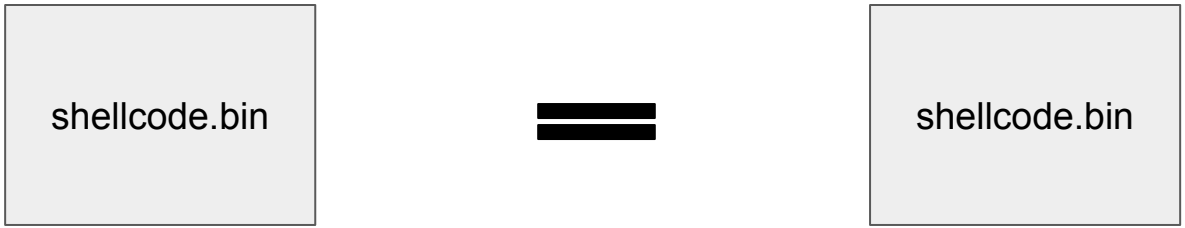
CSED702C-01 Walkthrough Presentation

shellcode-poly

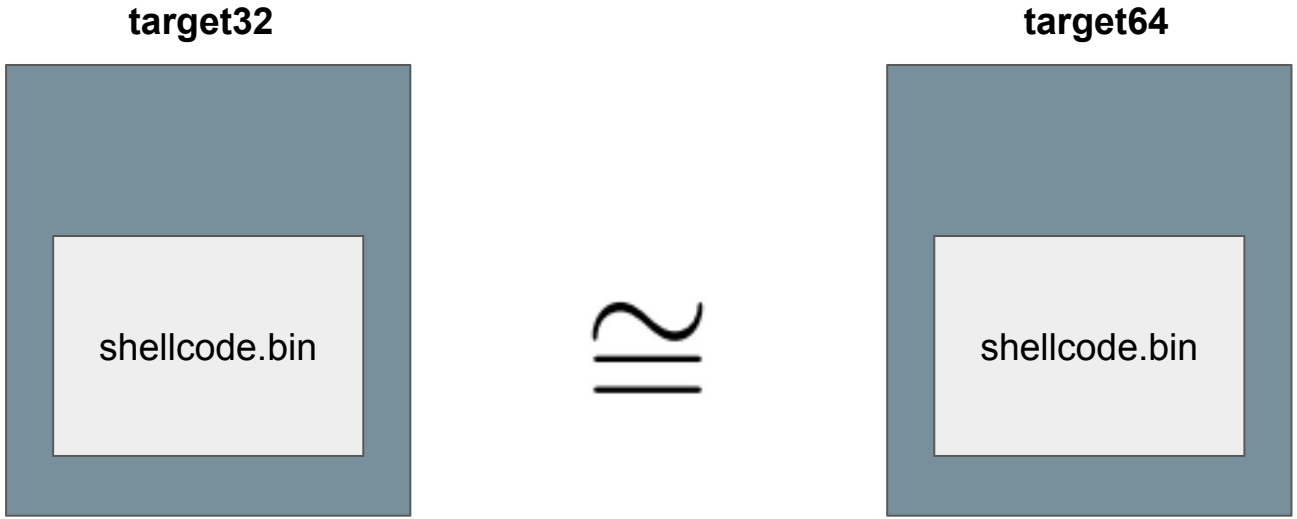
Byoungho Son

Challenge: shellcode-poly



Goal: construct a *single* shellcode.bin that

Challenge: shellcode-poly

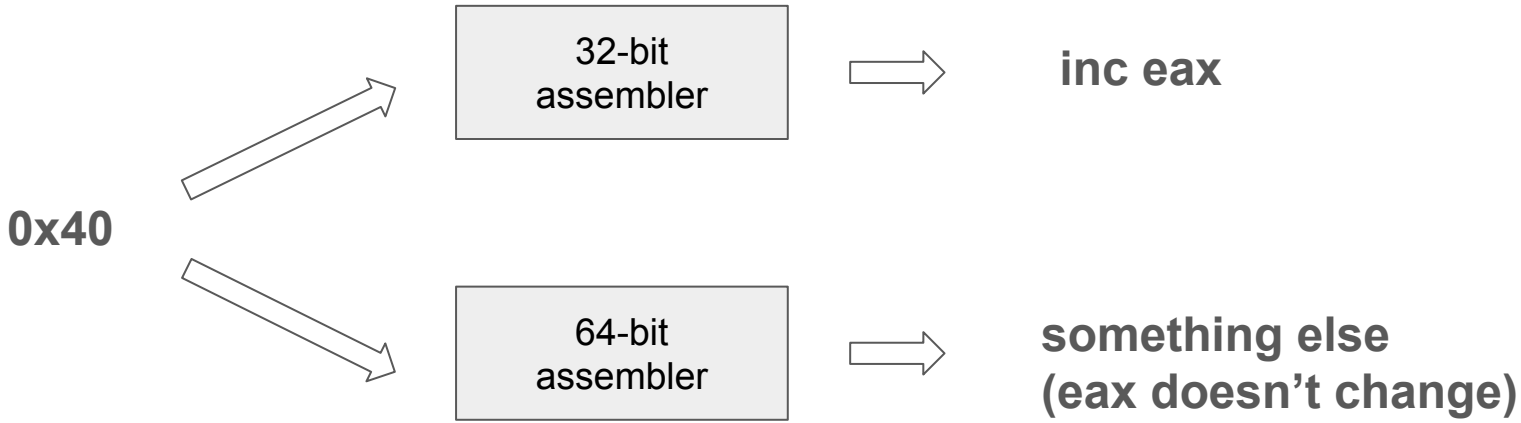


Goal: construct a *single* shellcode.bin that
