Editorial

Tai-hoon Kim*

University of Tasmania,
Room 350, Centenary Building, Private Bag 87 Hobart,
TAS 7001, Australia
and
Department of Convergence Security,
Sungshin University,
2 Bomun-ro 34da-gil, Seongbuk-gu, Seoul 136-742, South Korea
Email: taihoonn@daum.net
Email: taihoonn@sungshin.ac.kr
*Corresponding author

Sabah Mohammed

Department of Computer Science,
Lakehead University,
ATAC 5013, 955 Oliver Road, Thunder Bay, Ontario P7B 5E1, Canada
Email: mohammed@lakeheadu.ca

Carlos Ramos

Department of Informatics,
Institute of Engineering (ISEP-IPP),
Polytechnic of Porto,
R. Dr. Roberto Frias, 4200-465 Porto, Portugal
Email: csr@isep.ipp.pt
Email: csr@dei.isep.ipp.pt

Wai-Chi Fang

Department of Electronics Engineering,
National Chiao Tung University,
1001 Ta Hsueh Road, Hsinchu, 300, Taiwan
Email: Dr.WFang@gmail.com

Biographical notes: Tai-hoon Kim received his MS degree and PhD in Electrics, Electronics and Computer Engineering from the Sungkyunkwan University, South Korea. He also got his second PhD in Computer Engineering from the Bristol University, UK. After working with Korea Information Security Agency as a senior researcher, he worked at the Defense Security Command (DSC) for about two years. He is currently a Professor from the Sungshin W. University in South Korea, and Visiting Scholar of UTAS in Australia.

Sabah Mohammed is a Full Professor and Professional Engineer from the Department of Computer Science and Co-Founder of the Smart Health FabLab at the Lakehead University. His research is focused on intelligent systems. He is an Adjunct Professor from the University of Western Ontario. He is also the Chair of Smart and Connected Health with IEEE ComSoc and EiC of *International Journal of Extreme Automation and Connectivity in Healthcare* at IGI Global.

Carlos Ramos graduated from the University of Porto, Portugal, in 1986 and the obtained his PhD degree from the same university, in 1993. He is the Coordinator Professor from the Department of Informatics at the ISEP-IPP. His main interests are artificial intelligence and decision support systems, recently with more emphasis on ambient intelligence. He is the Director of GECAD, the largest R&D centre of the polytechnic system in Portugal, and is dedicated to AI topics.

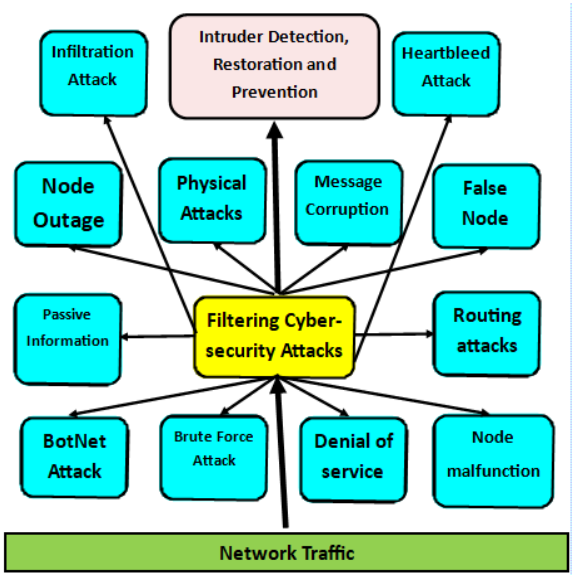
Wai-Chi (Winston) Fang is currently the TSMC Distinguished Chair Professor of the National Chiao Tung University, Taiwan. Since joining JPL in 1985, he has been actively pursuing extensive research and technology work in areas that include VLSI/SoC circuits and systems. He is an IEEE Fellow and was an elected Governor of the IEEE Circuits and Systems Society (CASS). He serves as an officer of the IEEE Systems Council as the Vice President with an additional duty as the Chairman of Transnational and Liaison Committee.

