COINS - Information Security Conference

Yi-Ching Liao
Norwegian Information Security laboratory
yi-ching.liao@hig.no

The Information Security Conference (ISC) emphasizes on the research of theory and applications of information security. Since my Ph.D. project is about process tracking for forensic readiness, I found one of the publications: "Dynamically Provisioning Isolation in Hierarchical Architectures" [1] beneficial for my research. Falzon and Bodden observe the scoped channels by analysing side channel and covert channel attacks from different system architectural levels, including core-level, machine-level, cross-virtual-machine-level, hypervisor-level, and network-level. To prevent a process from leaking its internal state, the authors propose the SafeHaven framework for the migrations of processes and virtual machines by the enhancement through hardware event counters, post-copy migration, and process containers. They demonstrate the proposed framework to be an efficient and feasible measure against system-wide covert-channel attacks through conducting two case studies: system-wide covert channel [2] and moving target defence [3]. Even though the use of migration is practicable to thwart a system-wide covert-channel, evaluating different levels of granularity for isolation is still necessary for cost-benefit analysis.

Two other publications presented in the system and software security session: "Software Security Maturity in Public Organisations" [4] and "Factors Impacting the Effort Required to Fix Security Vulnerabilities" [5] are also interesting. To examine the factors impacting the vulnerability-fix time, Othmane et al. conduct a qualitative case study by interviewing 12 participants in the vulnerability fixing process. The result presents the eight categories of factors that impact the vulnerability-fix time: vulnerabilities characteristics, software structure, technology diversification, communication and collaboration, availability and quality of information and documentation, experience and knowledge, code analysis tool, and others. Jaatun et al. also evaluate software security maturity of Norwegian public organisations through interviewing 20 Norwegian public-owned (municipalities, government) organisations based on the Building Security In Maturity Model (BSIMM) [6] activities. The result shows the Norwegian public-owned organisations stand out at the compliance and policy activities, but need to enhance the metrics, penetration testing, and training activities.

References

[1] K. Falzon and E. Bodden, "Dynamically Provisioning Isolation in Hierarchical Architectures," in *Information Security*, ser. Lecture Notes in Computer Science,

J. Lopez and C. J. Mitchell, Eds. Springer International Publishing, Sep. 2015, no. 9290, pp. 83–101, dOI: 10.1007/978-3-319-23318-5_5. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-319-23318-5_5

[2] Z. Wu, Z. Xu, and H. Wang, "Whispers in the Hyper-space: High-speed Covert Channel Attacks in the Cloud," in *USENIX Security symposium*, 2012, pp. 159–173. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final97.pdf

[3] Y. Zhang, M. Li, K. Bai, M. Yu, and W. Zang, "Incentive Compatible Moving Target Defense against VM-Colocation Attacks in Clouds," in *Information Security and Privacy Research*, ser. IFIP Advances in Information and Communication Technology, D. Gritzalis, S. Furnell, and M. Theoharidou, Eds. Springer Berlin Heidelberg, Jun. 2012, no. 376, pp. 388–399, dOI: 10.1007/978-3-642-30436-1_32. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-642-30436-1_32

[4] M. G. Jaatun, D. S. Cruzes, K. Bernsmed, I. A. Tndel, and L. Rstad, "Software Security Maturity in Public Organisations," in *Information Security*, ser. Lecture Notes in Computer Science, J. Lopez and C. J. Mitchell, Eds. Springer International Publishing, Sep. 2015, no. 9290, pp. 120–138, dOI: 10.1007/978-3-319-23318-5_7. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-319-23318-5_7

[5] L. b. Othmane, G. Chehrazi, E. Bodden, P. Tsalovski, A. D. Brucker, and P. Miseldine, "Factors Impacting the Effort Required to Fix Security Vulnerabilities," in *Information Security*, ser. Lecture Notes in Computer Science, J. Lopez and C. J. Mitchell, Eds. Springer International Publishing, Sep. 2015, no. 9290, pp. 102–119, dOI: 10.1007/978-3-319-23318-5_6. [Online]. Available: http://link.springer.com/chapter/10.1007/978-3-319-23318-5_6

[6] G. McGraw, S. Migues, and J. West, *Building Security In Maturity Model: BSIMM-V*, Oct. 2013. [Online]. Available: http://bsimm.com