APPS 2021: Third International Workshop on Adaptive and Personalized Privacy and Security

Argyris Constantinides

Department of Computer Science, University of Cyprus & Cognitive UX LTD, aconst12@cs.ucy.ac.cy

Marios Belk

Cognitive UX GmbH & Department of Computer Science, University of Cyprus, belk@cognitiveux.de

Christos Fidas

Department of Electrical and Computer Engineering, University of Patras, fidas@upatras.gr

Juliana Bowles

School of Computer Science, University of St Andrews, jkfb@st-andrews.ac.uk

Andreas Pitsillides

Department of Computer Science, University of Cyprus, andreas.pitsillides@cs.ucy.ac.cy

The Third International Workshop on Adaptive and Personalized Privacy and Security (APPS 2021) aims to bring together researchers and practitioners working on diverse topics related to understanding and improving the usability of privacy and security software and systems, by applying user modeling, adaptation and personalization principles. Our special focus in 2021 is on challenges and opportunities related to the Covid-19 outbreak, more specifically on ensuring security and privacy of sensitive data and secure user interactions in online systems. The third edition of the workshop includes interdisciplinary contributions from Belgium, Cyprus, Germany, Greece, Portugal, the Netherlands, and United Kingdom, that introduce new and disruptive ideas, suggest novel solutions, and present research results about various aspects (theory, applications, tools) for bringing user modeling, adaptation and personalization principles into privacy and systems security. This summary gives a brief overview of APPS 2021, held online in conjunction with the 29th ACM Conference on User Modeling, Adaptation and Personalization (ACM UMAP 2021).

CCS CONCEPTS • Human-centered computing • Security and privacy.

Additional Keywords and Phrases: Security, Privacy, Usability, Trust, User-centric Systems.

ACM Reference Format:

Argyris Constantinides, Marios Belk, Christos Fidas, Juliana Bowles, and Andreas Pitsillides. 2021. APPS 2021: Third International Workshop on Adaptive and Personalized Privacy and Security. In Adjunct Publication of the 29th ACM

Conference on User Modeling, Adaptation and Personalization (UMAP '21 Adjunct). Association for Computing Machinery, New York, NY, USA.

1 Introduction

Information and security systems encompass concepts and methods for the protection of sensitive information. In this context, millions of users worldwide are daily engaged with privacy and security tasks that commonly relate to user authentication, human interaction proofs (*e.g.*, captcha), and setting privacy and security features in online user profiles to name a few. Recent privacy and security breaches and incidents of widely used online services, as well as notable challenges due to the Covid-19 outbreak (*e.g.*, the need for touchless authentication, distance learning, access to e-Government services), have once more underpinned the need for further investigation and improvement of current approaches related to the design of efficient and effective privacy and security. A possible direction to achieve this objective relates to providing adaptive and personalized characteristics to privacy- and security-related user tasks, given the diversity of the user characteristics (*e.g.*, culture, cognition), the technology (*e.g.*, standalone, mobile, wearables) and interaction context of use (*e.g.*, being on the move, social settings). Hence, adaptive and personalized privacy and security implies the ability of an interactive system or service to support its end-users, who engage in privacy- and/or security-related tasks, based on user models that describe holistically the user's physical, technological and interaction context of use.

APPS 2021 aims to connect researchers and practitioners working on diverse topics related to understanding and improving the usability of privacy and security systems, by applying user modeling, adaptation and personalization principles. *Our special focus in 2021 is on challenges and opportunities related to the Covid-19 outbreak, more specifically on ensuring security and privacy of sensitive data and secure user interactions in online systems.* The workshop addresses the following objectives:

- increase our understanding and knowledge on supporting usable privacy and security interaction design through novel user modeling mechanisms and adaptive user interfaces;
- discuss methods and techniques for understanding user attitudes and perceptions towards privacy and security issues in various application areas;
- identify human-centered models for the design, development and evaluation of adaptive and personalized privacy and security systems;
- discuss methods for evaluating the impact and added value of adaptation and personalization in privacy and security systems.

