld. Input from industrial sponsors is welcomed and matching research efforts to capabilities and industry needs is a program goal.

4 Challenges in Cyber Security Education

4.1 Recruiting student talent

A key aspect of any academic program is attracting the right talent. Very few college students go to school with the intent to study automotive or heavy vehicle cyber security. It is incumbent on the faculty and program managers to help identify and recruit students for the program. Clearly, the ability to hire undergraduate research assistants can guarantee placement, but the question of how to recruit students into the program remains.

The interesting part of an automotive or heavy vehicle cyber security program is that the cross disciplinary activities can both attract and accommodate several different fields of study including computer science, electrical engineering, mechanical engineering, and even mathematics. There are multiple benefits to the students who participate in this program, which are useful to the recruiting effort:

- The participation in the program can enrich the overall education of the student in their chosen major by providing concrete practical applications
- The program offers paid summer job opportunities as well as some paid work during the year
- The practical experiences the program offers with connected vehicles will also help students find employment once they graduate
- The hands-on experience with cyber-physical systems and cyber security increases the opportunities for employment and graduate studies for participating undergraduate students

Recruitment of these students requires capturing their interest through videos and hands-on activities during campus visits, as well as outreach to high schools. Once attracted, it is essential to retain the students. Thus, additional incentives for student programs, such as conference travel, engaging with OEMs and motor freight carriers, and invitations to participate in the NMFTA bi-annual meetings on heavy vehicle cyber security.

4.2 Underrepresented demographics

Women are especially underrepresented in STEM fields due to a number of different factors. A recent report by CNN (Petroff, 2017) shows that most girls lose interest in STEM fields by the time they are 15 years old. Some of the key reasons include lack of role models, lack of equal participation by women in existing programs, as well as many other social factors. NMFTA’s Heavy Vehicle Cyber Security (HVCS) program seeks to support young women to pursue STEM related degrees and jobs as part of their overall strategy to develop more qualified resources for the industry. However, the process by which this objective can be achieved is not clear. Recently, Chickowski (2017) stated that industry figures show that cyber security has a very poor male-to-female ratio in the workforce. Thus, growing the female workforce in the area of cyber security, and its involvement with heavy vehicles, cannot only rely on female role models, which Chickowski cites as needed for more participation by women. The expectation that the women professionals in these fields have the additional time, energy, and interest to perform this duty by virtue of their gender is nonsensical. They may prefer to coach little league or teach martial arts classes. Plus, these women were likely mentored by men, given the statistics. Therefore, all professionals must be proactive in mentoring all young people in the field and tailor their mentoring to the needs to the individuals and their challenges as early in the educational process as possible. Tailoring mentoring is an essential component of the process, while consistent expectations of involvement and achievement are delivered across a group of students. Ensuring a work environment with engaging, individual project goals and forums for positive, collaborative exchanges among peers that highlight advancing skillsets can provide benefits to all demographics. The knowledge that such an environment exists will be what attracts and retains high quality men and women.

4.3 Targeted Scholarships

In a very competitive field of engineering and computer science, especially where cyber security is highlighted, the competition for students is significant. To help attract the students early in their careers, programs should be established and maintained by private industry for scholarship opportunities. The success of the NSF and NSA’s CyberCorps® : Scholarship for Service programs demonstrate how the government can use academic scholarships to train and recruit aspiring talent into the various government agencies that deal with cyber security issues on a regular basis. These lucrative scholarships contract with the students, requiring them to serve the government as employees for a minimum of two years in addition to being summer interns while in school. Students who have self-identified as wanting to work in cyber security for the government seek to enroll in these programs, which speaks to the effectiveness of recruiting talent by having college expenses reduced and a job waiting for them upon graduation.

Scholarships that are sponsored by the industry can also be effective recruiting tools. Tuition and expenses for college education is quite high, but many students are offered financial aid to bring their out-of-pocket expenses down. However, the expenses are often not zero, so motivated students seek additional opportunities. For example, if a student wishes to pursue a minor in cyber security, they may have to pay for additional credits to take the necessary classes because of it increasing their load. Since engineering graduates with a minor in cyber security will help fill the talent gap in the heavy duty and automotive sector, it makes sense for the industry to target support for these aspiring students and eliminate any financial burden of pursing this unique combination of skills.

