Damian Koper, 241292
SR-TN-17
Wrocław, 08.05.2019r.

Lab 5: Wątki, alokacja pamięci, atak z przepełnieniem stosu

Cel ćwiczenia

- Utworzenie dwóch wątków w obrębie jednej przestrzeni adresowej
- Porównanie czasu wykonania operacji wypełniania tablicy "po" wierszach i kolumnach
- Symulacja ataku typu przepełnienie stosu
- Przydział pamięci funkcjami systemowymi

Wątki

Wątki są procesami (na poziomie kernela), które współdzielą wszystkie dane, poza stosem i rejestrami. Z tego powodu przełączanie kontekstu pomiędzy wątkami jest dużo tańsze, niż pomiędzy odseparowanymi procesami.

Ochrona sekcji krytycznej

Wątki, mając dostęp do tych samych obszarów pamięci mogą konkurować między sobą o jej zasoby, nieraz prowadząc do zjawisk zakleszczenia lub zagłodzenia wątku/procesu. Sposobem przeciwdziałania takim zjawiskom jest odpowiednia ochrona sekcji krytycznej - sekcji, w której wszystkie operacja muszą być traktowane jako jedna operacja atomowa.

W zależności od sytuacji istnieją różne sposoby ochrony sekcji krytycznej:

1. Operacje atomowe - operacje, które muszą wykonać się w całości, zanim ktokolwiek inny uzyska dostęp do używanych zasobów. W porzypadku pojedynczych rozkazów możliwe jest użycie prefixu `LOCK`, który blokuję magistralę na czas wykonywania operacji.
2. Mutexy (Mutual Exclusion, wspólne wykluczenie) - Zablokowanie dostępu do zasobu dla wszystkich, poza jednym z wątków, któremu to dostęp został przydzielony na podstawie zasady *uczciwości* lub kolejki *FIFO*.
    1. SpinLock - wątek w pętli oczekuje na dostęp do zasobu na podstawie ustawionej flagi przez inny wątek. Po wyjściu z sekcji krytycznej czyści flagę. Użyte są tu niepodzielne instrukcje test-and-set np. `LOCK BTS`.
3.

Atak typu "Przepełnienie stosu"

Funkcje systemowe do alokacji pamięci

Wnioski

Literatura

1. Raw Linux Threads via System Calls - https://nullprogram.com/blog/2015/05/15/

2.