The Future of Vehicular Privacy and Security

Alexander M. Wyglinski, James Irvine, and Joseph Chapman

Vehicles, and the transportation systems within which they operate, are becoming increasingly smart with more sophisticated sensing and control functionality. Most of these enhancements are designed to improve the safety of these systems as well as the support of both semi- and fully autonomous operations, such as driverless cars in the case of automotive applications. Consequently, we are beginning to realize a highly integrated network of numerous electronic control units (ECUs) on-board these various transportation platforms that perform a wide range of tasks in unison. The controller area network (CAN) is one of the more common communication technologies employed for this purpose. Different applications possess different protocols for enabling the communications of ECUs across the CAN bus, although the concept is approximately the same with respect to how information is shared in real time between devices to perform various operations.

Access to the CAN bus network was initially designed to only have a couple interfaces, thus limiting access to the network. Although this frame-work has helped protect the CAN bus and the ECUs connected to it during the past several decades, we have recently begun to witness several serious and well-publicized/published security breaches of CAN networks employing relatively low-cost methods, such as off-the-shelf embedded computing devices and open-source software. These exploits transformed various elements connected to the CAN bus and lever-aged them as new attack surfaces, such as obtaining unauthorized access via the Bluetooth connection in a car's stereo system, feeding false information into a transportation platform's array of environmental sensors, or ac-cessing the CAN bus via the wireless tire-pressure-monitoring system used on a growing number of automotive platforms. With the advent of the connected vehicle, issues with security and privacy are expected to worsen unless new research, techniques, and tools are designed to help the vehicular technology community combat these significant threats.

This special issue of IEEE Vehicular Technology Magazine presents the latest findings and perspectives on the emerging and important area of vehicular security and privacy. Five articles form this special issue, all of which introduce a breadth of new solutions that will help the community combat the growing threat of vehicular cyber attacks. These solutions include cryptographic methods, blockchain, and new architectural considerations for CAN to protect these transportation systems both from a wireless perspective as well as from inside the vehicle itself.

Many of the growing number of threats against vehicular systems originate outside the system, leveraging some form of wireless interface to gain access to the system or com-promise the way in which the system utilizes wireless information. The first article of this special issue, "Secure Blockchains for Dynamic Spectrum Access," by Khashayar Kotobi and Sven G. Bilén, addresses the threat resulting from wireless connectivity and the motivation for new approaches for vehicular wireless security. Specifically, this article proposes a new approach for securing vehicular communications when spectrum sharing is performed. Applying the concept of blockchain to a vehicular spectrum-sharing architecture, the authors show a significant improvement in terms of spectrum access relative to conventional Aloha medium-access control.

Cryptography is used in security solutions to protect a system or a communications signal from being compromised. The second article of this special issue, “Security Solutions for the Controller Area Network,” by Bogdan Groza and Pal-Stefan Murvay, explores the various cryptographic methods that are suitable for CAN networks. In many applications involving CAN networks, almost all communications performed between the ECUs attached to the bus are not encrypted, making them readily susceptible to at-tack once an adversary gains access to the CAN bus. The authors present an overview of several studies on employing encryption to protect the

CAN bus communications from such attacks, and they include quantitative performance comparisons highlighting the various trade-offs between different countermeasures.

Another sector affected by cyber-security threats and privacy issues is the rail industry. In the third article, “Cybersecurity—the Forgotten Issue in Railways,” by Leonardo J. Valdivia, Iñigo Adin, Saioa Arrizabalaga, Javier Añorga, and Jaizki Mendizabal, the authors present a detailed overview of the railway environment and identify potential cybersecurity threats against it. In addition to describing the various forms of cyberattacks that a railway environment could experience, the authors go into detail about how these threats can be employed against safety-critical systems and operations. Finally, the authors describe how safety and security are incorporated into the rail standards to ensure that these systems are protected from cyberattacks.

