Cryptology: Where Is the New Frontier?

Ross Anderson

University of Cambridge, UK
`Ross.Anderson@cl.cam.ac.uk`

Abstract. Twenty years ago, the crypto community was relatively homogeneous, with the people who went to Crypto and Eurocrypt spanning everything from theory to applications. Now it's much more diverse, with several underlying bodies of theory (from complexity to protocol analysis) and a great variety of applications. Where should a young researcher focus?

Doing good cryptographic engineering to support complex socio-technical systems is hard, and I will discuss three examples. First, payment protocols such as EMV (which is just being adopted in India) and the more recent work in mobile wallets, have a major problem in managing complexity. Second, infrastructure protection such as DNSSEC and BGPSEC is a good thing but often runs up against a lack of deployment incentives. Finally, the UEFI proposal for authenticated boot revives many of the questions of trust that were previously discussed during the crypto wars, during the debate over “Trusted Computing”, and in the context of SSL CAs. The lesson is that the security and cryptology research communities in India should engage with the policy and economic implications of our field. Although India's situation may be different from America's or Europe's, many of the same issues of trust, control, innovation and privacy will surely come round again and again. What's more, good research tends to come from real problems; researchers who engage with the real world can spot these more quickly.