



HAL
open science

Human Aspects of Information Security and Assurance

Nathan Clarke, Steven Furnell

► **To cite this version:**

Nathan Clarke, Steven Furnell. Human Aspects of Information Security and Assurance: 14th IFIP WG 11.12 International Symposium, HAISA 2020, Mytilene, Lesbos, Greece, July 8–10, 2020, Proceedings. Springer International Publishing, AICT-593, 2020, IFIP Advances in Information and Communication Technology, 978-3-030-57403-1. 10.1007/978-3-030-57404-8 . hal-03657705

HAL Id: hal-03657705

<https://inria.hal.science/hal-03657705>

Submitted on 3 May 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

Editor-in-Chief

Kai Rannenber, *Goethe University Frankfurt, Germany*

Editorial Board Members

TC 1 – Foundations of Computer Science

Luís Soares Barbosa, *University of Minho, Braga, Portugal*

TC 2 – Software: Theory and Practice

Michael Goedicke, *University of Duisburg-Essen, Germany*

TC 3 – Education

Arthur Tatnall, *Victoria University, Melbourne, Australia*

TC 5 – Information Technology Applications

Erich J. Neuhold, *University of Vienna, Austria*

TC 6 – Communication Systems

Burkhard Stiller, *University of Zurich, Zürich, Switzerland*

TC 7 – System Modeling and Optimization

Fredi Tröltzsch, *TU Berlin, Germany*

TC 8 – Information Systems

Jan Pries-Heje, *Roskilde University, Denmark*

TC 9 – ICT and Society

David Kreps, *University of Salford, Greater Manchester, UK*

TC 10 – Computer Systems Technology

Ricardo Reis, *Federal University of Rio Grande do Sul, Porto Alegre, Brazil*

TC 11 – Security and Privacy Protection in Information Processing Systems

Steven Furnell, *Plymouth University, UK*

TC 12 – Artificial Intelligence

Eunika Mercier-Laurent, *University of Reims Champagne-Ardenne, Reims, France*

TC 13 – Human-Computer Interaction

Marco Winckler, *University of Nice Sophia Antipolis, France*

TC 14 – Entertainment Computing

Rainer Malaka, *University of Bremen, Germany*

IFIP – The International Federation for Information Processing

IFIP was founded in 1960 under the auspices of UNESCO, following the first World Computer Congress held in Paris the previous year. A federation for societies working in information processing, IFIP's aim is two-fold: to support information processing in the countries of its members and to encourage technology transfer to developing nations. As its mission statement clearly states:

IFIP is the global non-profit federation of societies of ICT professionals that aims at achieving a worldwide professional and socially responsible development and application of information and communication technologies.

IFIP is a non-profit-making organization, run almost solely by 2500 volunteers. It operates through a number of technical committees and working groups, which organize events and publications. IFIP's events range from large international open conferences to working conferences and local seminars.

The flagship event is the IFIP World Computer Congress, at which both invited and contributed papers are presented. Contributed papers are rigorously refereed and the rejection rate is high.

As with the Congress, participation in the open conferences is open to all and papers may be invited or submitted. Again, submitted papers are stringently refereed.

The working conferences are structured differently. They are usually run by a working group and attendance is generally smaller and occasionally by invitation only. Their purpose is to create an atmosphere conducive to innovation and development. Refereeing is also rigorous and papers are subjected to extensive group discussion.

Publications arising from IFIP events vary. The papers presented at the IFIP World Computer Congress and at open conferences are published as conference proceedings, while the results of the working conferences are often published as collections of selected and edited papers.

IFIP distinguishes three types of institutional membership: Country Representative Members, Members at Large, and Associate Members. The type of organization that can apply for membership is a wide variety and includes national or international societies of individual computer scientists/ICT professionals, associations or federations of such societies, government institutions/government related organizations, national or international research institutes or consortia, universities, academies of sciences, companies, national or international associations or federations of companies.

More information about this series at <http://www.springer.com/series/6102>

Nathan Clarke · Steven Furnell (Eds.)

Human Aspects of Information Security and Assurance

14th IFIP WG 11.12 International Symposium, HAISA 2020
Mytilene, Lesbos, Greece, July 8–10, 2020
Proceedings

Editors

Nathan Clarke 
University of Plymouth
Plymouth, UK

Steven Furnell 
University of Plymouth
Plymouth, UK

ISSN 1868-4238

ISSN 1868-422X (electronic)

IFIP Advances in Information and Communication Technology

ISBN 978-3-030-57403-1

ISBN 978-3-030-57404-8 (eBook)

<https://doi.org/10.1007/978-3-030-57404-8>

© IFIP International Federation for Information Processing 2020

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

Preface

It is now widely recognized that technology alone cannot provide the answer to security problems. A significant aspect of protection comes down to the attitudes, awareness, behavior, and capabilities of the people involved, and they often need support in order to get it right. Factors such as lack of awareness and understanding, combined with unreasonable demands from security technologies, can dramatically impede their ability to act securely and comply with policies. Ensuring appropriate attention to the needs of users is therefore a vital element of a successful security strategy, and they need to understand how the issues may apply to them and how to use the available technology to protect their systems.