Automotive vehicles, such as cars, trucks, and buses, commonly contain tens of networked ECUs. There have been several papers in the literature detailing how these networks of ECUs on-board a single vehicle can be com-promised unless measures are taken to identify potential cyberattacks and to mitigate them. In the fourth article of this special issue, “Securing the Connected Car” by Kim Strandberg, Tomas Olovsson, and Erland Jonsson, a methodology is proposed that will help automobile manufacturers build security into their vehicles be-fore they reach the road. Specifically, the authors propose a methodology called start-predict-mitigate-test (SPMT), which is designed to both predict and mitigate vulnerabilities in vehicles via a systematic security analysis approach adapted specifically for vehicles. The authors provide extensive details about the SPMT approach and how it can be employed throughout the entire life cycle of the vehicle.

Over-the-air firmware updates, enabled by embedded cellular technology, offer advantages to automotive manufacturers by improving the customer experience while reducing costs through automation. However, to maintain safety in an increasingly hostile and unpredictable environment, manufacturers must consider the possibility of compromise and implement cyber-resilient designs. In the last article, “Uptane,” by Trishank Karthik Kuppusamy, Lois Anne DeLong, and Justin Cappos, the authors present an approach for performing software updates for vehicles in a secure manner. Their pro-posed approach, referred to as Uptane, presents a practical firmware-update system, and this article goes into detail about how such an approach would be implemented to achieve a relatively high level of security.

In conclusion, we anticipate that this special issue will provide new in-sights and knowledge on this growing threat within our vehicular technology community. As transportation systems become increasingly smart and connected, new security and privacy issues will continue to emerge and re-quire innovative solutions to mitigate them and keep society safe. Consequently, when designing new systems and proposing new solutions, it is important to take into consideration the elements of security and privacy.

About the Authors

Alexander M. Wyglinski (alexw@ieee.org) received his B.Eng. and Ph.D. degrees in 1999 and 2005, respectively, from McGill University, Montréal, Canada, and his M.Sc. (Eng.) degree from Queen's University in Kingston, Cana-da, in 2000, all in electrical engineering. He is an associate professor of electrical and computer engineering at Worcester Polytechnic Institute (WPI), Massachusetts, director of the Wireless Innovation Laboratory at WPI, and the president of the IEEE Vehicular Technology Society for 2018. He has published more than 40 journal papers, more than 80 conference papers, nine book chapters, and two textbooks. His current research activities include wireless communications, cognitive radio, connected vehicles, software-defined radio, dynamic spectrum access, electro-magnetic security, vehicular technology, wireless system optimization and adaptation, autonomous vehicles, and cyber-physical systems. He is a member of Sigma Xi, Eta Kappa Nu, and the American Society for Engineering Education. He is a Senior Member of the IEEE.

James Irvine (j.m.irvine@ieee.org) received his B.Eng. and Ph.D. degrees from the University of Strathclyde in Glasgow, United Kingdom, in 1989 and 1994, respectively. He is a reader at the University of Strathclyde, where he leads the Mobile Communications Group. His research focuses on cellular resource management and cryptography, with applications to transport and power networks. He is a co-author of two books and more than 150 technical papers, and he holds seven patents. He has served on three of the major boards of the IEEE: Technical Activities, Publications, and Educational Activities. He is currently on the executive committee of the IEEE Vehicular Technology Society, having served as president during 2008–2009 and vice president–publications 2010–2015. He is the chair of the IEEE Standards Education Committee and a member of the IEEE Fifth-Generation Initiative Steering Group.

Joseph Chapman (jchapman@mitre.org) received his B.S. degree in electrical and computer engineering from Worcester Polytechnic Institute, Massachusetts, in 2005 and his M.S. degree in electrical engineering with a concentration in signal processing and communication systems from Northeastern University, Boston, Massachusetts, in 2014. He is a principal hardware security engineer at the MITRE Corporation in Bedford, Massachusetts. His group's research focuses on implementation security topics, including cryptographic implementations, fault and side-channel attacks and countermeasures, secure design practices and architectures, and cyber- physical and legacy system security.

Digital Object Identifier 10.1109/MVT.2017.2787272

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8306170