Association for Computing Machinery

Advancing Computing as a Science & Profession

Contact: Jim Ormond
212-626-0505
ormond@hq.acm.org

CRYPTOGRAPHY PIONEERS RECEIVE ACM A.M. TURING AWARD

Diffie and Hellman's Invention of Public-Key Cryptography and Digital Signatures Revolutionized Computer Security and Made Internet Commerce Possible

NEW YORK, March 1, 2016 – ACM, the Association for Computing Machinery, (www.acm.org) today named Whitfield Diffie, former Chief Security Officer of Sun Microsystems and Martin E. Hellman, Professor Emeritus of Electrical Engineering at Stanford University, recipients of the 2015 ACM A.M. Turing Award for critical contributions to modern cryptography. The ability for two parties to use encryption to communicate privately over an otherwise insecure channel is fundamental for billions of people around the world. On a daily basis, individuals establish secure online connections with banks, e-commerce sites, email servers and the cloud. Diffie and Hellman's groundbreaking 1976 paper, "New Directions in Cryptography," introduced the ideas of public-key cryptography and digital signatures, which are the foundation for most regularly-used security protocols on the Internet today. The Diffie-Hellman Protocol protects daily Internet communications and trillions of dollars in financial transactions.

The ACM Turing Award, often referred to as the "Nobel Prize of Computing," carries a $1 million prize with financial support provided by Google, Inc. It is named for Alan M. Turing, the British mathematician who articulated the mathematical foundation and limits of computing and who was a key contributor to the Allied cryptoanalysis of the German Enigma cipher during World War II.

"Today, the subject of encryption dominates the media, is viewed as a matter of national security, impacts government-private sector relations, and attracts billions of dollars in research and development," said ACM President Alexander L. Wolf. "In 1976, Diffie and Hellman imagined a future where people would regularly communicate through electronic networks and be vulnerable to having their communications stolen or altered. Now, after nearly 40 years, we see that their forecasts were remarkably prescient."

"Public-key cryptography is fundamental for our industry," said Andrei Broder, Google Distinguished Scientist. "The ability to protect private data rests on protocols for confirming an owner's identity and for ensuring the integrity and confidentiality of communications. These widely used protocols were made possible through the ideas and methods pioneered by Diffie and Hellman."

Cryptography is a practice that facilitates communication between two parties so that the communication will be kept private and authenticated from a third party trying to read or alter what is being communicated. From ancient times, cryptography has been achieved through encryption, the conversion of readable information into gibberish that only a select few can decipher. In its earliest incarnations, encryption might have involved substituting one letter for another or rearranging the order of letters in the message. The development of radio in 1903, followed a decade later by World War I, gave cryptography a central role it never had before. At the same time, the development of electricity and machining allowed the development of machines that could encrypt far more securely than any human could. The post-World War I period saw the development of a number of enciphering machines that matured over the next 20 years and became the backbone of World War II cryptography. After the war, the development of computer technology led to faster and more secure cryptography by purely electronic machines.

In encryption, a “key” is a piece of information used to transform readable plain text into garbled incomprehensible cipher text. Encryption is much like keying a lock to accept a particular key and decryption is like using the key to open the lock. In the past, when two parties were seeking to establish secure communications, they needed to have identical keys. Supplying these keys—key management—was a major limitation of the flexibility of encrypted communications.

Two significant shortcomings of symmetric cryptosystems are the need for a secure means of key transfer and, because both parties have the same key, one could forge a message to oneself, claiming it came from the other. In addition, overuse of a particular key may provide an opponent with sufficient ciphertext to break the cryptosystem (i.e., discover the key). To limit the number of parties sharing the same key, separate keys are often distributed to each pair of communicating parties, posing additional key management challenges.

In “New Directions in Cryptography,” Diffie and Hellman presented an algorithm that showed that asymmetric or public-key cryptography was possible. In Diffie and Hellman's invention, a public key, which is not secret and can be freely distributed, is used for encryption, while a private key, that need never leave the receiving device, is used for decryption. This asymmetric cryptosystem is designed in such a way that the calculation of the private key from the public key is not feasible computationally, even though one uniquely determines the other.

Reversing the process provides a digital signature. The transmitter of a message uses a private key to sign the message, while the receiver uses the transmitter’s public key to authenticate it. Such digital signatures are more secure than written signatures because changing even one word of the message invalidates the signature. In contrast, a person’s written signature looks the same on a $10 check and a $1,000,000 check.

Any user of the World Wide Web is likely to be familiar with the use of public-key cryptography to establish secure connections. A typical secure URL begins with “https,” where the “s” means that the Secure Transport Layer protocol will be used to encrypt the communication. The secure connection is established using a combination of public-key cryptography to transport a key with symmetric cryptography that is used to encrypt subsequent communications.

In addition to laying the foundation for today’s online security industry and establishing cryptography as a leading discipline within computer science, Diffie and Hellman’s work made encryption technologies accessible to individuals and companies.

Background

Whitfield Diffie is a former Vice President and Chief Security Officer of Sun Microsystems, where he became a Sun Fellow. As Chief Security Officer, Diffie was the chief exponent of Sun’s security vision and responsible for developing Sun’s strategy to achieve that vision. Diffie is a graduate of the Massachusetts Institute of Technology (MIT).

Diffie received the 1996 ACM Paris Kanellakis Theory and Practice Award (with Leonard Adleman, Martin Hellman, Ralph Merkle, Ronald Rivest and Adi Shamir), and received the 2010 IEEE Richard W. Hamming Medal (with Martin Hellman and Ralph Merkle). He is a Marconi Fellow, a Fellow of the Computer History Museum, and received an honorary doctorate from the Swiss Federal Institute of Technology.

Diffie has authored more than 30 technical papers, and has testified several times to the U.S. Senate and House of Representatives on the public policy aspects of cryptography.

Martin E. Hellman is Professor Emeritus of Electrical Engineering at Stanford University, where he was Professor of Electrical Engineering for 25 years. A graduate of New York University, Hellman earned his Master's degree and his Ph.D. from Stanford.

Hellman received the 1996 ACM Paris Kanellakis Theory and Practice Award (with Leonard Adleman, Whitfield Diffie, Ralph Merkle, Ronald Rivest and Adi Shamir), as well as the 2010 IEEE Richard W. Hamming Medal (with Whitfield Diffie and Ralph Merkle). He is a Marconi Fellow, a Fellow of the Computer History Museum, and a member of the US National Academy of Engineering.

Hellman has authored more than 70 technical papers, 12 U.S. patents and a number of corresponding international patents.

ACM will present the 2015 A.M. Turing Award at its annual Awards Banquet on June 11 in San Francisco, Calif.

About the ACM A.M. Turing Award

The A.M. Turing Award **http://amturing.acm.org/** was named for Alan M. Turing, the British mathematician who articulated the mathematical foundation and limits of computing, and who was a key contributor to the Allied cryptanalysis of the German Enigma cipher and the German "Tunny" encoding machine in World War II. Since its inception in 1966, the Turing Award has honored the computer scientists and engineers who created the systems and underlying theoretical foundations that have propelled the information technology industry.

About ACM

ACM, the Association for Computing Machinery **www.acm.org,** is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

# # #