Sprawozdanie z projektu NiDUC

# Ochrona funkcji systemowych

### Maciej Myśków 272794

### Kacper Kostrzewa 272855

Data oddania

25.06.2024

Spis treści

[Wstęp 4](#_Toc169818563)

[Charakterystyka funkcji systemowych 4](#_Toc169818564)

[Jakich testów dokonano 7](#_Toc169818565)

[Jak dokonywano testów 7](#_Toc169818566)

[Wyniki testów 8](#_Toc169818567)

[Wnioski końcowe 10](#_Toc169818568)

# 

# Wstęp

Współczesne systemy operacyjne, w tym Linux wymagają skutecznego zarządzania pamięcią, aby zapewnić stabilność, efektywność i bezpieczeństwo działania aplikacji. Dynamiczne przydzielanie pamięci jest kluczowym elementem w programowaniu systemowym i aplikacjach operujących na niskim poziomie. Funkcje takie jak kmalloc, kmalloc\_array i kcalloc w jądrze Linux są fundamentalne do tego procesu, umożliwiając programistom elastyczne zarządzanie pamięcią w czasie rzeczywistym.

Dynamiczna alokacja pamięci jest procesem wymagającym dosyć sporej świadomości od programistów, gdyż niewłaściwa alokacja może zepsuć program a nawet uszkodzi system operacyjny.

Paradoksalnie sytuacje utrudniają tzw. Funkcje bliźniacze (funkcje dynamicznie alokujące pamięć). Przez to, że jest ich tak dużo i w swoim działaniu a nawet sygnaturze są tak podobne, może dojść do tzw. Nadużyć (skorzystanie z niewłaściwej funkcji systemowej). Z drugiej strony mnogość wyżej wspomnianych funkcji rozwiązuje wiele problemów i wprowadza większą elastyczność programistą – stąd tak ważne jest aby dokładnie wiedzieć z jakiej funkcji skorzystać.

W projekcie przyjrzeliśmy się trzem najpowszechniej korzystanym funkcją: Kmalloc, Kmalloc\_array, Kcalloc. Każdą z tych funkcji zbadaliśmy (sygnatury, jej działanie, testy niezawodności) a następnie wyciągnęliśmy wnioski z wyników testowych.

# Charakterystyka funkcji systemowych

Każda z wymienionych wyżej funkcji posiada swoją sygnaturę oraz sposób działania. Bardzo istotne jest aby zrozumieć charakterystyki tych funkcji, tak aby ich rozsądnie używać. Rozsądne używanie funkcji systemowych może ominąć problemy takie jak niekontrolowany dostęp do pamięci, wyciek pamięci czy też zepsucie systemu operacyjnego. Dlatego tak ważne jest aby znać te charakterystyki.

Sygnatury funkcji

|  |  |  |
| --- | --- | --- |
| Funkcja | Sygnatura | Parametry |
| Kmalloc | void \*kmalloc(size\_t size, gfp\_t flags); | size, flaga |
| Kmalloc\_array | void \*kmalloc\_array(size\_t n, size\_t size, gfp\_t flags); | n, size, flaga |
| Kcalloc | void \*kcalloc(size\_t n, size\_t size, gfp\_t flags); | n, size, flaga |

**size\_t**: oznacza rozmiar alokowanej pamięci w bajtach

**flags**: flagi sterujące, określają m.in. rodzaj pamięci, którą chcemy zaalokować

**n**: liczba elementów w tablicy

**size**: rozmiar pojedynczego elementu dla tablicy

Kmalloc

Jest to podstawowa funkcja do alokacji pamięci w Linuxie.

Praktyczne zastosowania:

* Przechowywanie danych: Alokacja pamięci na struktury danych, listy, bufory.
* Obsługa sterowników: Przechowywanie kontekstów sterowników, buforowanie danych wejściowych/wyjściowych.
* Obsługa plików: Bufory na dane do odczytu/zapisu.

Kmalloc\_array

Jest rozszerzeniem kmalloc i służy do alokacji dynamicznej tablicy o określonym rozmiarze.

Praktyczne zastosowania:

* Tablice dynamiczne: Przechowywanie listy elementów o zmiennej liczbie.
* Zarządzanie pamięcią: Alokacja pamięci dla dynamicznych struktur danych, np. list wiązanych.