From an industry perspective, there is little appetite to invest scholarship money into programs that do not lead to talent generation that they can use later. This makes general scholarships less attractive. Furthermore, the retention rate in engineering and computer science programs in the freshman and sophomore years is much lower than the likelihood to graduate with a technical degree once a student reaches their junior year. Scholarship donors can stipulate eligibility requirements for the student support. Institutional advancement offices can accept earmarked support for scholarships. For example, an industry partner may want to establish scholarship opportunities for veterans. Another example is gap funding, where industry may supply the university with additional funds to cover cost increases or family needs to keep a qualified student at the university through graduation. University advancement offices are quite adept with establishing the scholarship guidelines and properly administering awards.

For example, the NMFTA established partial masters and undergraduate tuition scholarships to help provide bridge funding for qualified candidates. While this aspect of the program is still in an early phase, several scholarships have already been awarded by NMFTA. With a system in place for selecting students and administering the program, this type of scholarship provides a mechanism for industry participation.

4.4 Engineering Ethics

Ethics education has been a requirement for degree granting programs in engineering based on the requirements set for by the Accreditation Board for Engineering and Technology (ABET, 2017). Accredited degree programs require a student outcome which states that graduates should have “an understanding of professional and ethical responsibility.” Not only has the profession identified ethics as a key outcome, the importance of ethical behavior regarding cyber security is paramount. The challenge, however, is to be able to instill the theory and practice into the students so they will make ethical decisions as they progress in their careers.

Ethics education requires purposeful engagement and training for students to understand the role of professional ethics. (Harvey et al., 1985) recognized the negative stereotype associated with hacking, especially when the ethical issues were only realized after law enforcement explained how there was an issue. Instead of letting students go explore with their own curiosity to guide them, Harvey suggested the better approach was to guide and empower the aspiring students with the following suggestions:

1. Professional involvement – A contributing member in the industry takes the time to model correct behavior to the students. As seen in (Chickowski, 2017), mentorship is important for student growth.
2. Access to real power – provide students with the actual tools and resources used in the industry.

3. Challenging problems – helping students define problems where their solutions make a difference and push their skill set.
4. Provide a safe space for learning – let student play out the role of being a hacker to satisfy their curiosity by encouraging them to participate in bug bounty programs, cyber challenges or other sanctioned hacking events.

Today, the term "ethical hacker" is used to describe cyber security talent who have the skills to potentially be malicious, but exercises those skills in an ethical way to improve the security posture for their clients. Ultimately, the goal for an educational program where pupils gain hacking skills is to also guide them to be ethical in their use.

Assessing the efficacy of approaches to teaching ethics is challenging, since there is rarely a measurable and objective student outcome that can be evaluated. Instead, most research regarding ethics education relies on student reaction surveys to assess psychological fidelity with the hopes that formative student experiences will encourage ethical decision making in the future. Not all ethical dilemmas are the same, but often the patterns someone experiences are the same. For example, a supervisor needs to submit a proposal for a big job and wants your test results to favor an outcome. However, there are results that you cannot explain that are not helpful. Should you discard the data? These and many other "case studies" help students identify ethical dilemmas. Once those situations are recognized, then the guidance provided by professional engineering societies can be used, such as found in (NSPE, 2007).

Tactics for teaching engineering ethics vary. At the University of Tulsa, mechanical engineering students experience their ethics training using a role play experience where they take on the role of an engineering expert witness that has to provide testimony in court. The students prepare a written report and undergo a mock interview to assess their suitability to serve as an expert. The interview is intended to push the students into ethical decision making under pressure. A group debrief session helps make sense of the experience and enables a deeper class discussion about engineering ethics. The approach for the role-play was published in (Brummel et al., 2014) with enhancements in the experience explained in (Brummel et al., 2015). Reaction surveys suggest this method of teaching engineering ethics through role-play has merit.

