UC SANTA BARBARA

THE Current

August 4, 2014
Sonia Fernandez

The Best of Both Worlds

In the era of Internet and social media, where much of our communication happens online, it's easy to take our privacy for granted and to trust that the messages we send and transactions we perform are kept unreadable to prying eyes.

But according to UC Santa Barbara cryptologist Stefano Tessaro, even the most widely used standardized cryptographic algorithm, the Advanced Encryption Standard (AES), could be only a break-in away from being catastrophically compromised.

"Security is not proven," he said. "Researchers have tried to break AES with known attacks and failed so far, and thus assume that no attack will be found.

In addition, standardization is a double-edged sword. An algorithm that gets recognized by an authority like the National Institute of Standards and Technology (NIST) will be put into wide use, even embedded into chips that are built into computers.

"It's great for efficiency and reliability," he said, "but if there's a successful attack, the vast majority of the world's electronic communications will suddenly be vulnerable to decryption and hacking," Tessaro explained.

There are, in principle, cryptographic algorithms that can be proved to be secure, said Tessaro, and their security can be demonstrated mathematically. However, the cost of security is speed, and the most protective algorithm is usually not the fastest. Since the algorithms have to run a multitude of times per second to encrypt

even the smallest bit of electronic communication, the focus has been on those that are designed with speed in mind.

Funded by a $500,000 grant from the National Science Foundation's Secure and Trustworthy Cyberspace program, Tessaro and his team hope to stay ahead of the curve by studying what it would take to close the gap between the algorithms researchers know to be secure and the level of service (i.e. speed) Internet users have come to expect.

"The work involves laying down a solid theoretical framework for the development of basic encryption algorithms that are both efficient and provably secure," said Tessaro. The researchers will examine some of the most fundamental issues of cryptography, such as privacy and integrity of information. They will also study block ciphers, widely used algorithms for encrypting large amounts of information.

"These are very simple encryption algorithms," Tessaro said. "They are fast but are not as strong as the fully secure encryption algorithms we would want them to be." The project involves determining ways to build stronger block ciphers, based on guidelines to be developed by Tessaro and his group.

Though mostly theoretical, the outcome should have very real impacts on the world of electronic communications. The results of the study would be disseminated to the institutions, communities and other entities involved in electronic cryptography in the hopes that the next wave of standardizations will take the new framework into account. NIST is expected to hold competitions to replace encryption standards in the foreseeable future, according to Tessaro. While the project is concerned mainly with developing the new, more secure encryption framework from which multiple cryptographic algorithms may be developed, one potential outcome is also that the group might develop its own algorithm as a candidate for standardization.

"The main point related to the grant is simply that there is a gap between cryptography satisfying the real world efficiency requirements — without provable security — and the algorithms that academics develop — with provable security — which are considered unpractical by system designers," he said.

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.