Linux Assembly

Armine Hayrapetyan

Outline

- db dw dd dq
- timespec

db dw dd dq

We have learned “db”, or “define bytes”, and how it can be used to define bytes of data. A “byte” is always 8 bits, ranging from 0 to 255 (or -128 to 127).

```
section .data
        somedata db 5
```

db dw dd dq

A “word” is a certain number of bytes arising from the processor’s design.

For x86_64 processors, a “word” is equal to 2 bytes, or 16-bits. A “dword” or “double-word” is 4 bytes, or 32-bits, and a “qword” “quadruple word” is 8 bytes o 64-bits.

These can be defined using “dw”, “dd”, and “dq”.

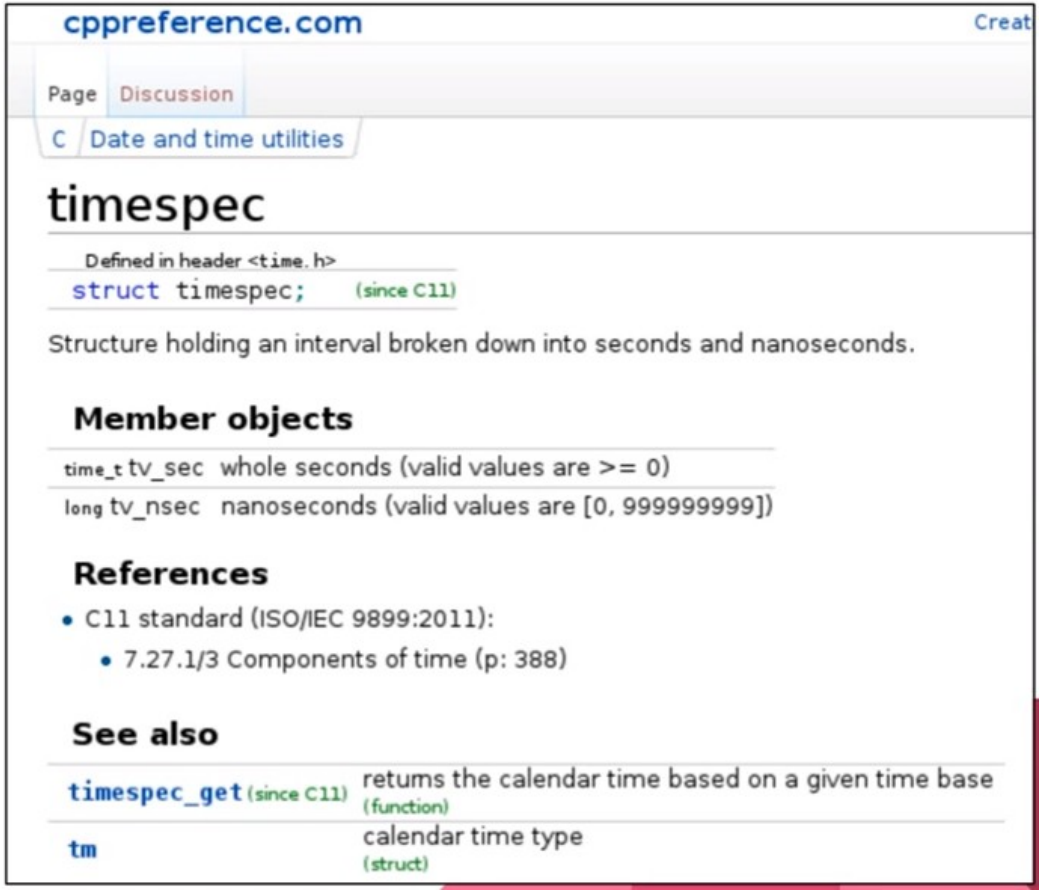
db	Define bytes
dw	Define word
dd	Define double word
dq	Define quadruple word

timespec

"Timespec" is a *structure* which holds two values, *tv_sec* and *tv_nsec*.

tv_sec and *tv_nsec* are both 64-bit integer values, in other words, they are *qwords*.

The max value for *tv_nsec* is 999,999,999, because 1 second = 1,000,000,000 nanoseconds.



cppreference.com Creat

Page Discussion

C Date and time utilities

timespec

Defined in header <time.h>

```
struct timespec;    (since C11)
```

Structure holding an interval broken down into seconds and nanoseconds.

Member objects

time_t tv_sec	whole seconds (valid values are >= 0)
long tv_nsec	nanoseconds (valid values are [0, 999999999])

References

- C11 standard (ISO/IEC 9899:2011):
  - 7.27.1/3 Components of time (p: 388)

See also

timespec_get (since C11)	returns the calendar time based on a given time base (function)
tm	calendar time type (struct)

sys_nanosleep

This system call can be used to suspend a program for a certain amount of time.

It is called “nanosleep” because its precision is down to nanoseconds.

The two arguments are both pointers to *timespec* values.

The first argument is the length of the delay, the second is often just left blank (rsi is set to 0).

syscall	ID	ARG1	ARG2	ARG3	ARG4	ARG5	ARG6
sys_nanosleep	35	$timespec	$timespec				

Example

This code will sleep for 5 seconds and 500,000,000 nanoseconds, or, 5.5 seconds.

After 5.5 seconds, the program will end.

```
section .data
        delay dq 5, 500000000

section .text
        global _start

_start:

        mov rax, 35
        mov rdi, delay
        mov rsi, 0
        syscall

        mov rax, 60
        mov rdi, 0
        syscall
```

References

- https://www.youtube.com/watch?v=bV0NJ7zvap8&list=PLetF-YjXm-sCH6FrTz4AQhfH6INDQvQSn&index=13