PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A

Phil. Trans. R. Soc. A (2009) **367**, 2717–2727
doi:10.1098/rsta.2009.0027

Review

Information security: where computer science, economics and psychology meet

By Ross Anderson[1,*] and Tyler Moore[2]

[1]*Computer Laboratory, University of Cambridge, 15 JJ Thomson Avenue, Cambridge CB3 0FD, UK*
[2]*Center for Research on Computation and Society, Harvard University, 33 Oxford Street, Cambridge, MA 02138, USA*

Until ca. 2000, information security was seen as a technological discipline, based on computer science but with mathematics helping in the design of ciphers and protocols. That perspective started to change as researchers and practitioners realized the importance of economics. As distributed systems are increasingly composed of machines that belong to principals with divergent interests, incentives are becoming as important to dependability as technical design. A thriving new field of information security economics provides valuable insights not just into 'security' topics such as privacy, bugs, spam and phishing, but into more general areas of system dependability and policy. This research programme has recently started to interact with psychology. One thread is in response to phishing, the most rapidly growing form of online crime, in which fraudsters trick people into giving their credentials to bogus websites; a second is through the increasing importance of security usability; and a third comes through the psychology-and-economics tradition. The promise of this multidisciplinary research programme is a novel framework for analysing information security problems—one that is both principled and effective.

Keywords: information security; economics; incentives; psychology

1. Introduction

As the Internet has grown, system engineers have realized that security failure is caused at least as often by bad incentives as by bad design. Indeed, the former often explain the latter. Systems are particularly prone to failure when the person operating them does not suffer the full costs of failure. Things also break when system users have conflicting interests, or even just no real reason to cooperate. Thus, while security engineers used to worry about malicious outsiders, the greatest concern now is selfish insiders. As a result, the tools of game theory and microeconomic theory are becoming just as important to the security engineer as the mathematics of cryptography.

* Author for correspondence (ross.anderson@cl.cam.ac.uk).

One contribution of 16 to a Theme Issue 'Crossing boundaries: computational science, e-Science and global e-Infrastructure II. Selected papers from the UK e-Science All Hands Meeting 2008'.

