Stack Overflow Detection and Prevention on Operating Systems Using Machine Learning and Control-Flow Enforcement Technology

Authors : Cao Jiayu, Lan Ximing, Huang Jingjia, Burra Venkata Durga Kumar

Abstract : The first virus to attack personal computers was born in early 1986, called C-Brain, written by a pair of Pakistani brothers. In those days, people still used dos systems, manipulating computers with the most basic command lines. In the 21st century today, computer performance has grown geometrically. But computer viruses are also evolving and escalating. We never stop fighting against security problems. Stack overflow is one of the most common security vulnerabilities in operating systems. It may result in serious security issues for an operating system if a program in it has a vulnerability with administrator privileges. Certain viruses change the value of specific memory through a stack overflow, allowing computers to run harmful programs. This study developed a mechanism to detect and respond to time whenever a stack overflow occurs. We demonstrate the effectiveness of standard machine learning algorithms and control flow enforcement techniques in predicting computer OS security using generating suspicious vulnerability functions (SVFS) and associated suspect areas (SAS). The method can minimize the possibility of stack overflow attacks occurring.

Keywords : operating system, security, stack overflow, buffer overflow, machine learning, control-flow enforcement technology

Conference Title : ICCOS 2022 : International Conference on Computer Operating Systems

Conference Location : Prague, Czechia

Conference Dates : September 08-09, 2022