Interdisciplinary Approaches to Cybersecurity Education for Autonomous Vehicle Engineers

By Dr. Sébastien Lachapelle

Associate Professor of Geomatics Engineering, University of Calgary, Canada

1. Introduction to Cybersecurity in Autonomous Vehicles

With autonomous vehicles (AV), to date, no cybersecurity aerospace military education encourages, much less achieves, novice-to-advanced skills when encountering novel, imaginative, or sophisticated, multi-vector attacks that include social engineering as well as physical blending, unstoppable threats that could occur under a time-granular real-time limited latency or denial of service attack mitigations; all this, while considering safely intermingling autonomous vehicles with non-autonomous vehicles. Furthermore, there is no certification program for AV cybersecurity available today. Based on the exception-driven state, defense-in-depth, fail silent, and integrate modularity concepts, we present the development approach and results of the first cybersecurity-dedicated education and experimental testbed-hardware-software platform used by the Graduate School of Engineering and Applied Sciences, Oceana Virginia campus, U.S. Naval Postgraduate School, Department of the Navy.

Although the military has a history of cybersecurity experience and use in aerospace, the commercial vehicle sector does not. Aerospace avionics cybersecurity intrusions fall under national defense thresholds such as wartime emergency or full-mobilization defense activities. Aviation components are similarly utilized, tested, and maintained with self-contained and modular hardware and software due to high criticality, regulatory oversight, and testing regimes. Additionally, the pilots of these high-performance military- and commercial-grade air vehicles receive significant education and training in order to operate, control, and navigate them in tandem with these redundant and maneuvering safety systems.

Interdisciplinary approaches to cybersecurity education for autonomous vehicle engineers

1.1. The Importance of Cybersecurity in Autonomous Vehicles

The dynamic nature of the automated driving environment, cross-collaborations from different industries, research disciplines, and development cycles have to be recognized as mutually reinforcing actors. To promote awareness of the importance of cybersecurity in AV engineering, an educational program is essential to form the future automotive engineers. Introducing interdisciplinary perspectives to AV engineers is critical to ensure the skills necessary for ensuring both the safety and security of autonomous vehicles that operate in increasingly complex and connected vehicle environments. The curriculum of the associated educational programs should indeed incorporate the relevant broad knowledge and practical experiences and prepare engineering students for their future professional work. This paper presents a summary of the cybersecurity topics previously published to emerging AV engineers and promulgates an interdisciplinary educational structure for AV cybersecurity education.

Autonomous driving research has rapidly progressed within the past decade. With advances in artificial intelligence, sensor technology, and vehicle-to-everything (V2X) communication, autonomous vehicles (AVs) are capable of safe driving on public roads and bring significant payoffs in saving lives. However, the increasing complexity of automated vehicle systems and the future social and economic critical mass where autonomous vehicles will play an important role also require significant attention to ensure the emerging level of autonomous vehicle trustworthiness. The cybersecurity vulnerabilities in automated vehicles are more striking compared to isolated embedded electronic control units (ECUs) in vehicle components, which in turn affects system cost and development time. The real-world safety and security of AVs are key attributes in the assessment and decision required to put an AV in motion compared to conventional vehicles.

2. Foundations of Cybersecurity

2.1.2. Components and Anatomy of Cybersecurity. Cybersecurity is fundamentally an interdisciplinary field that weaves together a range of previously-established processes, laws, and norms to protect information and data. Six general components of cybersecurity guide the field: CIA triad, confidentiality, integrity, and availability. These components offer a high-level view for reasoning about the broad classes of initiatives that might be taken in designing secure systems.

