

Machine Learning and Cyber Threat Intelligence and Analytics: An Overview and Introduction to the Mini-Track

Kim-Kwang Raymond Choo
University of Texas at San Antonio
raymond.choo@fulbrightmail.org

Ali Dehghantanha
University of Guelph
adehghan@uoguelph.ca

Glenn Dietrich
University of Texas at San Antonio
Glenn.Dietrich@utsa.edu

Abstract

Cyber threat intelligence and analytical solutions, such as those leveraging machine learning techniques, can help organizations to perceive, reason, learn and defend against sophisticated cyber attackers or advanced persistent threat actors (e.g., nation states), as well as facilitating the collection, preservation and analysis of evidence (also referred to as cyber / digital forensics) that may then be used to identify and prosecute the perpetrators. However, given the dynamic nature of the cyberthreat landscape, it is important to keep pace and design innovative solutions to mitigate the evolving threats. This is the focus of the ‘Machine Learning and Cyber Threat Intelligence and Analytics’ mini-track. In this introduction article, we will describe the three accepted papers contributed by researchers from Universität Würzburg (Germany), Mayachitra Inc (United States), U.S. Naval Research Laboratory (United States), Sam Houston State University (United States), University of Nebraska Omaha (United States), and University of South Alabama (United States).

1. Introduction

Cyber security remains one of the top policy and national security agenda items in U.S., and many technologically advanced nations such as the other four Five Eyes nations (i.e., Australia, Canada, New Zealand, and the United Kingdom). For example, Cyber and Technical Operations is listed as one of the five strategic objectives / critical areas in the recently released National Counterintelligence Strategy of the United States of America, 2020-2022 [1]. The Australian Government has also recently committed in their cyber security strategy 2020 to “invest \$1.67 billion over 10 years to achieve [the] vision of creating a more secure online world for Australians, their businesses and the essential services upon which we all depend” [2].

The importance of cyber threat intelligence in our digitalized society is also partly evidenced by the interest in this mini-track, since it was first introduced in HICSS 2018 ([3], [4], [5]).

In this year, we accepted three papers contributed by researchers from Universität Würzburg (Germany), Mayachitra Inc (United States), U.S. Naval Research Laboratory (United States), Sam Houston State University (United States), University of Nebraska Omaha (United States), and University of South Alabama (United States).

The three accepted papers are as follows:

- (1) A Meta-Model for Real-Time Fraud Detection in ERP Systems, by Anna Fuchs, Kevin Fuchs, Fabian Gwinner, and Axel Winkelmann
- (2) Malware Detection Using Frequency Domain-Based Image Visualization and Deep Learning, by Tajuddin Manhar Mohammed, Lakshmanan Nataraj, Satish Chikkagoudar, Shivkumar Chandrasekaran, and B.S. Manjunath
- (3) Deception Detection Using Machine Learning, by Alberto Alejandro Ceballos Delgado, William Glisson, Narasimha Shashidhar, Jeffrey McDonald, George Grispos, and Ryan Benton

2. Concluding Remarks

In addition to the topics discussed in these three accepted papers, there are several other topics of relevance and importance our cyber and national security conversation, such as the following:

- Blockchain and its application in cyber security
- Detection and analysis of advanced threat actors tactics, techniques and procedures
- Application of machine / deep learning tools and techniques in cyber threat intelligence

- Theories and models for detection and analysis of advanced persistent threats
- Automated and smart tools for collection, preservation and analysis of digital evidences
- Threat intelligence techniques for constructing, detecting, and reacting to advanced intrusion campaigns
- Applying machine / deep learning tools and techniques for malware analysis and fighting against malicious cyber activities (e.g., cyber crime)
- Intelligent incident response tools, techniques and procedures for contemporary technologies, such as cloud and cyber-physical systems
- Intelligent analysis of different types of data collected from different layers of network security solutions
- Threat intelligence in cyber security domain utilizing big data solutions such as Hadoop
- Intelligent methods to manage, share, and receive logs and data relevant to variety of adversary groups
- Interpretation of cyber threat and forensic data utilizing intelligent data analysis techniques
- Infer intelligence of existing cyber security data generated by different monitoring and defense solutions
- Automated and intelligent methods for adversary profiling
- Automated integration of analyzed data within incident response and cyber forensics capabilities