Kcalloc

kcalloc to specjalna odmiana kmalloc\_array, która dodatkowo zeruje zaalokowaną pamięć. Mówiąc krótko stosując ten typ alokacji tablicowej, dostajemy zaalokowany obszar pamięci przeznaczony na typ tablicowy, którego wszystkie elementy są inicjalizowane zerami już podczas kompilacji.

Praktyczne zastosowania:

* Inicjalizacja zerami: Tworzenie tablic, które wymagają początkowej inicjalizacji zerami.
* Bezpieczeństwo danych: Zapewnienie, że pamięć jest czysta i nie zawiera danych z poprzednich alokacji.

Flagi i ich znaczenie

W funkcjach kmalloc, kmalloc\_array i kcalloc w jądrze Linux, istotną rolę odgrywają flagi, które określają sposób alokacji pamięci. Flagi te są przekazywane jako parametry do funkcji alokujących i wpływają na zachowanie procesu przydzielania pamięci. Zrozumienie tych flag jest kluczowe dla prawidłowego i efektywnego zarządzania pamięcią w jądrze Linux. W naszym projekcie przyjrzymy się dwom flagom, mianowicie: GFP\_kernel oraz GFP\_atomic.

* **GFP\_KERNEL**

Flaga ta jest używana, gdy alokacja pamięci jest wykonywana w kontekście jądra, gdzie można bezpiecznie wywołać funkcje, które mogą być w trybie sleep. Ponadto ta flaga nie może być wykorzystywana, gdy używamy przerwań systemowych podczas alokacji.

Zastosowanie:

Jest to najczęściej używana flaga dla alokacji pamięci w większości części jądra.

Zachowanie:

Funkcja może blokować wykonanie i czekać na dostępność pamięci, co zapewnia wysoką szansę na powodzenie alokacji (wywołanie alokacji funkcji nie zwróci nam wartości NULL).

* **GFP\_ATOMIC**

Flaga ta jest używana w kontekstach, gdzie alokacja pamięci nie może być w trybie sleep, czyli w sekcjach kodu, które muszą być wykonywane szybko i nieprzerwanie. Pozwala na zastosowanie przerwań systemowych.

Zastosowanie:

Używana w kontekstach przerwań i innych miejscach, gdzie alokacja musi być natychmiastowa.

Zachowanie:

Funkcja nie może blokować wykonania. Jeśli pamięć nie jest dostępna, alokacja może się nie powieść, co oznacza mniejsze szanse na powodzenie w porównaniu z GFP\_KERNEL – możliwe zwrócenie wartości NULL przy próbie alokacji.

# Jakich testów dokonano

W projekcie przeprowadziliśmy testy na najpowszechniej stosowanych funkcjach systemowych: kmalloc, kmalloc\_array, kcalloc. Testy zostały u nas podzielone na dwie kategorie: testy działania i poprawności alokacji pamięci przez funkcje oraz testy złożoności czasowej alokacji i zwalniania pamięci.

Testy alokacji pamięci

Testy te miały na celu sprawdzić wydajność oraz poprawność alokacji pamięci w zależności od inicjalizacji. Testy te są bardzo istotne z punktu widzenia wyboru funkcji systemowej, gdyż ich wyniki mogą być pomocne w podjęciu właściwej decyzji co do wyboru funkcji bliźniaczej.

Testy czasów alokacji i zwalniania pamięci

Badanymi funkcjami w tym teście były Kmalloc\_array oraz Kcalloc. Testów dokonano w celu zbadania czasów użytkowania funkcji systemowych alokujących struktury tablicowe w zależności od ich rozmiaru. Wyniki tych badań pozwalają odpowiedzieć na pytanie, której funkcji użyć jeśli np. obie spełniają tak samo testy i wymagania alokacji pamięci.

# Jak dokonywano testów

Ponieważ testowaliśmy alokacje pamięci bezpośrednio na jądrze (kernel) Linuxa, używając języka C, wymagało to od nas znajomości programowania powłoki kernel oraz napisania własnego małego modułu do poruszania się po tej powłoce.

Wszystkich testów dokonywano w środowisku testowym – zwirtualizowanym na podstawie obrazu systemu ISO – Linux Ubuntu wraz zainstalowanym nagłówkiem jądra systemu, który umożliwiał kompilacje do jądra. Stworzono również Makefile, aby zautomatyzować proces kompilacji.

Wygenerowaliśmy w sumie cztery moduły, gdzie każdy z nich był odpowiedzialny za inny rodzaj przeprowadzanych testów.

