Is a False Positive really False Positive?

Hong Jun Choi, Hyuk Lee, Jin-Young Choi

School of Cybersecurity, Korea University, Seoul, 02841, Republic of Korea

hjcho1@korea.ac.kr, fmlab_hlee@korea.ac.kr, narnia@korea.ac.kr

Abstract—As the number of devices with software increases, software reliability and security has become more critical. To improve reliability and security, developers and test engineers use static analysis tools to find defects early in the development process. However, it takes a lot of time and effort to determine whether alarms from performing static analysis are true or false positive. In this paper, we argue that all integer overflows generated by static analysis tools are weaknesses and should eventually be corrected. To show that our argument is reasonable, we explain static analysis results for binary search program code and CWE:190 example code in terms of reliability and security. It is unnecessary to identify whether the integer overflow generated by static analysis tools is true or false positive.

Keyword—Software Reliability, Software Security, Static Analysis, Integer Overflow, True Positive, False Positive

Hong Jun Choi received B.S. degree in the School of Computer Software, Daegu Catholic University, Korea in 2019. He is currently a M.S. candidate in School of Cybersecurity, Korea University. His current research interests are in static analysis, secure software engineering, formal methods.

Hyuk Lee received the B.S. degree from the University of Technology Sydney, Sydney, Australia, in 2006, and M.S. degree in 2009 and the Ph.D. degree in 2019 from the Korea University, Seoul, Korea. He is currently a research professor with the School of Cybersecurity, Korea University, Seoul, Korea. His current research interests are in formal methods, constraint problem solving, and secure software engineering.

Jin-Young Choi received the B.S. degree from Seoul National University, Seoul, Korea, in 1982, received the M.S. degree from Drexel University, Philadelphia, PA, in 1986, and the Ph.D. degree from the University of Pennsylvania, Philadelphia, in 1993. He is currently a Professor with the School of Cybersecurity, Korea University, Seoul, Korea. His current research interests are in real-time computing, formal methods, programming languages, process algebras, security, and secure software engineering.