Addressing cybersecurity problems involves an understanding of adversaries who might manipulate these systems with expectable criminal, political, or economic motivations, seeking ways to protect these systems using various mechanisms, tools, regulations, laws, methods, and accepting that adversaries will potentially exploit these systems for their nefarious purposes. The motivation for protecting systems should be familiar to all engineers: trade-offs between the cost of systems and the economic impact of threats play an essential part in justifying investment in cybersecurity. A critical economic and ethical question focuses on how those who build, obtain, and use these systems can be convinced to invest in ways and amounts that maintain sufficiently secure systems. Thus, one key challenge facing the field of cybersecurity is not merely the protection of systems in general; instead, it is the necessity to convince companies, organizations, governments, and ultimately society that these investment decisions are important and valuable.

2.1.1. Introduction and Key Concepts. What is cybersecurity, and why should engineers in general, and autonomous vehicle (AV) engineers in particular, care about it? Put simply, cybersecurity is the discipline that addresses the threats and vulnerabilities that arise in ICT systems that may harm investors, owners, users, and the systems themselves. Cybersecurity considers threats and vulnerabilities manifested in conditions like unauthorized access to data, suppression of business operations made possible through ICT, destruction or malfunction of safety-critical systems (as would be present in AV and industrial control system applications), disruptions to essential governmental activities, and more.

2.1. Cybersecurity Background

2.1. Basic Concepts and Terminology

2.1.4. Trustworthiness Cybersecurity bounds a system's integrity, confidentiality, and availability within some specified probability. Meanwhile, privacy and resilience play critical roles. Respectively, they are: (i) establishment and maintenance of some degree of control over personally identifiable information; and (ii) capability of anticipating, enduring, recovering from, and adapting to conditions which can block conformity to system goals without breach, and potentially create new goals. Information system security is deemed trustworthy when it offers these bounds and plays these roles with justification and completeness according to specified categories of observables, interpretations, methods, and assurances. At a level of confidence, experimental observations are not surprising for most system states. The justifications and completions are logical implications of specified properties which security control designs and threat defenses are assessed at achieving. Requirements, designs, threat defenses, assessments, and evidences must be available and can be audited appropriately for inherent risks in implementation, operation, and deployment to be managed effectively. Cybersecurity has largely evolved into a science of trustworthiness, often implicitly.

2.1.3. Safety Safety is freedom from accidents with unacceptable effects - damage to health, environment, or economy. These accidents include unintended errors, omissions, ambiguities, or misinterpretations in software specified or implemented to achieve some system goal or function. The software is part of an embedded system, and the system could be part of a sociotechnical system, such as a transportation system that includes autonomous vehicles. However, safety is primarily associated with safety-critical systems, like a transportation control system, whereas security is primarily associated with security-sensitive systems, like an identity management system.

2.1.2. Security Security is a set of measures intended to protect computing systems from threats to their integrity, confidentiality, and availability. Integrity exists when data or system function is correct or uncorrupted. Confidentiality exists when data is accessible only to people who are authorized to access it. Availability exists when systems are available for authorized uses. A threat is the possibility that an adversary may exploit a system weakness (a vulnerability) to breach security and thereby cause damage. Breaches can be caused by accident, fraud, or malice. Security is a well-developed field with respect to information systems. It is far less well-developed for CPS. Reasons for this state of affairs are: (i) differences between information systems and CPS; (ii) extremely small market incentives; (iii) distributed responsibility.

2.1.1. Cyber-Physical Systems A cyber-physical system (CPS) - also known as an embedded system - integrates computation, networking, and physical processes. The physical processes are controlled by embedded computing devices, which are networked to achieve operating safety and efficiency. Examples include medical devices, robotic manufacturing assemblies, energy production and distribution, transportation systems, and buildings.

This section describes the basic concepts and terminology used throughout the article.

3. Interdisciplinary Perspectives on Cybersecurity Education

Encouraged by the experiences in the educational programs shared in this paper, university research performed by researchers to keep graduate and undergraduate engineering students updated is encouraged.

