Journal of Universal Computer Science, vol. 24, no. 4 (2018), 338-340
submitted: 16/4/18, accepted: 20/4/18, appeared: 28/4/18 © J.UCS

Advances in Security and Privacy of Multimodal Interfaces

J.UCS Special Issue

Robertas Damaševičius
(Kaunas University of Technology, Kaunas, Lithuania
robertas.damasevicius@ktu.lt)

Marcin Woźniak
(Silesian University of Technology, Gliwice, Poland
Marcin.Wozniak@polsl.pl**)**

Vicente Alarcon-Aquino
(Universidad de las Américas Puebla, Mexico
vicente.alarcon@udlap.mx)

Ivan Ganchev
(University of Limerick, Ireland / Plovdiv University "Paisii Hilendarski", Bulgaria
ivan.ganchev@ul.ie)

Wei Wei
(Xi'an University of Technology, China
WeiWei@xaut.edu.cn)

With the rapid development and increasing complexity of communication systems and interfaces using multiple modalities of communication in human-computer systems such as speech, tactile, gestures, gaze, head and body movements, facial expressions, gait, electroencephalogram (EEG) and electromyogram (EMG) signals, the user requirements for trust, security, and privacy are becoming more demanding. The main objective of this special issue was to provide a forum for researchers interested in the latest research results in the rapidly developing field of security and privacy in multimodal interfaces, therefore providing a valuable information venue to researchers as well as practitioners.

In particular, papers on access control, privacy protection, and secure communication in multimodal interfaces, advanced multimodal interfaces for security, authentication and authorization mechanisms using human behavior data for man-machine interactions, biometric authentication systems and applications for assistive technologies, cryptography and encryption techniques for human behavior data, data privacy and security in physiologic & affective computing, human and social factors of security and privacy in man-machine interactions, identity management using physiological and behavioral characteristics, multimodal interfaces for secure sensitive applications in e-health and m-health, privacy and security in emotionally intelligent

dialog systems, security of natural user interfaces, security, privacy, and trustworthiness in Assisted Living / Enhanced Living environments, security, reliability, and performance in biometrics systems, trust management for multimodal interfaces, voice biometrics for user authentication were invited.

Combining cryptography and biometrics in a secure way can ensure privacy protection and secure communication as demonstrated by Alawi A. Al-Saggaf in "Secure Method for Combining Cryptography with Iris Biometrics".

Multimodal interfaces often use computer vision techniques to track body and limbs, hand gestures and detect face expressions from image processing algorithms, which ensure high level of security and privacy such as "The Bag-of-Words Method With Different Types of Image Features and Dictionary Analysis" described by Marcin Gabryel.

As many of IT services are moving to cloud, cloud biometric authentication can be applied to increase security and reliability as suggested in "Cloud Biometric Authentication: An Integrated Reliability and Security Method Using the Reinforcement Learning Algorithm and Queue Theory" by A. M. N. Balla Husamelddin, Guang Sheng Chen and Weipeng Jing.

In multimodal heterogeneous environments, hybrid access control models can be used as, for example, in "A New Hybrid Access Control Model for Security Policies in Multimodal Applications Environments" by Hasiba Ben Attia, Laid Kahloul and Saber Benharzallah.

Another behavioral authentication system, working on sparse geographical data generated by mobile devices, is described in "Large Scale Mobility-based Behavioral Biometrics on the Example of the Trajectory-based Model for Anomaly Detection" by Piotr Kałużny and Agata Filipowska.

Audio processing domain is another venue of multimodal interface system which face the privacy and security challenges. Audio records can be used for identity verification as described in "How to Extract Interesting Information for Identity Verification Process from Spectrograms?" by Kamil Książek, Karolina Kęsik and Zbigniew Marszałek.

Identity verification can be performed both on voice sample and on iris images as shown in "Model of Identity Verification Support System Based on Voice and Image Samples" by Dawid Połap.

Developing a path finding system for visually impaired people in the context of assisted living environment is described in "Real Time Path Finding for Assisted Living Using Deep Learning" by Ugnius Malūkas, Rytis Maskeliūnas, Robertas Damaševičius and Marcin Woźniak.

As modern multimodal interfaces often include multi-party communication and exchange of data between parties, applications that use encryption of information require special algorithms of sorting data in order to preserve the secrecy of the information, which is analyzed in "Parallel Fast Sort Algorithm for Secure Multiparty Computation" by Zbigniew Marszałek.

On a hardware level, multimodal systems usually run on embedded systems, which are subjected to various adversaries including software attacks, physical attacks, and side channel attacks. Most of these malicious attacks can lead to the invalid execution of programs, and launch of destructive actions or reveal critical

information. However, most previous security mechanisms suffer from coarse checking granularity and unacceptable performance overhead, due to strict restriction on system resources. To address this problem, in „A Fine-Grained Hardware Security Approach for Runtime Code Integrity in Embedded Systems“, Xiang Wang, Weike Wang, Bin Xu, Pei Du, Lin Li and Muyang Liu presented a fine-grained hardware-based security approach to ensure runtime code integrity in the embedded systems by offline profiling of software features and runtime integrity check.

Finally, in „Design of Computational Intelligence Based Language Interface for Human-Machine Secure Interaction“ Marcin Woźniak, Dawid Połap, Robertas Damaševičius and Wei Wei presented a model for language processing to verify some basic aspects of correctness in human-machine secure interaction.

Acknowledgements

To conclude, the editors would like to thank the members of the program committee and all the reviewers for their care and time in reviewing and selecting the submitted papers. We also would like to thank all the authors of submitted papers, including those authors of papers which could not be included in this special issue. Finally, the special issue editors thank Dana Kaiser and the Managing Editor Christian Gütl at J.UCS for their considerable efforts and patience in co-ordinating the production of this special issue.

Robertas Damaševičius
Marcin Woźniak
Vicente Alarcon-Aquino
Ivan Ganchev
Wei Wei
April 2018