Analysis of software weakness detection of CBMC based on CWE

Minjae Byun*, Yongjun Lee*, Jin-Young Choi*

**Department of Information Security, Korea university, Seoul, Korea*

minjae_byun@korea.ac.kr, yjlee@formal.korea.ac.kr, choi@formal.korea.ac.kr

***Abstract*—Model checking is a method of verifying whether a target system satisfies a specific property using mathematical and logical proofs. Model checking tools to verify design (1) require a formal description of the design and (2) there can be discrepancies between the model and actual implementation. To solve these problems, various tools such as CBMC and BLAST that can directly input C codes have been proposed. However, in terms of security, it is difficult to figure out which software weaknesses these tools can verify. In this paper, we matched the properties that CBMC can verify with corresponding CWEs, considering interdependencies of CWEs. We also conducted an experiment using Juliet Test Suite to check CBMC can actually verify the codes including these CWEs.**

***Keyword*—CBMC, information security, model checking, software weakness**

Minjae Byun received the two B.E. degrees in computer science and engineering and information security from Korea University, Seoul, South Korea, in 2018. She is currently pursuing the M.E. degree in information security at Graduate School of Information Security, Korea University, Seoul, South Korea. Her current research interests are in secure software engineering, formal methods, and cryptography.

Yongjun Lee received the two B.S degrees in Department of computer and information security and optical engineering from Sejong University, Seoul, South Korea, in 2018. He is currently pursuing the M.E. degree in information security at Graduate School of Information Security, Korea University, Seoul, South Korea. His current research interests are in formal methods, security vulnerability assessment, deep learning, and secure software engineering.

Jin-Young Choi received the M.S. degree from Drexel University, Philadelphia, PA, USA, in 1986, and the Ph.D. degree from the University of Pennsylvania, Philadelphia, PA, USA, in 1993. He is currently a Professor with the Graduate School of Information Security, Korea University, Seoul, South Korea. His current research interests are in real- time computing, formal methods, programming languages, process algebras, security, and secure software engineering.