4.5 Responsible Disclosure

A critical aspect of ethical professional research conduct is understanding and abiding by responsible disclosure. While the term "responsible disclosure" has been falling out of favor recently, the core concept remains the same. If the research conducted by the university students reveal a security flaw or issue in a commercial product, it is incumbent upon the students and university to report the issue to the responsible party to allow them the opportunity to fix the issue before going public. This would be true regardless of whether the company in question is a direct sponsor of the program or not. The heavy vehicle ecosystem is tightly integrated and one security issue may have a wide impact.

When using a vehicle or specific piece of hardware for videos and demonstration, it is important that the students notify the company in question even if the make/model or manufacturer has been concealed or obfuscated. While putting a piece of tape on the steering wheel does block the name of the truck, most industry insiders can still pick out the exact make and model by the dash. Such professional courtesy goes a long way to help foster industry trust and significantly increase collaboration and support.

Often students are eager to share results, especially if there is a chance for them to be in the news. Media training is a necessary element of student programs dealing with cyber security. The media should not be isolated, but students should understand the goal of the media may not have everyone's best interest in mind. Core messaging concepts, bridging, and the art of the pivot are some tools that student researchers can use to represent themselves, the university, and the industry in the best light possible. Actively countering the sensationalism associated with the malicious hacking of cars is an important activity in a formal program.

Responsible and careful disclosure is a critical aspect of the program since it is directly supported by industry funding rather government funding. Without assurances of responsible disclosure and professional courtesy notifications, private industry will be hesitant to support the effort.

4.6 Handling Proprietary Information

The graphic of Figure 3 showing the broad base of student progressing towards the peak of the research program has a line between the undergraduate experience and the graduate programs. The level and capability of the research performed by the students above that line can provide real value to an industrial sponsor. However, to engage in university/industry partnerships, the exchange of proprietary information may be necessary for application research. This information adds value to the research because students can examine real components and data.

While a university can contract to maintain the confidentiality of proprietary data for a project, it is more difficult to find mechanisms to publish results without any data disclosure. There can even be an issue with a company not wanting any information in the publication where it could be inferred that the research pertained to them. From a university perspective, the ability to disseminate research results through publication and presentation is the standard to active research. It is equally essential for PhD students to publish their work in order to obtain an academic or industry research position. Thus, some universities decline to partner with businesses that limit publication. Others have begun adopting contract language that explores ways to collaborate with business representatives on a publication, allow for limited review by the business of the results prior to submission, and provide guidance on responsible disclosure, which as discussed earlier, introduces limitations on when and how to disclose results.

To accommodate responsible disclosure, theses and dissertations can be held from publication for a time period of six months to a year. The advantage of this strategy allows for results to be responsibly disclosed and addressed by the industry while not preventing the student from graduating. The disadvantage is that the student may be restricted from publishing any of the research effort while looking for a job before graduation. In addition, if the issue is addressed by industry before publication, the student may not receive credit for the result.

Patenting and copyrighting results can also be issues with the collaboration. First is whether the business has right of first refusal should an invention be disclosed. Second is who pays for the patent documentation creation and filing.

These issues indicate the contracting between universities and industry must be carefully constructed to meet the objectives of each entity to participate in the partnership. Some avenues for examination between the partners are:

- Determining why publication should be limited. Perhaps the business is concerned with competitors recognizing their flaws, such the disclosure of a security vulnerability, or their successes, such as having found a way to make a correction to a common problem and obtain increased market share.
- Addressing the need for limitation by increasing flexibility elsewhere. If certain results require limiting publication until the business can address the results, then in addition to the core research funding, the business could supply funds for the university to investigate and experiment with security issues that are peripheral to the core research to allow for publication in those areas and still have the benefits of early action on the results.

- Accounting for the benefits of applied research. Universities may need to be more flexible in their publication requirements from contracts. Many students that wish to be involved in the cross disciplinary training that accompanies heavy vehicle cyber security may not be concerned with publication but rather be prepared to directly enter the company that is supplying the research funds or another company that wants the same skillset. Acknowledging that this avenue is available may produce more synergistic relationships between businesses and the students being supported, without results dissemination issues.

