UC SANTA BARBARA
THE Current

August 21, 2014
Sonia Fernandez

The People Behind the Code

Martijn Stam was only about 10 years old when he discovered cryptology.

“I borrowed a book from the library about how to become a spy,” recalled Stam, who is now a researcher at the University of Bristol. The book contained simple ways of creating secret codes, such as a rudimentary substitution method in which each letter of the alphabet represents another letter at a fixed place before or after it. Not long after reading that book, he was devising all sorts of encryption keys.

Other people, like Bogdan Warinschi, also from Bristol, were intrigued by questions and problems around encryption, such as how to verify the security of an encryption system. Yet others, like UC Santa Barbara computer scientists Stefano Tessaro and Rachel Lin, dwell in the fascinating intersection of computer science and arithmetics, where the end goal is to derive encryption keys that are mathematically proven impenetrable, but are not too unwieldy for modern computers.

Whatever brought them to cryptology, Stam, Warinschi, Tessaro and Lin joined about 400 or so likeminded researchers from all over the world who came to UCSB for the weeklong CRYPTO 2014 conference, one of three flagship conferences held around the world by the International Association for Cryptological Research (IACR). The conference, the 34th to be held at UCSB, began on Sunday, Aug. 17, and concluded on Thursday, Aug. 21.

For five days, attendees were immersed in talks and presentations on campus, both formal and informal, on a dizzying array of topics related to cryptology: random

number generation, cipher models, security and attacks, password protection, new technologies and trends in the digital world, just to name a few.

Though the conference spanned a variety of topics, according to Tessaro, who was on the conference's program committee, two broad issues were the mainstays of the event. One was the fundamental problem of program obfuscation, or the encryption of a computer program in such a way that people could use it without reverse engineering it or otherwise finding out how it worked.

"There was an interesting result at this conference, in my opinion, one of the coolest results in terms of the talks," Tessaro said of a demonstration that showed how the use of a highly sensitive microphone near a laptop could yield information about the computations being made inside via the noise signature.

Lin, meanwhile, presented her results in the area of secure computation protocols, research that contributes to one of the long-term goals of cryptology: tools that can allow users to manipulate encrypted data with a versatility comparable to unencrypted data, while still keeping the information private.

"One example is hospitals," said Lin. "They might want to do some computation together, but their data is not supposed to be revealed by either end." Banks could also benefit from some collaborative computation, she added, but they might not want to reveal sensitive financial information.

The other overarching topic was how the gap between theory and practice could be bridged in wider applications. From theoretical algorithms that are deemed too inefficient because of the time and power needed to encrypt and decrypt each keystroke of electronic communication, to the vagaries of theory and practice in research that were discussed in UC San Diego cryptographer Mihir Bellare's Distinguished Lecture, researchers were interested in turning the purely intellectual into the concrete.

Though it can be traced back as far as the ancient Greeks and Romans who used early cipher devices to send secret codes across the battlefield, cryptology didn't become an extensive established academic research topic until the mid 1970's. With the rise of computers and the availability of increasingly more complex ciphers, the field grew.

UCSB capitalized on the emerging field, with a push by computer scientist Richard Kemmerer and electrical and computer engineer Allen Gersho, along with Steve Weinstein from American Express. In 1981 the first CRYPTO conference took place at UCSB. A couple of years later, cryptographer David Chaum, who came to UCSB in 1982, almost singlehandedly started the IACR, which took over the sponsorship of CRYPTO. IACR went on to sponsor what became its two other flagship conferences, EuroCRYPT and AsiaCRYPT.

“Part of the attraction of the CRYPTO conference is that most of the participants stay in the dorms and, as a result, people are always around. Significant discussions take place in the dorm lounges or while walking around campus,” said Kemmerer. The initial conference had about 100 attendees, he said. At the height of the attention around computer security at the turn of the century, attendance peaked at 500, and has since settled to 300 to 400.

“People come here to learn about the most recent state of the art and the research,” said Sasha Boldyreva of IACR, and lead organizer of this year’s conference. “It’s a rapidly developing field.” Because research in the world of computer science happens so fast, conferences like CRYPTO also provide venues for researchers to present their work and hear from colleagues about their research before it is published in journals. This can also be extremely valuable, given the relatively slow place of academic journal publication. Many of this year’s attendees, she said, were students exploring the field. Others are also colleagues who use the conference to network.

As technology develops, the reach of cryptology expands. Particularly in the realm of computers and the online world, virtually any digital communication is prone to hacking, whether it comes from a user, or any node in a network. This leads to rising consideration for effective encryption in areas as diverse as business (think Bitcoin); health, in which there is a push for electronic medical records; and even more futuristic developments, such as self-driving cars and smart homes.

But it wasn’t all seriousness for the CRYPTO attendees. Among the mathematics- and theory-laden sessions led by some of the brightest cryptographers in the world, participants found time to catch up with one another and talk shop. An evening Rump Session — a freewheeling, rapid-fire series of presentations — gave participants just a few minutes to communicate on virtually anything cryptological: educational tools such as ciphers and videogames; insights on a specific problem;

updates from representatives of the National Institute of Standards and Technology; and even jokes and songs. Another conference activity brought attendees to the beach. Meeting the people behind the research, IACR President Christian Cachin said, is the primary reason most participants come to the conference.

“In the end, every scientific contribution is authored by people,” said Cachin, “and this is why we are socializing here.”

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.