Title:

Applications of Machine Learning in Cyber Security

Abstract:

Machine Learning techniques are increasingly used in the field of Security. They are applied to solve quite different problems, ranging from Intrusion Detection to Biometric Authentication, from Code Analysis to Network Traffic analysis, and in many privacy-related scenarios.

Furthermore, the support of Machine Learning algorithms is becoming essential as security problems face an increasing complexity in terms of the amount of data that needs to be analyzed and of the number and diversity of the attacks and vulnerabilities that need to be detected.

This workshop aims at providing such forum for researchers, practitioners and developers from different background areas such as artificial intelligence, data mining, machine learing, information security and privacy protection, to exchange the latest experience, research ideas and synergic research and development related with the design and usage of Machine Learning techniques and algorithms in Cyber Security.

Scope and Topics:

The objective of this workshop is to invite authors to submit original manuscripts that demonstrate and explore current advances in all aspects of machine learning and its security applications. The workshop solicits novel papers on a broad range of topics, including but not limited to:

- ✧ machine learning to advance cyber security analytics
- ✧ deep learning applied to security and privacy
- ✧ machine learning for malware analysis and classification
- ✧ machine learning for anomaly detection
- ✧ biometric authentication
- ✧ machine learning for discovering vulnerabilities and attacks
- ✧ machine learning used for large scale security analysis
- ✧ privacy-preserving machine learning
- ✧ privacy-preserving classifier learning
- ✧ machine Learning on Encrypted Data
- ✧ learning in presence of a Security adversary

Program Committee Chairs:

Zhiping Cai, National University of Defense Technology, China
zpcai@nudt.edu.cn
http://individual.utoronto.ca/zcai/
Dr. Zhiping Cai is a full Professor in Computing Science Department, College of Computer, National University of Defense Technology (NUDT) at Changsha, China. Zhiping Cai received his bachelor's, master's and Ph.D degree in computer science and technology with honor from NUDT in July 1996, April 2002 and December 2005, respectively. His doctoral dissertation has been rewarded with the Outstanding Dissertation Award of the Chinese PLA. Zhiping Cai's current research interests include Network Security, SDN and Network Virtualization. He serves as a referee of paper review for the ToN, TPDS, ComNet and serves on many conference program committees. He is a senior member of China Computer Federation. Zhiping Cai received the Silver Awards for Education from the Chinese PLA in July 2009. He has published over 140 academic papers which achieve 2000 plus citations according to Google Scholar. He has also received several best paper awards in the international conferences.

Daniel Xiapu Luo, Hong Kong Polytechnic University, Hong Kong
csxluo@comp.polyu.edu.hk
http://www4.comp.polyu.edu.hk/~csxluo/
Daniel received his B.S. in Communication Engineering and M.S. in Communications and Information Systems from Wuhan University. He obtained his Ph.D. degree in Computer Science from the Hong Kong Polytechnic University, under the supervision of Prof. Rocky K.C. Chang. After that, Daniel spent two years at the Georgia Institute of Technology as a post-doctoral research fellow advised by Prof. Wenke Lee. His current research interests include Mobile Security and Privacy, Network Security and Privacy, Software Engineering, Blockchain, Internet Measurement, and Cloud Computing.

Program Committee:

Chengchen Hu, Xi'an Jiaotong University, Xi'an, China
Kai Zheng, Huawei Technologies, Shenzhen, China
Yang Xu, New York University, New York, USA
Qiang Fu, Victoria University of Wellington, Wellington, New Zealand
Mohammad Mannan, Concordia University, Canada
Samuel Marchal, Aalto University, Finland
Tatsuya Mori, Waseda University, Japan
Adwait Nadkarni, North Carolina State University, USA
Shirin Nilizadeh, University of California, Santa Barbara, USA

Arthur Gervais, ETH Zurich, Switzerland
Feng Hao, Newcastle University, UK
Andrei Homescu, Immunant, Inc., USA
Tibor Jager, Ruhr-Universität Bochum, Germany