Heap Overflow

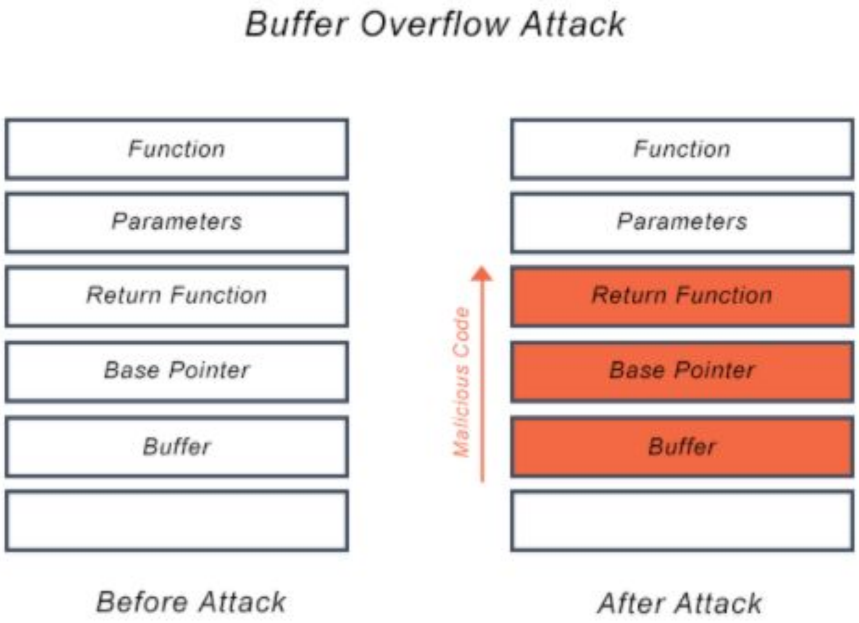
Tysen Radovich (j86j296),
Allen Simpson (r29b821),
Spencer Lawry(w58z387),
Arash Ajam (f63m331)

Buffer Overflow

int arr[5];

[1, 2, 3, 4, 5], 6, 7, H, A, C, K, M, E

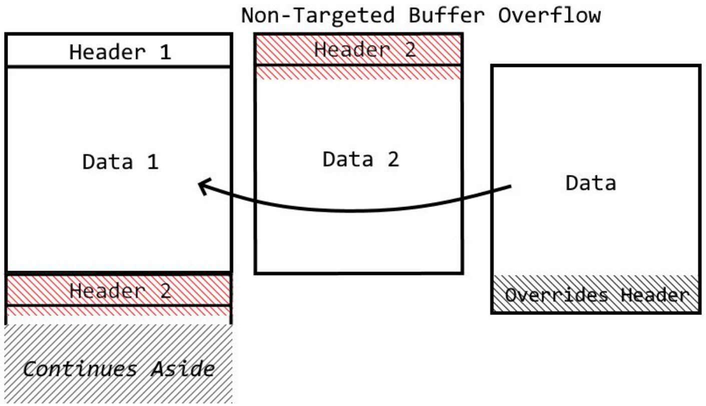
Overlap to adjacent memory areas

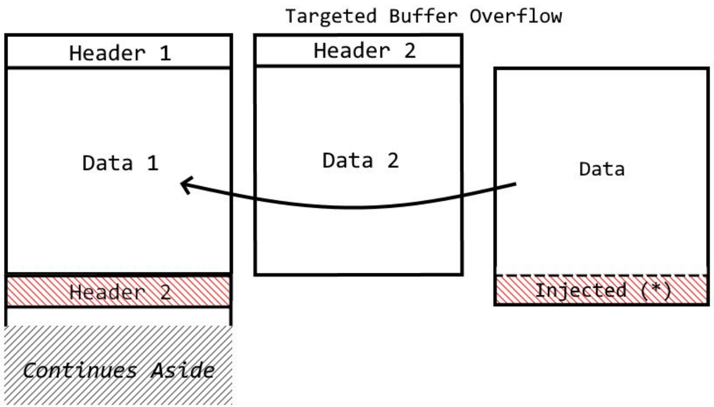


Heap Overflow

Heap overflow occurs when more data is written into a data block that that data-block has allocated space

Can override headers
-Gibberish (causes crash)
-Injected pointers (to execute code)





Security Solutions - Canaries

Pros:

Effective against Non-Targeted Buffer Overflows

Simple to set up

Cons:

Ineffective against Targeted Buffer Attacks

Significantly increases heap update times

Security Solutions - Guard Pages

Pros:

Headers/Data Cannot be manipulated by anything but the heap manager

Protects against ALL Buffer Overflows

Cons:

Complicated to set up

Can cause issues when debugging segmentation faults

Can increase the update times for the heap

Security Solutions - Random Allocation

Pros:

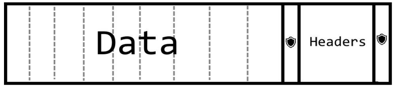
Targeted attacks cannot predict what the Heap memory looks like

Relatively Simple to set up

Cons:

Does not protect from Non-Targeted Buffer Overflows

Security Solutions - Grouped Headers



Pros:

Heap Overflow attacks cannot change pointers

Only two guard pages required

Effective against targeted attacks

Cons:

