Journal of Computer Security 30 (2022) 325–326
DOI 10.3233/JCS-220950
IOS Press

Special issue on socio-technical aspects in security – editorial

Thomas Groß [a] and Luca Viganò [b]
[a] *School of Computing, Newcastle University, London, UK*
E-mail: thomas.gross@ncl.ac.uk
[b] *Department of Informatics, King's College London, London, UK*
E-mail: luca.vigano@kcl.ac.uk

Successful attacks on information systems often exploit not only IT systems and networks, but also the human element in the system. It is vital to understand technical vulnerabilities and how user behavior contributes to their exploitation, 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 user behavior involved in security exploits can be understood 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.

Finding the right balance between technical and social security measures remains, however, largely unexplored, and different security communities (theoretical security, systems security, usable security, and security management) rarely work together. 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. This is an attitude that results in deficient or unsuitable security solutions. The research domain of socio-technical security was born after many realized that practical attacks against information services often succeed because of a combination of social engineering practices and technical skills. Often, such attacks were possible because of vulnerable security mechanisms, ill-designed system interfaces, unusable security policies, or carelessly conceived human computer ceremonies – and not because humans just "don't get security right", as it was wrongly put not a long time ago.

In 2011, Giampaolo Bella and Gabriele Lenzini created the international Workshop on "Socio-Technical Aspects in Security and Trust" (STAST) to gather experts in security and experts in social science with an interest in security, and thus foster an interdisciplinary discussion on how to model and analyze the socio-technical aspects of modern security systems and on how to protect such systems from socio-technical threats and attacks. Since then, the workshop has taken place annually, shortening its name to "Socio-Technical Aspects in Security", but continuing to stimulate an active exchange of ideas and experiences from different communities of researchers in order to identify weaknesses potentially emerging from poor usability designs and policies, from social engineering, and from deficiencies hidden in flawed interfaces and implementations. STAST has been bringing together experts in computer security and in cognitive, social, and behavioral sciences; it has been collecting the state of the art, identifying open and emerging problems, and proposing future research directions.

It was our pleasure and honor to chair the STAST workshop in 2020. In addition to publishing the post-proceedings with Springer as usual, to celebrate the 10th edition of the workshop, we decided to organize also a special issue of the Journal of Computer Security. The editors of the journal enthusiastically accepted our proposal for a special issue and we thus invited the authors of the best papers of STAST 2019 and 2020 to submit a revised and extended version of their papers. Nine papers were submitted to the special issue. The submissions underwent the standard reviewing process of the Journal of Computer Security, including the requirement that the extension/novel contents should be at least 25% compared to the version published in the workshop proceedings. All submissions were reviewed by at least 3 reviewers, and some of them underwent two rounds of revision. In the end, we accepted 7 excellent papers, which are now collected in this special issue:

- *A Cyber-risk Framework for Coordination of the Prevention and Preservation of Behaviours* by Simon Parkin and Yi Ting Chua
- *Exploiting WiFi Usability Features for Association Attacks in IEEE 802.11: Attack Analysis and Mitigation Controls* by George Chatzisofroniou and Panayiotis Kotzanikolaou
- *How to Measure Usable Security: Natural Strategies in Voting Protocols* by Wojciech Jamroga, Damian Kurpiewski and Vadim Malvone
- *Modelling Human Threats in Security Ceremonies* by Giampaolo Bella, Rosario Giustolisi and Carsten Schürmann
- *The boundedly rational employee: Security economics for behaviour intervention support in organizations* by Albesë Demjaha, Simon Parkin and David Pym
- *User Privacy Concerns in Commercial Smart Buildings* by Scott Harper, Maryam Mehrnezhad and John Mace
- *WARChain: Consensus-based trust in web archives via proof-of-stake blockchain technology* by Imre Lendák, Balázs Indig and Gábor Palkó

We are pleased that the papers accepted for this STAST special issue reflect the breadth and diversity of topics typically considered in the workshop.

We would like to thank Giampaolo Bella and Gabriele Lenzini, the masterminds of STAST, Véronique Cortier and Peng Liu, the Editors-in-Chief of the Journal of Computer Security, Steffen de Jong and the team at IOS Press for their support, and all the reviewers for their thorough work (Ala Altaweel, Giampaolo Bella, Zinaida Benenson, Pam Briggs, Kyung-Shick Choi, Lynne Coventry, Changyu Dong, Andrea Flamini, Markus Jakobsson, Christian Johansen, Florian Kammüller, Mat Kelly, Gabriele Lenzini, Jean Everson Martina, Tyler Moore, Masakatsu Nishigaki, Jason Nurse, Federica Paci, Evangelos Pournaras, Saša Radomirović, Kopo Marvin Ramokapane, Karen Renaud, Nishanth Sastry, Steve Schneider, Diego Sempreboni, William Seymour, Melanie Volkamer).

June 9, 2022
Thomas Groß and Luca Viganò