FIRST CALL FOR PAPERS

(STAST-2014) - 4th International Workshop on
Socio-Technical Aspects in Security and Trust
http://www.stast2014.uni.lu

Co-located with IEEE 27th Computer Security Foundation Symposium
(CSFW-14) - `http://csf2014.di.univr.it/`

Important Dates

Paper (extended) : 30th April
Final versions: 6th July (pre-proceedings)
Notification: 31st May
27th 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. 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 & Insider Attacks
- Game Theory and Security
- Threat and Adversary Models
- Experiences and Test Cases

Both qualitative and quantitative modelling approaches are welcome.

Submission. Contributions consist of ≤ 8 pages, including bibliography and well-marked appendices. Papers should be formatted in the two-column proceedings style of Conference Publishing Services (CPS). The conference proceedings will be submitted to Xplore and CSDL.

Programme Committee

Bishop, Matt (Univ. of California Davis, USA)
Herley, Cormac (Microsoft Research, USA)
Martina, J. Everson (Univ. Fed. de S. Catarina, BR)
Moore, Andrew P. (CERT/SEI, USA)
Moore, Tylor (Souther Methodist Univ., USA)
Pellegrino, Giancarlo (Eurecom, FR)
Pieters, Wolter (Univ. of Twente and TU Delft, NL)
van Deursen, Nicole (Edinburgh Napier Univ., UK)
Wash, Rick (Michigan State University, USA)
Yan, Jeff (Newcastle Univ., UK)
Garg, Vaibhav (Drexel Univ., USA)
Kammueller, Florian (Middlesex Univ., UK)
Montoya, Lorena (Univ. of Twente, NL)
Morgan, H. Llewellyn (specularX, USA)
Nadjm-Tehrani, Simin (Linköping Univ., SE)
Ortlieb, Martin (Google, CH)
Ryan, Peter Y. A. (Univ. of Luxembourg, LU)
Volkamer, Melanie (TU Darmstadt, DE)
Woodruff, Allison (Google, USA)

Program Chairs

Probst, Christian W. (DTU, DK)
Ashenden, Debi M. (Cranfield Uni., UK)

Workshop Organizers

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