Report on the 2nd Workshop on Human Centric Software Engineering & Cyber Security (HCSE&CS 2021)

Mohan Baruwal Chhetri
CSIRO's Data61
Australia
mohan.baruwalchhetri@csiro.au

Xiao Liu
Deakin University
Australia
xiao.liu@deakin.edu.au

Marthie Grobler
CSIRO's Data61
Australia
marthie.grobler@csiro.au

Thuong Hoang
Deakin University
Australia
thuong.hoang@deakin.edu.au

Karen Renaud
University of Strathclyde
United Kingdom
karen.renaud@strath.ac.uk

Jennifer McIntosh
Monash University
Australia
jenny.mcintosh@monash.edu

ABSTRACT

As the creators, designers, coders, testers, users, and occasional abusers of all software systems — including cyber security systems — humans should be at the centre of all design and development efforts. Despite this, most software engineering and cyber security research and practices tend to be function, data, or process oriented. In contrast, human-centric software engineering focuses on the human-centric issues critical to successful software systems' engineering. The aim of the *International Workshop on Human Centric Software Engineering & Cyber Security* (HCSE&CS) was to provide a venue for sharing research ideas and outcomes on enhanced theory, models, tools, and capability for next-generation human-centric software engineering and cyber security. The Second HCSE&CS Workshop was held on 15 November 2021 in conjunction with ASE 2021, the 36th IEEE/ACM International Conference on Automated Software Engineering. It was originally intended to be held in Melbourne, Australia but was instead held virtually due to the COVID-19 pandemic. This post-workshop report provides an overview of the aims and motivation of the workshop as well as a summary of the presentations and discussions that took place during the workshop.

1. INTRODUCTION

Humans are a key part of software development, as customers, designers, coders, testers, end-users, and even occasional abusers of software systems. Despite this, most current software engineering research and practices are function, data, or process-oriented and do not pay much attention to human-centric issues such as accessibility, usability, emotions, personality, age, gender, and culture, leading to the problem of misaligned software systems. The International Workshop on Human Centric Software Engineering and Cyber Security (HCSE&CS) serves as a venue for sharing research ideas and outcomes on enhanced theory, models, tools, and capability for next-generation human-centric software engineering that are aimed at improving software quality, user experience, developer productivity, and cost savings.

In addition, the workshop also has a special focus on cyber security. In recent years, there has been a strong push towards embedding human behaviour and cognitive perception into the design, development and deployment of cyber security solutions to ensure that they not only protect humans from the harmful after-effects of cyber security events but do so in unison with human thinking and behavioural patterns. Therefore, this workshop also solicits recent research works in the field of human-centric cyber security engineering.

HCSE&CS 2021 is the second edition of the workshop and was held in conjunction with the 36th IEEE/ACM International Conference on Automated Software Engineering (ASE 2021). HCSE&CS 2020, the first edition of the workshop was held in conjunction with ASE 2020.

The 2021 workshop solicited papers focussing on all software engineering tasks and processes during the human-centric software development lifecycle, including but not limited to:

- Human-centric modelling tools
- Human-centric requirements engineering
- Human-centric methodologies and practices
- Accessible and usable cyber security
- Incorporating human factors into requirements and design e.g., emotions, bias, personality, and culture
- Context-awareness in human-centric software (and systems) engineering
- Proactive help for modellers/designers/engineers e.g. design critics
- Impact of human factors on development processes and software teams
- Human factors considerations for engineers and developers
- Performance appraisal and software engineering tasks
- Tools and models for capturing and interpreting user behaviours
- Software applications that demonstrate the practice of human-centric software engineering
- Usable security/privacy evaluation of existing and/or proposed solutions
- Mental models that contribute to, or inform security and privacy design and deployment
- Design foundations of usable security and privacy including usable security and privacy patterns
- Modelling of security behaviours
- In-the-wild observation of security and privacy behaviour studies
- Conceptual/Position papers about the impact of the pandemic on personal privacy and security during home working

Following the call for papers, the workshop received a total of 18 submissions. After a strict review process, where each paper was peer-reviewed by at least three program committee members, eight papers were accepted for publication and presentation.

In addition to the eight presentations, the workshop also had two keynote talks and one panel discussion. This post-workshop report provides a summary of the presentations and discussions that took place at the workshop.

2. WORKSHOP SUMMARY

The workshop was originally intended to be held in Melbourne, Australia. However, due to the COVID-19 pandemic, it was moved to virtual mode (in line with the main ASE conference) and held online on 15 November 2021 using the Zoom video conference platform. It was organized as a whole-day-workshop starting at 12:00pm AEDT and finishing at 20:00pm AEDT, with presentations scheduled to accommodate the multiple timezones of the presenters. The workshop had two keynote talks, one panel discussion and eight paper presentations. In this section, we provide a brief summary of the presentations and discussions.