Addressing SPBD for the depths of an interdisciplinary graduate program might also be the initial challenge in that there are some. Graduates must be prepared to approach cybersecurity at the intersection of where intelligent software agents act, at the boundary where the cyber and physical worlds meet. Universities are updating their computer science (CS) and computing-accredited engineering (CSE) or electrical engineering (EE) graduate programs to recognize this computer-physical-scaffolding, forming new departments and courses.

As a security design principle, we argue that "Security- and Privacy-By-Design (SPBD)" should be the first step in any cyber-physical-architecture-building, including the building of a cyber-physical system (CPS) such as an autonomous vehicle (AV). SPBD graduate-level cybersecurity programs exist. At the time of formulating the research and educational proposal, such focused programs were nascent, and almost none were US-located, making it logistically unfeasible given the initial founder's professional, academic, and geographic profile.

In this paper, we present four teacher and supervisor approaches that were used to educate different cohorts of recent engineering graduates on advanced cybersecurity tools, techniques, and knowledge for autonomous automobiles (or advanced driver-assistance systems). Practices that can be improved at different institutions and directions for future research are offered.

Bridging the fields of ethical decision-making, machine learning (ML), and computer architecture, deep learning and robotics are being leveraged to make advances in self-driving. In the race to innovate, researchers are challenged to determine if models perform ethically and reliably under various states and transitions. This requires interdisciplinary input from researchers with primarily differing goals. In the eyes of some, security is often an afterthought, or sometimes thought of towards the end of the design process.

3.1. Engineering and Technology

Familiarity with the state of the art and current best practices in engineering and technology for security, privacy, and dependability is essential for all advanced vehicle engineers and scientists. A sufficient shared background with experts in security, privacy, and dependability ensures a more productive, efficient, and innovative research and development process. In the mandated continuing education path for these professionals, choosing a set of courses in security, privacy, and dependability draws not only ad-hoc connections across disciplines, but overlays and integrates methods and concepts emphasizing security, privacy, and dependability. As a result of this critical integration of interconnected and relevant methods and concepts, value and complexity are added, not just time and effort. Continuing education must align with the professional's epistemic motives, so emphasizing tangible linkages and including experts from these disciplines makes clear and direct connections.

Whether the focus is systems engineering, automation, robotics, or intelligent transportation systems, advanced vehicle engineers and scientists must understand the detailed technical underpinnings of these systems in order to successfully develop and deploy new concepts. From basic electrical and mechanical knowledge to advanced topics such as control engineering, communication networks, machine learning, and artificial intelligence, the skills required to make creative connections, refine and integrate principles, and address open questions across disciplines are at the core of an engineering education. Here, making interdisciplinary connections is essential to give a sufficiently rich understanding of the engineering and technology connection points.

4. Challenges and Opportunities in Cybersecurity Education for Autonomous Vehicle Engineers

Providing cyber education for engineers and scientists training for careers in established domains is difficult because of both the scale and the critical timing of the required added curricular components. In addition, at present the motivation and willingness of faculty to seek and commit to training that itself resides largely outside their area of expertise must be considered. The rapidly growing field of cybersecurity offers a contemporary setting to overcome historical barriers associated with infusing applied disciplines with new technologies having social implications. In revisiting the concept of cyber infrastructure, again used at a time when the capacities of digital communications technology for researchers and instructors were rapidly expanding, this chapter identifies common functional requirements for developing a cybersecurity curriculum in any developing grad-focused program. Programs alert to these requirements that emphasize an orientation supportive of innovation, practice, and connections to integral security challenges are particularly well-suited. Programs that share these roles between key technical and social science collaborators or course faculty are even better. High-quality collaborations of this nature may create the next-generation digital operator workforce possessing cross-disciplinary knowledge that relates technology study to its implications while simultaneously delivering commercially viable solutions for societal challenges.

