JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 1(1), 2015, 1–2
doi: 10.1093/cybsec/tyv010
Advance Access Publication Date: 28 November 2015
Editorial

Editorial

Welcome from the Editors-in-Chief

Cybersecurity is now widely recognized as essential by individuals, firms, and governments. As society has grown more dependent on information systems and the Internet, the need for a secure and reliable cyber infrastructure is clear. As this need has spread beyond the domains of computing and information technology, the number of disciplines contributing valuable perspectives has also expanded greatly. For instance, social scientists, lawyers, and policy scholars help improve our understanding of how people and institutions make decisions affecting security and privacy. Meanwhile, computer scientists, engineers, and cryptographers have begun designing secure technologies that take personal or institutional incentives into account.

The goal of the *Journal of Cybersecurity* is to provide a common publication outlet for top-quality, high-impact research and scholarship that spans the many disciplines investigating cybersecurity and privacy topics. The journal has been designed from the ground up to reflect the interdisciplinary nature of cybersecurity research, while ensuring disciplinary rigor in the articles we publish. To that end, we have appointed leaders across many disciplines as Area Editors. Their job is to coordinate peer review to ensure that papers published in the journal meet the disciplinary expectations of quality, while being written in such a way that the key results are accessible to those reading outside their specialty. To give the reader an idea of the wide coverage intended for the journal, and the expertise of our area editors, we list them here:

- Anthropological and Cultural Studies: *Rick Wash*, Michigan State University
- Computer Science and Security: *Andrew Martin*, University of Oxford
- Cryptography and Associated Topics: *Emiliano De Cristofaro*, University College London
- Game Theory and Complex Systems: *Jonathan Cave*, University of Warwick
- Economics of Information Security: *Rahul Telang*, Carnegie Mellon University
- Human Factors and Usability: *Angela Sasse*, University College London
- Legal Aspects of Information Security: *Deirdre Mulligan*, University of California at Berkeley
- Political and Policy Perspectives: *Susan Landau*, Worcester Polytechnic Institute
- Privacy: *Alessandro Acquisti*, Carnegie Mellon University
- Security, Crime Science and Psychology: *Michael Levi*, Cardiff University
- Replication Studies: *Andrew Adams*, Meiji University
- Strategy and International Relations: *Thomas Rid*, King’s College London

Moreover, we have appointed an Advisory Board with experts from academia, government, and industry. Full details can be found on the Journal’s website http://cybersecurity.oxfordjournals.org/.

Because the Journal’s goal is to publish highly relevant articles, of broad societal interest, we have adopted an Open Access model. All papers are made freely available online. Furthermore, we have established a publishing fund to ensure that authors who need to can obtain fee waivers. We thank our generous founding sponsors, who have contributed to the publishing fund and have helped ensure that articles published in the journal are freely accessible to all.

To celebrate the creation of the Journal, we are proud to have assembled an inaugural issue of excellent papers from leading scholars working in the area of cybersecurity and privacy. This issue demonstrates the great breadth of disciplinary perspectives that can contribute to our understanding of cybersecurity issues. Disciplines represented include accounting, anthropology, communications, computer science, criminology, cryptography, economics, game theory, international relations, and neuroscience. The authors include both rising stars in their home disciplines and senior leaders, including Turing Award winners.

In the first article, “Increasing Cybersecurity Investments in Private Sector Firms,” Gordon, Loeb, Lucyshyn, and Zhou construct an economic model that evaluates how prospective government interventions might stimulate cybersecurity investment among private sector firms. The paper examines two US regulatory interventions in great detail: the Sarbanes–Oxley Act of 2002 and the Security and Exchange Commission's 2011 Disclosure Guidance on Cybersecurity Risks and Incidents.

The next article, "From Physical Security to Cyber Security," by Sinha, Nguyen, Kar, Brown, Tambe, and Jiang, presents a survey of how game theory has been applied to both physical and information security applications. It is followed by two papers that leverage game theory, one written by computer scientists and another from an international relations scholar. In "Optimising Time Allocation for Network Defense," Caulfield and Fielder study the trade-offs system administrators face in devoting resources to defensive actions such as patching and repairing compromised computers compared to nonsecurity activities. Meanwhile, in "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyber Attack," Lindsay places the difficulty of identifying nation-state attackers in the context of the international relations literature. He argues that attribution is harder in cases where the stakes are lower, and vice versa, and then constructs a game that explains why most of the low-value attacks remain anonymous while the high-value ones do not.

In "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications," a team of cryptography luminaries and policy experts argue that recent US and UK proposals to require legal access to encrypted communications would greatly damage the operational security of legitimate private communications.

The final four papers illustrate how the perspectives from different disciplines can be profitably applied to the cybersecurity context. In "Scripting the Crime Commission Process in the Illicit Online Prescription Drug Trade," Leontiadis and Hutchings apply a method from criminology called crime script analysis to identify opportunities for intervention in the online sale of unauthorized prescription drugs. They map out the steps required for cybercriminals to be successful and use that information to identify which countermeasures are most likely to be effective and long lasting. In "Critical Visualisation: A Case for Rethinking How We Visualise Risk and Security," Hall, Heath, and Coles-Kemp argue that visualization is an underutilized but powerful tool for improving our understanding and response to cybersecurity threats. The authors juxtapose images from many topics beyond cybersecurity to demonstrate the potential use and misuse of visualizations. In "Neural Correlates of Gender Differences and Color in Distinguishing Security Warnings and Legitimate Websites: A Neurosecurity Study," cybersecurity intersects with neuroscience. Anderson, Kirwan, Eargle, Jensen, and Vance describe an experiment in which subjects monitored by EEG are presented with malware warnings. Among the findings is that women encountering the warnings exhibit higher brain activity. Finally, in "Identifying Patterns in Informal Sources of Security Information", Rader and Wash analyze widely available sources of security information to learn more about what is available to novice users when making security decisions. They find substantial differences between information available from peers (which tend to focus on attack perpetrators) and new sources (which tend to focus on attack consequences).

The papers included in this inaugural issue offer compelling examples of the wide range of approaches available to study cybersecurity challenges. It is our sincere hope that the new *Journal of Cybersecurity* will offer an authoritative and persuasive home for cybersecurity research that not only brings together diverse strands of research, but also helps to solve many of the inherently interdisciplinary problems affecting cybersecurity today and in the future.

Tyler Moore
Editor-in-Chief

David Pym
Editor-in-Chief