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

GUEST Editor's column

Frederick R. Chang, PhD

Considered by most to be the first computer worm ever, the Creeper worm was written over 40 years ago. Unlike today's worms and other malicious code, Creeper was not written with malicious intent, but rather as an experiment in self-replicating code. It spread through the ARPANET—a precursor to the modern Internet—by "jumping" from machine to machine, and it caused an infected system to display the message: "I'M THE CREEPER, CATCH ME IF YOU CAN." In response, the first antivirus program, Reaper (itself a computer worm), was created.

Back then it would have been nearly impossible to predict how dependent we would become on modern networking and computing infrastructure. As a sign of our increasing dependency on modern networking, this issue of *The Next Wave (TNW)* as well as future issues will be available primarily electronically instead of in print. As with commercial publishers, the federal government is finding the incentives to move from a print publication to an electronic publication irresistible—increased audience for lower cost.

It would also have been nearly impossible to predict the difficulty of defending the modern infrastructure. Early research on computer security had already begun by the time Creeper was spreading through the ARPANET. Yet, after over 40 years of research and development on computer and information security, we find ourselves searching for fundamental answers on how to secure systems in cyberspace. This existing research base has yielded important and significant findings through the decades, and computing systems are unquestionably more secure as a result. There is, however, an increasing awareness in the cybersecurity community that the research has not produced a consistent scientific understanding of cybersecurity and that such an understanding is now urgently required.

This issue of *TNW* is the second of two issues dedicated to the science of cybersecurity. The first issue, published in March of 2012, included contributions from experts primarily from academia and the private sector and offered an impressive collection of insights that touched on a wide range of perspectives on the problem, from technology to policy to strategy and more. This second issue includes contributions from experts within government (US and UK) and offers a wide array of perspectives on the problem as well as activities under way to develop and implement solutions.

There are some promising indications that a science of cybersecurity initiative is gaining momentum, including several workshops, conferences, and reports that point to the need for an interdisciplinary approach to addressing the problem. Most recently, in November of 2012, NSA sponsored the first annual Science of Security Community meeting to discuss issues foundational to the advancement of a science of cybersecurity. This issue of *TNW* provides additional detail on some other notable activities taking place both inside and outside of government.

The theme of interdisciplinarity is important. Indeed, there is evidence that scientific advances often occur at the boundaries of established but related fields, when scientists from different disciplines address a problem free from the ordinary constraints of working in a more intradisciplinary fashion. A science of cybersecurity offers many opportunities for advances based on a multidisciplinary approach, because, after all, cybersecurity is fundamentally about an adversarial engagement. Humans must defend machines that are attacked by other humans using machines. So, in addition to the critical traditional fields of computer science, electrical engineering, and mathematics, perspectives from other fields are needed. Cognitive science will help us understand adversarial intent and human decision making under uncertainty in cyberspace. Economics will illuminate how misaligned economic incentives hamper fundamental progress in cybersecurity. Biology will shed light on the extent to which it may be possible to transfer concepts from our understanding of the human immune system toward the conceptualization of a cyber immune system. Thinking from other scientific disciplines will offer perspectives that will trigger new, valuable ideas.

Progress in this new science will be unpredictable, uneven, and slower than we want. We will need to be patient. Cybersecurity research experts will have to resist the urge to focus their efforts on the cyberattack of the day. We will need our research scientists to help us understand not only what is possible, but also what is not possible. Indeed, a rigorous understanding of the limits of cybersecurity will be fundamental to the formation of the new science. We have learned much about how to defend computing systems since the first computer worm, but now we must advance our understanding through the creation of a disciplined and systematic science of cybersecurity. We cannot wait any longer; there is too much at stake.

Frederick R. Chang

Former Director of 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.

Vol. 19 | No. 4 | 2012