It is increasingly challenging to produce engineers and scientists who not only possess deep technical expertise related to their fields of inquiry, but also carry perspectives from outside their discipline, enabling them to think critically in an increasingly interdisciplinary research environment. This chapter comments viewing cybersecurity as a contemporary grand challenge impacting societies worldwide. Not only is interdisciplinary knowledge critical in addressing the cybersecurity design and training requirements of protocols and applications utilized by engineers and scientists specializing in virtually any field, it is particularly germane in the domain of autonomous vehicles. Shaik, Mahammad, et al. (2019) discuss the Achilles' heel of decentralized identity management.

4.1. Identifying Key Challenges

Although several disciplines offer essential cybersecurity content to AV engineering curricular materials - e.g., computer science and data science provide the technical knowledge needed to secure systems and detect malicious behavior, engineering provides design methods that integrate AV cybersecurity with safety and other systems properties, and social scientists and ethicists give insights into the motivations and heuristics of hackers and other malicious actors - interdisciplinary collaboration is rare. Such collaboration is especially critical to the design of secure AVs. However, we suggest that interfacing engineering, computer science, and democratic professional societies, such as the Committee for the Responsible Use of AI professional societies, including the IEEE and SAE International, can facilitate such cooperation among the relevant content disciplines.

Given the still maturing state of AV engineering as a field, it should come as no surprise that no field offers all of the key competencies needed to secure AVs. Instead, as we detail in the following section, key cybersecurity competencies are spread across engineering, computer science, and normative and descriptive disciplines. It is the task of cybersecurity education to distill such fields into key principles and best practices that can then form the backbone of an engineer's competency profile. Although currently employed curricular materials have been developed collaboratively by engineers and content experts involved in engineering ethics and related disciplines, many challenges remain to be addressed. An understanding of these challenges offers an important input that can be further shaped by the experiences and perspectives of the engineers, computer scientists, policymakers, and others with whom content experts collaborate, and from additional disciplines which may be relevant.

5. Innovative Teaching Methods and Tools

Fifty lectures of copyrighted original materials formatted in seven flexible modules are fully indexed, may be combined with non-copyrighted pertinent modules, and may be adapted to either blended (classroom-led or virtual instructor-led) or self-paced (digital) learning while easily integrating other materials or references to suit unique course needs or instructor preferences. All participants are required to be familiar with the covered material and to demonstrate its mastery through a comprehensive, summative assessment, thus ensuring an acceptable return on investment for multiple types of stakeholders. These modules cover applicable infrastructure fundamentals, basic autonomous concept generalities, three essential elements (especially software), and the unique concerns-based development process to help educate the stakeholders of jointly innovating a safe, secure, and cyber-resilient part of a cooperative system for which no single entity may have full end-to-end control. These conceptual modules should be followed by all participating stakeholders, including design authorities, their managers, development engineers, relevant regulators and their organizations, knowledge sharing bodies, and business partners. Systems engineers who desire to specialize in autonomous vehicles may want additional instruction, like risk-based security controls terminology and descriptions.

Virtually no tailored education or training solutions, digital or otherwise, were available when AVEs first emerged. Traditional vehicle engineering and systems design emphasize automation, security, and AI-related requirements that are seldom addressed in modern engineering curricula. The few security or privacy experts available—usually IT professionals from other domains—have shown to be somewhat more sensitive to mechanical, hydraulic, and electromechanical aspects, as well as established vehicle infrastructure that is slowly being upgraded with digital counterparts. Because almost no digital training or enabling solutions exist, standalone or interdisciplinary, we propose that a number of instructionally and pedagogically sound, technology-enhanced learning solutions that we already offer to targeted classes across multiple programs at our institution can and should be appropriately repackaged and made available to the broader community.

5.1. Simulation and Hands-On Labs

The tech implementation and low-level instruction sets used in these off-the-shelf exercises are often too low-level for the multi-disciplinary cyber-autonomous vehicle community. Because of fundamental differences between the original target applications and the current target environments, modern off-the-shelf exercises provide unequal coverage of the critical components needed to effectively illustrate attacks to this new audience. Guidance in selecting relevant components used by autonomous vehicles and the inclusion of elements that are unique to the vehicle operation should be considered.

