JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2(2), 2016, 119–120
doi: 10.1093/cybsec/tyv001
Advance Access Publication Date: 20 January 2015
Editorial

Editorial

Modern society requires a reliable and trustworthy Internet infrastructure. To achieve this goal, cybersecurity research has drawn from a multitude of disciplines, including engineering, mathematics, and social sciences, as well as the humanities. Cybersecurity is concerned with the study of protection of information — stored and processed by computer-based systems — that is vulnerable to unintended exposure and misuse.

Computer-based systems that store and process confidential, sensitive, and private information are vulnerable to attacks exploiting weaknesses at the technical, social, and policy level. Attacks may seek to compromise the confidentiality, integrity, or availability of the information, as well as violate the privacy of the information's owners and stakeholders.

One reason why achieving cybersecurity is so hard in practice is that systems are often designed in isolation, but operate as parts of a broader ecosystem. In such an environment, delivering complex sets of services, the defenders may be interested less in the security of a particular subsystem and more in the overall sustainability and resilience of the ecosystem.

Systems supporting (in no particular order) the financial, energy, transport, retail, industrial, manufacturing, space, communications, health, defence, educational, commercial, professional services, environmental, and governmental sectors are not only critical but also massively interconnected. Vulnerabilities in systems in one sector — that may be exploited by criminals, terrorists, nation-states, or pranksters — may lead to critical failures in others.

The extent of the threat to the information ecosystems upon which modern societies depend, and the scale of the required response, is increasingly being recognized by major governments, with substantial R&D funds being made available. Moreover, the solutions to cybersecurity problems also span the technical and policy layers. Consequently, a journal is needed to disseminate research results that often span the traditional disciplinary boundaries.

Understanding how these ecosystems operate requires an interdisciplinary approach: for example, computer scientists to design the software and networks; cryptographers to protect confidentiality of communications; economists to explain how the competing incentives of stakeholders might play out; anthropologists to explain cultural contexts and how they impact solutions; psychologists to explain how decisions are made and the impact on system design; the legal and policy scholars to set out regulatory constraints; criminologists and crime scientists to explain the motivations of perpetrators; and experts in strategy to frame the international context. Consequently, cybersecurity research should not remain siloed. Instead, rigorous, interdisciplinary scholarship that incorporates multiple perspectives is required.

The *Journal of Cybersecurity* (*JCS*) is a new, open-access publication from Oxford University Press, developed specifically to deliver a venue that can bridge the many different disciplines and specialisms in information security. Future successes in cybersecurity policy and practice will depend on dialogue, knowledge transfer, and collaboration.

Tyler Moore

David Pym

JCS publishes accessible articles describing original research in the inherently interdisciplinary world of computer, systems, and information security. *JCS* is premised on the belief that computer science-based approaches, while necessary, are not sufficient to tackle cybersecurity challenges. Instead, scholarly contributions

from a range of disciplines are needed to understand the human aspects of cybersecurity. *JCS* provides a hub around which the interdisciplinary cybersecurity community can form. *JCS* is committed to providing quality empirical research, as well as scholarship, that is grounded in real-world implications and solutions. It will appeal to academics and researchers in security and related fields, senior security managers in industry, and policy-makers in government.

JCS will initially publish research on the following aspects of cybersecurity: anthropological and cultural studies; computer science and security, including mathematical and systems perspectives; security and crime science; cryptography and associated topics; security economics; human factors and psychology; law and regulation; political and policy perspectives; strategy and international relations; and privacy.

We sincerely hope that *JCS* will play a major role in fostering an interdisciplinary community of cybersecurity scholars.

Tyler Moore
Editor-in-Chief

David Pym
Editor-in-Chief