Buffer overflow attack mitigation via Trusted Platform Module (TPM)

ABSTRACT

As of the date of writing of this paper, we found no effort whatsoever in the employment of Trusted Computing (TC)'s Trusted Platform Module (TPM) security features in Buffer Overflow Attack (BOA) mitigation. Such is despite the extensive application of TPM in providing security based solutions, especially in key exchange protocols deemed to be an integral part of cryptographic solutions. In this paper we propose the use of TPM's Platform Configuration Register (PCR) in the detection and prevention of stack based buffer overflow attacks. Detection is achieved via the integrity validation (of SHA1 hashses) of both return address and call instruction opcodes. Prevention is achieved via encrypting the memory location addresses of both the return and call instruction above using RSA encryption. An exception is raised should integrity violations occur. Based on effectiveness tests conducted, our proposed solution has successfully detected 6 major variants of buffer overflow attacks attempted in conventional application codes, while incurring overheads that pose no major obstacles in the normal, continued operation of conventional application codes.

Keyword: Buffer overflow attack; Trusted platform module; Platform configuration register (PCR); ptrace; TPM_Extend; TPM_Sea