Sean Peisert
Editor in Chief

Reflections on the Past, Perspectives on the Future

I've been a member of the *IEEE Security & Privacy* Editorial Board for several years now, as an associate editor, associate editor in chief (EIC), and a guest editor of a couple of special issues, but today I'm honored to introduce myself as the new EIC of the magazine. I feel both humbled and privileged by my appointment to this position, amid an editorial board consisting of, and following in the footsteps of, many of the finest computer scientists and security and privacy professionals in the world. Prior to joining the Editorial Board, in 2014, at the invitation of then-EIC Shari Lawrence Pfleeger, I'd been a long-time reader of the magazine and coauthored a handful of articles. Little did I know where that path would take me in a few short years.

Many of you in the community know me best through my roles on the conference side of the IEEE Computer Society, including as general chair of the 36th IEEE Symposium on Security and Privacy, in 2015, and most recently as chair of the IEEE Computer Society's Technical Committee on Security and Privacy. Those roles have brought me a great deal of perspective on where we're making progress in security and privacy, where we're not, and what the research communities see as the most promising directions in the coming years. You've seen some of the work from those communities published in these pages before, and, given my history with those communities, I'm looking forward to sharing more of it with you.

My day jobs are at the Lawrence Berkeley National Laboratory—the Berkeley Lab—and the University of California, Davis, where I've been working on computer security and privacy in a variety of domains. Before my current positions, I spent many years working on both high-performance computing and computer security at the San Diego Supercomputer Center (SDSC). At SDSC and the Berkeley Lab, computing is all about solving the problems of science, which means that there is always a new domain to learn about. Indeed, as I have come to know and appreciate, computer security is always about the security of *something*, which is what has brought a lot of interest and excitement to me through the years and enabled me to learn more about the electrical power grid, voting and elections, health informatics, high-performance computing and networking, data privacy, legal evidence and forensics, and more. I get excited about learning all the areas that computer security and privacy touches. It is through this lens that I look forward to sharing with you, as well.

It goes without saying that we will continue to have diversity of all kinds among the members of the Editorial Board (and the magazine's authors).

The History of *IEEE Security & Privacy*

IEEE Security & Privacy began in 2003. George Cybenko was its founding EIC. Its inception is thanks to the extremely hard work and years of planning by Cybenko, members of the task force that advised the scope and content of the magazine, and IEEE Computer Society staff.[1] In his inaugural "From the Editors" column, Cybenko introduced *IEEE Security & Privacy* as "a new magazine with an ambitious mission—to build a world-class community of professionals at the leading edge of research and practice in information

Digital Object Identifier 10.1109/MSEC.2020.3034670
Date of current version: 25 January 2021

technology security and privacy."[2] He outlined the vision of the magazine, including "provid[ing] readers with a trustworthy source of information" and "striv[ing] to meet the professional needs of a diverse readership." Vitally, he noted, "When writing for an archival technical journal, an author needs to sound smart. But when writing for a time-critical, widely read magazine such as this, an author must be useful as well."

This the magazine has done with aplomb. Consider the somewhat startling experimental work by Garfinkel and Shelat about computer forensics from recovered hard drives, published in *IEEE Security & Privacy* in 2003, or the 2004 interview with Richard Clarke, a former special advisor to President George W. Bush. Consider Ralph Langner's work, published in 2011, which was one of the first pieces to reveal that Stuxnet really was an attack on Windows systems and that the worm manipulated supervisory control and data acquisition (SCADA) devices, rather than attacking SCADA devices directly. Or consider the work of Trope and Ressler, published in this magazine in 2016, that provided evidence (before the national newspapers) that Volkswagen likely cheated on its emissions software, encouraging further scrutiny.

In his inaugural column as EIC, Carl Landwehr noted the difficulty of succeeding Cybenko, whom he described as a "hard act to follow."[3] Given the magazine's past success, I couldn't agree more. Thankfully, the magazine's structure is solid and robust, and you can expect to continue to see a lot the current editors and departments. At the same time, we also have some members rotating off the Editorial Board, so you'll see some new names on the masthead. It goes without saying that we will continue to have diversity of all kinds among the members of the Editorial Board (and the magazine's authors), and we will work to expand that diversity, as well. Please also keep your eyes open for some exciting new departments, features, and formats in the coming months.

The most significant global pandemic in a century is still going very much in the wrong direction, with all its collateral impact.

As I write this, it is clear that we live in a daunting time. The most significant global pandemic in a century is still going very much in the wrong direction, with all its collateral impact, such as necessary curtailments of travel and other activities for public health and safety, the largest economic recession in decades, and the international upheaval of democratic norms, including the most acrimonious United States election in memory. Civil unrest. Social injustice. Brexit. In a number of parts of the world, including where I live, there are annual wildfires that cloud the sky with smoke and cause power outages. Elsewhere, humanity witnessed the strongest measured typhoon ever to make landfall. Despite these things, *IEEE Security & Privacy* has an 18-year history of excellence that can, should, and will continue. In the beginning, the magazine strove to meet and maintain Cybenko's vision through the creation of a world-class Editorial Board—a description that still applies today. The Editorial Board, which is composed of people from all walks of academia, government, industry, research labs, and think tanks, represents a well-honed machine that continues to bring important security and privacy content to its readership.

