2023 38th IEEE/ACM International Conference on Automated Software Engineering Workshops (ASEW) | 979-8-3503-3032-8/23/$31.00 ©2023 IEEE | DOI: 10.1109/ASEW60602.2023.00033

Report on the 4th Workshop on Human-Centric Software Engineering & Cyber Security (HCSE&CS 2023)

Mohan Baruwal Chhetri
CSIRO's Data61
Australia
mohan.baruwalchhetri@data61.csiro.au

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

Marthie Grobler
CSIRO's Data61
Australia
marthie.grobler@data61.csiro.au

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

Karen Renaud
University of Strathclyde
United Kingdom
cyber4humans@gmail.com

Chetan Arora
Monash University
Australia
chetan.arora@monash.edu.au

***Abstract*—In the domain of software design and development, humans play crucial roles as creators, designers, coders, testers, users, and, on occasion, even abusers of software systems, especially in cyber security. The *International Workshop on Human-Centric Software Engineering & Cyber Security* (HCSE&CS) focuses on human-centric concerns in software engineering and cyber security, addressing the various roles of individuals in these domains. The fourth edition of the HCSE&CS Workshop was conducted in a hybrid format and took place in Kirchberg, Luxembourg, on September 11, 2023, in conjunction with the 38th IEEE/ACM International Conference on Automated Software Engineering. This post-workshop report serves to outline the workshop's goals and motivations, while offering a concise summary of the presentations and discussions that took place during this event.**

I. Introduction

Humans play a vital role in software design and development, serving as customers, designers, coders, testers, end-users, and even, occasionally, those who misuse software systems. Nevertheless, prevailing software engineering research and practices primarily revolve around functionality, data, or process-driven approaches, often neglecting crucial human-centric aspects such as accessibility, usability, emotions, personality, age, gender, and culture. This oversight leads to the problem of misaligned software systems. The *"International Workshop on Human-Centric Software Engineering and Cyber Security"* (HCSE&CS) serves as a platform for the exchange of research ideas and outcomes that revolve around enhancing theories, models, tools, and capabilities in the domain of next-generation human-centric software engineering. The overarching goal is to enhance software quality, improve user experiences, boost developer productivity, and achieve cost savings by addressing these human-centric considerations.

In today's rapidly evolving digital landscape, cyber security is not merely a technical challenge but a profoundly human one too. In this context, the HCSE&CS workshop places a special emphasis on human-centric cyber security engineering and actively seeks papers that specifically delve into the topic of human-centric cyber security.

The fourth edition of the HCSE&CS workshop was held in hybrid format alongside the 38th IEEE/ACM International Conference on Automated Software Engineering (ASE 2023) in Kirchberg, Luxembourg on September 11, 2023. This edition of the workshop solicited papers on a wide range of human-centric software development topics including, but not limited to:

- Impact of human factors on software development teams and processes
- Human factors considerations for engineers/developers
- Incorporating human factors into requirements and design e.g., emotions, bias, personality, and culture
- Human-centric modelling tools
- Human-centric requirements engineering
- Human-centric methodologies and practices
- Context-awareness in HCSE
- Proactive help for modellers, designers, and engineers
- Human-centric applications of emerging technologies
- Accessible and usable cyber security
- Usable security/privacy evaluation of existing and/or proposed solutions
- Mental models that contribute to, or inform, security/privacy design and deployment
- Human-centric design patterns
- In-the-wild observation of security/privacy behaviour studies
- Tools and models for capturing and interpreting user behaviours
- Software applications demonstrating HCSE practices
- CS studies in developing countries
- Case studies on insider whistleblowing

- Systematisation of knowledge papers that integrate and systematise existing knowledge on HCSE and/or CS
- Replicating or extending previously published studies and experiments on human-centric security

After a thorough peer review process involving a minimum of three program committee members, the workshop accepted five papers for presentation, along with one keynote talk. The next section outlines the workshop program.

II. Workshop Summary

This year, the workshop featured a half-day event that included an onsite keynote presentation and two in-person paper presentations, alongside three remote papers presentations. This section provides a concise summary of the presentations.

