

Banking Security: Attacks and Defences

Steven Murdoch

University of Cambridge, Cambridge, UK
Steven.Murdoch@cl.cam.ac.uk

Abstract. Designers of banking security systems are faced with a difficult challenge of developing technology within a tightly constrained budget, yet which must be capable of defeating attacks by determined, well-equipped criminals. This talk will summarise banking security technologies for protecting Chip and PIN/EMV card payments, online shopping, and online banking. The effectiveness of the security measures will be discussed, along with vulnerabilities discovered in them both by academics and by criminals. These vulnerabilities include cryptographic flaws, failures of tamper resistance, and poor implementation decisions, and have led not only to significant financial losses, but in some cases unfair allocation of liability. Proposed improvements will also be described, not only to the technical failures but also to the legal and regulatory regimes which are the underlying reason for some of these problems not being properly addressed.