CALL FOR PAPERS

STAST 2019 9th WORKSHOP ON SOCIO-TECHNICAL ASPECTS IN SECURITY
Socio-Technical Aspects in Security
Luxembourg City, Luxembourg

Luxembourg City, Luxembourg
http://www.stast.uni.lu

affiliated with ESORICS 2019
the European Symposium on
Research in Computer Security
(https://esorics2019.uni.lu/)

Full Papers: ~~June 30, 2019~~ July 10, 2019
Camera Ready: August 6, 2019
(all deadlines at 23:59 - AoE = UTC-12))

Notification: July 30, 2019
Workshop Date: September 26, 2019

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:

- Usability and user experience in security
- Requirements for socio-technical systems
- Feasibility of policies from the socio-technical perspective
- Threat models that combine technical and human-centered strategies
- Socio-technical factors in decision making in security and privacy
- Balance between technical measures and social strategies
- Studies of real-world security incidents from a socio-technical perspective
- Social factors in organizations security policies and processes
- Lessons from 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 humans
- Interplay of law, ethics and politics with security and privacy measures
- Social engineering, persuasion, and other deception techniques
- Socio-technical analysis of security incidents
- Strategies, methodology and guidelines cyber-security intelligence analysis

We welcome qualitative and quantitative research approaches from academia and industry.

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. Accepted papers will be published as post-proceedings with Springer in their Lecture Notes in Computer Science series (final approval pending).

PC Chairs
Theo Tryfonas (University of Bristol)
Thomas Gross (Newcastle University)

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

Website Chair
Itzel Vazquez Sandoval (University of Luxembourg)

Publicity Chair
Borce Stojkovski (University of Luxembourg)