2021 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W) | 978-1-6654-3950-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/DSN-W52860.2021.00008

International Workshop On Application of Intelligent Technology in Security — AITS 2021

Xiaofeng Lu
School of Cyberspace Security
Beijing University of Post and Telecommunications
Beijing, China
luxf@bupt.edu.cn

Pietro Lio
Computer Laboratory
University of Cambridge
United Kingdom
pl219@cam.ac.uk

On behalf of the Organizing Committee, it is our pleasure to welcome you to the International Workshop on Application of Intelligent Technology in Security (AITS). AITS workshop will be held in conjunction with the 51th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) on 21 June 2021.

With the development of the Internet, cyber security becomes more and more important. Facing the increasingly cyber-attack, the traditional methods to protect the information system are becoming lagging and powerless. Fortunately, artificial intelligent technology offer a completely new and challenging opportunity to the security practitioners. Cyber security intelligent analytics is among one of the fastest growing interdisciplinary fields of research bringing together researchers from different fields such as information security studies, criminology, cyber security, big data analytics, machine learning, etc. to detect, contain and mitigate advanced persistent threats and fight against malicious cyber activities (e.g. organized cyber crimes and state-sponsored cyber threats).

The aim of Internet Workshop on Application of Intelligent Technology in Security (AITS 2021) is to provide a platform to the researchers and practitioners from both academia as well as industry to meet and share knowledge and results in theory, methodology and applications in cyber security using intelligent technology, such as machine learning and deep learning. The workshop looks for significant research results, projects, surveying works and industrial experiences in cyber security fields, using intelligent technology to deal with emerging security threats.

The workshop features two sessions, including 10 research papers. We received 20 regular paper submissions this year, of which we accepted 9 regular papers and 1 short paper. The papers were selected by the program committee based on reviews and online discussion – each paper was reviewed by three or four PC members. The workshop sessions are organized as follows:

The first session presents research papers on *vulnerability detection and attack detection*. The titles of the papers are: “BBregLocator: A vulnerability detection system based on bounding box regression”, “Automatically Constructing Peer Slices via Semantic- and Context-Aware Security Checks in the Linux Kernel”, “Detection Algorithm of the Mimicry Attack based on Variational Auto-Encoder”, “Network Intrusion Detection Based on Active Semi-supervised Learning” and “A Statistical Learning Model with Deep Learning Characteristics”. The second session presents research papers on *IoT and traffic security*. The titles of the papers are: “Whether the sensitive information statement of the IoT privacy policy is consistent with the actual behavior”, “Sensitive Instruction Detection Based on the Context of IoT Sensors”, “Insight into traffic security: A correlation discovery of urban spatial features and traffic flow patterns”, “Authenticating Mobile Wireless Device Through Per-packet Channel State Information” and “Ant Hole: Data Poisoning Attack Breaking out the Boundary of Cluster”.

We would like to thank the program committee members for their collective efforts in reviewing the papers, and for helping us develop the workshop program. Moreover, we would like to thank the organizers of the DSN conference for their help and support of the AITS workshop and the community for their valued contributions to the workshop.

Program Committee:

Yuqing Zhang, University of the Chinese Academy of Sciences
Shouling Ji, Zhejing University
Guangquan Xu, Tianjin University
Shengwei Yi, China Information Technology Security Evaluation Center
Cheng Huang, Sichuan University
Gang Wang, Nankai University
Zhanyong Tang, Northwest University
Yulai Xie, Huazhong University of Science and Technology
Benhui Chen, Dali University
Yongkai Fan, china university of petroleum
Anmin Fu, Nanjing University of Science and Technology
Qixu Liu, Chinese Academy of Sciences
Junfeng Tian, Hebei University
Zhenchao Zhu, Southeast University
Guangxia Xu, Chongqing University of Posts and Telecommunications

Juhua Pu, Beihang University
Zhiwen Pan, Chinese Academy of Sciences