Emerging Paradigms in Vehicular Cybersecurity

By Himanshu Thapliyal, Saraju P. Mohanty, Stacy Prowell

INTRODUCTION

Current generation vehicles include on an average of 100 million lines of code and 60 Electronic Control Units (ECUs). It is estimated that there will be 220 million connected cars globally by 2020 [1]. With the growth of Internet-of-Things (IoT) enabled technologies in vehicles such as power and infotainment systems, remote locking and unlocking, remote engine start, navigation, and autonomous driving features [1], [2], the potential threat vectors for malicious cyber-attacks are rapidly expanding. A taxonomy of vehicular security attacks to provide the general outline of an attack including who the attackers could be, what tools they might use in the attack, the actions taken with those tools, and the attackers' overall objective for the attack is presented in in Figure 1 [3]. As an example, software vulnerabilities could be exploited to remotely take control of safety-critical systems including the brakes in the vehicle. Thus, there is a growing concern that vehicles can be hacked, and the user data can be stolen. These cyberattacks are threat to the reliability and safety of the car and to the privacy of the driver.

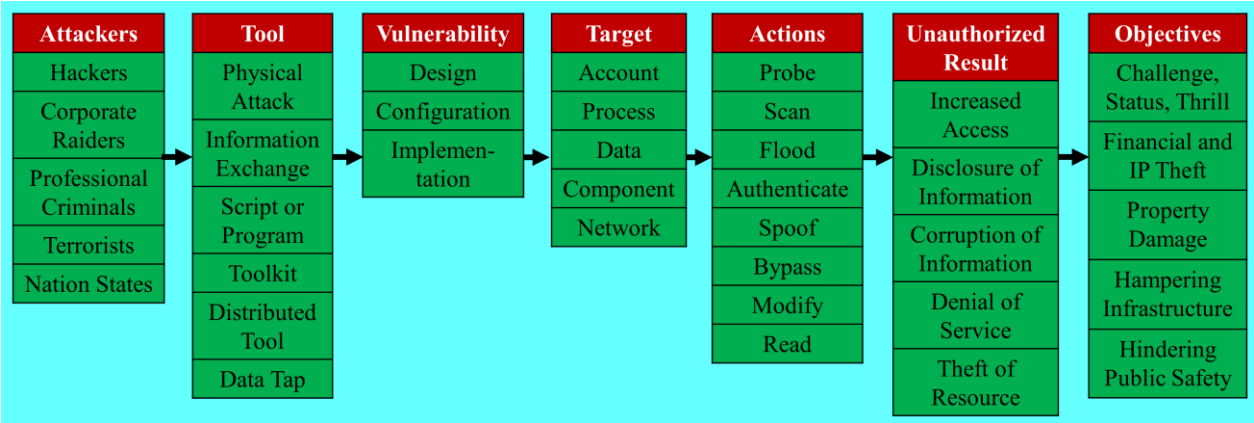

FIGURE 1. Taxonomy of vehicular security attacks adapted from [3].

As per the report "Cybersecurity Best Practices for Modern Vehicles" published by National Highway Traffic Safety Administration (NHTSA) [4], the United States Department of Transportation (DOT)'s top priority is to enhance vehicle cybersecurity for mitigating cyber-threats that could present unreasonable safety risks to the public or compromise sensitive information such as consumers' personal data [5]. Various vehicular attacks can be broadly classified into the following categories [3]:

- **Eavesdropping:** Listening to communication channels such as the CAN bus or intra-vehicle messages.
- **Data Tampering:** Undetected modification of data/messages such as sensor readings.
- **Impersonation/Forgery:** Making the attacked vehicle believe that it is communicating with a trusted party such as spoofing a trusted identify in a vehicular network.
- **Man-in-the-middle:** An attacker can be both intercept and forward, filter or modify messages without being detected.
- **Denial of Service (DoS):** Prevent the normal use of a network by flooding the target with illegitimate messages.

Within each category there exists a multitude of attacks that widely vary depending on factors such as the attack's target and expected goal. As a reference, we have provided one example of each type of attack in Table 1 along with the goal of the attack for which possible countermeasures can be developed.

Table 1. Examples of attacks on vehicles and possible countermeasures.

Attack Category	Example Attack	Goal of Example Attack	Possible Countermeasures
Eavesdropping	Access to ODB-II port allows monitoring of ECU communications	Data harvesting to enable future attacks	Improved protocols or message encryption
Data Tampering	Sensor data is modified so vehicle appears to be moving slower than its actual speed	Cause hazardous driving situation	Data encryption
Impersonation/Forgery	Attacker pretends to be trusted party	Target unknowingly provides sensitive information to attacker	Improved cryptography/protocols
Man-in-the-Middle	Attacker selectively filters out warning messages between vehicles	Confuse support and safety systems	Verification redundancies (e.g. vehicle tracking via radar)
Denial of Service (DoS)	Network is flooded with erroneous messages	Network performance degradation	Ignore messages from non-authenticated network nodes

NHTSA believes that vehicular cybersecurity should be an organizational priority of the automotive industry. Further, NHTSA and industry stakeholders expect that there will be an increase in the threat of vehicle cyber-attacks in the coming years because of autonomous and connected-vehicle technologies. The potential benefits of the improved vehicular security include increasing the public safety and securing driver's personal data. Therefore, this special issue will provide a publication medium for articles that either address the review of existing vehicular systems, and platforms, or explore novel research paradigms in vehicular cybersecurity. This special issue consists of 5 papers and is aimed at educators, researchers, and students who are engaged in vehicular cybersecurity research and education.

