Filtering Malicious Routines in Web Browsers Using Dynamic Binary Instrumentation

Jae Won Min *, Sung Min Jung *, Tai Myoung Chung **

* Department of Electrical and Computer Engineering, Sungkyunkwan Univ, 300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, Korea
** School of Information Communication Engineering, Sungkyunkwan Univ, 300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, Korea
jwmin@imtl.skku.ac.kr, smjung@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Abstract—Extension of web browser capability has introduced variety of security problems. Attackers exploit vulnerabilities found in internals of web browsers or plugins to compromise the system and execute arbitrary code. In this paper, we present a filtering method which blocks malicious routines from being executed. Filtering is done by keeping a blacklist of dangerous routines and arguments separately to compare with the routines being called by the web browser at runtime. To show the concept, we built a prototype by using dynamic binary instrumentation framework called Pin. Pin provides rich API that allows us to build a custom tool that inserts instrumentation codes in the program. Using this tool, we are able to block malicious instructions from being executed.

Keywords— Web Browser, Security, Sandbox, Vulnerability, Dynamic Binary Instrumentation