With the above in mind, the Human Aspects of Information Security and Assurance (HAISA) symposium series specifically addresses information security issues that relate to people. It concerns the methods that inform and guide users' understanding of security, and the technologies that can benefit and support them in achieving protection.

This book presents the proceedings from the 2020 event, held virtually due to the COVID-19 pandemic, during July 2020. A total of 27 reviewed papers are included, spanning a range of topics including issues related directly to the pandemic and the impacts on contact-tracing applications and privacy, education and awareness, and management and modeling of security. All of the papers were subject to double-blind peer review, with each being reviewed by at least two members of the International Program Committee. We are grateful to all of the authors for submitting their work and sharing their findings.

The HAISA symposium is the official event of IFIP Working Group 11.12 on Human Aspects of Information Security and Assurance, and we would like to thank Prof. Kerry-Lynn Thomson for supporting the event as Working Group chair. We would also like to acknowledge the significant work undertaken by our International Program Committee and recognize their efforts in reviewing the submissions and ensuring the quality of the resulting event and proceedings. Finally, we would like to thank Dr. Christos Kalloniatis and the organizing team for making all the necessary arrangements to enable this symposium to take place.

July 2020

Nathan Clarke
Steven Furnell

Organization

General Chairs

Nathan Clarke University of Plymouth, UK
Steven Furnell University of Plymouth, UK

IFIP TC11.12 Conference Chair

Kerry-Lynn Thomson Nelson Mandela University, South Africa

Local Organizing Chair

Christos Kalloniatis University of the Aegean, Greece

Publicity Chair

Fudong Li University of the Portsmouth, UK

International Program Committee

Sal Aurigemma	University of Tulsa, USA
Maria Bada	University of Cambridge, UK
Peter Bednar	University of Portsmouth, UK
Matt Bishop	UC Davis, USA
Patrick Bours	Norwegian University of Science and Technology, Norway
William Buchanan	Edinburgh Napier University, UK
Mauro Cherubini	University of Lausanne, Switzerland
Jeff Crume	IBM, USA
Adele Da Veiga	University of South Africa, South Africa
Ronald Dodge	Palo Alto Networks, USA
Paul Dowland	Edith Cowan University, Australia
Jan Eloff	University of Pretoria, South Africa
Simone Fischer-Huebner	Karlstad University, Sweden
Stephen Flowerday	Rhodes University, South Africa
Lynn Futcher	Nelson Mandela University, South Africa
Sarah Gordon	USA
Stefanos Gritzalis	University of Piraeus, Greece
Karen Hedström	Örebro University, Sweden
Yuxiang Hong	Hangzhou Dianzi University, China
John Howie	Cloud Security Alliance, USA
Kévin Huguenin	University of Lausanne, Switzerland

William Hutchinson	Edith Cowan University, Australia
Murray Jennex	San Diego State University, USA
Andy Jones	University of Suffolk, UK
Christos Kalloniatis	University of the Aegean, Greece
Fredrik Karlsson	Örebro University, Sweden
Vasilios Katos	Bournemouth University, UK
Sokratis Katsikas	Open University of Cyprus, Cyprus
Joakim Kavrestad	University of Skövde, Sweden
Stewart Kowalski	Norwegian University of Science and Technology, Norway
Hennie Kruger	North-West University, South Africa
Costas Lambrinouidakis	University of Piraeus, Greece
Michael Lavine	Johns Hopkins University, USA
Gabriele Lenzini	University of Luxembourg, Luxembourg
Shujun Li	University of Kent, UK
Javier Lopez	University of Malaga, Spain
George Magklaras	University of Oslo, Norway
Herb Mattord	Kennesaw State University, USA
Haris Mouratidis	University of Brighton, UK
Marcus Nohlberg	University of Skövde, Sweden
Jason Nurse	University of Kent, UK
Malcolm Pattinson	The University of Adelaide, Australia
Jacques Ophoff	Abertay University, UK
Nathalie Rebe	University of Burgundy, France
Karen Renaud	Abertay University, UK
Nader Sohrabi Safa	Coventry University, UK
Rossouw Von Solms	Nelson Mandela University, South Africa
Theo Tryfonas	University of Bristol, UK
Aggeliki Tsohou	Ionian University, Greece
Kerry-Lynn Thomson	Nelson Mandela University, South Africa
Ismini Vasileiou	De Montfort University, UK
Jeremy Ward	Security Consultant, UK
Merrill Warkentin	Mississippi State University, USA
Zihang Xiao	Palo Alto Networks, USA
Wei Yan	Trend Micro, USA
Ibrahim Zincir	İzmir University of Economics, Turkey