Moduł o nazwie test\_performance\_allocation zawiera testy alokacji dużych bloków pamięci. Testowaliśmy tutaj wydajność alokacji a jednostką wydajności były tzw. Jiffies czyli jednostka czasu używana przez jądro systemu operacyjnego Linux’a do mierzenia upływu czasu. Jest to liczba ticków (tyknięć) zegara systemowego, które upłynęły od momentu uruchomienia systemu. Rezultat pomiaru może wskazać najwydajniejszą funkcję do alokacji pamięci z trzech testowanych.

Moduł o nazwie test\_non\_initialized testuje poprawność inicjalizacji zaalokowanej pamięci przez funkcji systemowe. W tym teście celowo nie inicjalizowaliśmy pamięci żadnymi wartościami początkowymi, aby sprawdzić jak funkcje sobie radzą z zerową inicjalizacją. W szczególności skupiliśmy się na wyniku zerowej inicjalizacji Kmalloc\_array i Kcalloc, gdyż według dokumentacji ta druga funkcja powinna zainicjalizować na tablicę zerami.

Moduł test\_max\_allocation sprawdza jak funkcje radzą sobie z inicjalizacją maksymalnych rozmiarów bloków pamięci. Wynikiem tego testu jest informacja czy funkcja zdołała przydzielić zaalokowaną pamięć dla bloku czy też próba alokacji skończyła się błędem – co by świadczyło o poprawnym wykryciu przez funkcje przekroczenia dozwolonego rozmiaru oraz zablokowaniu takiej możliwości. W przeciwnym razie mogłoby dojść do braku pamięci dla innych procesów np. systemowych co skutkuje zawieszeniem systemu.

Ostatnim modułem testowym jest moduł test\_times. Moduł ten testuje czasy alokacji pamięci i zwalniania jej dla funkcji alokujących tablice – Kmalloc\_array i Kcalloc. Pomiary czasu są dokonywane w zależności od reprezentatywnych ilości elementów tablicy n (od 1 do 1000) a wynik jest podawany w nanosekundach. Test jest wykonywany za pomocą pętli a czas jest mierzony za pomocą modułu standardowego time. Test ten miał na celu sprawdzić jak funkcje radzą sobie z alokacją danych tablicowych w kontekście złożoności czasowej.

# Wyniki testów

Po przeprowadzeniu wszystkich wyżej wymienionych testów, zebrano wyniki oraz przedstawiono je w formacie tabelarycznym.

Wyniki alokacji pamięci

|  |  |  |  |
| --- | --- | --- | --- |
| Funkcja | Wydajność alokacji dużych bloków pamięci (Jifies) | Test pustej inicjalizacji - zwrócona wartość | Test maksymalnej alokacji (sukces/błąd) |
| **Kmalloc** | 52 | pusta alokacja | błąd |
| **Kmalloc\_array** | 28 | pusta alokacja | błąd |
| **Kcalloc** | 31 | 0 | błąd |

1. Wydajność alokacji dużych bloków pamięci:

* **kmalloc\_array** wykazała najwyższą wydajność (28 jiffies) w porównaniu do kmalloc (52 jiffies) i kcalloc (31 jiffies). Sugeruje to, że kmalloc\_array jest najbardziej optymalną funkcją do alokacji dużych bloków pamięci.
* **kcalloc** jest nieco mniej wydajna od kmalloc\_array, ale bardziej efektywna niż kmalloc.

1. Pusta inicjalizacja:

* Zarówno kmalloc, jak i kmalloc\_array zwracają pustą alokację, co oznacza brak dodatkowej inicjalizacji przydzielonej pamięci.
* **kcalloc** zwraca 0, co oznacza, że dodatkowo inicjalizuje przydzieloną pamięć do zera, co może być korzystne w programach, które wymagają czystej pamięci po alokacji.