2.1 Keynote Talks

The workshop had two keynote talks: one focused on human-centric software engineering, and the second focused on human-centric cyber security.

Dr. Kelly Blincoe was the first keynote speaker. She is a Senior Lecturer in Software Engineering at the University of Auckland and Director of the Human Aspects of Software Engineering Lab (HASEL) in New Zealand. Her research focuses on the human aspects of software engineering, including collaborative software development, software requirements, and diversity and inclusion. Her talk was titled **Leveraging requirements from the crowd for more inclusive software**.

In her talk, Dr. Blincoe talked about recent research into leveraging online user feedback of software products to better understand user needs and identify software product improvements. She also presented some of her recent work on identifying software requirements from online feedback, the representativeness of this online feedback, and key considerations for future research in this area.

Professor George Loukas was the second keynote speaker. He is currently a Professor of Cyber Security and Head of the Internet of Things and Security Centre at the University of Greenwich, UK. Professor Loukas has held several leadership positions in international research projects, especially about involving the human as an active component of threat detection in cyber security and information trustworthiness. The title of his keynote talk was **Empowering the human as a sensor for cyber security and information trustworthiness**.

In his talk, Prof. Loukas introduced the *Human-as-a-sensor* (HaaS) paradigm, in which people are not only encouraged to participate actively in preventing but also in detecting and reporting threats against them. The same is the case for information hygiene measures that are routinely recommended for addressing disinformation in social media. Depending on the area of application, human sensors can be supported with additional information for helping them recognise threats, the technical means for reporting them, and mechanisms for predicting how reliable they are as sensors of different types of threats. Prof. Loukas explored the different solutions and remaining challenges in the use of HaaS to address semantic social engineering attacks, disinformation, and novel threats to AI systems at home.

2.2 Panel Discussion

The workshop included a panel discussion on the topic of **Fallouts from failures caused by human errors or errors in software engineering**. The panel members were Prof. Karen Renaud from University of Strathclyde, United Kingdom, Prof. Jean-Guy Schneider from Deakin University, Australia, and Associate Prof. Carsten Rudolph from Monash University, Australia.

It is well understood that an information security breach can have serious consequences for an organisation, such as loss of reputation, competitive advantage, funds, future revenue, productivity and intellectual property. Therefore, it is necessary to consider all aspects that can mitigate the risk of information security breaches. However, human errors are considered a major cause of information security breaches, be it through password sharing with colleagues, writing login information on sticky notes, sending sensitive information to the wrong person, or misconfiguring a system for example.

The panelists presented several examples from aviation, the postal service, and social media to highlight human errors in software engineering. Some of the examples discussed included (i) the Boeing 737 Max disaster due to poorly designed/tested software and the need for better regulation of the software industry, (ii) the UK Post Office scandal in which the Horizon software from Fujitsu has been shown to be responsible for unexplained accounting shortfalls across Post Office branches between 2000 and 2014 leading to the wrongful criminal conviction of more than 700 branch managers, and (iii) the Facebook outage on October 4, 2021 due to a human error in configuring the internal network, which did not get picked up by the audit tool due to a bug and led to Facebook and its subsidiaries including Messenger, Instagram, and WhatsApp become globally unavailable for 6-7 hours. Other examples discussed included the payment redirection scams due to lack of support for checking the authenticity of bank transfers (using platforms like STRIPE), as well as the COVID vaccination certificate, which could not be checked for authenticity in Australia.

Some of the strategies presented to mitigate errors included defensive coding, changing the mindset of quality assurance, and better regulation of the software industry. The panel concluded by agreeing that there is no ‘silver bullet’ to fix the problem, but it requires a multi-faceted approach including incremental changes to education, communication, and standardisation methods.

2.3 Papers

The eight papers accepted by the workshop were presented across three different sessions in the following order:

2.3.1 Session 1

The first paper in this session was **Decision-Making Biases and Cyber Attackers** by Chelsea K. Johnson, Robert S. Gutzwiller, Joseph Gervais and Kimberly J. Ferguson-Walter. In this paper, the authors examined an initial list of decision-making biases that can affect adversarial cyber actors, and presented examples of how they can be exploited by cyber attackers. Their research goal was to increase awareness of decision-making biases in cyber operational environments so that it is easier to remove the ability of cyber attackers to exploit others’ biases and to detect and mitigate biases in cyber defenders.

The second paper presented in this session was **ACSIMA: A Cyber Security Index for Mobile Health Apps** by Hamza Sellak, Mohan

Baruwal Chhetri, Marthie Grobler and Kristen Moore. In this exploratory study, the authors presented ACSIMA as a curated cyber security checklist that can be used for the cyber security assessment of mobile health apps. The authors validated ACSIMA's usability and practicability by conducting an online survey with different stakeholder groups including health professionals, app users, app developers, policy makers and researchers.