Contents

Privacy and COVID-19

Australian Attitudes Towards Privacy of Information: Will COVID-19 Make a Difference?	3
<i>Leah Shanley, Michael N. Johnstone, Michael Crowley, and Patryk Szewczyk</i>	
Concern for Information Privacy: A Cross-Nation Study of the United Kingdom and South Africa.	16
<i>Adéle Da Veiga and Jacques Ophoff</i>	
A Review of Information Security Aspects of the Emerging Covid-19 Contact Tracing Mobile Phone Applications.	30
<i>Georgios Magklaras and Lucia N. López-Bojórquez</i>	

Awareness and Training

Towards a Cross-Cultural Education Framework for Online Safety Awareness	47
<i>R. Herkanaidu, S. M. Furnell, and M. Papadaki</i>	
Towards an Heuristic Approach to Cybersecurity and Online Safety Pedagogy	58
<i>Simon Marsden</i>	
ContextBased MicroTraining: A Framework for Information Security Training	71
<i>Joakim Kävrestad and Marcus Nohlberg</i>	

Social Engineering

Employees' Interest in Professional Advancement on LinkedIn Increases Susceptibility to Cyber-Social Engineering: An Empirical Test	85
<i>Mohammed Khaled N. Alotaibi</i>	
Does Ubuntu Influence Social Engineering Susceptibility?	97
<i>Ntsewa B. Mokobane and Reinhardt A. Botha</i>	
Quantifying Susceptibility to Spear Phishing in a High School Environment Using Signal Detection Theory	109
<i>P. Unchit, S. Das, A. Kim, and L. J. Camp</i>	

Security Behaviour

KidsDoodlePass: An Exploratory Study of an Authentication Mechanism for Young Children 123
Esra Alkhamis, Helen Petrie, and Karen Renaud

Information Security Behavioural Threshold Analysis in Practice: An Implementation Framework 133
D. P. Snyman and H. A. Kruger

Information Security Behavior: Development of a Measurement Instrument Based on the Self-determination Theory 144
Yotamu Gangire, Adéle Da Veiga, and Marlien Herselman

Education

Addressing SME Characteristics for Designing Information Security Maturity Models 161
Bilge Yigit Ozkan and Marco Spruit

Cyber Security Education and Training Delivering Industry Relevant Education and Skills via Degree Apprenticeships 175
Ismini Vasileiou

Internet Self-regulation in Higher Education: A Metacognitive Approach to Internet Addiction 186
Dean John von Schoultz, Kerry-Lynn Thomson, and Johan Van Niekerk

End-User Security

Bayesian Evaluation of User App Choices in the Presence of Risk Communication on Android Devices 211
B. Momenzadeh, S. Gopavaram, S. Das, and L. J. Camp

Exploring Information Security and Domestic Equality 224
Marcus Nohlberg and Joakim Kävrestad

Responding to KRACK: Wi-Fi Security Awareness in Private Households 233
Jan Freudenreich, Jake Weidman, and Jens Grossklags

Usable Security

Exploring the Meaning of “Usable Security” 247
Markus Lennartsson, Joakim Kävrestad, and Marcus Nohlberg

Dyslexia and Password Usage: Accessibility in Authentication Design 259
Karen Renaud, Graham Johnson, and Jacques Ophoff

Securing User eXperience: A Review for the End-Users’
 Software Robustness 269
Panagiotis Zagouras and Christos Kalloniatis

Security Policy

SMEs’ Confidentiality Concerns for Security Information Sharing. 289
Alireza Shojaiifar and Samuel A. Fricker

Validation of an Information Privacy Perception Instrument
 at a Zimbabwean University 300
Kudakwashe Maguraushe, Adéle Da Veiga, and Nico Martins

Are We Really Informed on the Rights GDPR Guarantees? 315
Maria Sideri and Stefanos Gritzalis

Attitudes and Perceptions

“Most Companies Share Whatever They Can to Make Money!”:
 Comparing User’s Perceptions with the Data Practices of IoT Devices. 329
*Mahdi Nasrullah Al-Ameen, Apoorva Chauhan, M. A. Manazir Ahsan,
 and Huzeyfe Kocabas*

Analysis of the ‘Open Source Internet Research Tool’:
 A Usage Perspective from UK Law Enforcement 341
Joseph Williams and Paul Stephens

Critical Analysis of Information Security Culture Definitions 353
Zainab Ruhwanya and Jacques Ophoff

Author Index 367