References

(All URLs valid as of November 13, 2020)

- [1] National Counterintelligence Strategy of the United States of America, 2020-2022. Available on https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf
- [2] Australia's Cyber Security Strategy 2020. Available on <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy>
- [3] Kim-Kwang Raymond Choo and Ali Dehghantanha 2018. Introduction to the Minitrack on Cyber Threat Intelligence and Analytics. In Proceedings of 51st Hawaii International Conference on System Sciences (HICSS 2018). Available on <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1672&context=hicss-51>
- [4] Kim-Kwang Raymond Choo and Ali Dehghantanha 2019. Introduction to the Minitrack on Cyber Threat Intelligence and Analytics. In Proceedings of 52nd Hawaii International Conference on System Sciences

(HICSS 2019). Available on <http://hdl.handle.net/10125/60373>

- [5] Kim-Kwang Raymond Choo and Ali Dehghantanha. Introduction to the Minitrack on Machine Learning and Cyber Threat Intelligence and Analytics. In Proceedings of 53rd Hawaii International Conference on System Sciences (HICSS 2020). Available on <http://hdl.handle.net/10125/64530>

Mini-Track Chairs Biography

Kim-Kwang Raymond Choo holds the Cloud Technology Endowed Professorship at The University of Texas at San Antonio (UTSA). He was included in Web of Science's Highly Cited Researcher in the field of Cross-Field – 2020, and in 2015 he and his team won the Digital Forensics Research Challenge organized by Germany's University of Erlangen-Nuremberg. He is the recipient of the 2019 IEEE Technical Committee on Scalable Computing Award for Excellence in Scalable Computing (Middle Career Researcher), 2018 UTSA College of Business Col. Jean Piccione and Lt. Col. Philip Piccione Endowed Research Award for Tenured Faculty, British Computer Society's 2019 Wilkes Award Runner-up, 2019 EURASIP Journal on Wireless Communications and Networking Best Paper Award, Korea Information Processing Society's JIPS Survey Paper Award (Gold) 2019, IEEE Blockchain 2019 Outstanding Paper Award, Inscript 2019 Best Student Paper Award, IEEE TrustCom 2018 Best Paper Award, ESORICS 2015 Best Research Paper Award, 2014 Highly Commended Award by the Australia New Zealand Policing Advisory Agency, Fulbright Scholarship in 2009, 2008 Australia Day Achievement Medallion, and British Computer Society's Wilkes Award in 2008.

Ali Dehghantanha is a leader in the field of cybersecurity and threat intelligence. He has been an invited or keynote speaker in many national and international conferences, is a well-known media contributor in cybersecurity and has published more than 100 peer-reviewed papers in top journals and conferences in the field. Dr. Dehghantanha is a professor of Cybersecurity at the University of Guelph, Ontario, Canada, the director of Cyber Science Lab (<https://cybersciencelab.org/>) and the director of the Master of Cybersecurity and Threat Intelligence program (<https://bit.ly/34sfFB0>). He was awarded a Tier 2 Canada Research Chair in Cybersecurity and Threat Intelligence in 2020 and a prestigious EU Marie Curie International Incoming Research Fellowship in "Privacy Respecting Digital Forensics" in 2015. His lab is continually offering

positions to talented Ph.D. and postdoctoral candidates in cybersecurity (<https://cybersciencelab.org/open-positions/>).

Glenn Dietrich received his Ph.D. from The University of Texas at Austin, and he is currently the Professor of Information Systems and Cyber Security at The University of Texas at San Antonio (UTSA). He started the information assurance (IA) program in the College of Business at UTSA, developing an undergraduate degree in IA as well as a concentration at the master's level. He has also been responsible for developing minors in information assurance, technology management, digital forensics and data center and network management. The curriculum now includes 20 classes related to cyber security. He founded and was the first director of the Center for Infrastructure Assurance and Security (CIAS) at UTSA. His research interests include intrusion detection and security on the smart grid and data correlation and visualization. He has published in leading journals such as Decision Support Systems, Communications of the Association for Information Systems (CAIS), MISQ Executive, and IEEE Transactions on Engineering Management. Prior to joining UTSA, he worked in private industry building information systems for the government. Dr. Dietrich is a Certified Information Systems Security Professional (CISSP).