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

Semester 1

2011/12

The Dependability of Complex Socio-technical Infrastructure
&
Smart Grids and Smart Meters: Game Changer, or Serious Danger?

by

Prof Ross Anderson

Monday 5 December 2011

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

Biography

Ross Anderson is Professor of Security Engineering at Cambridge University. He was one of the founders of a vigorously-growing new academic discipline, the economics of information security. Ross was also a seminal contributor to the idea of peer-to-peer systems and an inventor of the AES finalist encryption algorithm "Serpent". He has well-known publications on many other technical security topics including hardware tamper-resistance, emission security, copyright marking, and the robustness of APIs. He is a Fellow of the Royal Society, the Royal Academy of Engineering, the IET and the IMA. He also wrote the standard textbook "Security Engineering - a Guide to Building Dependable Distributed Systems".

Programme: Monday 5 December 2011

13.30-14.00	Coffee & Tea with Biscuits
Purdie Building Common Room	Break
14.00 – 15.30	**Lecture 1:** The Dependability of Complex Socio-technical Infrastructure
Purdie Building (Lecture Theatre **B**)	**Abstract:** We have all become dependent on large complex systems such as Facebook, the bank payment system and even the Internet itself. Keeping these systems dependable in the face of accidents, errors and malice is one of the most important, and interesting, challenges facing engineers today. It brings not only technical problems of the highest order, but also some intricate economics; how do we persuade firms to invest in spare capacity that will mostly help their competitors offer better service? I'll discuss such problems in two contexts: frauds against payment networks, and the resilience of the Internet. The talk will draw on a recent major study we did for ENISA of the resilience of the Internet interconnect.
15.30 – 16.00	Coffee & Tea with Biscuits
Purdie Building Common Room	Break
16.00– 17.30	**Lecture 2:** Smart Grids and Smart Meters: Game Changer, or Serious Danger?
Purdie Building (Lecture Theatre **B**)	**Abstract:** The European Union has started a €100bn project to replace all our electricity meters with smart meters. Officials hope that making energy use more salient to householders will lead to energy savings; that time-of-day pricing will shave peak demand; and that in a smart grid, demand response will help accommodate fluctuating energy sources such as solar and wind. This project could create plenty of work for security engineers! As smart meters can be commended remotely, they may be open to attacks ranging from scalable fraud to wholesale service denial. Moving distribution assets such as substations online creates further hazards. The architectures in some Member States are complex, heavily centralised or both, leading to protocol design and project management issues. Some smart meters accept many commands, raising the possibility of API attacks. Updating device software to patch vulnerabilities is hard. Energy companies want fine-grained consumption data but this may contravene European privacy law. And there are many incentive problems: smart meters will be operated by energy companies, who don't really want us to save energy. I suggest that part of the solution might be to develop an open platform that will enable users to connect up their meters, appliances and suppliers, and control them via a web interface.