REFERENCES

[1] Awad, R. A. and Sayre, K. D., "Automatic Clustering of Malware Variants," *2016 IEEE Conference on Intelligence and Security Informatics (ISI 2016)*, pp. 298–303, 2016.

[2] Ceron, J. M., Margi, C. B., and Granville, L. Z., "MARS: An SDN-based Malware Analysis Solution," *2016 IEEE Symposium on Computers and Communication (ISCC)*, pp. 525–530, June 2016.

[3] Fujino, A., Murakami, J., and Mori, T., "Discovering Similar Malware Samples Using API Call Topics," *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*, pp. 140–147, Jan 2015.

[4] Hansen, S. S., Larsen, T. M. T., Stevanovic, M., and Pedersen, J. M., "An Approach for Detection and Family Classification of Malware Based on Behavioral Analysis," *2016 International Conference on Computing, Networking and Communications (ICNC)*, pp. 1–5, Feb 2016.

[5] Islam, A., Oppenheim, N., and Thomas, W., "SMB Exploited: WannaCry Use of Eternalblue." [Online]. Available: https://www.fireeye.com/blog/threat-research/2017/05/smb-exploited-WannaCry-use-of-Eternalblue.html

[6] Kharaz, A., Arshad, S., Mulliner, C., Robertson, W., and Kirda, E., "UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware," *25th USENIX Security Symposium (USENIX Security 16)*, pp. 757–772, USENIX Association, 2016.

[7] Liska, A. and Gallo, T., *Ransomware: Defending Against Digital Extortion*, 1st Edition, O'Reilly Media Inc., pp. 1-22, 2016.

[8] Microsoft, "Microsoft Security Bulletin MS17-010 - Critical: Security Update for Microsoft Windows SMB Server (4013389)." [Online]. Available: https://technet.microsoft.com/en-us/library/security/ms17-010.aspx

[9] Mosli, R., Li, R., Yuan, B., and Pan, Y., "Automated Malware Detection Using Artifacts in Forensic Memory Images," *in 2016 IEEE Symposium on Technologies for Homeland Security (HST)*, pp. 1–6, May 2016.

[10] Rousseau, A., "WCry/WanaCry Ransomware Technical Analysis." [Online]. Available: https://www.endgame.com/blog/wcrywanacry-ransomware-technical-analysis

[11] Rudman, L. and Irwin, B., "Dridex: Analysis of the Traffic and Automatic Generation of IOCs," *2016 Information Security for South Africa (ISSA)*, pp. 77–84, Aug 2016.

Da-Yu Kao received the B.S. and M.S. degree in information management from Central Police University, Taiwan, in 1993 and 2001, the Ph.D degrees in Crime Prevention and Correction from Central Police University, Taiwan, in 2009, respectively. From 1993 to 1996, he was with Taipei City Police Department, Taiwan, where he was an information technology police officer involved in the development of policing information systems. From 1996 to 2007, he was with Criminal Investigation Bureau, National Police Administration, Taiwan, where he was a detective and forensic police officer in cybercrime investigation and digital forensics. From 2007 to 2013, he was with Maritime Patrol Directorate General, Coast Guard Administration, Taiwan, where he was an information technology section chief in the department of information and communication. Since 2013, he has been with Central Police University, Taiwan, where he is currently an associate professor in the Department of Information Management. His research interests include cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.

Shou-Ching Hsiao received the B.S. degree in information management from Central Police University, Taiwan, in 2016. Since 2016, she has been with Haishan Precinct, New Taipei City Police Department, Taiwan, where she is currently an information lieutenant and is responsible for information system management, information security, malware analysis, and real-time video for security control. In 2018, she is also working toward the M.S. degree in the Department of Computer Science, National Chengchi University, Taiwan. Her current research interests include malware analysis, cybercrime investigation, digital forensics, digital evidence, information management, criminal profiling, and cyber criminology.

Raylin Tso received the B.S. degree in Industrial Engineering from National Tsing Hua University, Hsinchu, Taiwan and M.S. degree in Management Science - Division of Management and Public Policy, University of Tsukuba, Tsukuba, Ibaraki, Japan, in 2002, M.S. degree in Risk Engineering, Graduate School of Systems and Information Engineering, University of Tsukuba, Tsukuba, Ibaraki, Japan, in 2004, the Ph.D degrees in Risk Engineering, Graduate School of Systems, University of Tsukuba, Tsukuba, Ibaraki, Japan, in 2006, respectively. From 2006 to 2008, he was with Graduate School of Systems and Information Engineering, University of Tsukuba, Japan, where he was an academic researcher. Since 2008, he has been with National Chengchi University, Taiwan, where he is currently an associate professor and chairman in the Department of Computer Science. His research interests include cryptography, information security, post-quantum, blockchain and privacy enhancement.