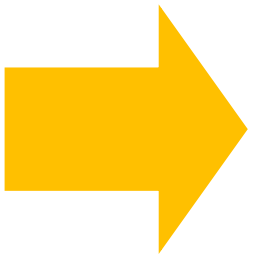
VEX

김영철

2016. 5. 16.

VEX

```
)0400549 <+0>:     push   rbp
)040054a <+1>:     mov    rbp,rsp
)040054d <+4>:     push   rbx
)040054e <+5>:     sub    rsp,0x8
)0400552 <+9>:     mov    esi,0x2
)0400557 <+14>:    mov    edi,0x1
)040055c <+19>:    call   0x40052d <max>
)0400561 <+24>:    mov    esi,eax
)0400563 <+26>:    mov    edi,0x400664
```



```
------ IMark(0x400549, 1, 0) ------
t0 = GET:I64(rbp)
t10 = GET:I64(rsp)
t9 = Sub64(t10,0x0000000000000008)
PUT(rsp) = t9
STle(t9) = t0
------ IMark(0x40054a, 3, 0) ------
PUT(rbp) = t9
PUT(rip) = 0x000000000040054d
------ IMark(0x40054d, 1, 0) ------
t2 = GET:I64(rbx)
t12 = Sub64(t9,0x0000000000000008)
PUT(rsp) = t12
STle(t12) = t2
------ IMark(0x40054e, 4, 0) ------
t4 = Sub64(t12,0x0000000000000008)
PUT(cc_op) = 0x0000000000000008
PUT(cc_dep1) = t12
PUT(cc_dep2) = 0x0000000000000008
------ IMark(0x400552, 5, 0) ------
PUT(rsi) = 0x0000000000000002
------ IMark(0x400557, 5, 0) ------
PUT(rdi) = 0x0000000000000001
PUT(rip) = 0x000000000040055c
------ IMark(0x40055c, 5, 0) ------
t16 = Sub64(t4,0x0000000000000008)
PUT(rsp) = t16
STle(t16) = 0x0000000000400561
t18 = Sub64(t16,0x0000000000000080)
```

VEX

- statement의 tag
  - IMark : original instruction 정보
  - Put : guest register에 쓰기
  - WrTmp : 임시변수에 값 할당
  - Store : memory에 쓰기
  - …

    *guest register : ebp, esp …

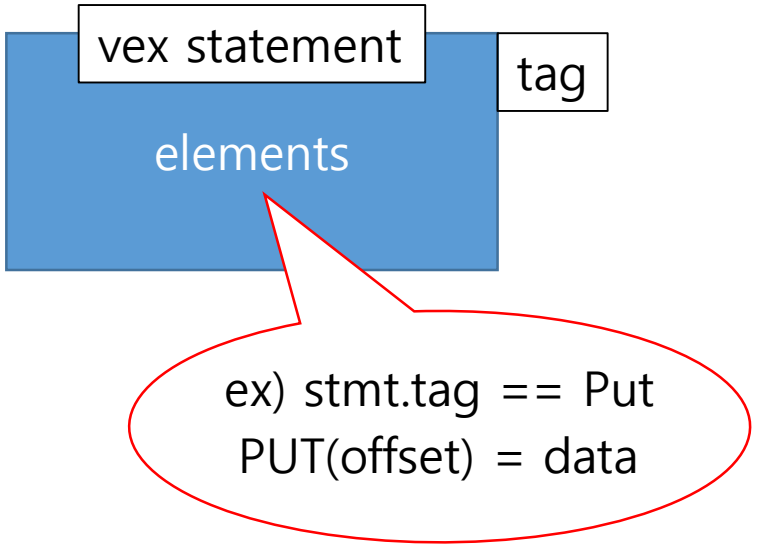
```
------ IMark(0x400549, 1, 0) ------
t0 = GET:I64(rbp)
t10 = GET:I64(rsp)
t9 = Sub64(t10,0x0000000000000008)
PUT(rsp) = t9
STle(t9) = t0
------ IMark(0x40054a, 3, 0) ------
PUT(rbp) = t9
PUT(rip) = 0x000000000040054d
------ IMark(0x40054d, 1, 0) ------
t2 = GET:I64(rbx)
t12 = Sub64(t9,0x0000000000000008)
PUT(rsp) = t12
STle(t12) = t2
------ IMark(0x40054e, 4, 0) ------
t4 = Sub64(t12,0x0000000000000008)
PUT(cc_op) = 0x0000000000000008
PUT(cc_dep1) = t12
PUT(cc_dep2) = 0x0000000000000008
------ IMark(0x400552, 5, 0) ------
PUT(rsi) = 0x0000000000000002
------ IMark(0x400557, 5, 0) ------
PUT(rdi) = 0x0000000000000001
PUT(rip) = 0x000000000040055c
------ IMark(0x40055c, 5, 0) ------
t16 = Sub64(t4,0x0000000000000008)
PUT(rsp) = t16
STle(t16) = 0x0000000000400561
t18 = Sub64(t16,0x0000000000000080)
```

