Call for Paper

Invited Session: (IS50) Emerging Technologies, Challenges and Solutions for Zero Trust

27th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems

We are pleased to announce that the KES 2023 conference will take place in the stunning city of Athens, Greece as a conference, organised by KES International.

The conference will be held in the breath-taking Royal Olympic Hotel, located within the centre of the city. The venue directly overlooks the Temple of Zeus and National Garden, with grand views of Acropolis and other archaeological sites. Its rooftop terrace provides the perfect viewing platform to see the city in all of its natural beauty.

One of the world's oldest cities, the city of Athens lies within the heart of Greece and is widely referred to as the 'birthplace of democracy', where ancient philosophers would share their knowledge and findings. It homes many ancient monuments, including the Acropolis, the Pantheon and the Ancient Agora. Rich in culture and artwork, it is also the home of the modern Olympic game and was named the European Capital of Innovation in 2018.

The conference will consist of keynote talks, oral and poster presentations, invited sessions and workshops, on the applications and theory of intelligent systems and related areas.

Title of Session:

(IS50) Emerging Technologies, Challenges and Solutions for Zero Trust

Name and Affiliation of Chair:

Kuo-Hui Yeh, National Dong Hwa University, Hualien 974301, Taiwan

Shi-Cho Cha, National Taiwan University of Science and Technology, Taipei 106335, Taiwan
Hsing-Kuo Pao, National Taiwan University of Science and Technology, Taipei 106335, Taiwan
Hsin-Chin Liu, National Taiwan University of Science and Technology, Taipei 106335, Taiwan
Nai-Wei Lo, National Taiwan University of Science and Technology, Taipei 106335, Taiwan

Details of Session:

Recently, more and more organizations have embraced the zero-trust technologies due to minimizing risk in enforcing accurate, least privilege per-request access decisions in service applications under the circumstance of a compromised network. In a zero-trust architecture, each access request should be authenticated and evaluated whether the request is permitted no matter it originated from external or internal network. In addition, unauthorized people from utilizing devices of authorized users to intrude other devices for lateral movement. Organizations need to evaluate trustworthiness of access requests based on user behaviours and threat intelligence and adapt associated access control policies. To date, the research community has stressed the importance of innovative technologies and integrated solutions for zero-trust.

This session solicits original and high-quality works on recent advances on the innovative technologies, challenges and solutions for zero-trust. We aim to enhance the current state of development of zero-trust technologies including algorithms, methodologies, frameworks to evaluate risk of access requests for achieving zero trust and accordingly reduce potential cybersecurity risks. Topics of interest include, but are not limited to:

- Trust evaluation algorithm for zero-trust
- Cyber threat intelligence for zero-trust
- Edge device risk evaluation for zero-trust
- Emerging innovative access control for zero-trust
- Access policies and selective restrictions for zero-trust
- Novel theories, architectures, applications and paradigms with zero-trust
- Practices and experiences for zero-trust architecture
- Security modelling for zero-trust architecture
- Privacy enhanced technologies for zero-trust
- Effectiveness evaluation and benchmark of zero-trust technologies
- Advances in the use of zero-trust underlying technologies (e.g., AI, blockchain, deterministic networks, cloud/edge computing, etc.)
- Miscellaneous issues for zero-trust

Information for Authors (http://kes2023.kesinternational.org/submission.php)

Papers are invited for KES2023 on topics lying within the scope of the conference. All contributions must be of high quality, original, and must not have been previously published elsewhere or intended for publication elsewhere. All papers will be reviewed by members of the International Programme Committee and depending on their level and attributes, may be selected for oral or poster presentation, and publication in the conference proceedings.

Full papers will be reviewed by the IPC and if accepted and presented, they will be published in Elsevier's Procedia Computer Science open access journal, available in ScienceDirect and submitted to be indexed/abstracted in CPCI (ISI conferences and part of Web of Science), Engineering Index, and Scopus.

Authors of selected papers may be invited to submit extended versions of their papers for publication as full journal papers, such as KES Journal or some special issues (please refer to the below list) of prestigious journals.

- Special Issue on Cyber Security Challenges and Opportunities of IoT and Cyber-Pyhsical Systems in Quantum Era, Turkish Journal of Electrical Engineering and Computer Sciences, https://journals.tubitak.gov.tr/elektrik/news.html
- Special Issues in application (IEEE Internet of Things Journal, Symmetry, etc.)

Submission Instructions
Submissions for the conference must be made as complete papers (there is no abstract submission stage) submitted as PDF documents through the PROSE online submission and review system.

Full papers should be detailed academic articles in conventional format. The guide length for full papers is 8 to 10 pages (maximum).

