THE Next Wave
The National Security Agency's review of emerging technologies

GUEST

Editor's column

Robert Meushaw

The world's most extensive case of cyberespionage, including attacks on US government and UN computers, was reported at the 2011 Black Hat conference by security firm McAfee. Concluding five years of investigation, McAfee analysts were "surprised by the enormous diversity of the victim organizations and were taken aback by the audacity of the perpetrators." *Wired* magazine recently broke a story revealing that "a computer virus has infected the cockpits of America's Predator and Reaper drones, logging pilots' every keystroke as they remotely fly missions over Afghanistan and other war zones." These are but two examples of what have become almost routine reports of failures in system security. Increasingly, these problems directly affect us in important parts of our daily lives. And even more alarming is the rapid growth in the breadth and severity of these spectacular failures.

How are such widespread problems possible after decades of investment in computer security research and development? This question has gained the attention of increasing numbers of security professionals over the past several years. An emerging view is that these problems demonstrate that we do not yet have a good understanding of the fundamental science of security. Instead of fundamental science, most system security work has focused on developing ad hoc defense mechanisms and applying variations of the "attack and patch" strategy that emerged in the earliest days of computer security. Our national reliance on networked information systems demands that we approach security engineering with the same rigor that we expect in other engineering disciplines. We should expect designers of our digital infrastructure to have a well understood scientific foundation and advanced analytic tools comparable to those used in the production of other critical assets such as bridges, aircraft, power plants, and water purification systems.

The National Security Agency, the National Science Foundation (NSF), and the Intelligence Advanced Research Projects Activity jointly responded to this problem by sponsoring a workshop in November 2008 to consider whether a robust science of security was possible and to describe what it might look like. Academic and industry experts from a broad set of disciplines including security, economics, human factors, biology, and experimentation met with government researchers to help lay the groundwork for potential future initiatives. Since that meeting, a number of programs focused on security science have been initiated, along with an effort to help build a robust collaboration community.

This issue of *The Next Wave* is focused upon the important topic of security science. Included are articles from six of the experts who attended the 2008 workshop and have continued to work in the area of security science. Carl Landwehr from NSF provides a few historical examples of the relationship between engineering and science and shows how these examples might help us understand the evolution of cybersecurity. Adam Shostack from Microsoft provides another perspective on how science evolves and describes some steps he considers necessary to advance the development of cybersecurity science. Roy Maxion from Carnegie Mellon University (CMU) calls for greater scientific rigor in the way experimental methods are applied to cybersecurity. Dusko Pavlovic from Oxford University provides a unique and unexpected model for security to reason about what a security science might be. Anupam Datta from CMU and John Mitchell from Stanford University describe some of their joint work in one of the core problem areas for security—how to compose secure systems from smaller building blocks. Alessandro Chiesa from the Massachusetts Institute of Technology and Eran Tromer from Tel Aviv University describe a novel approach based upon probabilistically checkable proofs to achieve trusted computing on untrusted hardware. Their insights may lead to new strategies for dealing with a host of security problems that are currently considered intractable, including supply chain security.

The capstone article for this issue of *The Next Wave,* contributed by Fred Schneider of Cornell University, methodically constructs a "blueprint" for security science. Building on his keynote at the 2008 workshop, Schneider suggests that security science should describe features and

relationships with *predictive* value rather than create defenses *reactively* responding to attacks. Schneider's blueprint outlines the foundation for a security science comprising a body of laws that allow meaningful predictions about system security.

Developing a robust security science will undoubtedly require a long-term effort that is both broad based and collaborative. It will also demand resources well beyond those available to any single organization. But even with a generally acknowledged need for science, the temptation will be to continue fighting security fires with a patchwork of targeted, tactical activities. Good tactics can win a battle but good strategy wins the war. We need to create a better strategy for computer security research. As we continue to struggle with daily battles in cyberspace, we should not forget to pursue the fundamental science—the fundamental strategy—that will help to protect us in the future.

Technical Director emeritus
Trusted Systems Research, NSA

Contents

The Next Wave is published to disseminate technical advancements and research activities in telecommunications and information technologies. Mentions of company names or commercial products do not imply endorsement by the US Government.

To receive printed copies of *The Next Wave,* please use the Internet address below and provide a mailing address and the number of copies requested. For more information, please contact us:

National Security Agency
Attn: Kathleen Prewitt, Managing Editor
Suite 6541
Ft. George G. Meade, MD 20755–6541
301.688.9604 | TNW@tycho.ncsc.mil

Vol. 19 | No. 2 | 2012