# Foreword from the Programme Chairs

# STAST 2012

Over about 30 years the security community has made significant strides in the design and analysis of cryptographic algorithms and protocols. We have, for example, remarkably subtle models for defining notions of security, for example in the form of “Universal Composability”, and very powerful tools for the automated analysis of protocols. And yet, systems continue to be routinely broken! If we step back and try to understand this situation we realize that most system breaches do not involve cryptanalysis or manipulations of design flaws in protocols, but typically involve, for example, social engineering attacks. Social engineering attacks are an iconic example of what we think of as a socio-technical exploitation of a system. The centrality of the human has always been understood by the information security community but with our roots strongest in computer science and mathematics we have lacked the necessary tools with which to explore the human dimension.

Recently, the security community has started to actively promote and seek out research that explores socio-technical aspects of security. Over the last five years there has been an increasing emphasis on interdisciplinary research with a focus on the social. However there still remains relatively few venues in which to publish and present such work. STAST is a response to the need for venues. The first STAST workshop was highly successful in bringing together researchers in this rather nascent domain, and we hope that STAST’12 will be even more successful in disseminating ideas and fostering communication and collaboration in this small but growing community. We are particularly pleased that this year the workshop is in conjunction with CSF, the premiere conference on the foundations of computer security.

This volume comprises the proceedings of the second workshop on Socio-Technical Aspects of Security and Trust (STAST). The diversity of the topics covered in this proceedings reflect the vibrancy of the socio-technical research community within information security. Contributions range from HCI-oriented research through organizational process design and decision making. Twelve papers were submitted of which six papers were judged to be of high quality accepted for presentation and publication. We should like to offer our thanks for the professionalism of the authors, reviewers, sub-reviewers and the program committee members. All papers were reviewed by at least three reviewers from the program committee, with the help of external reviewers.

**Lizzie, Coles-Kemp and Peter Y. A., Ryan**
Programme Chairs, STAST 2012