STAST
socio-technical aspects in security and trust

(STAST 2012) - 2nd International Workshop on
Socio-Technical Aspects in Security and Trust
URL: `http://www.stast2012.uni.lu`

Co-located with IEEE 25th Computer Security Foundation Symposium - Harvard University, Cambridge, MA, USA

Scope. Due to the huge yet increasing number of people carrying out sensitive Internet transactions, security threats hardly ever reduce to technical threats. Rather, they are socio-technical, as they come from adversaries who combine social engineering practices with technical skills. Humans obviously cannot be treated as machines, as they take actions that may seem irrational although they are perfectly justifiable from a cognitive and a social perspective. Computer security hence appears to acquire more and more the facets of an interdisciplinary science with roots in both interpretive and positivist research traditions.

STAST intends to foster an interdisciplinary discussion on modelling and analysing the socio-technical aspects of security systems and on how to protect them from socio-technical threats and attacks. Its goals are to stimulate an active exchange of ideas and experiences from different communities of researchers, to collect the state-of-the-art, to identify open problems and to point out future research. We welcome experts in computer security, social and behavioural sciences, philosophy, and psychology.

Programme. STAST is one day workshop. The programme consists of three sessions as follows:

• Keynote

Joshua D. Guttman	Trust Engineering via Security Protocols

• Session: Security Ceremonies and Interactions •

M. Jakobsson and H. Saidati	SpoofKiller: You can teach people how to pay, but not how to pay attention
J. R. C. Nurse and J. E. Sinclair	Towards A Model to Support the Reconciliation of Security Actions across Enterprises

• Session: Security Awareness and Decision-Making •

M. Jakobsson and H. Saidati	Improved Visual Preference Authentication
J. R. C. Nurse, S. Creese, M. Goldsmith and K. Lamberts	Using Information Trustworthiness Advice in Decision-Making
A. Nochenson and L. Heimann	Optimal Security Investments in Networks of Varying Size and Topology

Registration and Venue   Registration is open. More information at URL: `http://www.stast2012.uni.lu`.

Workshop Chairs

Bella, Giampaolo (Univ. of Catania, IT)
Lenzini, Gabriele (Univ. of Luxembourg, L)

Programme Chairs

Coles-Kemp, Lizzie (Royal Holloway London, UK)
Ryan, Peter Y. A. (Univ. of Luxembourg, L)

Programme Committee   Bishop, Matt (Univ. of California, CA, USA); Boyd, Colin (QUT, AU), Curzon, Paul (Queen Mary. Univ. of London, UK); Hartel, Pieter (Univ. of Twente, NL); Jakobsson, Markus (PayPal, USA); Koenig, Vincent (Univ. of Luxembourg, L); Llewellyn, Morgan (IMT, IT); Marsh, Stephen (Comm. Research Centre, CA); Mauw, Sjouke (Univ. of Luxembourg, L); Moore, Tyler (Wellesley College, MA, USA); Mulder, Ingrid (Univ. of Rotterdam & TU Delft, NL); Ortlieb, Martin (Google, CH); Probst, W. Christian (DTU, DK); Sasse, Angela (UCL, UK); Staddon, Jessica (Google, CA, USA); van Moorsel, Aad (Univ. of Newcastle, UK); Volkamer, Melanie (TU Darmstadt, D); Wang, Yang (CMU, PA, USA); Wash, Rick (Michigan State Univ., MI, USA); Williams, Trish (Edith Cowan University, AU).