COMPUTER SCIENCE
North Haugh, St Andrews, Fife, KY16 9SX Scotland
Tel: (01334) 463253 Fax: (01334) 463278
www.cs.st-andrews.ac.uk/

DISTINGUISHED LECTURE SERIES 2009/10

Cryptography: From Black Art to Popular Science

By

Professor Fred Piper
Professor Peter Wild

Royal Holloway University, London

18 & 19 November 2009

Lecture Theatre B, Purdie Building, North Haugh, St Andrews

Biography

Prof Fred Piper BSc PhD (London) CEng CMath FIEE ARCS DIC FIMA was appointed Professor of Mathematics at the University of London in 1975 and has worked in information security since 1979. In 1985, he formed a company, Codes & Ciphers Ltd, which offers consultancy advice in all aspects of information security. He has acted as a consultant to over 80 companies including a number of financial institutions and major industrial companies in the UK, Europe, Asia, Australia, South Africa and the USA. The consultancy work has been varied and has included algorithm design and analysis, work on EFTPOS and ATM networks, data systems, security audits, risk analysis and the formulation of security policies. He has lectured worldwide on information security, both academically and commercially, has published more than 100 papers and is joint author of Cipher Systems (1982), one of the first books to be published on the subject of protection of communications, Secure Speech Communications (1985), Digital Signatures - Security & Controls (1999) and Cryptography: A Very Short Introduction (2002).

Fred has been a member of a number of DTI advisory groups. He has also served on a number of Foresight Crime Prevention Panels and task forces concerned with fraud control, security and privacy. He is currently a member of the Scientific Council of the Smith Institute, the Board of Trustees for Bletchley Park and the Board of the Institute of Information Security professionals. He is also a member of (ISC) 2's European Advisory Board, the steering group of the DTI's Cyber Security KTN, ISSA's advisory panel and the BCS's Information Security Forum.

In 2002, he was awarded an IMA Gold Medal for "services to mathematics" and received an honorary CISSP for "leadership in Information Security". In 2003, Fred received an honorary CISM for "globally recognised leadership" and "contribution to the Information Security Profession".

Prof Peter Wild BSc (Adelaide) PhD (London) received his B.Sc. (Hons) degree in Pure Mathematics in 1976 from the University of Adelaide, and the Ph.D. degree in Mathematics in 1980 from the University of London. He has worked at the Ohio State University, Columbus, Ohio; the University of Adelaide; and with the CSIRO, Australia. In 1984 he joined Royal Holloway where he is currently employed as a Professor in Mathematics. His research interests are in combinatorics, design theory, cryptography and coding theory. He has acted as a data security consultant for a number of companies offering advice in algorithm analysis, key management and user identification protocols.

Program

Abstract

The last few decades have seen cryptography 'transform' from a black art, practised mainly by governments , the military and a few financial organisations, to a popular science that is widely taught as an academic subject and features in a number of popular novels and films. At the same time, cryptographic services have become much more widely used and are now a central feature of many e-commerce and other business applications.
In this talk we will look at how technological advances have influenced cryptography and how the concept of public key cryptography has dramatically increased the range of cryptographic services that are available.

Wednesday 18 November 2009

11.15 – 12.00	Coffee & Tea with Biscuits
Common area, Jack Cole Building	
12.00 – 13.00	**Lecture 1:** Understanding cryptography and why we need it
Lecture Theatre B, Purdie Building, North Haugh	In this talk we give a high level introduction to the basic concepts and discuss how and why cryptography has become so important to our everyday lives. We discuss some of the social and political implications of its use. NOTE: this will be a non-technical talk accessible to anyone who is interested.
15.00 – 16.00	**Lecture 2:** Algorithms, services and key management
Lecture Theatre B, Purdie Building, North Haugh	In his talk we will discuss cryptographic services and investigate how different services have differing implications for the design of the algorithm being used. No matter which service is being provided, there is always a need for secure key management. We will introduce some of the fundamental issues and discuss some solutions.
16.15 – 16.45	Coffee & Tea with cakes
Common area, Jack Cole Building	

Thursday 19 November 2009

10.00 – 11.00	**Lecture 3:**Two Sides of Security
Lecture Theatre B, Purdie Building, North Haugh	In this talk we give an example of key management which provides security in an insecure environment (wireless sensor networks) and an example of poor implementation of a protocol (SSH) that leads to an insecurity that allows plaintext recovery. Wireless sensors are small, battery-powered devices with the ability to take measurements of quantities such as temperature or pressure, and to engage in wireless communication. When a collection of sensors is deployed the sensors can communicate with each other and thus form an ad hoc network, known as a *wireless sensor network* (WSN), in order to facilitate the transmission and manipulation of data by the sensors. When they are deployed in a hostile environment the communications may be required to be secured. We describe a key management scheme for such a network. *Secure Shell or SSH* is a network protocol that allows data to be exchanged using a secure channel between two networked devices. We discuss a variety of plaintext-recovering attacks against SSH. We explain why a combination of flaws in the basic design of SSH leads some implementations to be open to our attacks, and how the attacks can be prevented in practice.
11.15 – 11.45	Coffee & Tea with Biscuits
Common area, Jack Cole Building	