HCI International 2019

21st International Conference
on Human-Computer Interaction
Walt Disney World Swan and Dolphin Resort
Orlando, Florida, USA
26 - 31 July 2019

http://2019.hci.international/

ADVANCE CALL FOR PARTICIPATION

HCI-CPT 2019

1st International Conference on HCI for Cybersecurity, Privacy and Trust

Jointly held under one management and one registration with HCI International 2019

Chair: Abbas Moallem

The Cybersecurity field, in all its dimensions, is exponentially growing, evolving and expanding. New security risks emerge with the continuous increase of Internet interconnections and the development of the Internet of Things. Cyberattacks endanger individuals and companies, as well as vital public services and infrastructures. Confronted with spreading and evolving cyber threats, organizations and individuals are falling behind in defending their systems and networks, and they often fail to implement and effectively use basic cybersecurity and privacy practices and technologies.

Successful security depends on companies and governments collaborating to identify threats, weaknesses and solutions. In this context, users have been identified as one of the major security weaknesses in today's technologies, as they may be unaware that their behavior while interacting may have security consequences. However, if users are to be considered as one of the greatest risks to system security, they are also one of the greatest hopes for system security. In this perspective, Human – Computer Interaction (HCI) becomes a fundamental pillar for designing more secure systems. By considering the user—what they know, how they use the system, what their needs are—designers will be better positioned to empower them in their digital security role, and increase the usability of security solutions.

The 1st International conference on HCI for cybersecurity, privacy, and trust (HCI-CPT) intends to help, promote and encourage research in this field by providing a forum for interaction and exchanges among researchers, academics, and practitioners in the fields of HCI and cyber security. The Conference addresses HCI principles, methods and tools in order to address the numerous and complex threats which put at risk computer-mediated human-activities in today's society, which is progressively becoming more and more intertwined with and dependent on interactive technologies.

The related topics include, but are not limited to:

- **Authentication and identification:** Adaptive access control; Context-aware authentication and authorization; Frictionless authentication; Security and usability of combinations of authentication factors; Remote identity proofing; Privacy implications of authentication technologies; Obtaining informed consent in the federated login; Preservation of privacy in the federated login; Security and usability of derived credentials; Web of trust
- **Biometrics:** Privacy and security implications of biometric architectures; Detection of biometric presentation attacks; Emerging biometric modalities; Fusion of biometric modalities; Behavioral biometrics; Revocable biometrics
- **Applications of cryptography to cybersecurity, privacy, and trust:** Cryptographic authentication; Applications of anonymous credentials and group signatures; Identification with selective disclosure of attributes; Mitigation of fraudulent credential sharing; Usability of TLS client certificates; Usability of encrypted messaging; BYOK: Bringing your own key to the cloud
- **Human factors:** User acceptance of security and privacy technologies; Identification through peer-to-peer vouching; End-user best practices for malware avoidance; Mitigation of phishing attacks; Mitigation of social engineering attacks; Mitigation of insider threats; Behavior-based cybersecurity; Communication of security risks to end-users; Human identification of websites; Human detection of trusted execution; Non-repudiation and repudiability; Behavior-based cybersecurity; User awareness of privacy threats
- **Cybersecurity, privacy and trust in computing areas:** Web technologies; Mobile computing; Cloud computing; Enterprise computing; Peer-to-peer networking; Blockchains, distributed ledgers, and gossip protocols; Internet of Things; SCADA: Supervisory control and data acquisition; Ubiquitous computing; VR/AR systems
- **Cybersecurity, privacy and trust in application areas:** Electronic payments; Social networks; Smart cities; Connected Cars and Autonomous Driving; Smart home; Healthcare and patient monitoring; Wearables; Smart environments
- **Legal, ethical, economic and societal issues in cybersecurity:** Ethnic bias in face recognition accuracy; Trust frameworks; Tracking; Privacy by design & default; Fake news; Bots in social networks; Cyberwarfare; Attacks against elections; Surveillance; Money laundering and black markets; User privacy and data protection regulations; Big data impact on user privacy

Conference proceedings published by

Springer