Lecture Notes in Computer Science 13176

More information about this series at https://link.springer.com/bookseries/558

Simon Parkin · Luca Viganò (Eds.)

Socio-Technical Aspects in Security

11th International Workshop, STAST 2021
Virtual Event, October 8, 2021
Revised Selected Papers

Springer

Editors
Simon Parkin
Delft University of Technology
Delft, The Netherlands

Luca Viganò
King's College London
London, UK

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-10182-3 ISBN 978-3-031-10183-0 (eBook)
https://doi.org/10.1007/978-3-031-10183-0

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The 11th International Workshop on Socio-Technical Aspects in Security (STAST 2021) aimed at creating an exchange of ideas and experiences on how to design systems that are secure in the real world where they interact with users. The term "socio-technical," in this context, means a reciprocal relationship between technology and people. The 2021 workshop focused especially on the interplay of technical, organizational, and human factors in achieving or breaking computer security, privacy, and trust.

As typical for STAST, the workshop received a wide range of inter-disciplinary submissions with a number of distinct methodologies.

The peer-review was organized as a double-blind process, with a strong conflict-of-interest management system. Each submission received a minimum of three reviews. Submissions with appreciable variance in review scores were assigned a fourth review as a tie-breaker. The peer-review process included an active discussion phase, facilitated by a designated discussion lead for each submission, who subsequently summarized the discussion outcome and, when needed, agreed conclusions in a meta-review.

All of the 25 papers initially submitted to the workshop were retained by the chairs for peer-review after an initial check against the stipulations of the call for papers. Eventually, we accepted 10 submissions for publication in this volume, yielding an acceptance rate of 40%.

We prepared this volume with the following three sections. First, the section 'Web and apps' includes investigations on social media and applications. Second, the section 'Context and modelling' considers how to model the context of socio-technical systems in order to reason about their security. Finally, the section 'From the present to the future' includes analyses of, and positions on, the past, the present, and the future of the field itself.

Ashwin Mathew was recognized with the STAST 2021 Best Paper Award for the paper 'Can Security be Decentralised? The Case of the PGP Web of Trust.'

Overall, we were very pleased with the quality of STAST's 11th anniversary volume. We are grateful for the high-quality work of the authors involved and for the invaluable contributions of the 30 Program Committee members and three additional reviewers, whose dedication and attention to detail enabled this volume. We thank Borce Stojkovski and Itzel Vazquez Sandoval for their help with the publicity for the workshop and the workshop's web site.

February 2022

Simon Parkin
Luca Viganò

Message from the Workshop Organizers

It has been eleven years since we had the idea of founding a workshop dedicated to socio-technical aspects of cyber-security. At that time, something was missing in the landscape of events in security research: a venue to discuss security in a broader manner, a manner that combined technical discussion with other topics traditionally linked to usability and human computer interaction research, yet much broader than just these. There was a need to discuss attacks that exploit technical hacking in combination with social engineering and, equally, there was a need to discuss user practices, organizational processes, and social culture as instruments to establish security or, by contrast, as possible vectors to break it.

Discussing such matters was, and still is, relevant since evidence shows that designing systems that are secure when analyzed from a merely technical perspective, regardless of the values and merits of the approach, does not guarantee that security works as expected once deployed. The common and arguable explanation is that the human, the "weakest link," did not comply. However, blaming users neither helps nor gives us instruments to design stronger systems. We have learned by experience that a better strategy is to holistically conceive systems whose security emerges by harmonizing the technical features with the modalities in which humans, organizations, and societies operate. The manifesto of addressing the security problem socio-technically means exactly that all those components are to be addressed as a whole. We have also learned that such a manifesto has a very wide impact, concerning virtually all application areas where human beings may play a role through the effectiveness of security measures, hence on virtually every ICT application that must be protected from criminals.

Looking at the proceedings of this year's edition of the workshop, the published contents clearly attest that the idea outlined above has rooted well. As a result, the Workshop on Socio-Technical Aspects in Security (STAST) is now fully mature. Its aims have come to a clear focus, while the affiliation with the European Symposium on Research in Computer Security (ESORICS) is naturally well principled and practically fruitful.

We would like to thank all the Program Chairs and Committee members that in this decade have helped STAST to become a successful series. And we are particularly grateful to this year's Program Chairs, Simon Parkin and Luca Viganò: they have done an impeccable job and brought, with a top-level Program Committee, this year's edition to a unmatched success with a great scientific program.

February 2022

Giampaolo Bella
Gabriele Lenzini

Organization

General Chairs

Giampolo Bella	University of Catania, Italy
Gabriele Lenzini	University of Luxembourg, Luxembourg

Program Committee Chairs

Simon Parkin	Delft University of Technology, The Netherlands
Luca Viganò	King's College London, UK

Program Committee

Panagiotis Andriotis	University of the West of England, UK
Ingolf Becker	University College London, UK
Giampaolo Bella	University of Catania, Italy
Zinaida Benenson	University of Erlangen-Nuremberg, Germany
Vladlena Benson	Aston University, UK
Jan-Willem Bullee	University of Twente, The Netherlands
Michael Carter	Queen's University, Canada
Lynne Coventry	Northumbria University, UK
Sarah Diesburg	University of Northern Iowa, USA
Rosario Giustolisi	IT University of Copenhagen, Denmark
Thomas Groß	Newcastle University, UK
Pieter Hartel	University of Twente, The Netherlands
Ulrike Hugl	Innsbruck University, Austria
Markus Jakobsson	ZapFraud, USA
Kat Krol	Google UK
Gabriele Lenzini	University of Luxembourg, Luxembourg
Shujun Li	University of Kent, UK
Alexandra Mai	SBA-Research, Austria
Jean Everson Martina	Universidade Federal de Santa Catarina, Brazil
Masakatsu Nishigaki	Shizuoka University, Japan
Norbert Nthala	Michigan State University, USA
Jason Nurse	University of Kent, UK
Simon Parkin	Delft University of Technology, The Netherlands
Saša Radomirović	Heriot-Watt University, UK
Karen Renaud	University of Strathclyde, UK

Peter Y. A. Ryan	University of Luxembourg, Luxembourg
Diego Sempreboni	King's College London, UK
Kerry-Lynn Thomson	Nelson Mandela University, South Africa
Luca Viganò	King's College London, UK
Konrad Wrona	NATO Communications and Information Agency, The Netherlands/Military University of Technology in Warsaw, Poland

Publicity and Web Site Chairs

Borce Stojkovski	University of Luxembourg, Luxembourg
Itzel Vazquez Sandoval	University of Luxembourg, Luxembourg

Additional Reviewers

Ehsan Estaji
Masoud Tabatabaei
Sarah Turner

Fonds National de la Recherche Luxembourg

SnT securityandtrust.lu

UNIVERSITÀ degli STUDI di CATANIA

uni.lu UNIVERSITÉ DU LUXEMBOURG

Contents