CALL FOR PARTICIPATION

STAST
socio-technical aspects in security and trust

(STAST-2013) - 3rd International Workshop on
Socio-Technical Aspects in Security and Trust
http://www.stast2013.uni.lu

Co-located with 2013 IEEE 26th Computer Security Foundation Symposium
(CSFW-13) - `http://csf2013.seas.harvard.edu`

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. 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 fosters 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.

- **Keynote**

Jean E. Martina	The ever changing Threat Model - A social-technical perspective

- **Assessments and Perception of Risks**

E. Lastdrager, L. Montoya, P. Hartel and M. Junger	Applying the Lost-Letter Technique to Assess IT Risk Appetite
S. Afroz, A. C. Islam, J. Santell, A. Chapin and R. Greenstadt	How Privacy Flaws Affect Consumer Perception
M. Janic, J. P. Wijbenga and T. Veugen	Transparency enhancing tools (TETs): an overview

- **Security Properties and Cultural Differences** •

C. Huth, D. Mundie and S. Perl	Toward an Ontology for Insider Threat Research: Varieties of Insider Threat Definition
R. Tembe, K. W. Hong, C. Mayhorn, E. Murphy-Hill and C. Kelley	American and Indian Conceptualizations of Phishing
M. Volkamer, S. Stockhardt, S. Bartsch and M. Kauer	Adopting the CMU/APWG Anti-Phishing Landing Page idea for Germany

Registration and Venue Registration is open. More information at http://www.stast2013.uni.lu.

Workshop Chairs	**Programme Chairs**
Bella, Giampaolo (Univ. of Catania, IT)	Christian Probst (DTU, DK)
Lenzini, Gabriele (Univ. of Luxembourg, L)	This Williams (Edith Cowan Univ., AU)

Programme Committee Bishop, Matt (Univ. of California, CA, USA) Boyd, Colin (QUT, AU), Coles-Kemp, Lizzie (RHUL, UK), Garg, Vaibhav (Univ. of Indiana, USA), Hartel, Pieter (Univ. of Twente, NL), Herley, Cormac (Microsoft Research, USA), Jakobsson, Markus (PayPal, USA), Kammueller, Florian (Middlesex Univ. of, UK), Koenig, Vincent (Univ. of Luxembourg, L), Martina, Jean (Univ. Fed. de Santa Catarina, BR), Mauw, Sjouke (Univ. of Luxembourg, L), Moore, Andrew P. (CERT/SEI, USA), Moore, Tyler (Southern Methodist Univ., USA), Ortlieb, Martin (Google, CH), Pieters, Wolters (Univ. of Twente & TU Delft, NL), Ryan, Peter Y. A. (Univ. of Luxembourg, LU), Staddon, Jessica (Google, CA, USA), Viganó, Luca (Univ. of Verona, IT), Volkamer, Melanie (TU Darmstadt, D), Yan, Jeff (Univ. of Newcastle, UK)