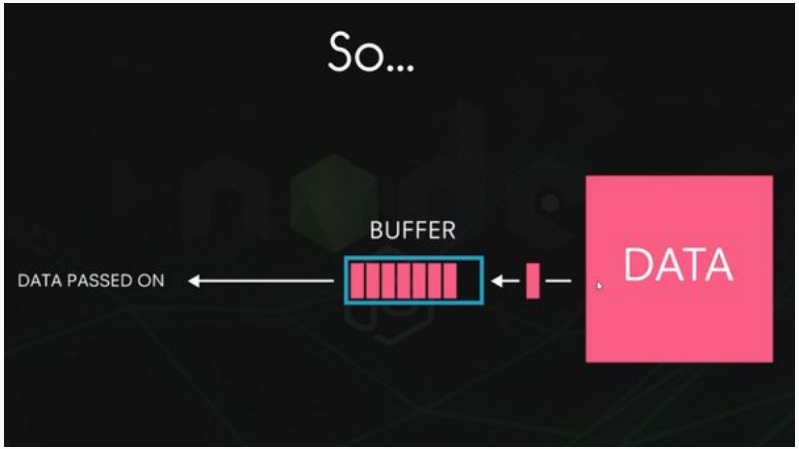
Buffer-Overflow Attack and Heap-based buffer overflow attack

By Tyler Poor, Evan Hack, and Lucas Neidlinger

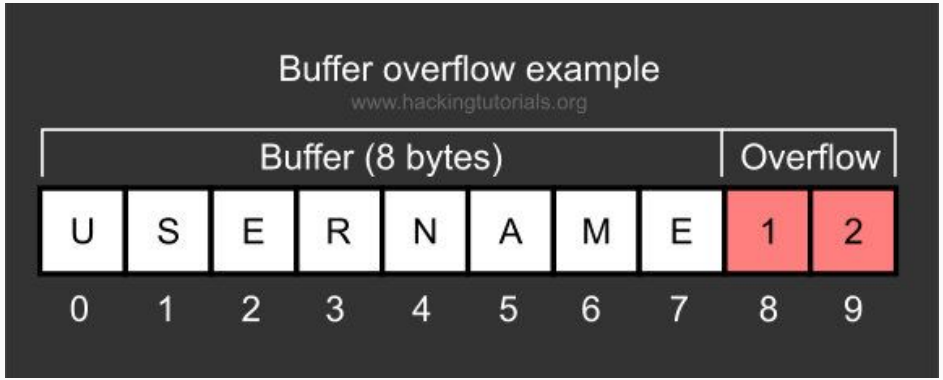
What are Buffers?

Buffers are a collection of memory storage that temporarily hold data while it is being pushed from one location to another.



What is a buffer overflow?

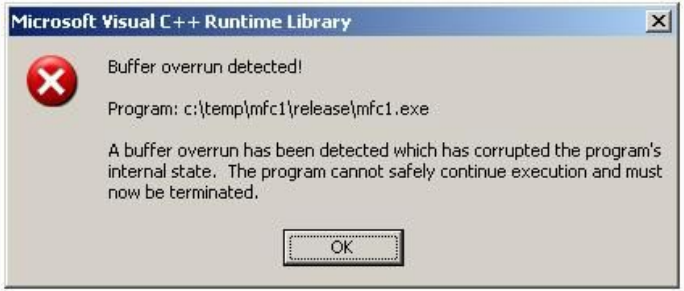
A buffer overflow is an instance where a computer program overruns its capacity while writing data to a buffer. It will then spread into boundaries of other buffers and it can potentially corrupt/overwrite the data present.



What is a buffer overflow attack?

A buffer overflow attack is when an attacker exploits the issues of buffer overflows by overwriting the memory of multiple applications.

By doing this it will change the execution of the program and cause files to be damaged or cause the exposure of private information.



What is a Heap-based buffer overflow attack?

A heap-based overflow attack is when a piece of memory is allocated to the heap and data is written to the memory without any bound checking being done on the data. This will lead to the overwriting of crucial data structures in the heap like heap headers of any heap-base data like dynamic object pointers, this can lead to the overwriting of the virtual function table.

How to prevent Buffer overflow attacks

- Perform routine code auditing
- Use compiler tools
- Avoid using functions which don't automatically perform buffer checks
- Use canaries

Work Cited

https://resources.infosecinstitute.com/topic/heap-overflow-vulnerability-and-heap-internals-explained/

https://www.comparitech.com/blog/information-security/buffer-overflow-attacks-vulnerabilities/#:~:text=Heap%20overflow%20attack%3A%20A%20heap-based%20buffer%20overflow%20is,the%20open%20memory%20pool%20known%20as%20the%20heap.

https://www.imperva.com/learn/application-security/buffer-overflow/

https://www.freecodecamp.org/news/buffer-overflow-attacks/