CALL FOR PAPERS

STAST 2021 Socio-Technical Aspects in Security

11th WORKSHOP ON SOCIO-TECHNICAL ASPECTS IN SECURITY

https://stast.uni.lu

affiliated with ESORICS 2021
(https://esorics2021.athene-center.de/)
(fully virtual event)

Abstract and Title: 04 July 2021
Notification: 15 August 2021
Workshop Date: virtual event on 07 or 08 October 2021

Full Papers: 11 July 2021
Camera Ready: 06 September 2021

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

Concept & Goal Attacks on information systems often exploit not only IT systems and networks, but also the human element in the system. It is critical to limit technical vulnerabilities and insecure user behavior, but also poorly designed user interfaces, and unclear or unrealistic security policies. To improve the security of systems, technology and policies must consider the characteristics of the users, where research in social sciences and usable security has demonstrated that insecure behavior can be justified from cognitive, emotional, and social perspectives. When there is a good 'fit' of technology to users, workable security policies and targeted behavioral support can augment technical security. There remains a need for focused, holistic research in socio-technical 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 solutions. The workshop aims at bringing together experts in various areas of computer security and in social and behavioral sciences, to stimulate an exchange of ideas and experiences on how to design systems that are secure in the real world where they interact with users of varying expertise and diverse needs.

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
- Models of user behaviour and user interactions with technology
- Perceptions of related risks, as well as their influence on humans
- Social engineering, persuasion, and other deception techniques
- Requirements for socio-technical systems
- Decision making in/for socio-technical systems
- Feasibility of policies from the socio-technical perspective
- Social factors in organizations's policies and processes
- Interplay of law, ethics and politics with security and privacy measures
- Balance between technical measures and social strategies
- Threat models that combine technical and human-centered strategies
- Socio-technical analysis of security incidents and vulnerabilities
- Studies of real-world vulnerabilities/incidents from a socio-technical perspective
- Lessons from design and deployment of mechanisms and policies
- Strategies and guidelines for analysis of intelligence and data from a socio-technical perspective
- Methodologies and methodological reflections in pursuit of these goals

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

Submissions (1) Full Papers discussing original research, answering well-defined research questions, and presenting full and stable results; (2) Position Papers discussing existing challenges and introducing and motivating new research problems; (3) Work in Progress describing original but unfinished research, which is nevertheless based on solid research questions or hypothesis soundly argued be innovative compared with the state of the art.

Post-proceedings. Published with Springer LNCS (pending final approval)

PC Chair/Co-chair
Simon Parkin (Delft University of Technology)
Luca Viganò (King's College London)

PC Members
(see our web page)

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

Invited Speaker
(to be announced)