Volume 2, No. 3 | May–June 2019

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 2, No. 3 | May–June 2019

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquires and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please call:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

CTIA's IoT Cybersecurity Certification Program May Inform the Future of Transportation and Smart Cities

Renee R. Gregory and Jill Guidera Brown*

The trade association representing the U.S. wireless communications industry released its Cybersecurity Certification Test Plan for IoT Devices, establishing a baseline for device security on wireless networks. The authors of this article explain the Test Plan and the association's Cybersecurity Certification Program, which provides helpful guidance for stakeholders as they develop smart, secure, and connected communities and transportation systems.

CTIA, the trade association representing the U.S. wireless communications industry, released its Cybersecurity Certification Test Plan for IoT Devices[1] ("Test Plan"), establishing a baseline for device security on wireless networks. The Test Plan is unique in that its testing requirements and plans were developed specifically for, and in collaboration with, nationwide wireless providers. Specifically, the Test Plan defines testing requirements for the CTIA Cybersecurity Certification Program for managed Internet of Things ("IoT") devices connecting to either LTE or Wi-Fi networks to exchange data with other devices, vehicles, home appliances, infrastructure elements, and more. CTIA-authorized test labs began accepting devices for testing in October 2018.

Proponents of connected and self-driving cars and smart cities should take note of the Certification Program as they increasingly integrate LTE and Wi-Fi and participate in the larger IoT ecosystem.

The CTIA Cybersecurity Certification Program Draws From Existing Cybersecurity Frameworks

The Test Plan draws from and adapts existing cybersecurity frameworks, and each testing procedure is accompanied by reference to relevant sections of existing standards, most notably the National Institute of Standards and Technology ("NIST") Cybersecurity

Robotics, Artificial Intelligence & Law / May–June 2019, Vol. 2, No. 3, pp. 177–181.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online)

Framework.[2] Recognizing the need for a tailored approach to cybersecurity, NIST itself identifies that its framework is "not a one-size-fits-all approach to managing cybersecurity risk." While the Test Plan highlights existing standards, CTIA-authorized test labs will develop the specific testing procedures and equipment in accordance with program-specific requirements set forth by CTIA.

The Test Plan is organized into three categories of testing, moving from core IoT device security features in the first category, to security elements of increasing device complexity, sophistication, and manageability in the second and third categories:

Category 1:

- Terms of service and privacy policies;
- Password management;
- Authentication;
- Access controls;
- Patch management; and
- Software upgrades.

Category 2:

- Audit log;
- Multi-factor authentication;
- Remote deactivation;
- Secure boot;
- Threat monitoring; and
- IoT device identity.

Category 3:

- Encryption of data at rest;
- Digital signature generation and validation;
- Tamper evidence; and
- Design-in features.

Future Developments in Transportation and Smart Cities May Put the Wireless Industry in the Driver's Seat

Similarly to any device connected to the internet, connected and self-driving cars and smart city devices are vulnerable to malicious

attacks and human error, raising significant public safety concerns and legal risk. For example, in 2015 researchers were able to exploit vulnerabilities in a vehicle's infotainment system and remotely control the driving and safety functionalities of the car on the road. As a result, in July 2018 the U.S. District Court for the Southern District of Illinois certified a class[3] of consumers in a suit against the same auto manufacturer for cybersecurity defects in cars' cellular connections.

To combat those risks, local governments, automotive manufacturers and suppliers, and wireless communications industry leaders may turn collectively to the CTIA Cybersecurity Certification Program as a roadmap for building secure systems from the ground up. The program could supplement or even replace existing non-binding guidance documents and voluntary consensus standards, described below, that address security concerns inherent in the deployment of smart cities, connected cars, and automated driving systems. Measured against these various approaches to standardizing transportation and smart city–related IoT, the CTIA Cybersecurity Certification Program is unique not only because it was developed from the perspective of the wireless communications industry that enables IoT connectivity but also because it puts cybersecurity front and center in developing new IoT technologies and applications.

