New Challenges for the New Year

Carl E. Landwehr
Editor in Chief

You've heard from me in this space before, but this is my first column as *IEEE Security & Privacy*'s editor in chief. I feel both honored and privileged to have the opportunity to assume this responsibility. George Cybenko, as both the driving force behind the magazine's creation and its EIC for the first four years, is a hard act to follow. But because he created such a strong base for the magazine, I'm hoping it won't be a difficult act to continue. You can expect the mix of articles, departments, and special issues on current topics to continue. You'll see some new names in the masthead as we replace those rotating off the editorial board; this is a normal process for all IEEE publications. We'll continue to strive for fresh and interesting material to keep you at the forefront of technology and issues in security and privacy.

These are changing times for print publications and for professional societies. The technology that many of us helped develop is having tremendous impact in publishing and in information distribution generally. As a trial, the IEEE has allowed us to offer subscriptions to nonmembers of the IEEE Computer Society at a greatly reduced price: US$29 per year. Together with our content, this offer has helped us increase our subscription base in a time of generally declining participation in professional societies. We're also trying to take advantage of new media. A prime example is Gary McGraw's Silver Bullet Security podcasts. Digested versions of these appear in the magazine (p. 9 of this issue).

I'm especially interested in hearing from you about what you like and don't like in *S&P*. We can and do monitor the download rates for various articles that we print, but those statistics tell only part of the story. This is a volunteer effort, and we depend on freely submitted contributions from the community. To ensure the quality of what we publish, we also depend on a peer-review process, which requires volunteer work. I want our volunteers' time to be well spent.

If you would like to help—particularly if you have ideas for improvements—please get in touch with me by email (landwehr@isr.umd.edu), but if you see me at a meeting, feel free to corner me. If you would like to submit a contribution to one of the magazine's departments, please contact the department editor (their email addresses are at the top of each department's opening page). Information on how to submit regular articles is available on the magazine's Web site (www.computer.org/security/).

Shifting gears a little, there's another activity in which I would like to engage you: grand challenges. Few people can have failed to notice the interest that Darpa's challenges for autonomous vehicles have generated. Similarly, I've been impressed by the great interest that the RoboCup soccer competitions have generated. In addition to possibly advancing the state of the art, such competitions can be highly educational and entertaining. A few years ago when I asked Google cofounder Sergey Brin what he had found most beneficial in his undergraduate career at the University of Maryland, he pointed to the programming competitions in which he had participated.

While at the US National Science Foundation, I spent some time trying to figure out how to structure a challenge or a competition that would help us move beyond our present stage of penetrate-and-patch security. A colleague with experience on both the defensive and offensive sides of software security told me why offense is easier: Most software comes bundled, and something in the bundle is likely to have an exploitable flaw; once the flaw is exploited, today's systems have few internal barriers to contain attacks. He attributed this situation, in part, to deficiencies in computer science education. In his view, students rarely face the responsibility of developing a significant piece of software and then integrating it into a larger system. Without such experience, students are unlikely to grasp the need to carefully check input parameters and provide strong internal barriers in software systems.

I thought it would be great to come up with a competition that could help students learn these lessons, but doing so isn't easy. The US National Institute of Standards and Technology has made very effective use of competitions to design new, open source cryptographic algorithms, but

continued on p. 4

Willis Ware: Data privacy pioneer

IEEE Security & Privacy editor in chief Carl E. Landwehr presents Willis Ware with the Pioneer Award.

IEEE Security & Privacy magazine awarded Willis Ware the Pioneer Award for outstanding contributions to data privacy issues and his pioneering efforts in information security research and policy development. *S&P* editor in chief Carl Landwehr presented Ware with the award on 6 November 2006 at RAND in Santa Monica, California. *S&P*'s editorial board and RAND executives attended a reception immediately following the ceremony.

Ware joined Princeton's Institute for Advanced Study in 1946, contributing to the design of the first parallel and asynchronous digital computer with John von Neumann. In 1952, he joined RAND and remains a senior computer scientist emeritus. In addition to his work at RAND, the early 1970s saw Ware chair the Special Advisory Committee on Automated Personal Data Systems. The committee's report, nicknamed the Ware Report, was the cornerstone of the Federal Privacy Act of 1974. The late US President Gerald Ford appointed Ware to the Privacy Protection Study Commission, which authored a report that remains the most definitive examination of record-keeping practices in the private sector. Ware was the first chair of the Computer System Security and Privacy Advisory Board (now called the Information Security and Privacy Advisory Board), which advised the US government on computer technology's societal impacts.

Ware has a PhD in electrical engineering from Princeton University. He is a fellow of the IEEE, the ACM, and the American Association for the Advancement of Science, as well as a member of the National Academy of Engineering. In addition, Ware served as the first president of the American Federation of Information Processing Standards.

continued from p. 3

the primary competitions I've seen in computer and network security have been capture-the-flag exercises or penetration tests of one sort or another. These have their benefits, but they don't seem likely to lead to long-term technical progress in security.

But just because I haven't been able to come up with the right idea doesn't mean you can't. Here are my desiderata for a challenge problem in computer and network security:

1. It must be difficult enough, and relevant enough, that accomplishing it will lead to a measurable advance of some sort in security technology.
2. It must be possible to impartially and repeatedly rank the results of efforts by different competitors.
3. It must be interesting enough to attract widespread interest and simple enough to explain to those not involved in the field.

There's much more to be said on this topic, but I would like to hear your views. If you'll contribute, I'll summarize the results in a future column. ▢

Letters

Dear Editor,

I read with interest the recent theme issue of *IEEE S&P* (Data Surveillance). With the disclaimer that data surveillance is precisely what I do for a living and in modern societies if you do something for a living then no one should trust your opinion about it, I want to say something anyway, I'll just confine myself to fact.

These are facts:

- Data has value;
- The fraction of corporate wealth that is data is growing;
- Data is most valuable when it is most used.

These are facts except in a few special cases:

- Institutional data perimeters barely exist;
- In fact-changing environments, authentication is diseconomic for fine-grained data control;
- Accountability is to behavior as gravity is planetary orbits.

To keep data in enough use to be valuable, but not so much use as to reach escape velocity, there is no choice but to impose the right amount of accountability. To not gum up machinery nor keep people from getting their work done, that accountability cannot rely on the sentience or the cooperation of whatever is involved. Accountability without cooperation means surveillance.

As such, the fork in the road we face is either to surveil people or data. Yes, the books and records produced are homeomorphs of each other, but if my choice is a datum or a person as the primary unit of observation, then I'll take the datum; it's the lesser of two evil necessities. Your choice may differ, but not to decide is to decide.

—Daniel E. Geer, Jr., Sc.D.
Verdasys