CALL FOR PAPERS

STAST
Socio-Technical Aspects in Security and Trust

http://stast2017.uni.lu

7th **I**nternational Workshop on
Socio-Technical Aspects in Security and Trust (STAST 2017)
affiliated with ACSAC 2017
Orlando, Florida, USA December 5, 2017

Abstract and Title: September 27, 2017
Notification: November 6, 2017
(all deadlines at 23:59 - AoE = UTC-12))

Full Papers: October 2, 2017
Camera Ready: November 20, 2017

Terminology Socio-technical means the reciprocal relationship between people and technology.

Concept and Goal Successful attacks on information systems often combine social engineering practices with technical skills. Research in social sciences and usable security has demonstrated that insecure behavior can be justified from cognitive, emotional, and social perspectives and to improve security, technology must adapt to the users. However, finding the right balance between the technical and the social security measures remains largely unexplored, which motivates the need for this workshop. There is no established holistic research in security, and the respective communities tend to offload on each other parts of problems that they consider to be out of scope, an attitude that results in deficient or unsuitable security solutions.

The workshop intends to stimulate an exchange of ideas and experiences on how to design systems that are secure in the real world where they interact with non-expert users. It aims at bringing together experts in various areas of computer security and in social and behavioral sciences.

Topics Contributions should focus on the interplay of technical, organizational and human factors in breaking and in achieving computer security, for example:

- Feasibility of policies from the socio-technical perspective
- Requirements for socio-technical systems
- Threat models that combine technical and human-centred strategies
- Technical and social factors that influence decision making in security and privacy
- Balance between technical measures and social strategies in ensuring security and privacy
- Studies of real-world security incidents from the socio-technical perspective
- Social factors that influence changes in organizations security policies and processes
- Lessons learned from holistic design and deployment of security mechanisms and policies
- Models of user behaviour and user interactions with technology
- Perceptions of security, risk and trust and their influence on human behaviour
- Interplay of law, ethics and politics with security and privacy measures
- Social engineering, persuasion, and other deception techniques
- Socio-technical analysis of security incidents
- Methodology and guidelines for socio-technical and cyber-security intelligence analysis

Both qualitative and quantitative research approaches, from academia and industry, are welcome.

Submissions We accept (1) Full Papers presenting new results; (2) Position Papers discussing existing challenges and introducing new research topics; (3) Case Studies describing lessons learned from design and deployment of security mechanisms and policies in research and in industry; (4) Work in Progress..

Proceedings. Published with the ACM International Conference Proceedings Series

PC Members
(see our web page at http://stast2017.uni.lu)

Invited Speaker
Robert L. Biddle (Carleton University)

PC Chairs
Zinaida Benenson (University of Erlangen-Nuremberg)
Daniela Oliveira (University of Florida)

Organizers
Giampaolo Bella (University of Catania)
Gabriele Lenzini (University of Luxembourg)