VEX

- expression의 tag
  - Get : guest register로부터 읽기
  - RdTmp : 임시변수로부터 읽기
  - Binop : binary operation (인자 2개)
  - …

```
------ IMark(0x400549, 1, 0) ------
t0 = GET:I64(rbp)
t10 = GET:I64(rsp)
t9 = Sub64(t10,0x0000000000000008)
PUT(rsp) = t9
STle(t9) = t0
------ IMark(0x40054a, 3, 0) ------
PUT(rbp) = t9
PUT(rip) = 0x000000000040054d
------ IMark(0x40054d, 1, 0) ------
t2 = GET:I64(rbx)
t12 = Sub64(t9,0x0000000000000008)
PUT(rsp) = t12
STle(t12) = t2
------ IMark(0x40054e, 4, 0) ------
t4 = Sub64(t12,0x0000000000000008)
PUT(cc_op) = 0x0000000000000008
PUT(cc_dep1) = t12
PUT(cc_dep2) = 0x0000000000000008
------ IMark(0x400552, 5, 0) ------
PUT(rsi) = 0x0000000000000002
------ IMark(0x400557, 5, 0) ------
PUT(rdi) = 0x0000000000000001
PUT(rip) = 0x000000000040055c
------ IMark(0x40055c, 5, 0) ------
t16 = Sub64(t4,0x0000000000000008)
PUT(rsp) = t16
STle(t16) = 0x0000000000400561
t18 = Sub64(t16,0x0000000000000080)
```

VEX



➔우항의 data는 stmt.expressions로 접근

```
------ IMark(0x400549, 1, 0) ------
t0 = GET:I64(rbp)
t10 = GET:I64(rsp)
t9 = Sub64(t10,0x0000000000000008)
PUT(rsp) = t9
STle(t9) = t0
------ IMark(0x40054a, 3, 0) ------
PUT(rbp) = t9
PUT(rip) = 0x000000000040054d
------ IMark(0x40054d, 1, 0) ------
t2 = GET:I64(rbx)
t12 = Sub64(t9,0x0000000000000008)
PUT(rsp) = t12
STle(t12) = t2
------ IMark(0x40054e, 4, 0) ------
t4 = Sub64(t12,0x0000000000000008)
PUT(cc_op) = 0x0000000000000008
PUT(cc_dep1) = t12
PUT(cc_dep2) = 0x0000000000000008
------ IMark(0x400552, 5, 0) ------
PUT(rsi) = 0x0000000000000002
------ IMark(0x400557, 5, 0) ------
PUT(rdi) = 0x0000000000000001
PUT(rip) = 0x000000000040055c
------ IMark(0x40055c, 5, 0) ------
t16 = Sub64(t4,0x0000000000000008)
PUT(rsp) = t16
STle(t16) = 0x0000000000400561
t18 = Sub64(t16,0x0000000000000080)
```

