Critique on
Gene Novark and Emery D. Berger. 2010. DieHarder: Securing the Heap.

Astha Sharma
asharma6@uno.edu

SUMMARY

The paper presented here analyzes a number of widely-deployed memory allocators and shows that they are vulnerable to security related attacks. These memory allocators are generally used by Windows, Linux, Free BSD, and Open BSD. DieHarder was introduced as a solution to the heap based security attacks. It was designed based on the extensive analysis of the impact made by memory allocator design decision on their vulnerability to attacks.

With modest performance overhead (running only 20% slower (on average) than OpenBSD across a suite of CPU-intensive benchmarks), DieHarder was considered as a new allocator with highest degree of security. Its performance is also equivalent to the Linux allocator on the Firefox web browser.

STRENGTH

- DieHarder combines the feature of both DieHard and Open BSD's allocator
- It significantly reduces the risk of heap buffer overflow/underflow attacks and heap spraying.
- Firefox runs as fast with DieHarder than with the Linux allocator.
- Prevents dangling-pointer based attacks by destroying the freed data, erasing the content of freed objects, and fully randomizing object for reuse.

WEAKNESSES

- There is a performance overhead that may lead to slower results.