The Royal Academy of Engineering

UCL

THE ROYAL ACADEMY OF ENGINEERING DISTINGUISHED VISITING FELLOWSHIP

Information Security and its Impact upon Society

By

Prof. Vijay K. Bhargava, FRSC, FIEEE

Department of Electrical and Computer Engineering

University of British Columbia, Canada

Date	11:00am ~ 12:00pm, Wednesday 20th May 2009
Venue	Barlow Room (807), Roberts Building, UCL, London WC1E 7JE
Maps	http://www.ucl.ac.uk/about-ucl/location/maps

ABSTRACT There is no point in having information unless it can be communicated from one point to another point (telecommunications) or from one time to another time (storage). In both cases, protecting information from unauthorized access, modification and disruption is critical. Cryptography is a key technology in protecting information. It was traditionally concerned with maintaining confidentiality. Recently, there has been a dramatic growth in the applications of cryptography in other areas such as commerce.

Modern cryptography can be divided into symmetric-key cryptography and public-key cryptography. In this talk, we outline some of the current symmetric-key and public-key cryptographic techniques used in achieving information security. These include the Advanced Encryption Standard (AES) which is the symmetric-key encryption standard adapted by the US government, and two well-known public-key cryptosystems, namely RSA (the initials of its inventors) and Elliptic Curve Cryptography (ECC).

We then outline the impact of information security upon society. In particular, we focus on the usage of information security in Internet filtering. The Internet filtering can take place in different levels: local, organizational or national. In all these levels, the objective of filtering is to prevent or limit access to information/content that is against national/cultural values or is considered harmful for the users whether they are children or adults. In this talk, we will give a rough idea about some of the current filtering techniques as well as some of the circumventing methods to bypass it.

BIOGRAPHY Vijay K. Bhargava is a Professor in the Department of Electrical and Computer Engineering at the University of British Columbia where he served as Department Head from 2003 to 2008. He served as the Founder and President of Binary Communications Inc. (1983-2000). He is a co-author (with D. Haccoun, R. Matyas and P. Nuspl) of Digital Communications by Satellite (New York: Wiley 1981), a co-editor (with S. Wicker) of Reed Solomon Codes and their Applications (IEEE Press 1994), a co-editor (with V. Poor, V. Tarokh and S. Yoon) of Communications, Information and Network Security (Kluwer: 2003) and a co-editor (with E. Hossain) of Cognitive Wireless Communications Networks (Springer: 2007). In January 2007, he

was appointed Editor-in-Chief of the IEEE Transactions on Wireless Communications and in January 2009 he was renewed for a further two year term.

A Fellow of the IEEE, the Engineering Institute of Canada (EIC), the Royal Society of Canada, and the Canadian Academy of Engineering, Vijay has been honoured many times by his colleagues and has received numerous awards. Vijay is very active in the IEEE and has served as the President of the Information Theory Society. He is a candidate for the office of Vice-President, Membership Affairs in the forthcoming election of the IEEE Communications Society.

CONTACT Dr. Yang Yang, Department of Electronic & Electrical Engineering, University College London (UCL), UK, Tel: 020 7679 3973, Email: y.yang@ee.ucl.ac.uk

REGISTRATION IS NOT REQUIRED, ALL ARE WELCOME !