CALL FOR PAPERS

(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`

Important Dates	Papers: 28st April (extended)	Notification: 15th May
	Final versions: 10th June (pre-proceedings)	14th July (post-proceedings)

Scope. Attacks against information security are still threatening the digital society due to the fast increasing number of people carrying out sensitive Internet transactions. However such threats hardly ever reduce to the technical side of security: 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 is acquiring more and more the facets of an interdisciplinary science.

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 present the state of the art, identify open and emerging problems, and propose future research directions. We welcome experts as in computer security as well in social and behavioural sciences, philosophy, and psychology.

Topics. Works should focus on <u>Socio-Technical (ST) Security and Trust</u> in, but not limited to:

- Usability Analysis
- ST Attacks/Defences
- Users Practise & Behavioural Models
- Social Engineering & Insider Attacks
- Cyber Crime Science
- Security Ethics
- System-User Interfaces
- User Perception of Security & Trust
- Design of ST Secure Systems
- Workflows & Ceremonies
- Threat and Adversary Models
- Technology & Trust Building Behavior
- Psychology of Deception
- Cognitive Aspects in HCI
- Analysis of ST Security
- Game Theory and Security
- Social Informatics and Networks
- ST Experiences and Test Cases

Both qualitative and quantitative modelling approaches are welcome.

Submission. Contributions should be $\leq$ 8 pages, including the bibliography and well-marked appendices, and should follow the IEEE $8.5'' \times 11''$ Two-Columns Format. Both theoretical and applied research papers are welcome.

Programme Committee

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

Programme Chair and Co-Chair

Probst, W. Christian (DTU, DK)
Williams, Trish (Edith Cowan University, AU)

Workshop Organizers

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