2 Workshop Topics of Interest

The workshop focuses on the following topics of interest:

- Adaptation and personalization approaches in usable privacy and security;
- Effects of human factors (e.g., cognition, personality, etc.) in privacy and security systems;
- Novel user interaction concepts and user interfaces for achieving usable security;
- Cultural diversity in usable privacy and security;
- Context-aware privacy and security;
- Adaptive usable security in various domains (e.g., e-Learning, e-Government, IoT, healthcare, etc.);
- Adaptive user authentication policies;
- Novel approaches to the design and evaluation of usable security systems;
- Lessons learned from the deployment and use of usable privacy and security features;
- Ethical considerations in adaptive and personalized privacy and security.

3 Workshop Program

The workshop is held as a half-day virtual event. The program starts with a short introduction provided by the workshop organizers and invited talks from researchers working on areas related to the area of APPS. The main workshop includes oral presentations by authors of accepted full papers and short papers, followed by questions and discussion on each paper. This year's edition consists of two tracks: *i)* main track on adaptive and personalized privacy and security; and *ii)* focused track on challenges and opportunities related to the Covid-19 outbreak for ensuring security and privacy of sensitive data and secure user interactions in online systems. The main program has been shaped as follows:

- *Invited talks. (i)* **Florian Alt** (Bundeswehr University Munich, Germany): Out-of-the-Lab Research in Usable Security and Privacy; *(ii)* **Nikos Komninos** (City, University of London, United Kingdom): Preserving Privacy of Data with Efficient Attribute Based Encryption Schemes; and *(iii)* **Christos Fidas et al.** (University of Patras, Greece): Privacy-preserving Biometric-driven Data for Student Identity Management: Challenges and Approaches.
- *Full papers. (i)* **Ivana de Boer et al.** (Radboud University, the Netherlands): The Illusion of Control in Privacy Trade-Offs: Does Familiarity Play a Role?
- *Short papers. (i)* **Hossein Abroshan et al.** (Ghent University, Belgium): A Phishing Mitigation Solution using Human Behaviour and Emotions that Influence the Success of Phishing Attacks; *(ii)* **Matthew Banton et al.** (University of St Andrews, United Kingdom): On the Benefits and Security Risks of a User-centric Data Sharing Platform for Healthcare Provision; and *(iii)* **Christodoulos Constantinides et al.** (University of Cyprus, Cyprus): A Comparative Study among Different Computer Vision Algorithms for Assisting Users in Picture Password Composition.

4 Workshop Organization

The workshop consists of the following chairs and members of the international program committee:

4.1 Workshop Chairs

Argyris Constantinides (University of Cyprus, Cyprus & Cognitive UX LTD, Cyprus), **Marios Belk** (Cognitive UX GmbH, Germany & University of Cyprus, Cyprus); **Christos Fidas** (University of Patras, Greece); **Juliana Bowles** (University of St Andrews, United Kingdom); **Andreas Pitsillides** (University of Cyprus, Cyprus).

4.2 International Program Committee

We appreciate the reviewers' efforts, comments, and suggestions, and would like to thank the international program committee members for their valuable support.
Esma Aïmeur (University of Montreal, Canada); **Marios Constantinides** (Nokia Bell Labs, United Kingdom); **George Hadjidemetriou** (University of Twente, the Netherlands); **Eelco Herder** (Radboud University, the Netherlands); **Vladimir Janjic** (University of Dundee, United Kingdom); **Georgia Kapitsaki** (University of Cyprus, Cyprus); **Axel Legay** (Université Catholique de Louvain, Belgium); **Michael Rossbory** (Software Competence Center Hagenberg, Austria).

ACKNOWLEDGMENTS

The work has been partially supported by the EU Horizon 2020 Grant 826278 "Securing Medical Data in Smart Patient-Centric Healthcare Systems" (Serums), and by a new European project, TRUSTID - Intelligent and Continuous Online Student Identity Management for Improving Security and Trust in European Higher Education Institutions, which is funded by the European Commission within the Erasmus+ 2020 Programme.