Digital Threats: Research and Practice Inaugural Issue Editorial

We are very excited to present this first issue of *ACM Digital Threats: Research and Practice* (DTRAP) as co-editors-in-chief. This journal has been in the making since 2015, when Leigh first sent a proposal to the ACM Publication Board. The board then asked the question we are sure you are asking: Why another journal? It is appropriate that in this first editorial we answer that question, as that drives the vision of the journal.

The increasing specialization of job functions has created a gulf between the creators of new knowledge (the researchers) and those who put the knowledge to use (the practitioners). There are researchers, mostly in academia and government, who specialize in doing research. They spend a career conjuring up research problems, solving them, and moving on to the next. Being far removed from practice, that the problems they conjure up are timely, relevant, and important is a matter of chance. However, practitioners have access to problems that are timely, relevant, and important, but the fast pace at which the industry moves does not leave them with the time and resources needed to innovate. This gulf is further compounded because the two do not “drink from the same watering hole.” The round trip from a problem being identified in the field, reaching researchers, and its solution coming back may take decades.

Although in other areas one can let time take its course, it is a luxury we cannot afford in cybersecurity. The threats to users of computers, or more broadly any system made of digital devices, are not only real but a daily issue. From ransomware attacks on individual computers to advanced persistent threats on power plants, the attack vectors and the consequences of those attacks are growing. New threats are often in the field, whereas solutions to the threats often originate in academic research. There is thus a dire need to shorten the cycle time between the identification and solution of digital threats.

The vision of DTRAP is new and different from traditional scientific research journals. Whereas the other research journals are of, by, and for researchers, DTRAP aims to bridge the gulf between researchers and practitioners. We are doing this by actively bringing practitioners in every stage of the publication process—editorial board, guest editors, reviewers, and authors—and seeking their guidance in shaping the direction of the journal. This is visible in the editorial board. The two editors-in-chief have a foot each in research and practice. Leigh has a doctoral degree in mathematics and had more than 10 years of industry experience before joining CERT. Arun is a professor of computer science at the University of Louisiana at Lafayette and the CEO of Cythereal Incorporated, a company he founded to transition his research. The rest of the editorial board has 19 members from universities, 9 members from industry, and 5 from government entities.

After forming the editorial board, one of the first issues we focused on was how to attract practitioners to write for an archival, academic journal. For DTRAP to serve as a bridge between researchers and practitioners, it had

CCS Concepts: • **General and reference** → Document types; • **Security and privacy**;

Additional Key Words and Phrases: Digital threats, research and practice

ACM Reference format:

Arun Lakhotia and Leigh Metcalf. 2020. Digital Threats: Research and Practice Inaugural Issue Editorial. *Digit. Threat.: Res. Pract.* 1, 1, Article 1 (March 2020), 3 pages.

<https://doi.org/10.1145/3380320>

© 2020 Copyright held by the owner/author(s).

2576-5337/2020/03-ART1

<https://doi.org/10.1145/3380320>

Digital Threats: Research and Practice, Vol. 1, No. 1, Article 1. Publication date: March 2020.

to have traffic flowing both ways. Attracting papers from academic researchers is not a challenge, as publishing forms a significant part of their performance measure. It is evident from the talks at industry conferences such as BlackHat, DEFCON, the FIRST Annual Conference, and others that there are many interesting problems being solved in the industry, and additionally that there are thought leaders eager and willing to share the insights they have gained. These forums, however, do not require written paper, and certainly not at the level of rigor needed for an academic journal. The question then was in the absence of any incentive in their primary employment for publishing, what we could do to encourage practitioners to write and, moreover, subject their writing a grilling peer-review?

The solution we arrived at is a new class of articles called *Field Notes*. Such reports are common in fields that include significant empirical observation, such as social sciences. Quite often, these reports are maintained as part of the research protocol so as not to rely on memory. Other times, they are also published and shared with others, such as in medicine, where medical practitioners publish reports on interesting and unusual cases. In medicine, they serve the purpose of documenting cases, which when combined over time and space may provide new insights.

At this time what constitutes a Field Note is still a work in progress. Borrowing from social studies and medicine, we first envisioned that a Field Note would capture interesting empirical observations that may provide a data point for future research. Over time, we learned that focusing on empirical observations replete with data was too limiting. As in medicine, it should capture some unusual or novel occurrence. Clearly, a Field Note had to be different from blogs replete over the Internet in that it should have archival value. Our working definition of a Field Note now is that it should be an article that provides some insights into some problem that is interesting and relevant for a graduate student to take on for further research investigation.

The final question was how could we attract papers from on topics that were topical? We learned quickly that “build it and they will come” is not an effective strategy for a journal. It does attract papers, although not necessarily those on topics that are current and relevant. In essence, we had to explicitly define the themes and reach out to people breaking new ideas along those themes. This led to the idea of “Special Issues” on specific topics, each led by a team of guest editors who are leaders in the topic, both from academia and industry.

This first issue you are reading is the outcome of all of the pieces coming together. Quite aptly, this first issue is a special issue of the annual FIRST (Forum of Incident Response and Security Teams) Conference, a practitioners’ conference with academic influence. The annual conference is a 5-day global event that brings together incident response and security professionals from around the world to share their experiences and expertise. The conference consists of presentations selected from abstracts submitted. The guest editors, Andrew Cormack of Jisc Technologies and Dr. Jeroen van der Ham of University of Twente, invited authors of selected abstracts to submit full-length papers, which were then subject to peer review by reviewers from academia and industry. This special issue is truly a collaborative work of researchers and practitioners, and a great start of turning our vision into reality.

As we go forward, we have many a special issues brewing. Manuscripts are under review for special issues on Cyber Risk and Insurance and on Digital Threats of Social Media (aka Fake News); manuscripts are being accepted for special issues on Election Security, on Adversarial Machine Learning, and IoT devices. Other special issues being contemplated are on Vulnerabilities, Cyber Situational Awareness, Threats to Human-Machine Interaction, and more. In keeping with the mission of the journal, the guest editors of each special issue has a mix of researchers and practitioners.

We would be remiss if we did not touch upon one final issue. The IT industry in general, and cybersecurity in particular, has been developed on a culture of open source. Individuals and corporations have freely shared their innovations and intellectual property with little or no encumbrances. Placing papers behind paywall when authors are freely sharing their ideas and innovations would run counter to the ethos. Yet running a publishing house has its costs, especially one that is expected to archive knowledge for posterity through all of the upheavals of technology, as ACM has done for the past 50+ years.

We are thankful to the board of FIRST and particularly Dr. Thomas Schreck for making their sponsorship to create this special issue open access. They have provided us a direction for how to work toward making research available freely to the public while ensuring the kind of permanence that an organization such as ACM can offer. For each of the special issues, we are seeking sponsors to make that issue open access. It is our hope that in time we will have sponsors for the entire journal, not just special issues.

We would like to acknowledge the assistance of Dr. Eric Hatleback and Dr. Jonathan Spring, both of CERT, for their invaluable aid in starting the journal, and Dr. Jack Davidson of the ACM Publications Board, Laura Landers, journals manager for ACM, and Holley Cornetto, assistant to the EIC, for their invaluable support from the initial conception of the idea for the journal to the publication of this first issue.

Arun Lakhotia
Leigh Metcalf

Co-Editors-in Chief