UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

Instrumente Structurale
2007-2013

Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

Sisteme de Operare 2

4. Spații de adresă

get_user

```
#define get_user(x,ptr) \
({ \
    int __ret_gu; \
    unsigned long __val_gu; \
    switch(sizeof (*(ptr))) { \
    case 1: 
        __get_user_x(1,__ret_gu,__val_gu,ptr); \
        break; \
    case 2: \
        __get_user_x(2,__ret_gu,__val_gu,ptr); \
        break; \
    ... 
    __ret_gu; \
})
```

__get_user_x

```
#define __get_user_x(size,ret,x,ptr) \
    __asm__ __volatile__( \
     "call __get_user_" #size \
     :"=a" (ret),"=d" (x) :"0" (ptr) \
    )

ENTRY(__get_user_1)
    GET_THREAD_INFO(%edx)
    cmpl TI_addr_limit(%edx),%eax
    jae bad_get_user
    1: movzbl (%eax),%edx
    xorl %eax,%eax
    ret
ENDPROC(__get_user_1)
```

__get_user_x

```
#define __get_user_x(size,ret,x,ptr) \
    __asm__ __volatile__( \
    "call __get_user_" #size \
    :"=a" (ret),"=d" (x) :"0" (ptr) \
)

ENTRY(__get_user_1)
    GET_THREAD_INFO(%edx)
    cmpl TI_addr_limit(%edx),%eax
    jae bad_get_user
    1: movzbl (%eax),%edx
    xorl %eax,%eax
    ret
ENDPROC(__get_user_1)
```

Este un pointer către userspace?

Instrucțiunea de copiere şi adresa ei

__get_user_x (2)

```
bad_get_user:
      xorl %edx,%edx
      movl $-14,%eax
      ret
END(bad_get_user)


.section __ex_table,"a"
.long 1b,bad_get_user
.long 2b,bad_get_user
.long 3b,bad_get_user
.previous
```

Adresa instrucțiunii ce face accesul în userspace din cadrul __get_user_1

Tabela de excepții

- Un vector de perechi (fault instruction address, fix-up code address)
- Generat la compilare în cadrul secțiunii __ex_table
- Rutina de tratare a page fault-ului va căuta adresa instrucțiunii ce a generat fault-ul în tabelă, şi dacă o găseşte va sări la adresa asociată

Accesul la datele din secțiunile speciale

- Scriptul de link editare (arch/*/kernel/*.lds.S) gardează secțiunea cu simboluri de genul __start / __stop
- Exemplu:

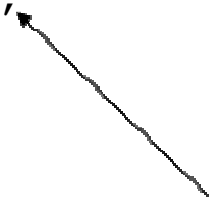
```
. = ALIGN(16); /* Exception table */
__ex_table : AT(ADDR(__ex_table) - LOAD_OFFSET) {
 __start___ex_table = .;
 *(__ex_table)
 __stop___ex_table = .;
}
```

fixup_exception

```
int fixup_exception(struct pt_regs *regs)
{
	const struct exception_table_entry *fixup;

	fixup = search_exception_tables(regs->eip);
	if (fixup) {
		regs->eip = fixup->fixup;
		return 1;
	}

	return 0;
}
```



Setăm instrucțiunea de la care se continuă execuția după ce ieşim din handler-ul de tratare al page-fault-ului