Journal of Cybersecurity and Privacy

MDPI

Editorial

Journal of Cybersecurity and Privacy: A New Open Access Journal

Wade Trappe [1,*] and Jeremy Straub [2,*]

[1] Department of Electrical and Computer Engineering, Rutgers, The State University of New Jersey, Piscataway, NJ 08854, USA
[2] Department of Computer Science, North Dakota State University, Fargo, ND 58102, USA
* Correspondence: trappe@winlab.rutgers.edu (W.T.); jeremy.straub@ndsu.edu (J.S.)

Received: 13 June 2018; Accepted: 13 June 2018; Published: 14 June 2018

Journal of Cybersecurity and Privacy is critical to society at large, and its importance is growing daily. The rapid advancement in technology has caused a large-scale integration of computing, communication, and information technologies into virtually every aspect of our modern society. Computing and communication technologies are at the heart of emerging advancements in transportation, production and manufacturing, logistics, healthcare, utility, recreation, social and many other domains. This incorporation of cyber technologies into a wide array of industries is tearing down barriers between industries as information is gathered and shared in order to facilitate previously unimaginable improvements in capabilities, efficiency, and cost.

Attacks against cyber systems, similarly, are not confined to one industry or area of focus. An attack designed to impact one type of system may inadvertently infect, impair or disable—or be deliberately modified to infect, impair or disable—other types of systems. Cyberattacks also blur the lines between state versus state "warfare" activities, state sponsored intelligence activities and criminal activities. National civilian and military agencies, law enforcement and the private sector must, thus, work together to prevent and respond to a myriad of different types of cyberattacks with varying targets.

The merging of information, computing and communication technology with many aspects of our personal and social life offers profound benefits, it also poses new security and privacy challenges. Our increasing reliance on sensors, software, and an anywhere-at-anytime communication infrastructure has led to and will lead to new classes of attacks against our daily life. Attacks on utility systems, such as illustrated by Stuxnet in 2010, are an illustration of the emergence of new and more sophisticated security threats that can be launched against systems that intimately integrate cyber technology with physical processes. Automotive systems, which are replete with many sensors providing data to various automated processes, have also been the target of attacks, such as hacks against a vehicle's LIDAR [1], the tire pressure monitoring system (TPMS) [2], and different automotive control systems [3]. Other examples of security exploits abound across industrial control, drones, automotive systems, medical devices, and many other technologies.

Beyond security risks are issues of privacy. As these new technologies gather and share data, the implication of such sharing of data between services can threaten many aspects of personal liberty that we hold important. While the pervasiveness of the Internet means that it is easier for cyberattackers to steal conventional forms of sensitive data, such as credit card numbers and government-issued personal identifiers (e.g., social security numbers, drivers' license numbers, and similar), the potential for privacy breaches is much broader and more profound. Data analytics applied across different modalities of data shared with cloud services can lead to personal information being inferred about individuals that they thought were protected and private. For example, supposedly privacy-enhanced GPS traces have been successfully reversed to infer the precise location of vehicles (and thereby

individuals) at a given time [4]. Similar risks are evident in the healthcare industry, where technologies meant to assist doctors and support patient well-being monitoring, unfortunately have been shown to leak unintended information [5]. Services that monitor our homes and offices, using data from networked digital cameras, also provide the means to track individuals and their personal activities.

The capabilities provided by and use of systems that attack, detect attacks and defend against them raise questions of ethics and policy that must be explored. Questions of where the line should be drawn between protective surveillance and invasive monitoring, what constitutes an act of war in the cyber domain and what types of actions are justified in both preventative and responsive capacities are among those that will vex society-at-large over the years and decades to come.

New security risks and privacy threats are created by data being generated using sensors, and shared across our communication infrastructure to various computing services. It is possible now for adversaries to attack from virtually everywhere and at any time in the data life cycle. Adversaries might attempt traditional attacks intended to subvert the confidentiality, integrity and availability of these new cyber systems and, while such threats can lead to privacy, data, and economic damage, they can also lead to physical damage to the world around us and directly affect our personal well-being.

With all this in mind, the goal behind *Journal of Cybersecurity and Privacy* is to provide a venue for articles and community engagement that will advance the state of the art in security and privacy research and practice for the increasingly cyber-enabled world. Towards this end, the journal's goal is to strategically attract articles on topics including:

- Traditional research-focused articles that convey new security and privacy technologies;
- Educational survey articles that instruct the broader community of security and privacy challenges and solutions;
- Articles that discuss the policy and legal implications of the development, adoption and utilization of security and privacy technologies;
- Editorials and position articles intended to pose new ideas and foster paradigm shifts;
- Practitioner perspective and implementation articles which discuss the transformation of basic and applied research into real-world applications.

The journal aims to strengthen the cybersecurity and cyberprivacy communities by sharing knowledge and practice between different communities that are traditionally separate, such as technology and public policy. The broader scope of this journal aims to engage the public policy, legal, crime prevention and law enforcement, economics, and social/psychology to guide and inform the technical community towards the development and adoption of high-impact security and privacy solutions. Specifically, since this journal aims to span communities, it not only supports the need of researchers to explore the state of the art in the science and engineering of security and privacy, but also foster the growth of this young field of research to ensure that scientists and engineers are examining technologies that are of societal importance. The technical scope of this journal is interdisciplinary, involving contributions from different technical disciplines, such as cryptography, computer security, network security, information theory, signal processing, communications theory, game theory, and machine learning/data mining. Broadly, our goal is to advance knowledge of the domain of cybersecurity and its applications and pose and answer key questions that may define our society for generations to come.

References

1. Harris, M. Researcher Hacks Self-Driving Car Sensors. Available online: https://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors (accessed on 11 June 2018).
2. Rouf, I.; Miller, R.; Mustafa, H.; Taylor, T.; Oh, S.; Xu, W.; Gruteser, M.; Trappe, W.; Seskar, I. Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study. In Proceedings of the 19th USENIX Security Symposium, Washington, DC, USA, 11–13 August 2010; USENIX Association: Berkeley, CA, USA, 2010; p. 21.

3. Hackers Remotely Kill a Jeep on the Highway—With Me in It. Available online: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (accessed on 11 June 2018).
4. Gao, X.; Firner, B.; Sugrim, S.; Kaiser-Pendergrast, V.; Yang, Y.; Lindqvist, J. Elastic pathing: Your speed is enough to track you. In Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp '14), Seattle, WA, USA, 13–17 September 2014; ACM: New York, NY, USA, 2014; pp. 975–986.
5. Kevin, F. Inside risks: Reducing risks of implantable medical devices. *Commun. ACM* **2009**, *52*, 25–27.