Does not protect data from being overwritten

Somewhat complicated to set up

Security Solutions - *HeapDefender*

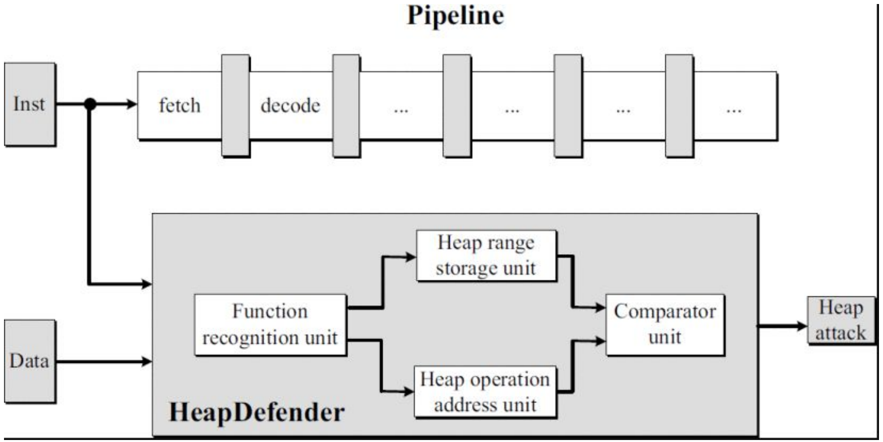
HEAP DEFENDER

Function unit - is heap doing as expected and in range that is supposed to be

Heap range-stores location of info

Heap operation - hold flag

Compares-if stuff in heap range is as long as supposed to be



Conclusion

References

[1] Black, Paul E, and Bojanova, Irena. “Defeating Buffer Overflow: A Trivial but Dangerous Bug.” IT Professional, vol. 18, no. 6, 2016, pp. 58–61.Web.9 Nov. 2020.

[2] Dalton, Michael, et al. “Real-World Buffer Overflow Protection for Userspace &amp; Kernelspace.”USENIX,USENIX.Web.9 Nov. 2020.

[3] Dongfang Li, et al. “HeapDefender: A Mechanism of Defending Embedded Systems against Heap Overflow via Hardware.” 2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing, 2012, pp. 851–856.Web.9 Nov. 2020.

[4] Du,Wenliang.”COMPUTER & INTERNET SECURITY:A Hands-on Approach 2nd Edition”.Syracuse University,Wenliang Du, May. 2019.

[5] Foster,James C.,et al. ”Buffer Overflow Attacks Detect”, Exploit, Prevent, 2005.Web.9 Nov. 2020.

[6] Huang, Ning, et al. “Analysis to Heap Overflow Exploit in Linux with Symbolic Execution.” IOP Conference Series. Earth and Environmental Science, vol. 252, 2019, p.Web.9 Nov. 2020. 42100.

[7] R. Hund, C. Willems and T. Holz, ”Practical Timing Side Channel Attacks against Kernel Space ASLR,” 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, 2013, pp. 191-205, doi: 10.1109/SP.2013.23.Web.9 Nov. 2020.

[8] Li, Dongfang, et al. “HeapDefender: A Mechanism of Defending Embedded Systems against Heap Overflow via Hardware.” IEEEXplore,IEEE, 18 Oct. 2012,Web. 9 Nov. 2020

[9] Marlow, Simon and Jones, Simon Peyton ”Multicore Garbage Collection with Local Heaps” Microsoft Research, Cambridge, U.K.Web.14 Nov. 2020.

[10] Thakur, Abhishek. “Stack Overflow Vulnerability.” StackOverflow Vulnerability, Hacker Noon, 7 Jan. 2020. Web 9 Nov. 2020

[11] Xu, Shu Xin,and Chen,Jun Zhang. “Analysis of Buffer Overflow Exploits and Prevention Strategies.” Applied Mechanics and Materials, vol. 513-517, 2014, pp.1701–1704.Web.9 Nov. 2020.

[12] Zhang, Chao, et al. “Using Type Analysis in Compiler to Mitigate Integer-Overflow-to-Buffer-Overflow Threat.” Journal of Computer Security, vol. 19, no. 6, 2011, pp. 1083–1107.Web.9 Nov. 2020.

Photo links

https://avinetworks.com/glossary/buffer-overflow/

https://payatu.com/blog/Siddharth-Bezalwar/understanding-stack-based-buffer-overflow

https://www.infona.pl/resource/bwmeta1.element.ieee-art-000006332095

https://www.google.com/search?q=that%27s+all+folks&rlz=1C1CHBF_enUS877US879&sxsrf=ALeKk02KXJhoGMLrFA61S116wTVVrM8HUQ:1605504965319&tbm=isch&source=iu&ictx=1&fir=bUotToTRrvIrLM%252CDjzHrtlFRXJUpM%252C_&vet=1&usg=AI4_-kSmvz-LIXLxTdi_ZKdk8bfwJ6-KWQ&sa=X&ved=2ahUKEwjDgJKJrlbtAhVzMX0KHYGjC0sQ9QF6BAgBEFg&biw=1920&bih=937#imgrc=bUotToTRrvIrLM