

## FIRST CALL FOR PAPERS



1st Int. Workshop on Socio-Technical Aspects in Security and Trust  
(STAST 2011) - <http://stast2011.uni.lu>

Co-located with the 5th International Conference on Network and System Security  
(NSS 2011) - <http://anss.org.au/nss2011>

### Important Dates

Papers: 5 June 2011

Notification: 4 July 2011

Final version: 20 July 2011

Workshop: 6-8 Sept 2011 (one day, to be decided)

**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.

The workshop will foster an interdisciplinary discussion on how to model and analyse the socio-technical aspects of security systems and on how to protect them from socio-technical threats and attacks. It aims to stimulate an active exchange of ideas and experiences from different communities of researchers. The workshop will collect the state of the art, identify open and emerging problems, and propose future research directions.

We welcome experts in computer security, in social and behavioural sciences, philosophy, and psychology.

**Topics.** Contributions should focus on Socio-Technical Aspects in, but not limited to, the following areas:

- Usability Design and Analysis
- System-User Interfaces
- Cognitive Aspects in HCI
- Modelling and Analysis of Security
- Cyber Crime Science
- Social Informatics and Networks
- Psychology of Deception
- User Perception of Security & Trust
- Users Practise & Behavioural Models
- Workflows & Ceremonies
- Security Properties & Requirements
- Technology Effects on Trust Building
- Social-Technical Attacks and Defences
- Socio-Technical Secure System Design
- Social Engineering
- Game Theory and Security
- Threat and Adversary Models
- Experiences and Test Cases

Both qualitative and quantitative modelling approaches are welcome.

**Submission.** Contributions consist of  $\leq 8$  pages, IEEE 8.5"  $\times$  11" two-columns format. Accepted papers will be published by IEEE and in the IEEE digital library. (Submission Guidelines: see web page.)

### Programme Committee

Colin Boyd (QUT, AU)  
José-Rodrigo Córdoba Pachón (RHUL, UK)  
Ferrari, Elena (Univ. of Insubria, IT)  
Hartel, Pieter (Univ. of Twente, NL)  
Moore, Tyler (SEAS Harvard, US)  
Mauw, Sjouke (Univ. of Luxembourg, L)  
Ortlieb, Martin (Google, CH)  
Sasse, Angela (UCL, UK)  
Williams, Trish (Edith Cowan University, AU)

Richard Clayton (Univ. of Cambridge, UK)  
Falcone, Rino (ISTC-CNR, IT)  
Gollmann, Dieter (TU, Hamburg, D)  
Koenig, Vincent (Univ. of Luxembourg, L)  
van Moorsel, Aad (Univ. of Newcastle, UK)  
Mulder, Ingrid (Univ. of Rotterdam & TU Delft, NL)  
Probst, W. Christian (DTU, DK)  
Volkamer, Melanie (TU Darmstadt, D)

### 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)

**NSS Conference General Chair** Sabrina De Capitani di Vimercati (Univ. Milan, IT)

**Sponsors** The workshop is co-sponsored by IEEE and IEEE council.