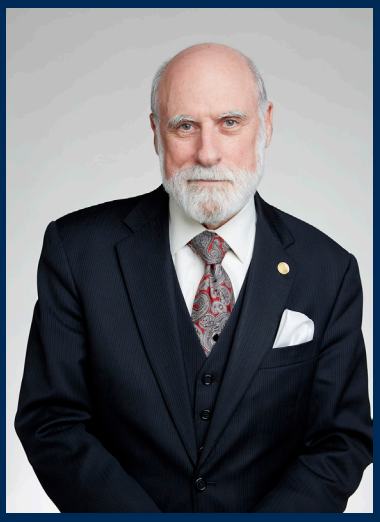
UCI Department of Computer Science

DISTINGUISHED LECTURE SERIES



VINT CERF

Vice President and Chief Internet Evangelist,
Google

"Ethical and Engineering Challenges in the Internet of Things"

Friday - April 28, 2017 - 11 a.m.

Donald Bren Hall, Room 6011

No cost to attend — Open to the public
Seating is on a first-come, first-served basis

BIO

At Google, Vint Cerf contributes to global policy development and continued spread of the Internet. Widely known as one of the "Fathers of the Internet," Cerf is the co-designer of the TCP/IP protocols and the architecture of the Internet. He has served in executive positions at the Internet Society, the Internet Corporation for Assigned Names and Numbers, the American Registry for Internet Numbers, MCI, the Corporation for National Research Initiatives and the Defense Advanced Research Projects Agency and on the faculty of Stanford University. Vint Cerf sits on US National Science Board and is a Visiting Scientist at the Jet Propulsion Laboratory. Cerf is a Foreign Member of the Royal Society and Swedish Academy of Engineering, Fellow of the IEEE, ACM, American Association for the Advancement of Science, American Academy of Arts and Sciences, British Computer Society, Worshipful Company of Information Technologists, Worshipful Company of Stationers and is a member of the National Academy of Engineering. Cerf is a recipient of numerous awards and commendations in connection with his work on the Internet, including the US Presidential Medal of Freedom, US National Medal of Technology, the Queen Elizabeth Prize for Engineering, the Prince of Asturias Award, the Japan Prize, the Charles Stark Draper award, the ACM Turing Award, the Legion d'Honneur and 29 honorary degrees.

ABSTRACT

We have a lot of work ahead of us to make the "Internet of Things" the beneficial wave that many expect. Access control to commands and data must be easy to configure and resistant to hijacking. The configuration of large numbers of devices should be easy, even for relatively naive consumers. Software in these devices will have errors and must be correctable. Devices must be able to reject updates from unauthorized sources. Designers need to think about scenarios in which many users have access to and control over devices - and may have differing degrees of access (think: parents, children, house guests. Administrative staff, engineering staff in the case of industrial applications of IOT.) Programmers, systems engineers, product designers among others must keep in mind a wide range of use scenarios and ask whether user safety and privacy have been preserved.

For further information, please contact
hbyrnes@ics.uci.edu or go to www.cs.uci.edu