Many academic institutions and professional training programs rely on simulation exercises based on advanced threat assessments to illustrate the vulnerabilities posed by new technologies in various domains. The creation and configuration of such virtual environments, equipped with vulnerable hosts and well-documented exercises that walk students (or professionals) through realistic cyber-attacks, require significant effort but provide a safe environment for hands-on laboratories that demonstrate the real-world impact of exposure to vulnerabilities. Ideally, these labs are accompanied by a comprehensive technical manual that enables instructors to customize the lab groupings and parameters based on the needs of particular classroom environments.

6. Case Studies and Best Practices

When considering a CSEE program, there are many approaches to consider. Should a new academic program be formed, or can existing cybersecurity and engineering courses be combined to provide these competencies? Here we present four related but varied cases that surround the establishment of a comprehensive interdisciplinary education program around CAVs for CSEEs. Together, these give examples of best practices and individual case studies that a regional or community college educator could use to provide similar training for their students. Beginning with an agile combination of Artificial Intelligence, Machine Learning, and Information Security techniques in the form of Cybersecurity Programs for CAVs, the next chapters cover the creation of a National Science Foundation for Cybersecurity Education for the Three Revolution model of CAVs. The mission is to educate future generations of automotive cybersecurity professionals through developing and delivering new courses, summer camps, diversity and veteran recruitment, extensible lab infrastructure, and real-world CAV student experiences. The rapid completion and deployment of Project Kotoba, our all-online undergraduate cyber defense competitions and curriculum, helped us fulfill the need to develop a cybersecurity curriculum suitable for Smart Cyber-Physical Systems—Noah's Ark and Dino Magnus.

6.1. Real-World Examples

In terms of results, this paper provides insights into the resolution of differences in proposed curricula embodying the embedded cybersecurity apprentice approach. It also provides lessons learned from implementing holistic introduction of cybersecurity, removing barriers to learning for a traditional specialized technical discipline. Educators and faculty developers will benefit from course development and implementation strategies from experienced education pedagogues in the areas discussion of industry practices and a space in future engineering community outreach for collaborative cybersecurity higher education programs. Lastly, it will highlight new teaching opportunities that further occupational expertise in engineering programs nationally, encouraging intradepartmental interdisciplinary cooperation and formal programs of study.

In response to the critical need to introduce cybersecurity as a specialized skill for autonomous vehicle engineers, different educational approaches are being promulgated. The oldest approach is the embedded apprenticeship model where the security and engineering domains are learned in isolated curricular silos until the senior year. The youngest approach is the holistic integrated security approach in which cybersecurity is introduced from the first course. The philosophical debate over the curriculum direction is ongoing among educators. There are significant scalability, teaching ability, and inter-private sector start-up and industry challenges in forward curricular movement. However, the credentials that will be granted to the majority of students as they prepare to enter industry are primarily contingent upon mastery of the existing discipline-based technical curricula and design project experiences from senior capstone design courses. Innovative interdisciplinary courses are now being developed with longer-term integrated curricula development absent either multiple faculty involvement in the course workflow or significant changes in university programs of teaching.

7. Ethical and Legal Considerations in Cybersecurity Education

In any event, beyond the important needs for future attention of smart and flexible civil liability rules there will be significant law and public policy issues such as the danger of exacerbating the tragedy of the commons. Relatedly, other significant legal issues will need to be addressed, such as the tendency for significant litigation matters. Finally, if society is not careful to manage the risk of tragic consequences caused by the combination of over-classification of the critical security test data plus over-exposure of the sensor fusion test model, we will likely awake to a DRM – dystopian regional monopoly – condition caused by 'soft-shell' jurisdictions. The first might be a foreclosure of the self-driving hardware resources as a result of private pursuit of a perceived legitimate interest enforced through the irresponsible use of public law. The engineering recommendations quickly come into focus.