Universities will continue to be very resistive to allow external entities to restrict publication. Thus, exploring creative ways to work with universities in ways that do not require the exchange of confidential or proprietary information may be the best approach. Undergraduate research projects, for example, are not conducive to proprietary research due to the newness of their skill set and competing time commitments. Precompetitive research projects that benefit the industry as a whole are preferred to projects that require proprietary information to succeed.

5 Conclusion

In this paper, we discuss the different strategies of fulfilling the need for talent that can address cyber security issues as it relates to the automotive and heavy-duty industries. The ideas and programs described give a template and examples of how industry and universities can work together to address the longer term need for cyber security talent needed in the industry. The focus on heavy vehicles throughout the paper was based on the authors' experiences, but strategies and concepts are equally applicable to the light passenger and medium duty vehicle segments as well.

The following are options for active industry participation with universities:

1. Sponsor specific research projects at the graduate or post-doctoral level. These contracts or consortiums can have mechanisms for dealing with proprietary information. Students must have some avenue for publication.
2. Undergraduate research experience programs provide undergraduate students opportunities to engage with faculty to do cyber security related research. This hands-on approach augments traditional classroom experiences and enables students to become familiar with industry technologies and challenges before they graduate.
3. Student scholarship programs targeted to supporting STEM students to pursue studies in cyber security are effective recruiting tools. Industry sponsored scholarships are needed to compete with the government based scholarship for service programs.
4. In-kind support helps students learn fundamental concepts on relevant systems. Most universities have advancement offices that can maximize industry contributions to these educational initiatives.

Educational initiatives in cyber security should place an emphasis on engineering ethics training. This is often driven by the professional or academic mentor. Proactive training related to responsible disclosure and dealing with the media are highly encouraged for any program related to cyber security.

The programs and strategies for talent generation are explained to help industry get a better understanding of how to work with universities regarding cyber security training. The specific examples and programs from the NMFTA and the University of Tulsa can provide actionable opportunities, or they can serve as templates and ideas for other industry/university partnerships. Combining traditional university approaches, hands-on research experiences and industry sponsored student challenge events may be a recipe to develop and maintain the talent pipeline for the cybersecurity needs in transportation for years to come.

6 References

(ABET, 2017) Criteria for Accrediting Engineering Programs, 2017 – 2018 available at http://www.abet.org/accreditation/accreditation-criteria/criteria-for-accrediting-engineering-programs-2017-2018/, 2017.

(ATA, 2006) American Trucking Association, “When Trucks Stop, America Stops,” available at http://www.trucking.org/ATA%20Docs/What%20We%20Do/Image%20and%20Outreach%20Programs/When%20Trucks%20Stop%20America%20Stops.pdf, 2006.

(Brummel et al., 2014) B. J. Brummel, J. S. Daily, “Developing Engineering Ethics through Expert Witness Role Plays, ” *2014 ASEE Annual Conference & Exposition*, Indianapolis, Indiana. https://peer.asee.org/20291, available at https://peer.asee.org/developing-engineering-ethics-through-expert-witness-role-plays.pdf, 2014.

(Brummel et al., 2015) B. J. Brummel, J. S. Daily, and J. T. Stauth, “Guidelines for Constructing Expert Witness Role-plays for Engineering Ethics,” *2015 ASEE Annual Conference & Exposition*, Seattle, Washington. p.24166, available at https://peer.asee.org/guidelines-for-constructing-expert-witness-role-plays-for-engineering-ethics.pdf, 2015.

(Burakova et al., 2016) Y. Burakova, B. Hass, L. Millar, and A. Weimerskirch, “Truck Hacking: An Experimental Analysis of the SAE J1939 Standard,” Usenix WOOT, Austin, TX, Available from https://www.usenix.org/system/files/conference/woot16/woot16-paper-burakova.pdf, August 11-12, 2016.

(Brennan, 2017) M. Brennan, “Walsh College Offers Nation’s First Auto Cybersecurity Course Starting April 4”, MITECHNEWS.com, last accessed 12 June 2017 from :https://mitechnews.com/cyber-defense/walsh-college-offers-nations-first-auto-cybersecurity-course-starting-april-4/, March 24, 2017

(Checkoway et al., 2011) S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, “Comprehensive Experimental Analyses of Automotive Attack Surfaces,” *USENIX Security*, available at http://www.autosec.org/pubs/cars-usenixsec2011.pdf, August 10–12, 2011.

