Reflections on the Past, Perspectives on the Future

Sean Peisert

November 6, 2020

I've been a member of the *IEEE Security & Privacy* Editorial Board for several years now, as an associate editor, associate editor-in-chief, and as a guest editor of a couple of special issues, but today I'm honored to introduce myself to you all as the new editor-in-chief of *S&P*. I feel both humbled and privileged by my appointment to this position, amidst 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 *S&P* Editorial Board in 2014, at the invitation of then-Editor-in-Chief Shari Lawrence Pfleeger, I'd been a long-time reader of the magazine and co-authored a couple of pieces. 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 security and privacy 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 histories with those communities, I'm looking forward to sharing more of it with you in the years to come.

My day jobs are at Lawrence Berkeley National Laboratory — 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 also at the Berkeley Lab, computing is all about solving the problems of science, which meant that there was always a new domain science to learn about. Indeed, as I came to learn and appreciate, computer security is always about security of *something*, which is what has brought a lot of interest and excitement to me over the years, and has allowed me to learn more about the electrical power grid, voting and elections, health informatics, research computing and networking, 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 share with you as well.

IEEE Security & Privacy began in 2003. Its founding Editor-in-Chief was George Cybenko. Its inception is thanks to the extremely hard work and years of planning by Cybenko, members of the task force that advised on the scope and content of the magazine, and IEEE Computer Society staff [1]. In his inaugural letter from the editor, 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 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 must 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 on computer forensics from recovered hard drives published in *S&P* in 2003. Or the 2004 interview with Richard Clarke, former special advisor to President George W. Bush. Consider Ralph Langer's work in published in *S&P* in 2011, was one of the first pieces to reveal that Stuxnet really was an attack on a Windows system that manipulated SCADA devices, rather than an attack on SCADA devices directly. Or, consider the work of Trope and Ressler, published in *S&P* in 2016, that convincingly demonstrated (before the national newspapers) that Volkswagen cheated on its emissions software.

In his inaugural letter as EIC, Carl Landwehr noted that following George Cybenko was a "a hard act to follow." [3] Given all of the magazine's amazing past successes, I couldn't agree more. Thankfully, the magazine's structure is solid and robust, and so 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 members of the Editorial Board (and magazine authors) and 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.

As I write this letter, it is clear that we live in a daunting time. The most significant global pandemic in a century — still going very much in the wrong direction — with all its collateral impact, including necessary curtailments of travel and other activities for public health safety, and the largest economic recession in decades. 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, annual wildfires, smoke, and power outages. Elsewhere, the strongest measured typhoon to make landfall in history. Despite these things, *S&P* has an 18-year history of excellence that can, should, and will continue forth. In the beginning, *IEEE Security & Privacy* strove to meet Cybenko's original visions with the creation of a world-class editorial board — a description which still applies today — that has maintained those visions of *S&P*. The *S&P* Editorial Board — comprised 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 letter from the editors, "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 in the need to "enlighten security in a scientific way" while "ensur[ing] that the science is appropriate and rigorous."

In his inaugural letter, my immediate EIC predecessor, David Nicol, referred to the vast array of considerations and coordinations that had to be taken into account in his work in 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 learned from working with utilities, regulators, and security auditors [5].

S&P will continue founding EIC Cybenko's charter to be smart and useful. It will continue the tradition that EIC Pfleeger observed, of connecting the the wide world and seeking to do so in an appropriate and rigorous scientific manner. And it will stay grounded in ways that EIC 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 will face the reality of the needs of the world head-on, looking for ways to contribute the collective expertise of the security and privacy community to support the needs of humanity and the planet. We will look to do so in practical, useful, and usable ways, bringing in views from those with hands-on experiences in implementing technologies that are actually deployed and used, writing policies, regulations, laws, and standards, and making decisions.

This magazine will also continue groundbreaking pieces such as those about Stuxnet and the Volkswagen emissions, as well as other issues of global importance. This magazine will, as it has in the past, continue to discuss security and privacy issues pertaining to *voting and elections*, an issue that has not ceased to be critically relevant and that connects with computer security and privacy in many ways, including voting machinery but also the processes and apparatuses that support and surround elections.

We will also address *privacy, surveillance, and cryptography*, including the pull and push of national security, secure system design, and fundamental privacy rights. We will address computer security in other *critical infrastructure* — such as the power grid, healthcare delivery systems, transportation systems, and manufacturing systems. We will address *artificial intelligence and automation*, and all of its impacts from rapid medical diagnoses, to the automated systems used to monitor social media for disinformation, to self-driving vehicles.

We will address *usability* issues in computer security and how the security community can advance past the expectation that it is somehow the responsibility of non-expert 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.

We will cover issues related to *cyberwar*, such as attribution and the handling of vulnerability disclosure. And we will cover *education and workforce development*, particularly in communities that have long been under-represented in the security and privacy fields. Finally, where it is in our purview, we will not avert our glance from *moral and ethical issues* in our field.

I have learned a great deal in my years on the *S&P* Editorial Board, and I would like to heartily tip my hat to a great many of those people, including numerous past and present Editorial Board members who have been distinctly formative in that education. I particularly thank past EICs George Cybenko, Carl Landwehr, Shari Lawrence Pfleeger, and David Nicol, as well as to numerous members of the IEEE Computer Society staff for the wisdom they've imparted to me over the past few months as I've prepared for this role. At the same time, I have a lot yet to learn as part of this new role, including a great deal from this 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 welcome you, the readership of this magazine, to contribute. 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 conference. I look forward to hearing from you and working with authors and Editorial Board members to continue this magazine's tradition of publishing world class security and privacy insights.

References

[1] George Cybenko and Kathy Clark-Fisher. IEEE Security & Privacy: The Early Years. *IEEE Security & Privacy*, 12(3):18–19, 2014.

[2] George Cybenko. A Critical Need, an Ambitious Mission, a New Magazine. *IEEE Security & Privacy*, 1(1):5–9, 2003.

[3] Carl E. Landwehr. New Challenges for the New Year. *IEEE Security & Privacy*, 5(1):3–4, 2007.

[4] Shari Lawrence Pfleeger. Enlightened Security: Shedding Light on What Works and Why. *IEEE Security & Privacy*, 11(1):3–4, 2013.

[5] David M. Nicol. Introduction from the New EIC. *IEEE Security & Privacy*, 16(2):3–4, 2018.