- Guidance notes for the preparation of Full Papers is available here
- An MS Word template is available (6.4Mbyte .zip archive). here
- A LaTeX template is available (5.7Mbyte .zip archive). here
- The paper format as a PDF document is available. here
- Please consult important FAQs about document preparation to be found. here

Important Dates:

Submission of Papers: 5th May 2023
Notification of Acceptance: 20th May 2023
Final paper publication files to be received by: 29th May 2023
Authors Registration Deadline: 29th May 2023

Website URL of Call for Papers:

IS50: Emerging Technologies, Challenges and Solutions for Zero Trust
http://kes2023.kesinternational.org/cmsISdisplay.php
http://kes2023.kesinternational.org/cms/userfiles/is50.pdf

Email & Contact Details:

Any questions regarding this invited session can be sent to Prof. Kuo-Hui Yeh (khyeh@gms.ndhu.edu.tw).

Biographies of Chairs:

Kuo-Hui Yeh (SM’16) is a full Professor with the department of Information Management, National Dong Hwa University, Hualien, Taiwan. He received M.S. and Ph.D. degrees in Information Management from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2005 and 2010, respectively. Dr. Yeh has authored over 100 articles in refereed journals and conferences. His research interests include IoT security, Blockchain, mobile security, NFC/RFID security, authentication, digital signature, data privacy and network security. Dr. Yeh is currently an Associate/Academic Editor of the Journal of Information Security and Applications (JISA), Symmetry, Security and Communication Networks (SCN), Mobile Information Systems (MISY), the Journal of Internet Technology (JIT), the Journal of Surveillance, Security and Safety (JSSS), Foundations, Research Reports on Computer Science and Frontiers in Communications and Networks – Security, Privacy and Authentication. In addition, he has served as an Associate Editor for IEEE Access and Data in Brief and a Guest Editor for Future Generation Computer Systems (FGCS), Cloud Computing, IEEE Access, Annals of Telecommunications, CMC-Computers, Materials & Continua, Mathematical Biosciences and Engineering (MBE), and the International Journal of Information Security (IJIS), JIT, Sensors and Cryptography. Moreover, Dr. Yeh has served as a TPC member for 50 international conferences/workshops on information security. He is a Senior Member of the IEEE and a Member of the (ISC)2, ISA, ISACA, CAA, CCISA, as well as holds CISSP, CISM, Security+, ISO 27001 LA, ISO 27701 LA and IEC 62443-2-1 LA certifications.

Shi-Cho Cha (SM’17) received the B.S. and Ph.D. degrees in information management from National Taiwan University, in 1996 and 2003, respectively. He is currently a professor and department chair with the Department of Information Management, National Taiwan University of

Science and Technology (NTUST), where he has been a faculty member since 2006. He is also the director of the information security center, NTUST. He is a certified PMP, CISSP, CSSLP, CCFP, and CISM. From 2003 to 2006, he was a Senior Manager with PricewaterhouseCoopers, Taiwan. His current research interests include security and privacy of blockchain applications, IoT security and privacy, and information security.

Hsing-Kuo Pao (Kenneth) received the bachelor degree in mathematics from National Taiwan University, and M.S. and Ph.D. degrees in computer science from New York University. From 2001 to 2003, he was a post-doctorate research fellow in the University of Delaware, and later he joined in Vita Genomics as a research scientist. In 2003, he joined the department of computer science and information engineering in National Taiwan University of Science and Technology, and now a professor and chairman in the department. His current research interests include machine learning methodology and its applications such as IoT analytics, computer vision and information security.

Hsin-Chin Liu received the B.S. degree in communication engineering from National Chiao Tung University, Taiwan, and the M.S. and Ph.D. degree in electrical engineering from the Pennsylvania State University, University Park, PA, USA. He has been an engineer with Taiwan Alcatel, Taiwan Siemens, and National Dong Hwa University, Taiwan. In 2003, he was an assistant professor in the department of electrical engineering, National University of Kaohsiung, Taiwan. He joined the department of electrical engineering, National Taiwan University of Science and Technology, Taiwan since 2004, and now a professor in the department. His current research interests include wireless communications, IoT, smart antennas, RFID, localization, physical layer security, machine learning, and signal detection.

Nai-Wei Lo received the B.S. degree in engineering science from National Cheng Kung University, Tainan, Taiwan, in 1988, and the M.S. and Ph.D. degrees in computer science and electrical engineering from The State University of New York, Stony Brook, NY, USA, in 1992 and 1998, respectively. He was the Director of the Taiwan Information Security Center, National Taiwan University of Science and Technology (TWISC@NTUST), from 2014 to 2018. He is currently a Full Professor with the Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan. He has published over 140 peer-reviewed articles and book chapters. His current research interests include blockchain security, IoT/RFID security, cloud security, crowdsensing, and web technology. He has been serving as a Board Member of the Chinese Cryptology and Information Security Association, Taiwan, since 2015. He was a recipient of the 2017 NTUST Outstanding Teacher Award, the 2018 NTUST Excellent Research Scholar Award, and the 2012 IBM Faculty Award. He is currently an Associate Editor of the Journal of Information Security and Applications.