One of the objectives of interdisciplinary education is to familiarize students with the legal and ethical implications associated with their work. Consequently, law and ethics were incorporated into all six modules. Discussing the issue of driverless vehicles cedes common authority to the underlying stakeholders: engineers, companies, government, police, insurance companies, and plaintiffs' lawyers are just the tip of the iceberg. In the cases of the Tesla and Uber crashes, the automobile companies settle quickly out-of-court with the released officers of the company testifying before the National Highway Transportation Safety Administration. However, when driverless cars begin to take a significant share of the automobile market, we predict that the law will be made the old fashioned way – through expensive litigation. At that time, we will see a new front in tort litigation – product liability lawsuits not against the drivers of the car but rather against the producer of the driverless software (e.g., Google/Waymo, Tesla, Uber).

7.1. Privacy and Data Protection

Ethical considerations are also relevant because unintentional privacy breaches cause harm. Additionally, there are ethical duties concerning the symmetry of information and the guidance of a person regarding their decision making, including possible legal obligations for manufacturers as well as service providers to protect the private information. Privacy legislation adds further complexity, but products and services are also protected by product liability laws. The upshot is that proactive security is good practice. For example, lawful autonomous driving dramatically increases the density of potential adversaries as individual hackers and hacktivist groups start to take advantage of this technology in order to help their criminal and lawbreaking enterprises, with the result that not only high-value would-be attackers utilize the services of a second party, but also an increasingly large group of third-party hackers-for-hire that are incentivized to attack and subvert lawful autonomous vehicles. With the legal regimes in developing countries and countries with autocratic governments being more relaxed with regard to the legitimate needs of privacy and data protection and government surveillance, a provincial solution that respects and upholds the legitimate expectations of privacy and data protection while also allowing the pursuit of autonomous vehicle research and development is to be implemented by manufacturers and suppliers along cybersecurity principles.

Privacy and data protection principles have a central role in guaranteeing the confidentiality, integrity, and availability of sensitive and private data such as, but not limited to, medical conditions, financial information, and even the location and identity of end-users. As lawful autonomous vehicles have a plethora of sensors capable of perceiving essentially the entire geographical location of a city, as well as market knowledge of potential trips at specific points in time, they are being designed to satisfy the expectations of end-users that their privacy and data protection expectations are addressed, in line with current and future legal frameworks. As such, the inclusion of privacy by design principles concerning the notice and consent of the data processing purposes, limiting the use and disclosure of the data to the specific agreed-upon purposes, and data quality concerns will create a market advantage because the privacy and data protection features are transparently legible to all potential as well as actual customers. Such privacy and data protection principles have a substantial impact on the secure management of hardware, software, and data for autonomous vehicle security concerns.

8. Future Directions and Emerging Trends

Previous research confirms that establishing a high level of cybersecurity for complex and autonomous systems is a challenge that exists within diverse domains. But it is regularly discussed within the context of the pervasion of these systems uniformly. Despite the differences in considerations required for diverse systems, most of this research applies an overlay of policy or procedure to ensure that the autonomous system is capable of secure operations. Establishing security of systems requires policies and guidelines that are responsive to both the unique characteristics and underlying technology required. The challenge of defining and distributing best practices and policy directions required to secure autonomous vehicle systems is establishing ownership for the execution of actions recommending the technical requirements. The goal of our research is to create an interdisciplinary learning environment to direct future research. To the best of our knowledge, we are one of only a few researchers that have undertaken this as their research aim. We address the core learning objectives that need to be established with a series of nine case studies of potential cyber threats targeting a range of autonomous vehicle system components.

