World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:11, No:07, 2017

An Improved Method on Static Binary Analysis to Enhance the Context-Sensitive CFI

Authors : Qintao Shen, Lei Luo, Jun Ma, Jie Yu, Qingbo Wu, Yongqi Ma, Zhengji Liu

Abstract : Control Flow Integrity (CFI) is one of the most promising technique to defend Code-Reuse Attacks (CRAs). Traditional CFI Systems and recent Context-Sensitive CFI use coarse control flow graphs (CFGs) to analyze whether the control flow hijack occurs, left vast space for attackers at indirect call-sites. Coarse CFGs make it difficult to decide which target to execute at indirect control-flow transfers, and weaken the existing CFI systems actually. It is an unsolved problem to extract CFGs precisely and perfectly from binaries now. In this paper, we present an algorithm to get a more precise CFG from binaries. Parameters are analyzed at indirect call-sites and functions firstly. By comparing counts of parameters prepared before call-sites and consumed by functions, targets of indirect calls are reduced. Then the control flow would be more constrained at indirect call-sites in runtime. Combined with CCFI, we implement our policy. Experimental results on some popular programs show that our approach is efficient. Further analysis show that it can mitigate COOP and other advanced attacks.

Keywords : contex-sensitive, CFI, binary analysis, code reuse attack
Conference Title : ICCCNC 2017 : International Conference on Computer, Computing, Networking and Communications
Conference Location : Singapore, Singapore
Conference Dates : July 04-05, 2017