VEX

- Put
  - ➔ PUT(register) = [tmp|const]
    def <- register
    use <- tmp

```
------ IMark(0x400549, 1, 0) ------
t0 = GET:I64(rbp)
t10 = GET:I64(rsp)
t9 = Sub64(t10,0x0000000000000008)
PUT(rsp) = t9
STle(t9) = t0
------ IMark(0x40054a, 3, 0) ------
PUT(rbp) = t9
PUT(rip) = 0x000000000040054d
------ IMark(0x40054d, 1, 0) ------
t2 = GET:I64(rbx)
t12 = Sub64(t9,0x0000000000000008)
PUT(rsp) = t12
STle(t12) = t2
------ IMark(0x40054e, 4, 0) ------
t4 = Sub64(t12,0x0000000000000008)
PUT(cc_op) = 0x0000000000000008
PUT(cc_dep1) = t12
PUT(cc_dep2) = 0x0000000000000008
------ IMark(0x400552, 5, 0) ------
PUT(rsi) = 0x0000000000000002
------ IMark(0x400557, 5, 0) ------
PUT(rdi) = 0x0000000000000001
PUT(rip) = 0x000000000040055c
------ IMark(0x40055c, 5, 0) ------
t16 = Sub64(t4,0x0000000000000008)
PUT(rsp) = t16
STle(t16) = 0x0000000000400561
t18 = Sub64(t16,0x0000000000000080)
```

VEX

- WrTmp
  - ➔ tmp = [GET|Binop(arg1, arg2)]
    def <- tmp
    use <- GET.offset
    <- arg1, arg2 if tmp

```
------ IMark(0x400549, 1, 0) ------
t0 = GET:I64(rbp)
t10 = GET:I64(rsp)
t9 = Sub64(t10,0x0000000000000008)
PUT(rsp) = t9
STle(t9) = t0
------ IMark(0x40054a, 3, 0) ------
PUT(rbp) = t9
PUT(rip) = 0x000000000040054d
------ IMark(0x40054d, 1, 0) ------
t2 = GET:I64(rbx)
t12 = Sub64(t9,0x0000000000000008)
PUT(rsp) = t12
STle(t12) = t2
------ IMark(0x40054e, 4, 0) ------
t4 = Sub64(t12,0x0000000000000008)
PUT(cc_op) = 0x0000000000000008
PUT(cc_dep1) = t12
PUT(cc_dep2) = 0x0000000000000008
------ IMark(0x400552, 5, 0) ------
PUT(rsi) = 0x0000000000000002
------ IMark(0x400557, 5, 0) ------
PUT(rdi) = 0x0000000000000001
PUT(rip) = 0x000000000040055c
------ IMark(0x40055c, 5, 0) ------
t16 = Sub64(t4,0x0000000000000008)
PUT(rsp) = t16
STle(t16) = 0x0000000000400561
t18 = Sub64(t16,0x0000000000000080)
```

VEX

- Store
  - ➔ STle(addr) = [tmp|const]
    def <- addr
    use <- tmp

```
------ IMark(0x400549, 1, 0) ------
t0 = GET:I64(rbp)
t10 = GET:I64(rsp)
t9 = Sub64(t10,0x0000000000000008)
PUT(rsp) = t9
STle(t9) = t0
------ IMark(0x40054a, 3, 0) ------
PUT(rbp) = t9
PUT(rip) = 0x000000000040054d
------ IMark(0x40054d, 1, 0) ------
t2 = GET:I64(rbx)
t12 = Sub64(t9,0x0000000000000008)
PUT(rsp) = t12
STle(t12) = t2
------ IMark(0x40054e, 4, 0) ------
t4 = Sub64(t12,0x0000000000000008)
PUT(cc_op) = 0x0000000000000008
PUT(cc_dep1) = t12
PUT(cc_dep2) = 0x0000000000000008
------ IMark(0x400552, 5, 0) ------
PUT(rsi) = 0x0000000000000002
------ IMark(0x400557, 5, 0) ------
PUT(rdi) = 0x0000000000000001
PUT(rip) = 0x000000000040055c
------ IMark(0x40055c, 5, 0) ------
t16 = Sub64(t4,0x0000000000000008)
PUT(rsp) = t16
STle(t16) = 0x0000000000400561
t18 = Sub64(t16,0x0000000000000080)
```

