I remember attending my first IEEE Symposium on Security and Privacy in 1982. It was my first year out of graduate school, and I was working at the MITRE Corporation. Many of the symposium’s early organizers came from MITRE’s security group, and the buzz in the halls was that the symposium was the most important conference of the year. It’s now in its 35th year and continues to be the premier forum for presenting developments in computer security and electronic privacy and bringing together researchers and practitioners in the field.

In this issue, Peter G. Neumann and his colleagues provide an opinion piece on history of the symposium in “The IEEE Symposium on Security and Privacy, in Retrospect,” offering thoughts on its significance since forming in 1980. Their historical retrospective includes a few anecdotes and tidbits about decisions made and serendipitous accidents that made the symposium what it is today.

Twenty-five years after the symposium began, a small group got together to create a magazine for the community—IEEE Security & Privacy. Interestingly, someone from MITRE again had a hand in this. “IEEE Security & Privacy: The Early Years,” by George Cybenko and Kathy Clark-Fisher, details its history.

This special issue is devoted to the ties between these two centers of the security and privacy community. The symposium has become the top conference for research publication, while the magazine is increasingly serving as a go-to place for articles on the cybersecurity community’s top issues as well as those accessible to the wider community.

**Articles in This Issue**
Capitalizing on the community’s strength as well as the worldwide attention to cybersecurity,
we at S&P present four articles based on papers from the 2013 IEEE Symposium on Security and Privacy:

- "Anon-Pass: Practical Anonymous Subscriptions,"
- "On the Workings and Current Practices of Web-Based Device Fingerprinting,"
- "On Secure Data Deletion," and
- "Eternal War in Memory."

To procure these articles, we consulted with the symposium’s program chairs and selected a number of papers based on general interest and accessibility. We then invited the authors to submit revised articles targeting the magazine’s broader audience and enhanced with new developments since the original paper’s publication.

Several selected papers were from the Systemization of Knowledge (SoK) sessions, which encourages work that evaluates, systematizes, and contextualizes existing knowledge. SoK papers are valuable to the community but might not be accepted for symposium proceedings because of a lack of novel research contributions. Nonetheless, they focus on the current research landscape, identifying areas that have enjoyed much research attention, pointing out areas with unsolved problems, and presenting prioritization models that can guide researchers solving important challenges. This sort of contribution is particularly useful for the magazine’s broad readership.

Unsurprisingly, we chose three articles addressing privacy and tracking issues, while the fourth provides an SoK discussion on a fundamental problem in memory corruption.

In “Anon-Pass: Practical Anonymous Subscriptions,” Michael Z. Lee and his colleagues describe a protocol and system implementation for anonymous subscription services that let users anonymously authenticate while preventing mass sharing of credentials. They show how the protocol prevents service providers from correlating users’ actions while guaranteeing that accounts are being used only once at a given time. They also describe two services using the protocol implementation—a streaming music service and a public transit pass—and analyze their operating costs.

“On the Workings and Current Practices of Web-Based Device Fingerprinting,” by Nick Nikiforakis and his colleagues, tackles the problem of websites tracking users. The authors analyze the techniques that allow websites to track users without needing client-side identifiers. They then describe questionable practices, such as circumventing HTTP proxies to discover a user’s real IP address and installing intrusive browser plug-ins. Finally, they measure fingerprinting’s adoption and evaluate browser extensions intended to counter these fingerprinting systems and practices.

Another aspect of privacy—and one often motivated by organizational practices—is the need to delete data completely. Joel Reardon and his colleagues’ SoK article “On Secure Data Deletion,” presents different approaches to erasing data permanently. The article classifies deletion techniques in the context of different adversary models and system interfaces and helps readers understand their true effects.

Another SoK article, “Eternal War in Memory,” by László Szekeres and his colleagues, addresses a long-standing problem with memory corruption bugs often found in software written in low-level languages such as C or C++. Although this issue has existed for more than 30 years and many potential solutions have been proposed, memory corruption attacks continue to pose a serious threat. The authors shed light on why this problem is still unsolved and analyze the factors inhibiting the deployment of techniques that might provide stronger protection.

By bringing a piece of the symposium to you, the magazine’s readership, we at S&P hope to enhance both the symposium’s and the magazine’s value in the community. We intend to make this a regularly occurring special issue, inviting submissions from symposium authors and publishing them each year just before the upcoming symposium, which is traditionally held in late May.

I look forward to seeing you at the symposium and connecting with you through the pages of the magazine throughout the year.

Terry Benzel

is the deputy director of the Internet and Networked Systems Division at the University of Southern California Information Sciences Institute. Contact her at tbenzel@isi.edu.