# STAST 2020

10th International Workshop on Socio-Technical Aspects in SecuriTy
http://stast.uni.lu
Easychair CfP: https://easychair.org/cfp/STAST2020

Affiliated with the 25th European Symposium on Research in Computer Security (ESORICS) 2020, https://www.surrey.ac.uk/esorics-2020

The workshop will take place on 17 or 18 September 2020 as an online one day workshop.

**Concept**

Successful attacks on information systems often combine social engineering practices with technical skills, exploiting technical vulnerabilities, insecure user behavior, poorly designed user interfaces, and unclear or unrealistic security policies. To improve security, technology must adapt to the users, because research in social sciences and usable security has demonstrated that insecure behavior can be justified from cognitive, emotional, and social perspectives. However, also adherence to reasonable security policies and corresponding behavioral changes should augment and support technical security.

Finding the right balance between the technical and the social security measures remains largely unexplored, which motivates the need for this workshop. Currently, different security communities (theoretical security, systems security, usable security, and security management) rarely work together. 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.

**Goals**

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.

**Workshop topics**

Contributions should focus on the interplay of technical, organizational and human factors in achieving or breaking security, privacy, and trust, 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' 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 incidents and vulnerabilities
- Studies of real-world vulnerabilities/incidents from a socio-technical perspective
- Lessons from design and deployment of mechanisms and policies
- Strategies, methodology and guidelines for intelligence analysis
- Methodologies and methodological reflections in pursuit of these goals

**Type of contributions:**

- *Full Papers*, discussing original research, answering well-defined research questions, and presenting full and stable results.
- *Position Papers*, original contributions discussing existing challenges and introducing and motivating new research problems.
- *Case Studies*, describing lessons learned from design and deployment of security mechanisms and policies in research and in industry.
- *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.

We welcome qualitative and quantitative research approaches from academia and industry.
We welcome meta-analytic as well as replication studies and consider them as original research eligible for full papers. We welcome negative or null results with sound methodology.

**Proceedings**

Accepted papers will be published as post-proceedings with Springer in their Lecture Notes in Computer Science series.
To celebrate the 10th edition of the workshop, the authors of the best papers will be invited to submit extended versions of their work for a special issue of the Journal of Computer Security.

**Invited speaker**

Angela Sasse (Ruhr University Bochum)

**Timeline**

- Abstract submission: July 3 (AoE)
- Full Paper Submission: July 10 (AoE)
- Notification: August 7 (AoE)
- Camera Ready: TBA

**Workshop organizers**

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

**Programme chairs**

- Thomas Gross (Newcastle University)
- Luca Viganò (King’s College London)