Notwithstanding the rapid evolution in the realm of autonomous vehicles, the issue of cybersecurity in this area is of particular urgency. There has been extensive research covering either of the following topics: use of autonomous vehicles for cybersecurity-related attacks, the vulnerabilities or requirements required to ensure that the autonomous vehicles are capable of secure and safe operations. The realization of the aforementioned research priorities creates an opportunity for multi-disciplinary engineering teams to concentrate on the development of safe and secure autonomous vehicle systems which function within complex cyber-physical environments.

8.1. Artificial Intelligence and Machine Learning in Cybersecurity

Artificial intelligence and machine learning are now a significant point of investment for both cybersecurity corporations and the Department of Defense, which recently announced plans to invest $2 billion in AI-related technologies leveraging big data. With this in mind, a viable path emerges for military artificial intelligence and cybersecurity education, which this chapter will recommend be modeled after current academic initiatives. "Starting in fiscal year 2017, the DARPA Cyber Grand Challenge (CGC) will give the cybersecurity speed at which machines can operate. While machine learning has potential to solve some of cybersecurity's most daunting technical challenges, there is also a need for both humans and machines to work together. Cyber vulnerabilities in military systems could lead to loss of mission objectives, damage to systems, and possible loss of life. Machine learning and artificial intelligence can play a central role in addressing these network vulnerabilities and can be used to secure and monitor critical systems. As such, the development of human capital in these areas is critical to the strength of DoD cybersecurity. Currently, the DoD and several other agencies are supporting a variety of K-12, undergraduate, and graduate programs that target education in artificial intelligence, machine learning, and cybersecurity, although little exists to tie these initiatives together. In summary, a revamp of military education in artificial intelligence, machine learning, and cybersecurity is necessary to provide capabilities beyond measure.

Rising use of artificial intelligence (AI) and machine learning (ML) in cybersecurity applications is helping to solve some of the biggest security problems and making threat detection and response faster, smarter, and more effective. Chris Morales, head of security analytics at Vectra, a San Jose, Calif.-based AI/ML security company, says the deeper truth about AI and security is that security applications are almost like the original algorithm for AI, providing a huge source of information and a problem that numerous researchers over the years have known could be addressed with machine learning. "The ability to incorporate enough operational and adversarial learning into AI and ML to make it an invaluable security tool has been an up-and-down journey dating back nearly three decades," he said. Today, the ML scene is in full revitalization mode in cybersecurity. From behavioral analytics to improving threat intelligence, AI offers potentially game-changing functionalities for protecting the security of big data.

9. Conclusion

When manual automobiles become the primary mode of transportation, the field of automotive safety borrows its engineering concepts from many different areas of engineering. For example, brake systems use hydraulic systems to amplify the force applied by drivers to slow down a vehicle. Other automotive safety systems use advanced materials such as body panels to keep passengers within the automobile before the airbag is deployed. Computer instrumentation systems are also used to enhance manual driver perception (i.e., mirrors). Within automotive engineering, automotive safety professionals work within their discipline alone for many years.

This think piece argues that interdisciplinary cybersecurity concepts should be integrated into the education of autonomous vehicle engineers. It advocates for engineering accreditation organizations and educational institutions that train autonomous vehicle engineers to include interdisciplinary cybersecurity material in their curriculum. The content should meet the CSA guide as published by SAE, SECEF, CAE, and GM. Most importantly, the authors have personal experience in writing and/or reviewing or working with the CSA guide, have developed history or STEM material, and have presented IEEE talks on autonomous interactive vehicle cybersecurity education material. Our approach also provides a roadmap for other ACS to follow to integrate ACSs or other models of cybersecurity education into similar areas.

10. References

1. F. Chen, K. T. Kim, S. S. Yau and D. Li, "Cybersecurity challenges and research opportunities for unmanned autonomous vehicles," 2011 IEEE International Conference on Cyber, Physical and Social Computing, Dalian, China, 2011, pp. 371-378.

2. Y. Liu, J. K. Liu, D. Chen, H. Su and X. Zhang, "Ensuring Security and Privacy Preservation for Vehicular Cloud Computing," in IEEE Transactions on Vehicular Technology, vol. 65, no. 7, pp. 5111-5122, July 2016.

