Invited Talk
Security, functionality and scale?

Ross Anderson

University of Cambridge Computer Laboratory
JJ Thomson Avenue
Cambridge CB3 0FD, UK
ross.anderson@cl.cam.ac.uk

Abstract. Since 2002 the UK has been attempting to build a system of federated databases containing all the nation's medical records. This project has encountered numerous problems and some feel that it is becoming the world's largest ever software disaster. One aspect of the problem is security. This means different things to different stakeholders: the government and its contractors boast about their ability to keep out 'hackers', while medics and patients' groups worry that making records available to large numbers of authorised insiders will lead to abuses that will fatally undermine privacy. A security policy that I developed for the BMA and that I discussed at DBSEC in 2002 was not used; instead the developers went for a combination of role-based access control plus a 'legitimate relationship'. This has been found insufficient and 'sealed envelopes' are planned as well. Medical databases are the first application involving very sensitive personal data being kept in large-scale systems which their operators hope will develop rich functionality over time. This combination of a stringent security requirement, complex functionality and great scale poses the most serious problems yet known to the security architect. I will discuss the options and ask whether it is in fact the case that you can have any two of these attributes - security, functionality and scale - but not all three.