This special issue discusses the recent research progress on protecting systems, networks, internet in any form like internet of things as well as the software and programs from digital attacks. The cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. A successful cybersecurity approach must have multiple layers of detection, protection, restoration and prevention spread across the computers, networks, programs, or even around data that one intends to keep safe. Figure 1 illustrates the basic component of a cybersecurity system. However, implementing effective cybersecurity measures is particularly challenging today because there is an exponential growth of the internet interconnections which has led to a significant growth of cyberattack incidents often with disastrous and grievous consequences. Malware is the primary choice of weapon to carry out malicious intents in the cyberspace, either by exploitation into existing vulnerabilities or utilisation of unique characteristics of emerging technologies. The development of more innovative, smart and effective malware defence mechanisms has been regarded as an urgent requirement in the cybersecurity community (Jang-Jaccard and Nepal, 2014).

As cyberattacks grow in volume and complexity, artificial intelligence (AI) is helping under-resourced security operations analysts stay ahead of threats. Curating threat intelligence from millions of research papers, blogs and news stories, AI provides instant insights to help you fight through the noise of thousands of daily alerts, drastically reducing response times (https://www.ibm.com/security/artificial-intelligence). However, one need to understand that is AI is also a threat to cybersecurity attackers commanded AI systems developed by Amazon, Apple, and Google to do things such as dial phones and open websites – without the knowledge of the AI systems' users (Goosen et al., 2018). It is a short step to more nefarious commands, such as unlocking doors and transferring money with the aid of new technological trends like Alexa, Siri, and Google Assistant. Actually in 2010, Yampolskiy coined the phrase 'artificial intelligence safety

engineering' and its shorthand notation 'AI safety' to give a name to a new direction of research that may include cybersecurity. Additionally, AI will be integrated with other advanced technologies such as blockchain to ensure better security protocols. And then, maybe AI with its safety measures will become our new cybersecurity sheriff (Joshi, 2019).

Figure 1 Basic components of a cybersecurity system (see online version for colours)



This special issue contains ten accepted articles representing 17% of the total submissions. Achieving such a high quality of papers would have been impossible without the huge work that was undertaken by the editorial board members and external reviewers. We take this opportunity to thank them all for their great support and cooperation. The following are the articles accepted in this special issue:

1 'Behavioural analysis approach for IDS based on attack pattern and risk assessment in cloud computing'

2 'A critical insight into the effectiveness of research methods evolved to secure IoT ecosystem'

3 'An efficient authentication and key agreement scheme for e-health applications in the context of internet of things'

4 'An ontology-based approach to improve access policy administration of attribute-based access control'

5 'A multi-agent system approach based on cryptographic algorithm for securing communications and protecting stored data in the cloud-computing environment'

6 'An efficient user authentication model for IOT-based healthcare environment'

7 'Cloud-based DDoS attack detection and defence system using statistical approach'

8 ‘Sequential pattern analysis for event-based intrusion detection’

9 ‘SQL injection attacks – a systematic review’

10 ‘Password security by encryption using an extended ADFGVX cipher’.

References

Goosen, R., Rontojannis, A., Deutscher, S., Rogg, J., Bohmayr, W. and Mkrtchian, D. (2018) *Artificial Intelligence Is a Threat to Cybersecurity. It’s Also a Solution*, BCG Publication, 13 November [online] https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx (accessed 30 June 2019).

Jang-Jaccard, J. and Nepal, S. (2014) ‘A survey of emerging threats in cybersecurity’, *Journal of Computer and System Sciences*, Vol. 80, No. 5, pp.973–993.

Joshi, N. (2019) ‘Can AI become our new cybersecurity sheriff?’, *Forbes*, February [online] https://www.forbes.com/sites/cognitiveworld/2019/02/04/can-ai-become-our-new-cybersecurity-sheriff/#601956a436a8 (accessed 30 June 2019).

Yampolskiy, R.V. (2011) ‘Artificial intelligence safety engineering: why machine ethics is a wrong approach’, presented at the *Philosophy and Theory of Artificial Intelligence (PTAI2011)*, Thessaloniki, Greece, 3–4 October.