FIRST CALL FOR PAPERS



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

Co-located with 25th Computer Security Foundation Symposium - Harvard University, Cambridge, MA, USA (CSFW-12) - http://csf2012.seas.harvard.edu/

Important Dates

Papers: 23th April 2012 (extended)

is acquiring more and more the facets of an interdisciplinary science.

Final version: 13th July 2012 (after the workshop)

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

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 Experiences and Test Cases
- Social-Technical Attacks and Defences

Notification: 18yh May 2012

Workshop: 28th June 2012

- Socio-Technical Secure System Design
- Social Engineering & Insider Attacks
- Game Theory and Security
- Threat and Adversary Models

Submission. Contributions consist of ≤ 8 pages, not counting bibliography and well-marked appendices. Papers should be formatted in the two-column IEEE Proceedings style available for various document preparation systems at the IEEE Conference Publishing Services page.

Programme Committee

Bishop, Matt (Univ. of California, CA, USA) Curzon, Paul (Queen Mary. Univ. of London, UK) Jakobsson, Markus (PayPal, USA) Llewellyn, Morgan (IMT, IT)

Both qualitative and quantitative modelling approaches are welcome.

Mauw, Sjouke (Univ. of Luxembourg, L)

Mulder, Ingrid (Univ. of Rotterdam & TU Delft, NL)

Probst, W. Christian (DTU, DK) Staddon, Jessica (Google, CA, USA)

Volkamer, Melanie (TU Darmstadt, D)

Wash, Rick (Michigan State Univ., MI, USA)

Workshop Chairs

Bella, Giampaolo (Univ. of Catania, IT) Lenzini, Gabriele (Univ. of Luxembourg, L) Boyd, Colin (QUT, AU)

Hartel, Pieter (Univ. of Twente, NL)

Koenig, Vincent (Univ. of Luxembourg, L)

Marsh, Stephen (Comm. Research Centre, CA)

Moore, Tyler (Wellesley College, MA, USA)

Ortlieb, Martin (Google, CH)

Sasse, Angela (UCL, UK)

van Moorsel, Aad (Univ. of Newcastle, UK)

Wang, Yang (CMU, PA, USA)

Williams, Trish (Edith Cowan University, AU)

Programme Chairs

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