NEWS RELEASE

Contact: Jim Ormond
ACM
212-626-0505
ormond@acm.org

ACM TO PUBLISH NEW JOURNAL ON DIGITAL THREATS

Article Submissions Now Being Accepted for Journal Bridging Research and Practice

NEW YORK, NY, June 27, 2018 – ACM, the Association for Computing Machinery, today announced the forthcoming publication of *ACM Digital Threats: Research and Practice (DTRAP)*, a new peer-reviewed journal that targets the prevention, identification, mitigation and elimination of digital threats. A central goal of *DTRAP* is to promote the development of scientific rigor in digital security by bridging the gap between academic research and industry practice. Submissions for the inaugural issue to be published in 2019 are now being accepted via the *DTRAP* website.

"Our new journal will promote scientific rigor in digital security," said *DTRAP* Co-Editor-in-Chief Leigh Metcalf of the CERT Cybersecurity Division at Carnegie Mellon University. "At the same time, the focus will be on concrete, rather than theoretical, challenges. So we are encouraging the submission of scientifically rigorous manuscripts that address extant digital threats, rather than laboratory models of potential threats."

"*DTRAP*'s vision is to create a bridge between researchers and practitioners to generate a more energized dialogue about problems and solutions," added *DTRAP* Co-Editor-in-Chief Arun Lakhotia of University of Louisiana at Lafayette and Cythereal, Inc. "The traditional model of practitioners and researchers working in their cocoons is not effective for a fast-moving field like cybersecurity. The threat landscape changes so rapidly that by the time researchers learn of a problem and begin working on it, it is too late."

In addition to research articles, *DTRAP* will invite contributions to two regular columns: "With the Benefit of Hindsight" and "Leaving the Laboratory: Putting Research into Practice." "With the Benefit of Hindsight" will detail what authors have learned from past cybersecurity successes or failures, exploring themes such as lessons learned during a security event, how the landscape has changed since the event, and what further development remains to be done.

Each installment of "Leaving the Laboratory" will examine a peer-reviewed research article from a recent issue of *DTRAP* with respect to implementing research, essentially taking the research into practice. Topics for this column will include general concerns for both researchers and practitioners that relate to doing research effectively, or examining actual changes seen in the security landscape as a result of researchers and practitioners collaborating.

"ACM is proud to launch *DTRAP*," said Scott Delman, ACM Director of Publications. "Computer security has become one of the fastest-growing areas in technology, and we have been planning to add a security-oriented publication to our roster of more than 50 computing journals. We were, however, looking for an approach that would complement ACM's unique role of bringing the academic research and practitioner communities together. We are confident that *DTRAP* will play an indispensable role in the field going forward."

In addition to Co-EICs Metcalf and Lakhotia, the *DTRAP* editorial team includes Managing Editor Eric Hatleback of the University of Pittsburgh and CERT, and an international team of 25 Associate Editors representing various countries including Belgium, Germany, Ireland, Italy, Japan, The Netherlands, and the United States.

About ACM

ACM, the Association for Computing Machinery **www.acm.org,** is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

###