

```
mov     ecx, 3E8h
rep stosd
mov     esi, [esi]
push    1
call    esi
add     esp, 4
xor     eax, eax
```

Pointer to fake object
constructed by attacker

Call to shellcode

Without CFG

```
mov     ecx, 3E8h
rep stosd
mov     esi, [esi]
mov     ecx, esi
push    1
call    @_guard_check_icall@4
call    esi
add     esp, 4
xor     eax, eax
```

With CFG