Sailing Away!

Carl E. Landwehr
Editor in Chief

Four years ago, I was honored and pleased to take the helm as editor in chief of *IEEE Security & Privacy*, and in accordance with IEEE Computer Society publication policies, my watch is ending. You'll next hear from John Viega, our new editor in chief, in this space, and I know he has some exciting plans for the magazine.

For my part, I first want to acknowledge the tremendous contributions of the volunteers who write the articles and departments we publish, who provide the reviews and recommendations that keep our content timely and of high quality, and who keep us in touch with the international technical community in security and privacy. Equally, I appreciate the contributions of the professional staff that does the editing, artwork and production; monitors the peer review process; and markets the magazine. I've thoroughly enjoyed working with all of you.

I offer special thanks to Fred Schneider, who on countless occasions has provided valuable comments and advice on matters of writing and policy, and Marc Donner, who has faithfully reviewed much of the content of each issue before it goes to press and improves its quality in numerous ways. Gary McGraw, in addition to faithfully producing Silver Bullet podcasts and interviews, has been a tireless advocate for the magazine.

This is an appropriate time to take stock. Have we (as a field, not as a magazine) made progress in the past four years? What are the prospects for the future?

A forecast I made publicly (though not in this space) four years ago was that things would get worse before they got better (but that they would get better), and that we were likely to see more integration of protection mechanisms into hardware. It's fair to say that things have indeed gotten worse. What we have seen in the past four years has been an increasingly visible and escalating threat. The most dramatic example for me this year was the discovery and analysis of the Stuxnet malware,[1], which for many people has moved the threat of sophisticated attacks against industrial control systems from hypothetical to real. And the attackers very often succeed. Earlier this year, the revelation that Google's email service had been hacked and its corporate response to that attack likewise raised public awareness of the threat to widely used cyberinfrastructure.

One of the most significant events of the past four years has been the recognition by those who control public policy at the highest levels that the threat to both military and civilian systems is real, and they have begun to act on that basis. In the US, a major government initiative (the Comprehensive National Cybersecurity Initiative) began in secret more than three years ago, and is now largely public.[2,3] While the major costs of this program are driven by near-term measures to stem the tide of information flowing out of defense and other government systems, the program has also provided some impetus and funding aimed at "changing the game." More recently, the UK launched a public national cybersecurity initiative stimulated in large part by growing financial losses from cybercrime.

Several significant events in the past four years have raised the profile of international cyber conflict. Relatively unsophisticated, politically motivated denial-of-service attacks were able to cripple commerce in Estonia. The conflict between Russia and Georgia provided an example of how military and cyberattacks might be coordinated. The US has recently created a full-scale Cyber Command that will presumably focus on warfare issues in cyberspace. International policy in this area remains very much an open question.

On the privacy front, the rush to embrace social networking systems and, in particular, Facebook has precipitated many dramatic and disturbing privacy-related incidents. It sometimes seems that today's youth have no interest in privacy—until they consider the effects of "friending" a parent. A recent series of investigative articles in *The Wall Street Journal* (http://online.wsj.com/public/page/what-they

-know-digital-privacy.html) has spotlighted common but largely hidden business practices for online user tracking and identification. Some of these also involve Facebook, but many are in much broader use. The exposure of images by Google Earth, as well as Google's apparently inadvertent vacuuming up of wireless data, has evoked legal action in Europe and added another dimension to privacy discussions. Again, the threat seems to be growing, but the public understanding and concern seems to be growing as well.

Technology has advanced incrementally but significantly in several areas. There has been a bit of migration of security-related mechanisms into hardware, though less than I expected. The technology for analyzing programs for security flaws continues to mature and has produced several tools in active use. Microsoft's investments in software development processes and tools seem to have had a significant effect on its products. But the response from the attack community has been simply to target vulnerabilities in other companies' products, and there has been no shortage of these. There has also been gradual progress in development of automated tools for assuring that complex networks are configured according to a specified security policy; this work has the potential to remove significant classes of operational vulnerabilities.

In sum, the threat is up, awareness is up, technology for dealing with the threat has advanced and is perhaps keeping up, but barely. What of the future?

In the near term, we must learn to swim with the sharks. Both the software and the hardware on which we increasingly depend come from all over the world, from sources of which we have little knowledge and less control. Today, we need to teach vigilance to users, we need tools that will help us distinguish valid from fraudulent websites and that will help us validate that our systems are configured as securely as possible. For the long term, we need to get out of these shark-infested waters and into some trustworthy vessels. We need new computing platforms and networking infrastructures that raise the cost of attacks to the point that the sharks go elsewhere. This activity requires both long-term investment and careful attention to transition paths. As a reader of this magazine, you have an important role to play in these processes. Please act! ☐

References

1. N. Falliere, L.O. Murchu, and E. Chien, "W32.Stuxnet Dossier," Symantec, 2010; www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
2. S. Saydjari, "Launching into the Cyberspace Race: An Interview with Melissa Hathaway," *IEEE Security & Privacy*, vol. 6, no. 6, 2008, pp. 11–17.
3. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009; www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.