**International Journal of Applied Engineering Research and Development (IJAERD)**
**ISSN(P): 2250-1584; ISSN(E): 2278-9383**
**Vol. 4, Issue 2, Apr 2014, 139-144**


# SAFE STACK: AUTOMATICALLY PATCHING STACK BASED BUFFER OVERFLOW VULNERABILITIES

**LALWANI JAI[1] & RINKU SHAH[2]**

[1]Alamuri Ratnamala Institute of Engineering and Technology, Mumbai, Maharashtra, India

[2]Vidyalankar Institute of Technology, Mumbai, Maharashtra, India

## ABSTRACT

Buffer overflow still pose a significant threat to security and availability of today's computer system. Although there are a number of solutions proposed to provide adequate protection against buffer overflow attack, most of existing solutions terminate the vulnerable program when buffer overflow occurs, effectively rendering the programs unavailable. The impact on availability is a serious problem on service oriented platforms. This paper presents safe-stack, a system that can automatically diagnose and patch stack based buffer overflow vulnerabilities. The key technique of our solution is to virtualized memory accesses and move the vulnerable buffer into protected memory regions, which provide a fundamental and effective protection against recurrence of the same attack without stopping normal system execution. We developed a prototype on a Linux system, and conducted extensive experiments to evaluate the effectiveness and performance of system using a range of applications. Our experimental results showed that safe-stack can quickly generate runtime patches to successfully handle the attack's recurrence. Furthermore, safe-stack only incurs acceptable overhead for the patched applications.

**KEYWORDS:** Linux System, Vulnerable Buffer, Safe-Stack