Since memory allocation problem is ubiquitous in computer science, academic work to determine the efficient and secure allocation mechanism becomes more important these days. In the following we want to present an overview of related work in this area.

As aforementioned, systems with insufficient user data validation can deal with dynamic memory storage. Dewey et al (2015) formulates the “use after free” vulnerability and conditions of this attack. The paper has focused on C++ compiled binaries where the memory manager cannot find and update pointers to program objects when they are moved. This same vulnerability can be present in other languages. The authors have demonstrated the example of code with attack proof of concept.

Further, Qiang Zeng et al (2019) classifies different attack types on such systems. The paper above notices how programs can be patched to gain required defense against “use after free” type. However, the method they are mentioned requires 64 bits of metadata for every memory allocation call and 4Kb of guard pages. In this work we propose the algorithm with less memory usage.

The other approach to prevent vulnerable was demonstrated and analyzed by Jonathan Ganz et al (2017). It suggests randomizing the address space and return random address pointers. Moreover, it is mentioned that most operating systems uses current approach. With respect to our work, we also use randomization approach to obtain security.

As mentioned in [4], TSLF like methods are the most effective one from the time complexity perspective. At the same the additional memory usage is required due to the hash map. Moreover, Masmano et al (2004) have introduced the TSLF algorithm that has O(1) and the proof of such behavior. The authors also overviewed the segregated free list like method and compared to the provided one. It is mentioned that such allocators do not use the hash map and therefore are free of its memory. Our paper introduces the time and memory balanced protocol of allocation based on segregated free list type.

Another question which corresponds with memory allocation is fragmentation. Nikola Zlatanov (2015) have overviewed this phenomenon and suggested to define a series of partition pools with block sizes in a geometric progression. We suppose that such approach tends to use memory inefficient. Nevertheless, as mentioned in [7], the current phenomenon is not a problem for most of applications. In addition, implementations of the best policies are already known and could be implemented in the client side.

In terms of safety and efficiency at the same time, Beichen Liu et al (2019) have introduced so-called “SlimGuard” allocator that is designed to be secure and effective. The authors have compared memory and time usage of SlimGuard and different state-of-the art memory management algorithms. Similar to this, we introduce lightweight allocator which performance still needs to be tested and compared with other.

As can be seen in the literature review above, state-of-the art memory management allocators are lack of either time/memory efficiency or attack protection. Only experimental methods try to approach the optimal state in both directions. In our study we have collected different ideas and proposed time and memory balanced allocator.

[1] David Dewey, Bradley Reaves, P. Traynor “Uncovering Use-After-Free Conditions in Compiled Code” // International Conference on Availability, Reliability and Security, ARES, 2015

[2] Qiang Zeng, Golam Kayas, Emil Mohammed, Lannan Luo, Xiaojiang Du, Junghwan Rhee “HeapTherapy+: Efficient Handling of (Almost) All Heap Vulnerabilities Using Targeted Calling-Context Encoding” // 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2019

[3] Jonathan Ganz, Sean Peisert “ASLR: How Robust Is the Randomness?” // IEEE Cybersecurity Development (SecDev), 2017

[4] Paul R. WilsonMark S. JohnstoneMichael NeelyDavid Boles “Dynamic Storage Allocation A Survey and Critical Review” // International Workshop on Memory Management, 1995

[5] M. Masmano U, I. Ripoll, A. Crespo, J. Real “TLSF: A new dynamic memory allocator for real-time systems” // Proceedings. 16th Euromicro Conference on Real-Time Systems, 2004

[6] Nikola Zlatanov “Dynamic Memory Allocation and Fragmentation” // ESC, 2015

[7] Mark S. Johnstone, Paul R. Wilson “The Memory Fragmentation Problem: Solved?” // ACM SIGPLAN Notices, 1998

[8] Beichen Liu, Pierre Olivier, Binoy Ravindran “SlimGuard: A Secure and Memory-Efficient Heap Allocator” // Middleware '19: Proceedings of the 20th International Middleware Conference, 2019