(Chickowski, 2017) E. Chickowski, “Is mentorship the key to recruiting women to cybersecurity”, *DARKReading - Careers and People, Information Week*, Mar. 7, 2017, available at http://www.darkreading.com/careers-and-people/is-mentorship-the-key-to-recruiting-women-to-cybersecurity/d/d-id/1328331. 2017.

(Daily et al., 2016) J. Daily, R. Gamble, S. Moffitt, C. Raines, J. Miran, I. Ray, S. Mukherjee, H. Shirazi, “Towards a Cyber Assurance Testbed for Heavy Vehicle Electronic Controls,” *SAE Int. J. Commer. Veh.*, 9(2):339-349, 2016.

(Foreman et al., 2015) C. Foreman, M. Turner , and K. Perusich, “Educational Modules in Industrial Control Systems for Critical Infrastructure Cyber Security,” *2015 ASEE Annual Conference & Exposition*, Seattle, Washington. https://peer.asee.org/23911, 2015.

(Harvey, 1985) B. Harvey, Computer Hacking and Ethics, an essay for a “Panel on Hacking" held by the *Association for Computing Machinery* in April, 1985, available at https://people.eecs.berkeley.edu/~bh/hackers.html, 1985.

(Hoffman et al., 2016) L. Hoffman, R. Heller, and C. Toregas, “Exploring Ways to Give Engineering Cybersecurity Students a Stronger Policy and Management Perspective,” *Spring 2016 Mid-Atlantic ASEE Conference*, George Washington University, available at https://www.asee.org/documents/sections/middle-atlantic/spring-2016/Exploring_Ways_to_Give_Engineering_Cybersecurity_Students_a_Stronger_Policy_and_Management_Perspective.pdf, 2016.

(Idziorek et al., 2011) J. Idziorek, M. Tannain, and D. Jacobson, “Teaching Computer Security Literacy To Students From Non-Computing Disciplines,” *2011 ASEE Annual Conference & Exposition*, Vancouver, BC. https://peer.asee.org/18741, 2011.

(Koscher et al., 2010) K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage. “Experimental Security Analysis of a Modern Automobile,” *IEEE Symposium on Security and Privacy*, Oakland, CA, available at http://www.autosec.org/pubs/cars-oakland2010.pdf May 16–19, 2010.

(Martin, 2017) K. Martin, “Closing the cybersecurity skills gap with STEM,” *DARKReading - Careers and People, Information Week*, Feb. 2, 2017, available at http://www.darkreading.com/careers-and-people/closing-the-cybersecurity-skills-gap-with-stem/a/d-id/1328181, 2017.

(Mishra, et al. 2016) S. Mishra, T. Howles, R. Raj, C. Romanowski, J.L. Schneider, A. McNett, and D. Dates, “A Modular Approach To Teaching Critical Infrastructure Protection Concepts To Engineering, Technology And Computing Students,” *IEEE Frontiers in Education Conference*, pp. 1-7, 2016.

(NMFTA, 2015) National Motor Freight Traffic Association, Inc., “NMFTA Heavy Duty Vehicle Cyber Security Whitepaper”, September 2015.

(NSPE, 2007) National Society of Professional Engineers, “Code of Ethics for Engineers” https://www.nspe.org/sites/default/files/resources/pdfs/Ethics/CodeofEthics/Code-2007-July.pdf

(Petroff, 2017) A. Petroff, “The exact age when girls lose interest in science and math,” *CNN tech*, available at http://money.cnn.com/2017/02/28/technology/girls-math-science-engineering/index.html, 2017.

(SAE, 2017) SAE Battelle CyberAuto Challenge, last accessed June 12, 2017 from http://www.sae.org/events/cyberauto/

(Smith, 2016) C. Smith, *Car Hacker’s Handbook, A Guide for the Penetration Tester*, No Starch Press, ISBN 978-1-59327-703-1

(Ullman, 1996) D. Ullman, *The Mechanical Design Process*, McGraw Hill, New York, ISBN 978-0-07-339826-6