A. Keynote Talk

This year's distinguished keynote speaker, Professor John Grundy, is an Australian Laureate Fellow and Professor of Software Engineering at Monash University, Australia, where he leads the *"HumaniSE"* lab. With over 25 years of influential research in human-centered software engineering, his work has been featured in prestigious conferences such as ASE, ICSE, and ESEC/FSE. Professor Grundy's leadership includes chairing flagship conferences such as ASE 2020, ASE 2021, and ICSE 2023. He is the recipient of the SIGSOFT Distinguished Service Award in 2023 for his remarkable contributions to the software engineering field.

In his talk, titled *"Human-Centred Software Engineering and Cyber Security in the Age of Generative AI"*, Professor Grundy delved into the profound impact of generative AI on HCSE&CS. His talk raised several thought-provoking considerations for the future of HCSE&CS research including:

- How generative AI can assist in realising the core principles and objectives of HCSE&CS,
- The potential impediments and challenges that generative AI might introduce into the pursuit of HCSE&CS goals,
- The specific HCSE&CS concerns arising from the integration of generative AI technologies,
- The challenges that generative AI technologies may face when applied within the realms of HCSE&CS, and
- The importance of defining future research directions and best practices that foster a productive synergy between HCSE, CS, and generative AI.

B. Papers

The five papers accepted by the workshop were presented across two sessions in the following order:

The first paper, titled *"Towards Developer-Centered Secure Coding Training"* by Vladislav Pikulin and colleagues, explores software developers' perceptions of secure coding training. Their study revealed that developers with agreeable personality traits may disregard secure coding standards, while experienced developers often request topics like storage management, responsible privilege use, security laws, and testing. Additionally, developers with higher levels of openness prefer hands-on training. These insights inform the design of adaptable secure coding programs for diverse developer backgrounds.

The second paper, titled *"DoS Attacks, Human Factors, and Evidence Extraction for the Industrial Internet of Things (IIoT) Paradigm"* by Sri Harsha Mekala and colleagues, highlights the significance of considering human factors, such as user awareness and expertise, in enhancing IIoT cyber security. The authors argue that technology alone is insufficient in combating evolving cyber threats, and emphasise on the value of combining technical frameworks like MITRE ATT&CK with human factors to protect critical industrial processes.

The third paper, titled *"Towards an Understanding of Developers' Perceptions of Transparency in Software Development: A Preliminary Study"* by Humphrey O. Obie and colleagues, explores the importance of transparency in software development. The study, involving interviews with experienced developers, highlights the fundamental role of transparency in building trust, ensuring accountability, and promoting ethical standards in software development. It also outlines the systematic processes developers follow to address transparency violations and calls for further research to comprehensively address transparency's significance in software development.

The fourth paper, titled *"Universal Design for Website Authentication"* by Jacques Ophoff and Karen Renaud, focusses on the accessibility and inclusivity of website authentication, particularly for senior citizens. Through qualitative analysis of data from 50 respondents, the study uncovers various barriers and challenges faced by senior citizens during website authentication processes. It highlights that relying on passwords for authentication poses usability challenges, leading to insecure practices and exclusion of senior users. The paper calls for a comprehensive approach to authentication standards and guidelines to enhance accessibility and inclusivity.

The fifth and final paper, titled *"A human-centric cybersecurity training tool for prioritising MSNAs"* by Vincent Depassier and Romina Torres, presents a human-centric approach to creating training scenarios for cyber security analysts, focusing on the detection and prioritisation of multi-stage and multi-step network attacks (MSNA). To address the scarcity of training datasets, the authors propose using Capture The Flag (CTF) archive data to simulate MSNA scenarios with their *"NetWars,"* tool. This tool employs gamification and human-centric principles for effective training. Usability testing and stakeholder surveys validate its effectiveness, showcasing its potential to revolutionise cyber security education and network security understanding.

Acknowledgement

We extend our gratitude to all the authors, the keynote speaker, workshop participants, and Program Committee members for their valuable contributions to this event. A special thank you is extended to the ASE 2023 organisers, particularly the ASE 2023 Workshop Chairs, for their invaluable support in facilitating the workshop's hybrid format, which significantly contributed to the success of our event.