Danger, Jean-Luc; Guilley, Sylvain; Porteboeuf, Thibault; Praden, Florian; Timbert, Michaël

Hardware-enforced protection against buffer overflow using masked program counter. (English) Zbl 1405.94057


Summary: The threat based on Buffer Overflow is one of the main software vulnerability which is exploited by many viruses and cyber attacks. A buffer overflow overwrites the return address to the parent program of a subroutine. To counter it, we propose in this paper to mask on-the-fly this return address by slightly modifying the processor architecture. We show that the hardware overhead, as well as software modification, is very small. The efficiency has been demonstrated on a bare metal program running on a Leon 3 processor. This paper also shows the limitation when using a real OS.

For the entire collection see [Zbl 1334.94030].

MSC:
94A60 Cryptography
68M99 Computer system organization

Full Text: DOI

References:

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.