ACM and Infosys Foundation honor pioneer in cryptography

Stanford's Dan Boneh Honored for Innovations in the Field of Cryptography
that Improve Computer Security and Privacy

NEW YORK and BANGALORE, INDIA, March 31, 2015 – ACM, the Association for Computing Machinery, (www.acm.org) and the Infosys Foundation announced today that Dan Boneh is the recipient of the 2014 ACM-Infosys Foundation Award in the Computing Sciences for his contributions to the ground-breaking development of pairing-based cryptography and its application in identity-based encryption. His work helped establish the field of pairing-based cryptography, a dominant area in cryptography for the last decade, by demonstrating the use of pairing functions to solve wide variety of problems in cryptography. Boneh, with Matt Franklin, showed how pairings could be used to develop a fully functional identity-based encryption scheme (IBE). This ushered in a new area of cryptography research to which Boneh's contributions have been central. Pairing-based cryptography makes security mechanisms easier to use and deploy, and improves computer security to keep data, devices and critical systems safe, private and accessible.

The ACM-Infosys Foundation Award recognizes the finest recent innovations by young scientists and system developers in the computing field. An endowment from the Infosys Foundation provides financial support for the $175,000 annual award. ACM will present the ACM-Infosys Foundation Award at its annual awards banquet on June 20 in San Francisco.

ACM President Alexander L. Wolf said, "Boneh's work on pairing functions and their application to identity-based encryption has revolutionized cryptography. He has added greatly to our understanding of important problems underlying modern cryptography systems. Boneh has produced new directions and given the field a fresh start."

Dr. Vishal Sikka, CEO and Managing Director, Infosys, said, "Boneh has helped forge connections between academic and commercial cryptography, helping improve commercial products while increasing the relevance of academic research. His innovations made foundational contributions to both theoretical cryptography and cybersecurity."

Boneh pioneered the use of new computational problems based on pairings to solve a broad range of problems in cryptography. This approach, called pairing-based cryptography, relies on complex problems arising from algebraic geometry (bilinear maps based on elliptic curves). Pairing-based cryptography has had tremendous academic and commercial impact.

Boneh demonstrated how pairings could be used to solve long-standing open problems in cryptography. Pairing-based cryptography, now a mainstream tool in cryptography, has generated a large volume of research activity showing entirely new capabilities as well as solutions that are superior in functionality to ones already in use.

Identity-based encryption is a type of public-key encryption in which any arbitrary string (such as a user's email address) can be used as a public key, enabling data to be protected without the need for long, randomly generated keys or certificates. Today, there are numerous standards for IBE based on Boneh's work, including IEEE P1363.3 and several IETF RFCs.

In addition to pairing-based cryptography, Boneh developed cryptosystems with novel properties, mechanisms for enhancing Web security and security for mobile devices. He developed new privacy tools, contributed to the study of cryptographic watermarking and runs a popular MOOC on cryptography.

Background
Dan Boneh is professor of Computer Science and Electrical Engineering at Stanford University, and leads the applied cryptography group there. He has written extensively on cryptography and computer security, publishing more than 150 refereed conference and peer-reviewed journal papers. Boneh served as an editor of *ACM Transactions on Internet Technology* (TOIT), *Journal of the ACM* (JACM), and *Journal of Cryptology*. He has served as program chair or general chair for several academic conferences and as member of more than 30 conference program committees.

Boneh, who holds nine patents, cofounded Voltage Security Inc. to commercialize IBE. Voltage Security's IBE-based SecureMail product, now owned by HP, is licensed to more than a thousand corporations worldwide, with 50 million users sending over one billion encrypted emails.

Boneh is an Alfred P. Sloan Fellow and a Packard Fellow. He received the Gödel Prize and the RSA Conference Award for Mathematics. Boneh earned a B.A. degree in Computer Science from The Technion – Israel Institute of Technology, and M.A. and Ph.D. degrees in Computer Science from Princeton University.

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.

About The Infosys Foundation
Established in 1996, the Infosys Foundation is the philanthropic arm of Infosys and has the sole objective of fulfilling the social responsibility of the company by creating opportunities and working toward a more equitable society. The Infosys Foundation has made effective strides in the areas of healthcare, education, social rehabilitation, and the arts. The company contributes up to one percent of its profit to the foundation each year.

About Infosys
Infosys is a global leader in consulting, technology and outsourcing and next-generation services. We enable clients, in more than 50 countries, to stay a step ahead of emerging business trends and outperform the competition. We help them transform and thrive in a changing world by co-creating breakthrough solutions that combine strategic insights and execution excellence.

Visit www.infosys.com to see how Infosys (NYSE: INFY), with $8.25billion in annual revenues and 165,000+ employees, is helping enterprises renew themselves while also creating new avenues to generate value.

For further information please contact:

Bruce Shriver ACM 212-626-0521 shriver@hq.acm.org	Marie Gentile Widmeyer 646-213-7249 marie.gentile@finnpartners.com
Sarah Gideon Infosys, Ltd. +91 80 4156 3373 Sarah_Gideon@Infosys.com	John Gallagher Brunswick Group 415-316-8060 jgallagher@brunswickgroup.com