Expanding the breadth and impact of cybersecurity and privacy research

July 31 2014

As our lives and businesses become ever more intertwined with the Internet and networked technologies, it is crucial to continue to develop and improve cybersecurity measures to keep our data, devices and critical systems safe, secure, private and accessible.

Today, the National Science Foundation's (NSF) Secure and Trustworthy Cyberspace (SaTC) program announced two new center-scale "Frontier" awards to support large, multi-institution projects that address grand challenges in cybersecurity science and engineering with the potential for broad economic and scientific impact.

The Frontier awards are part a diverse $74.5 million portfolio of more than 225 new projects in 39 states. These cybersecurity research and education projects are aimed at minimizing the misuses of cyber-technology, bolstering education and training in cybersecurity, establishing the science of security, and transitioning promising cybersecurity research into practice.

"NSF's investments are advancing knowledge to protect cyber-systems from malicious behavior, while preserving privacy and promoting usability," said Farnam Jahanian, head of NSF's Directorate for Computer and Information Science and Engineering (CISE).

"The cybersecurity research and education efforts we support enable our nation to continue as a world leader in innovating secure technologies and solutions. These new Frontier awards will enable novel approaches

to cybersecurity, with potential benefits to all sectors of our economy."

Expanding the Frontiers of cybersecurity

The first of the Frontier awards helps establish the Center for Encrypted Functionalities (CEF). The goal of the center is to use new encryption methods to make a computer program—and not just its output—invisible to an outside observer, while preserving its functionality—a process known as program obfuscation. Such a technology enhances cybersecurity by hiding vulnerabilities from potential adversaries, thereby preventing tampering and deterring reverse engineering; and by allowing one to hide cryptographic keys within software, thereby strengthening encryption and information transfer.

"Humanity has been encrypting messages using mathematics for hundreds of years. But the question of encrypting a functionality seemed out of reach," said Amit Sahai, a professor of computer science at the University of California, Los Angeles (UCLA), and the lead principal investigator of the project. "In human terms, this question is like asking whether it is possible for someone to keep a secret, if an adversary can see how every neuron in her brain behaves."

Last year, some members of Sahai's team discovered the first mathematically sound approach to encrypting functionalities. This breakthrough could reshape the way we think about security and computation.

"Our center's mission is to explore every aspect of the new world that is opened up by encrypted functionalities," Sahai said.

The project is a collaboration among researchers at UCLA, Stanford University, Columbia University, The University of Texas at Austin and Johns Hopkins University.

The second Frontier grant was awarded to the Modular Approach to Cloud Security (MACS) project, which aims to build information systems for the cloud with meaningful multi-layered security.

In the project, researchers will design and test a modular approach to cybersecurity. The project will build the cybersecurity system from smaller, separate functional components, each asserting its own security individually. As a result, the security of the system as a whole will be derived from the security of its components.

"Our goal is to build a cloud with clear and transparent security properties," said Ran Canetti, a professor of computer science at Boston University and lead researcher on the project. "Furthermore, we intend to make it modular, thus enabling the construction of cloud services from basic components in a security-preserving way. If successful, this project will transform the way we currently build and argue about secure systems."

The team—made up of researchers from Boston University, Massachusetts Institute of Technology, the University of Connecticut and Northeastern University—comprises experts in different aspects of information security and cryptography.

A key component of the MACS project is its integration into the Massachusetts Open Cloud, which provides the research team with a testbed for deploying and testing the mechanisms they develop at reasonable scale. The project continues NSF's commitment to support the transition of great ideas from research to practice.

Members of the MACS team will interpret early research results and code them into a privacy-preserving solution to allow users of the Massachusetts Open Cloud to share systems data, a novel idea that has no precedent. Allowing multiple users access to such information will

provide more choices for researchers conducting experiments on cloud computing and allow them to build high-performance systems at a fraction of the current cost.

Cybersecurity education and training

In addition to investments in cybersecurity research, the SaTC program has continued to expand opportunities and resources in cybersecurity education through its Cybersecurity Education Perspective. The goal of this perspective is to use fundamental cybersecurity research, together with research on learning, to expand educational opportunities and resources and nurture the next generation of cybersecurity professionals.

The SaTC education portfolio includes projects such as:

INSuRE, a self-organizing, cooperative, multi-disciplinary and multi-institutional student research network mentored by, and working on problems proposed by, technical directors from federal agencies;

Two informal learning projects that design and evaluate an environment that mimics the training that athletes undergo in preparation for major sporting competitions, including Cyber-gyms, coaches, mentors and Cyber Sports Federation, as well as state-wide, governor-sponsored Cyber Cups; and

A research study on the overall impact of the 70 existing cyber competitions and on the psychological characteristics of people who are qualified and willing to pursue careers in cybersecurity.

This year's two Frontier awards include strong education components as well. The Center for Encrypted Functionalities is developing free Massive Open Online Courses (MOOCs), to teach large numbers of learners the fundamental principles of encryption.

The MACS project plans to offer programs that familiarize technology professionals with cybersecurity and its central role in our society and economy.

Both projects will support new programs that will introduce K-12 students to cybersecurity and to computer science more broadly. The K-12 program will target students from both under-represented minorities and students with exceptional academic potential.

"Education investments in SaTC contribute to our mission to support the preparation of a diverse, globally component workforce," said Joan Ferrini-Mundy, assistant director for NSF's Directorate for Education and Human Resources.

"Cybersecurity professionals need to be critical-thinkers with strong STEM (science, technology, engineering and mathematics) foundations to respond to tomorrow's challenges. These Frontier awards, together with our investments through the Cybersecurity Education Perspective, emphasize connections between cybersecurity and STEM education and the important role of mathematics and computational thinking."

The 2014 SaTC awards continue NSF's long tradition of supporting foundational research and preparing the future workforce in cybersecurity. The awards are intended not only to combat today's threats, but to fundamentally "change the game" to enable long-term security and privacy.

Since 2008, NSF has invested more than $300 million in the fundamental theory, novel tools and technologies, and new education and workforce development approaches needed to secure our nation's cyberspace.

Provided by National Science Foundation