1. Maksymalna alokacja:

* Wszystkie testowane funkcje nie były w stanie przydzielić maksymalnego bloku pamięci, co wskazuje na ograniczenia funkcji systemowych, dzięki czemu unikamy możliwości zalokowania większej ilości pamięci niż dozwolona. Wskazuje to na poprawne działanie funkcji

Wyniki złożoności czasowej

|  |  |  |  |
| --- | --- | --- | --- |
| Funkcja | Czasy alokacji/zwalniania dla tablic n = 10 (ns) | Czasy alokacji/zwalniania dla tablic n = 100 (ns) | Czasy alokacji/zwalniania dla tablic n = 1000 (ns) |
| **Kmalloc\_array** | 674/386 | 10887/6154 | 173215/94821 |
| **Kcalloc** | 554/829 | 12844/6313 | 147357/188358 |
| **Uwagi** | Przy alokacji tablicy powyżej 1tys. elementów dochodzi do uszkodzenia jądra systemu operacyjnego na wskutek przepełnienia bufora | | |

* **kmalloc\_array** wykazała ogólnie szybsze czasy zwalniania pamięci niż kcalloc.
* Przy mniejszych tablicach (n = 10), kcalloc była szybsza w alokacji, ale wolniejsza w zwalnianiu w porównaniu do kmalloc\_array.
* Przy większych tablicach (n = 100 i n = 1000), **kmalloc\_array** była szybsza zarówno w alokacji, jak i zwalnianiu w porównaniu do kcalloc.

Na szczególną uwagę zasługuje fakt, iż alokacja pamięci w przypadku tablicy powyżej tysiąca elementów, dochodzi do uszkodzenia systemu, na wskutek przepełnienia bufora. Nie jest to pożądane zjawisku, gdyż w najlepszym razem nie mamy już pamięci na inne procesy a w najgorszym może dojść z uszkodzenia systemu operacyjnego.

# Wnioski końcowe

Po przeprowadzeniu testów oraz po wnikliwej analizie możemy wyciągnąć kilka wniosków. Możemy również przetestować tezę, iż wybór funkcji systemowej nie jest zależny tylko i wyłącznie od wydajności, czasu czy stabilności jej działania, lecz od głównego kontekstu użycia.

W przypadku testów wydajnościowych najlepiej wychodzi funkcja kmalloc\_array a najgorzej standardowe kmalloc. Nie determinuje to jednak wyboru, gdyż te dwie funkcje, pomimo, że są bliźniacze stworzone są do czegoś innego. Kmalloc to standardowa alokacja, podczas gdy kcalloc\_array to alokacja dla tablic. Stąd na tym polu mamy niejednoznaczność wyboru.

Jeśli chodzi o pustą inicjalizację, to tutaj każda z funkcji faktycznie zachowuje się tak jak jest to podane w dokumentacji. Mianowicie Kmalloc oraz Kmalloc\_array zwracają pustą inicjalizację, podczas gdy Kcalloc zwraca tablicę zainicjalizowaną zerami. Jeśli chodzi o wydajność to Kcalloc nieznacznie ustępuje jego bliźniakowi Kmalloc\_array, natomiast ten pierwszy gwarantuje poprawność tzw. pustej inicjalizacji – stąd do alokacji danych tablicowych naszym subiektywnym zdaniem lepiej sprawdzi się Kcalloc.

W przypadku zbyt dużego przydziału pamięci przez funkcję, każda z nich posiada – jak wykazaliśmy powyżej sprawny mechanizm zabezpieczający przed alokacją maksymalnego bloku pamięci. Co chroni system przed np. brakiem pamięci na inne procesy (w tym systemowe).

Pomimo, że kcalloc jest szybszy w alokacji bardzo małych (10 elementów) i bardzo dużych tablic (1000 elementów), kmalloc\_array jest ogólnie bardziej wydajny w zwalnianiu pamięci i w alokacji średnich rozmiarów tablic (100 elementów). To czyni kmalloc\_array bardziej wszechstronnym wyborem w przypadku, gdy zwalnianie pamięci jest częste i alokacje mają różny rozmiar. Chociaż kcalloc jest szybki w alokacji, jego czasy zwalniania pamięci są znacznie dłuższe niż kmalloc\_array, szczególnie dla bardzo dużych tablic. To może prowadzić do gorszej ogólnej wydajności w systemach, które często alokują i zwalniają pamięć.

Stąd jeśli zależy nam na poprawności inicjalizacji początkowej – skorzystajmy z Kcalloc, który zagwarantuje nam inicjalizację zerami. Natomiast jeśli zależy nam złożoności czasowej, to powinniśmy skorzystać z Kmalloc\_array.

Powyższe rozważanie potwierdzają tezę, że nie ma jednoznacznego wyboru, który będzie wyraźnie lepszy od drugiego. Każda z tych trzech funkcji – choć bliźniacze, to są stworzone do nieco innych zastosowań, co powinniśmy mieć na uwadze, przy podejmowaniu wyboru.