Smart Cities

Recognizing a need for a more cohesive framework for implementation of smart city technologies, which naturally take a city-by-city approach, NIST formed a working group of academics and policy makers and in early 2018 published a draft Consensus Framework for Smart Cities Architectures.[4] This framework considers cybersecurity challenges in the context of open data policies, interoperability, and standardization across smart city systems.

Connected Cars

Development of security and connectivity standards for connected cars has been largely driven by the automotive industry in partnership with engineers and transportation policy makers, assuming a transportation-specific standard for vehicle-to-vehicle

("V2V") and vehicle-to-infrastructure ("V2I") communications: Dedicated Short Range Communications ("DSRC"). For instance, the U.S. Department of Transportation's Intelligent Transportation Systems Joint Program Office[5] and the National Highway Traffic Safety Administration[6] ("NHTSA") have collaborated with technology and automotive industry stakeholders such as the Society of Automotive Engineers International[7] ("SAE") and the Institute of Electrical and Electronics Engineers[8] to develop connected vehicle standards[9] based on DSRC. However, the wireless industry has recently developed a cellular-based vehicle-to-everything ("V2X") standard that may replace DSRC.

Autonomous Vehicles

While no overarching federal law governing autonomous vehicles exists today, the U.S. House of Representatives has passed,[10] and the Senate has proposed,[11] self-driving vehicles legislation that would impose on manufacturers an obligation to maintain a written cybersecurity plan.

In parallel, in October 2018, the U.S. Department of Transportation ("DOT") and NHTSA issued Automated Vehicles 3.0: Preparing for the Future of Transportation,[12] voluntary guidance for stakeholders implementing automated driving systems. The voluntary DOT/NHTSA guidance does not prescribe specific technical or operational data security measures, though it generally encourages entities to implement cybersecurity protections and report discovered incidents or vulnerabilities to the Automotive Information Sharing and Analysis Center, and Department of Homeland Security, where appropriate. The guidance further recommends that entities undergo regular assessment of cybersecurity risks consistent with best practices set forth by NIST, NHTSA, SAE, and "other relevant organizations"—a list to which CTIA may now be added.

Conclusion

The enhanced cybersecurity risks raised by connected and self-driving cars and smart city infrastructure highlight the need for cybersecurity standards specifically tailored to IoT devices. Additionally, as next-generation transportation and smart cities

both are undergoing a period of rapid growth and development, there is now a unique opportunity to consider cybersecurity starting in the design phase. When taken in combination with existing legal and regulatory frameworks and industry best practices, the CTIA Cybersecurity Certification Program may provide helpful guidance for stakeholders as they develop smart, secure, and connected communities and transportation systems.

Notes

* Renee R. Gregory is counsel in Willkie Farr & Gallagher LLP's Communications & Media Department, solving problems at the intersection of business, technology, policy, politics, and the law. Jill Guidera Brown is an associate in the firm's Cybersecurity & Privacy Practice Group. The authors can be reached at rgregory@willkie.com and jgbrown@willkie.com, respectively.

1. https://api.ctia.org/wp-content/uploads/2018/08/CTIA-IoT-Cybersecurity-Certification-Test-Plan-V1_0.pdf.
2. https://www.nist.gov/cyberframework/framework.
3. https://dlbjbjzgnk95t.cloudfront.net/1060000/1060511/https-ecf-ilsd-uscourts-gov-doc1-06914181521.pdf.
4. https://s3.amazonaws.com/nist-sgcps/smartcityframework/files/ies-city_framework/IES-CityFrameworkdraft_20180207.pdf.
5. https://www.its.dot.gov/.
6. https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity.
7. https://www.sae.org/.
8. https://www.ieee.org/.
9. https://www.standards.its.dot.gov/.
10. https://www.congress.gov/115/bills/hr3388/BILLS-115hr3388rfs.pdf.
11. https://www.commerce.senate.gov/public/_cache/files/1fb8fa36-331b-4f0b-907a-6dededda4d31/37F56742A509A877F54FDF7389DFDAA7.s.-1885-av-start-act.pdf.
12. https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.