Politechnika Wrocławska

Architektura Systemów Komputerowych

Wykład 10

Dr inż. Radosław Michalski
Katedra Inteligencji Obliczeniowej, Wydział Informatyki i Zarządzania
Politechnika Wrocławska

Wersja 1.1, wiosna 2018

Źródła i licencja

Najbardziej aktualna wersja tego wykładu znajduje się tu:
https://github.com/rmhere/lecture-comp-arch-org

Zawartość tego wykładu

Rejestry `$hi` i `$lo`

Inline ASM

Przerwania i wyjątki

Buffer Overflow Attack

Rejestry `$hi` i `$lo`

Przeznaczenie

- wykorzystywane w mnożeniu i dzieleniu
- mnożenie:
  - `mult $t0, $t1`
  - mnożymy dwie 32-bitowe liczby
  - wynik może być 64-bitowy, a rejestry mają 32 bity
  - bity 0-31 wyniku - rejestr `$lo`
  - bity 32-63 wyniku - rejestr `$hi`
- dzielenie
  - `div $t0, $t1`
  - iloraz w `$lo`
  - reszta w `$hi`
- instrukcje `mfhi $rd` i `mflo $rd` do przenoszenia

Inline ASM

Demo

`inline.cpp`

Przerwania i wyjątki

Tryby pracy procesora

- user mode - ograniczone możliwości
  - ograniczony zestaw instrukcji
  - obszar pamięci programu
- kernel mode - bez ograniczeń
  - dowolna instrukcja
  - dowolny obszar pamięci

Przerwania i wyjątki

Wyjątki

Jak obsłużyć wyjątek?

- kernel obsługuje wszystkie wyjątki i przerwania
- rejestry `$k0` i `$k1`

Przerwania i wyjątki

Koprocesor 0 - rejestry

- $12 - status
- $13 - cause
- $14 - EPC

Przerwania i wyjątki

Rejestr 12 - status - obsługa przerwań

- bit 0 - interrupt enable (1 - tak, 0 - nie)
- bit 1 - exception level (0, ale 1 po wyjątku)
- bit 4 - user mode (1 - user mode, 0 - kernel mode)
- bity 8-15 - maska obsługiwanego przerwania

Przerwania i wyjątki

Rejestr 13 - cause - rodzaj wyjątku lub przerwania

- bity 2-6 - kod wyjątku
- bity 8-15 - oczekujące przerwania

Przerwania i wyjątki

Rejestr 14 - EPC - Exception Program Counter

W momencie wyjątku/przerwania $pc kopiowane do $epc aby móc do niego wrócić.

Przerwania i wyjątki

Demo

`mips_exception.asm`

Buffer Overflow Attack

Materiał wideo

Wideo

Computerphile - Buffer Overflow Attack

Slajd końcowy

Źródła i polecane materiały

- Karl Marklund, Operating systems, Uppsala University, Szwecja (materiały do kursu)

Slajd końcowy

Pytania? Komentarze?

Jeśli masz pomysł jak poprawić lub wzbogacić te wykłady,
proszę zgłoś to jako issue w tym repozytorium:

https://github.com/rmhere/lecture-comp-arch-org