SoK: Eternal War in Memory

Submitted by Heather Lucas on Wed, 09/17/2014 - 6:34pm

Title
SoK: Eternal War in Memory

Publication Type
Conference Paper

Year of Publication
2013

Authors
Szekeres, L., Payer, M., Tao Wei, Song, D.

Conference Name
Security and Privacy (SP), 2013 IEEE Symposium on

Date Published
May

Keywords
computer security, memory corruption attacks, memory corruption bugs, program debugging, protection mechanisms, protection techniques, security of data, software reliability, SoK, storage management

Abstract

Memory corruption bugs in software written in low-level languages like C or C++ are one of the oldest problems in computer security. The lack of safety in these languages allows attackers to alter the program’s behavior or take full control over it by hijacking its control flow. This problem has existed for more than 30 years and a vast number of potential solutions have been proposed, yet memory corruption attacks continue to pose a serious threat. Real world exploits show that all currently deployed protections can be defeated. This paper sheds light on the primary reasons for this by describing attacks that succeed on today’s systems. We systematize the current knowledge about various protection techniques by setting up a general model for memory corruption attacks. Using this model we show what policies can stop which attacks. The model identifies weaknesses of currently deployed techniques, as well as other proposed protections enforcing stricter policies. We analyze the reasons why protection mechanisms implementing stricter polices are not deployed. To achieve wide adoption, protection mechanisms must support a multitude of features and must satisfy a host of requirements. Especially important is performance, as experience shows that only solutions whose overhead is in reasonable bounds get deployed. A comparison of different enforceable policies helps designers of new protection mechanisms in finding the balance between effectiveness (security) and efficiency. We identify some open research problems, and provide suggestions on improving the adoption of newer techniques.

URL
ieeexplore.ieee.org/document/6547101/
computer security memory corruption attacks memory corruption bugs program debugging protection mechanisms protection techniques security of data software reliability SoK storage management