

ABSTRACT

Provided are an apparatus and method for hardware-based detection of a kernel code injection attack. The apparatus detects a code injection attack by using a trace manager configured to parse a packet received from a program trace interface (PTI) of a host system to detect indirect branch target addresses, a notification manager configured to receive a notification about an event, such as mode conversion, through execution of a trampoline, and a traffic manager configured to detect an attempt to write to a physical code region of a memory by snooping traffic on a bus.