Foreword from the Workshop Chairs

STAST 2012

The last few years have consolidated our understanding that security and trust are a socio-technical matter. Hence a call for researchers from different disciplines, such as sociology, psychology and informatics, to construct a holistic vision of security and trust. STAST, the workshop on Socio-Technical Aspects in Security and Trust, is an international event to support such interdisciplinary research. It reaches its second edition in 2012. The first took place at the University of Milano (Milan, Italy), hosted by the International Conference on Network and System Security (NSS). The second edition was held at Harvard University (Cambridge, MA, USA), hosted by the Computer Security Foundation Symposium (CSF) — this volume gathers its post-proceedings.

Socio-technical research is inherently multi-faceted. Taking a socio-technical approach to security reveals insights that could escape a purely technical analysis; this is because vulnerabilities exist and hide, often and more subtly, also in the social layers of information systems, that is in a system’s interaction with its users, in its interface with the environment, and in its physical spaces. For example, the benefits of using strong passwords have often been circumvented by writing them down on sticky notes that can be read by whoever happens to be in the same physical space. In general, effective security measures could fail if humans find them complicated to adhere to, or if the context where such measures are applied is not fully understood. While this recalls a notorious tension between security and usability, the matter is yet more complicated. A web site that is secure but keeps compelling its users to accept this and tick that may inspire a negative sense of loss of control: even security and trust may diverge.

The workshop’s topics of interest define a number of challenges for socio-technical research in security and trust. With the Program Chairs’ expert advice and the Program Committee’s in-depth reviews, this volume addresses some of those challenges. In “SpoofKiller: you can teach people how to pay, but not how to pay attention”, Jakobsson and Siadati prototype a system to minimise the opportunity for human interaction to cause a security violation during web site login. In “Towards a model to support the reconciliation of security actions across enterprises”, Nurse and Sinclair devise a model to support the humans in reconciling their enterprise-specific, hence potentially diverging, security views and needs. In “Using socio-technical and resilience frameworks to anticipate threat”, Worton advances a socio-technical framework to effectively anticipate real-world threats of cyber-attacks. Jacobsson and Siadati, in “Improved visual preference authentication”, advance a novel working system to authenticate humans by means of their preferences. Nurse et al, in “Using information trustworthiness advice in decision-making”, describe findings on how Internet users consider information trustworthiness while making their decisions. Finally, Nochenson and Heimann, in “Optimal Security investments in networks of varying size and topology”, study people’s security investments focusing on reciprocal repercussions in realistic scenarios.

We would like to thank Program Chairs, Programme Committee members and all reviewers for their excellent work, as well as authors and speakers for their contributions. Their combined efforts have made STAST 2012 a success. We wish you all a pleasant reading.

Giampaolo Bella and Gabriele Lenzini
Workshop Chairs, STAST 2012