SCANNING ARTICLES OF THE SPECIAL SECTION

Transferring the design to standardized hardware would enable software to take the key role and allow the horizontal approach in design, where each feature may be added as a module. This sets stage for a central vehicle computer – a brain for next generation vehicles which is everything but easy to design. The article on "Central Vehicle Computer design: Software Taking Over" by Bjelica and Lukac discusses one such design and identify the required building blocks for this rising market.

The article on "Cellular V2X Transmission for Connected and Autonomous Vehicles: Standardization, Applications, and Enabling Technologies" by Abou-zeid, Pervez, Adinoyi, Aljlayl, and Yanikomeroglu discusses the recent technological advances and standardization efforts in Cellular Vehicle-to-Everything (C-V2X) technologies that are being developed to support the ultra-reliable, low latency, and high throughput required by autonomous vehicles (AVs).

The article on "Hardware Security Primitives for Vehicles" by Labrado and Thapliyal highlights hardware security primitives which are hardware devices that can serve as building blocks to create full-fledged security solutions for vehicles. Specifically, the primitives are grouped into physically unclonable functions (PUFs) and security modules. Also, a few of the potential security applications of PUFs highlighted in the article include key storage, pseudonym generation, and vehicle-to-vehicle communication.

The article on "Data-Driven Extraction of Vehicle States from CAN Bus Traffic for Cyber Protection and Safety" by Moore, Bridges, Combs and Anderson develops a data driven, semi-supervised approach to learn physical relationships of CAN signals from only a limited set of CAN packets. These mappings are then used to develop a Hidden Markov Model (HMM) of the driver's actions upon which transaction analysis is performed to optimize the real-time identification of the states. The proposed approach builds an image from the CAN data, then trains a convolution neural network (CNN) to give emission probabilities to predicts drivers's actions.

The article on "Using Map Matching to Improve De-Identification of Sequences of Connected Vehicle Locations" by Carter and Ferber introduces a suppression-based control that uses road network structure and metadata to mitigate inference-based privacy attacks against sequences of locations. The introduced procedure has broad applicability, but it was designed to protect U.S. Department of Transportation (USDOT) vehicle-to-vehicle (V2V) communication data. The privacy control introduced in this article attempts to generate data useful for development of safety-critical applications.

ACKNOWLEDGMENTS

We would like to thank all the authors for their valuable contribution to this special issue. We would like to acknowledge and thank the reviewers for their valuable and timely efforts to ensure the high quality of the papers. We hope that this special issue will serve as a valuable resource for the CE community.

GUEST EDITORS' BIO

Himanshu Thapliyal (hthapliyal@uky.edu) is an Assistant Professor and Endowed Robley D. Evans Faculty Fellow at the Electrical and Computer Engineering, University of Kentucky, Lexington, KY.

Saraju P. Mohanty (saraju.mohanty@unt.edu) is a Professor in Computer Science and Engineering at the University of North Texas.

Stacy Prowell (prowellsj@ornl.gov) is the Chief Cyber Security Research Scientist at Oak Ridge National Laboratory and is the Program Manager for the lab's Cybersecurity for Energy Delivery Systems program.

REFERENCES

[1] F. Pieri, C. Zambelli, A. Nannini, P. Olivo and S. Saponara, "Is Consumer Electronics Redesigning Our Cars?: Challenges of Integrated Technologies for Sensing, Computing, and Storage," *IEEE Consumer Electronics Magazine*, vol. 7, no. 5, pp. 8-17, Sept. 2018.

[2] V. K. Kukkala, J. Tunnell, S. Pasricha and T. Bradley, "Advanced Driver-Assistance Systems: A Path Toward Autonomous Vehicles," *IEEE Consumer Electronics Magazine*, vol. 7, no. 5, pp. 18-25, Sept. 2018.

[3] R. R. Brooks, S. Sander, J. Deng and J. Taiber, "Automobile Security Concern," *IEEE* Vehicular *Technology Magazine*, vol. 4, no. 2, pp. 52-64, June 2009.

[4] National Highway Traffic Safety Administration. Cybersecurity best practices for modern vehicles. (Report No. DOT HS 812 333). Washington, DC: Author, Oct 2016.

[5] Vehicle Cybersecurity:DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack, U.S. Government Accountability Office, GAO-16-350: Published: Mar 24, 2016. Publicly Released: Apr 25, 2016.