UC SANTA BARBARA
THE Current

March 9, 2016
Sonia Fernandez

The Key to Cybersecurity

Every time you send an email, make an Internet purchase or submit a digital form with personal information, encryption algorithms kick in, encoding your information so that it's readable only to the recipient. In this way, Internet users can have a reasonable expectation of privacy and protection.

However, according to UC Santa Barbara cryptographer Stefano Tessaro, for all the security conventional encryption promises, there is often little theoretical proof that the industry standard is sufficiently safe.

"Most of the designs we find are very heuristically validated," said Tessaro, an assistant professor in the Department of Computer Science, who specializes in encryption algorithms. Once someone designs an algorithm, he said, if attempts at breaking it are unsuccessful, it is often deemed safe.

Factor in the widespread utilization of the same standard algorithm embedded in websites and computers and the potential for catastrophic security breaches grows: One successful hack can unlock a vast amount of encrypted data, from email communications to bank accounts and other private information. And hackers are only getting more sophisticated.

For his work to establish a new layer of certainty to encryption, Tessaro has received a National Science Foundation (NSF) CAREER Award.

"I'm very happy about it, of course," Tessaro said of the recognition. "It's a validation of your research area."

Using principles from theoretical computer science, applied mathematics and information theory, Tessaro and his team aim to develop a foundation from which demonstrably more secure encryption algorithms may emerge. Their focus will be on symmetric algorithms, a commonly used type of encryption that relies on both parties having a key to encode and decode communications between them.

“From the theory side, we would like to provide validation, and provide proofs that these methods are really sound,” he said.

However, he added, it’s not enough just to develop an encryption algorithm that’s theoretically sound.

“The big part of this challenge is that often we know how to build, theoretically, these secure algorithms, but often, these are not fast enough,” said Tessaro, pointing out that encryption algorithms have to run many times per second to secure even the simplest of communications. In an online world where speed and performance are essential, an effective — albeit unwieldy — algorithm is likely to be passed over for one that is less secure but allows for faster communications.

“The theoretical problems that arise are actually more difficult than the traditional problems we encounter in theoretical cryptography, where usually we have an additional degree of freedom, and if we can’t solve problems we can make things slower,” he said. This project, said Tessaro, aims to solve the problem of security while taking into account the existing constraints of the requirements of speed.

The NSF’s Faculty Early Career Development (CAREER) program offers the organization’s most prestigious awards in support of junior faculty who exemplify the role of teacher-scholars through outstanding research, excellent education and the integration of education and research within the context of the mission of their organizations. Such activities are intended to build a firm foundation for a lifetime of leadership in integrating education and research.

About UC Santa Barbara

The University of California, Santa Barbara is a leading research institution that also provides a comprehensive liberal arts learning experience. Our academic community of faculty, students, and staff is characterized by a culture of interdisciplinary collaboration that is responsive to the needs of our multicultural and global society.

All of this takes place within a living and learning environment like no other, as we draw inspiration from the beauty and resources of our extraordinary location at the edge of the Pacific Ocean.