Former EIC Pfleeger noted in her inaugural column, "These investigations were not done in isolation; in our columns, departments, articles, interviews, podcasts, and special features, we probed and prodded in the context of the wider world, including economics, human behavior, education and training, public policy, and national and international security."[4] She also referred to the derivation of the English word *science* and quoted Richard Feynman and Ben Goldacre about the need to "enlighten security in a scientific way" while "ensur[ing] that the science is appropriate and rigorous." In his debut column, my immediate predecessor, David Nicol, referred to the vast array of considerations and coordination that had to be taken into account in his work running a center focused on power grid security. He noted not just the huge research community that he led but also the real-world insights and constraints he learned from collaborating with utilities, regulators, and security auditors.[5]

IEEE Security & Privacy's Vision

The magazine will continue Cybenko's mandate to be smart and useful. It will continue the tradition that Pfleeger observed of connecting the wide world and seeking to do so in an appropriate and rigorous scientific manner. And it will stay grounded in ways that Nicol espoused. Indeed, it will not only continue its traditional role of ensuring academic and technical excellence in all the domains of computer security and privacy that you're used to hearing about—software security, hardware security, cryptography, and so on as well as the connections with broader domains, including economics, psychology, sociology, education, and policy—but it will face the reality of the needs of the world head-on, looking for ways to contribute the collective expertise of its community to support humanity and the planet. It will do so in practical, useful, and usable ways, bringing in views from those with hands-on experience with implementing technologies that are actually deployed and used; writing policies, regulations, laws, and standards; and making decisions.

This magazine will address usability issues in computer security and how the community can advance past the expectation that it is somehow the responsibility of nonexpert end users to deter cyberattacks.

The magazine will continue to seek out and publish groundbreaking pieces, such as those about Stuxnet and the Volkswagen emissions scandal, as well as other issues of global importance. It will, as it has in the past, discuss security and privacy issues pertaining to voting and elections, a topic that has not ceased to be critically relevant and that connects with computer security and privacy in many ways, including voting machinery and the processes and apparatus that support and surround the voting process.

It will also address privacy, surveillance, and cryptography, including the pull and push of national security, secure system design, and fundamental privacy rights. In addition, computer security in other critical infrastructure will be discussed, such as the power grid, health-care delivery systems, transportation systems, and manufacturing systems. It will explore artificial intelligence and automation and all their impacts, from rapid medical diagnoses to the automated systems used to monitor social media for disinformation to self-driving vehicles.

This magazine will address usability issues in computer security and how the community can advance past the expectation that it is somehow the responsibility of nonexpert end users to deter cyberattacks. As just one example, consider the security hoops that medical professionals in hospitals are asked to jump through, and yet when the tables are turned for medical issues, the lay public generally has to go to the Internet to figure out how to perform basic first aid. These pages will cover issues related to cyberwar, such as attribution and the handling of vulnerability disclosure. And they will relay education and workforce development, particularly in communities that have long been underrepresented in the security and privacy fields.

IEEE Security & Privacy will seek to continue and expand diversity of all kinds among its Editorial Board members and authors. This diversity includes, but is not limited to, race, ethnicity, national origin, gender, sexual orientation and identity, age, and more. In line with this commitment, we note that the IEEE Computer Society and this magazine are international institutions, and their editors and authors should reflect their readership. Further, as computer security and privacy touch people in different ways, article topics will reflect this diversity, as well. Finally, where it is in its purview, the magazine will not avert its attention from moral and ethical issues in our field.

A Call to the Security and Privacy Community

I have learned a great deal in my years on the Editorial Board, and I would like to heartily tip my hat to a great many people, including numerous past and present Editorial Board members who have been essential to that education. I particularly thank past EICs Cybenko, Landwehr, Pfleeger, and Nicol as well as numerous members of the IEEE Computer Society staff for the wisdom they've imparted to me during the past few months as I've prepared for this role. At the same time, I have a lot yet to learn, including a great deal from the Editorial Board, and I look forward to doing so, working alongside old friends and getting to know new ones.

Perhaps most importantly, in closing, I invite you, the readership, to contribute. The success of this magazine depends on its readership, both as consumers and as contributors, to keep its content vital and fresh. Please submit articles and, by all means, feel free to drop me an email with your suggestions. Once we are all able to travel again, come up and talk with me at a security

The success of this magazine depends on its readership, both as consumers and as contributors, to keep its content vital and fresh.

conference. Even prior to that, I will do what I can to make myself available for videoconference sessions at upcoming security events. I look forward to hearing from you and to working with authors and Editorial Board members to continue this magazine's tradition of publishing world-class security and privacy insights. ■

References

1. G. Cybenko and K. Clark-Fisher, “*IEEE Security & Privacy:* The early years,” *IEEE Security Privacy*, vol. 12, no. 3, pp. 18–19, 2014. doi: 10.1109/MSP.2014.48.
2. G. Cybenko, “A critical need, an ambitious mission, a new magazine,” *IEEE Security Privacy*, vol. 1, no. 1, pp. 5–9, 2003. doi: 10.5555/858866.859058.
3. C. E. Landwehr, “New challenges for the new year,” *IEEE Security Privacy*, vol. 5, no. 1, pp. 3–4, 2007. doi: 10.1109/MSP.2007.13.
4. S. L. Pfleeger, “Enlightened security: Shedding light on what works and why,” *IEEE Security Privacy*, vol. 11, no. 1, pp. 3–4, 2013. doi: 10.1109/MSP.2013.7.
5. D. M. Nicol, “Introduction from the new EIC,” *IEEE Security & Privacy*, vol. 16, no. 2, pp. 3–4, 2018. doi: 10.1109/MSP.2018.1870871.

Digital Object Identifier 10.1109/MSEC.2020.3031996