3. N. Kumar, S. Sahoo, M. Conti, A. Passarella and S. Giordano, "Urban surveillance for intelligent vehicular safety systems," 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 2013, pp. 3762-3767.

4. Tatineni, Sumanth. "Cost Optimization Strategies for Navigating the Economics of AWS Cloud Services." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.6 (2019): 827-842.

5. Vemori, Vamsi. "Towards Safe and Equitable Autonomous Mobility: A Multi-Layered Framework Integrating Advanced Safety Protocols, Data-Informed Road Infrastructure, and Explainable AI for Transparent Decision-Making in Self-Driving Vehicles." *Human-Computer Interaction Perspectives* 2.2 (2022): 10-41.

6. Mahammad Shaik, et al. "Unveiling the Achilles' Heel of Decentralized Identity: A Comprehensive Exploration of Scalability and Performance Bottlenecks in Blockchain-Based Identity Management Systems". Distributed Learning and Broad Applications in Scientific Research, vol. 5, June 2019, pp. 1-22, https://dlabi.org/index.php/journal/article/view/3.

7. M. H. Islam, D. X. Zhou, G. Ma, S. S. Kanhere and S. Jha, "A survey of routing attacks in mobile ad hoc networks," in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, pp. 30-54, First Quarter 2014.

8. L. Gao, S. Duan and H. Zhu, "Security in vehicular ad hoc networks," 2011 IEEE International Conference on Vehicular Electronics and Safety (ICVES), Beijing, China, 2011, pp. 258-263.

9. X. Hu, J. Xiong, Y. Chen and Y. Xiang, "A survey of attacks and countermeasures in cyber-physical systems," in IEEE Access, vol. 5, pp. 10559-10573, 2017.

10. P. Papadimitratos and L. Buttyan, "Securing vehicular communications," in IEEE Wireless Communications, vol. 13, no. 5, pp. 8-15, October 2006.

11. Y. Zhang, W. Liu, Z. Han and K. J. R. Liu, "Privacy-Preserving Data Aggregation in Vehicular Ad Hoc Networks: A Stackelberg Game Approach," in IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 9806-9817, Dec. 2016.

12. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," in Journal of Computer Security, vol. 15, no. 1, pp. 39-68, 2007.

13. C. Lin, Y. Liu and G. Chen, "On the design of incentive schemes for vehicular crowdsensing," 2013 IEEE Global Communications Conference (GLOBECOM), Atlanta, GA, USA, 2013, pp. 3221-3226.

14. Y. He, X. Sun, B. Liang, L. Wang and S. Chen, "An Efficient Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 65, no. 7, pp. 5423-5436, July 2016.

15. R. R. Choudhury, A. Mathur, A. G. Ganesh and N. H. Vaidya, "Adaptive security for vehicular networks," 2010 IEEE INFOCOM, San Diego, CA, USA, 2010, pp. 1-9.

16. A. A. Hossain, M. A. Matin and H. M. Alam, "A secure and efficient protocol for VANET," 2014 IEEE 17th International Conference on Computational Science and Engineering, Chengdu, China, 2014, pp. 661-666.

17. J. Huang, H. Zhu, L. Gao, X. Li and J. Ma, "A security scheme for vehicle-to-vehicle communication," 2013 IEEE 10th Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 2013, pp. 1071-1076.

18. J. Ben-Othman and L. M. Yung, "A survey of security attacks in vehicular ad hoc networks," in IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 854-871, Second Quarter 2013.

19. Y. Yang, R. H. Deng, J. Liang and J. W. Mark, "Toward Privacy-Preserving Data Sharing in Vehicular Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 65, no. 12, pp. 9752-9766, Dec. 2016.

20. S. Ruj, A. Nayak, I. Stojmenovic and M. Hassan, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 384-394, Feb. 2014.