2.3.2 Session 2

The first paper presented in this session was **Oppositional Human Factors in Cybersecurity: A Preliminary Analysis of Affective States** by Kimberly J. Ferguson-Walter, Robert S. Gutzwiller, Dakota D. Scott and Craig J. Johnson. In this paper, the authors presented the findings from the preliminary analysis of survey data collected following a controlled experiment involving network penetration in which more than 130 red teamers participated. The aim of the study was to understand the cognitive and emotional state of cyber attackers and use the findings to harden system defenses.

The second paper in this session was **Virtual Reality Enabled Human-Centric Requirements Engineering** by Owen Wang, Beng Cheng, Thuong Hoang, Chetan Arora and Xiao Liu. In this paper, the authors proposed the idea of using virtual reality (VR) for human-centric requirements engineering. They presented a prototype system using a VR platform that can create 3D avatars based on user persona descriptions, simulate different environmental factors (e.g. weather condition) and user conditions (e.g. colour blindness), and embody the user perspective via the first-person view.

The third paper of Session 2 was **A Methodology for Human Centred IoT Collectives Based On Socio-Ethical Policies** by Amna Batool, Seng W. Loke, Niroshinie Fernando and Jonathan Kua. In this paper, the authors proposed a policy-based approach to manage smart, internet-connected devices so that they behave in a more human-centred manner. They presented a four-phase methodology to define and map policies to the fundamental operations of smart devices, implement the processing of the policies, and deploy the devices. They applied the methodology to a supermarket scenario for illustration.

2.3.3 Session 3

The first paper in this session was **I need to know I'm safe and protected and will check: Users Want Cues to Signal Data Custodians' Trustworthiness** by Oksana Kulyk and Karen Renaud. In this paper, the authors tested whether users cared about statements that provided assurances about their security and privacy when they were considering whether or not to divulge their personal health information to an online service. Their study suggested that people did indeed care about their privacy and wanted reassurance that companies are trustworthy custodians of their personal data.

The second paper was **Crypto Experts Advise What They Adopt** by Mohammadreza Hazhirpasand, Oscar Nierstrasz and Mohammad Ghafari. In this paper, the authors investigated whether developers who are active in cryptography discussions on forums such as Stack Overflow also actively use cryptography in their projects. The study showed that the majority of the developers use cryptography in their projects.

The third paper of the session was **Worrisome Patterns in Developers: a Survey in Cryptography** by Mohammadreza Hazhirpasand, Oscar Nierstrasz and Mohammad Ghafari. In this paper, the authors investigated the security and cryptography practices of 97 developers who have used cryptography in their projects. Their study found that although experienced developers had more background knowledge about security, had attended security and cryptography courses and used security tools in their projects, there were some worrisome patterns among all the participants including a high reliance on unreliable sources such as Stack Overflow, and a low rate of security tool usage.

All eight papers have been published by IEEE as part of the ASE'21 workshop proceedings and are now available online[1]. The authors have also been invited to consider submitting extended versions of their paper/s to the Elsevier Journal of Systems and Software (JSS) Special Issue on Human-Centric Software Engineering – Approaches, Technologies, and Applications[2].

3. CONCLUSION

The HCSE&CS Workshop provides a venue for researchers and practitioners from multiple disciplines including software engineering, cyber security, and human computer interaction to share their research ideas and outcomes in the area of human-centric software engineering and cyber security.

We are pleased to have been associated with the CORE A* ranked ASE conference for the past two years. We plan to continue our association going forward and will be organizing the 3rd International Workshop on Human Centric Software Engineering and Cyber Security (HCSE&CS 2022) in conjunction with the 37th IEEE/ACM International Conference on Automated Software Engineering (ASE 2022) in Michigan, USA.

We have tried to make the workshop an interactive one with a strong focus on discussions. The feedback we have received from the participants has been overwhelmingly positive. So We will continue to use the interactive workshop format going forward. In order to encourage more submissions and greater participation in future editions, we will solicit *Systematization of Knowledge (SoK) papers* that integrate and systematize existing knowledge on human-centric software engineering and/or cyber security and *Replication papers* that replicate important studies on human-centric software engineering and cyber security.

Acknowledgement

We would like to thank all the authors of the presented papers, the keynote speakers, the panel members, and general workshop participants for making the workshop a success. Special thanks also go to the Program Committee members for their invaluable help in reviewing the papers on time. Thanks also to the organizers of the main conference ASE 2021 for giving us the opportunity to hold our workshop in conjunction with such a prestigious conference. Last but not least, we would like to thank Dr Jacopo Soldani, the Editor-in-Chief of ACM SIGSOFT SEN, for inviting us to publish this post-workshop report in his journal.

[1] https://ieeexplore.ieee.org/xpl/conhome/9680270/proceeding

[2] https://www.journals.elsevier.com/journal-of-systems-and-software/call-for-papers/special-issue-on-human-centric-software-engineering-approaches-technologies-and-applications