VEX

```
defi = []
use = []
for stmt_idx, stmt in enumerate(stmts):
    #vex information : angr.io/api-doc/pyvex.html
    #                 https://github.com/lu-zero/vex/blob/master/pub/libvex_ir.h
    exprs = stmt.expressions
    if      stmt.tag == 'Ist_IMark': #original inst info
        continue
    elif    stmt.tag == 'Ist_Put':   #PUT(offset) = data  e.i. PUT(rsp) = t9
        if stmt.offset not in defi:
            defi.append(stmt.offset)
        if exprs[0].tag == 'Iex_RdTmp':
            if exprs[0].tmp not in defi:
                use.append(exprs[0].tmp)
    elif    stmt.tag == 'Ist_PutI':  #PutI(descr)[ix,bias] = data
        continue
    elif    stmt.tag == 'Ist_WrTmp': #tmp = data    e.i. t2 = GET:I64(rbx)
        if stmt.tmp not in defi:
            defi.append(stmt.tmp)
        if   exprs[0].tag == 'Iex_Get': #GET:ty(offset)
            if exprs[0].offset not in defi:
                use.append(exprs[0].offset)
        elif exprs[0].tag == 'Iex_Binop':
            if exprs[1].tag == 'Iex_RdTmp':
                if exprs[1].tmp not in defi:
                    use.append(exprs[1].tmp)
            if exprs[2].tag == 'Iex_RdTmp':
                if exprs[2].tmp not in defi:
                    use.append(exprs[1].tmp)
    elif    stmt.tag == 'Ist_Store': #
        if stmt.addr.tmp not in defi:
            defi.append(stmt.addr.tmp)
        if   exprs[0].tag == 'Iex_RdTmp':
            if exprs[0].tmp not in defi:
                use.append(exprs[0].tmp)
```

VEX

```
python def_use.py
def : [0, 10, 9, 48, 56, 184, 2, 12, 4, 144, 152, 160, 64, 72, 16, 18]
use : [56, 48, 40]
```

48 : rbp
56 : rsp
184 : rip
144 : cc_op
152 : cc_dep1
160 : cc_dep2
64 : rsi
72 : rdi

```
------ IMark(0x400549, 1, 0) ------
t0 = GET:I64(rbp)
t10 = GET:I64(rsp)
t9 = Sub64(t10,0x0000000000000008)
PUT(rsp) = t9
STle(t9) = t0
------ IMark(0x40054a, 3, 0) ------
PUT(rbp) = t9
PUT(rip) = 0x000000000040054d
------ IMark(0x40054d, 1, 0) ------
t2 = GET:I64(rbx)
t12 = Sub64(t9,0x0000000000000008)
PUT(rsp) = t12
STle(t12) = t2
------ IMark(0x40054e, 4, 0) ------
t4 = Sub64(t12,0x0000000000000008)
PUT(cc_op) = 0x0000000000000008
PUT(cc_dep1) = t12
PUT(cc_dep2) = 0x0000000000000008
------ IMark(0x400552, 5, 0) ------
PUT(rsi) = 0x0000000000000002
------ IMark(0x400557, 5, 0) ------
PUT(rdi) = 0x0000000000000001
PUT(rip) = 0x000000000040055c
------ IMark(0x40055c, 5, 0) ------
t16 = Sub64(t4,0x0000000000000008)
PUT(rsp) = t16
STle(t16) = 0x0000000000400561
t18 = Sub64(t16,0x0000000000000080)
```