when injected into x86 and x64 binary separately, they behave the same

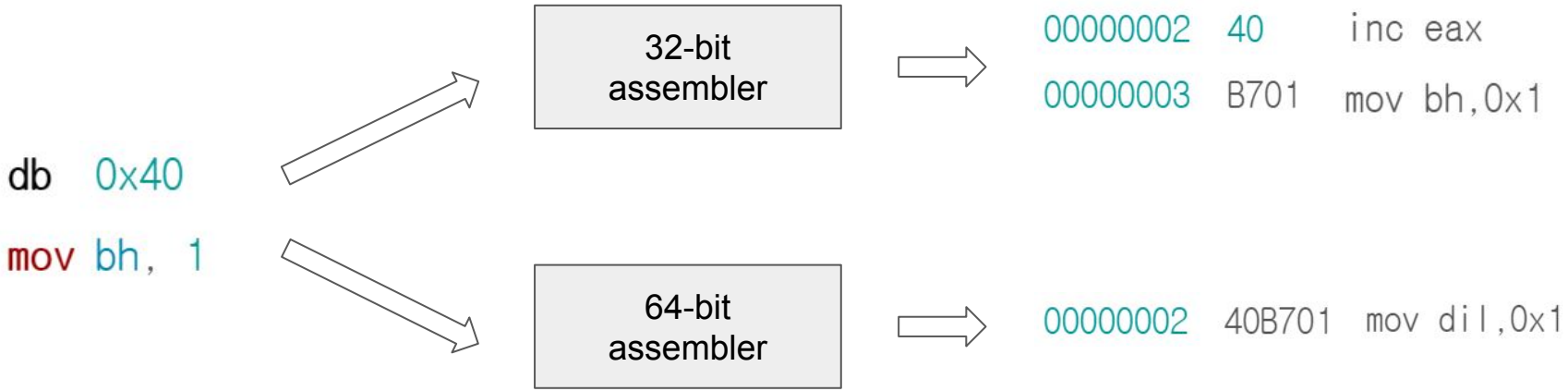
Q. How do we detect which environment we’re in?

A. Find a single bytecode that when interpreted differently, they behave differently (ironic!)

Idea from the article

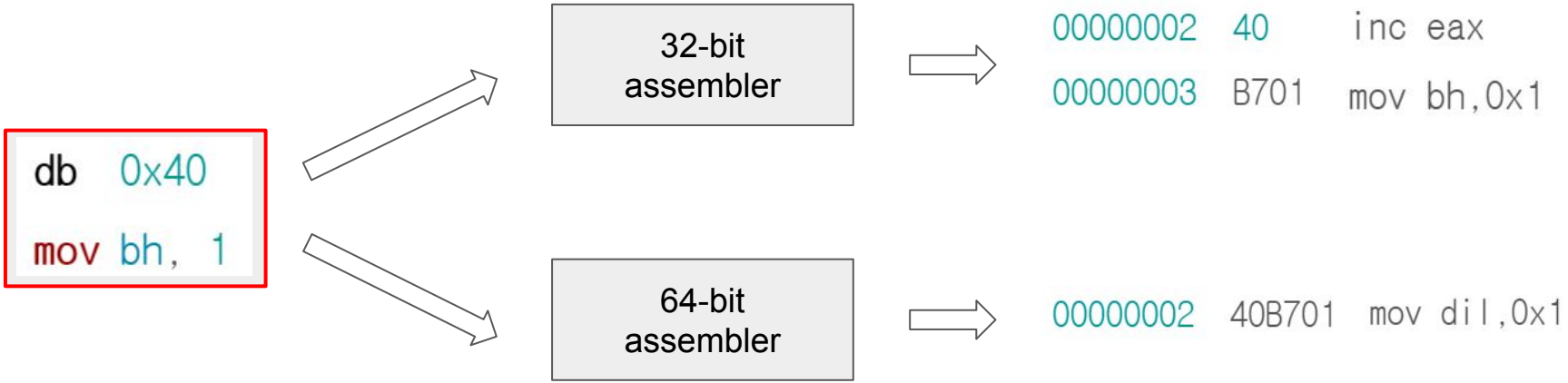


Idea from the article



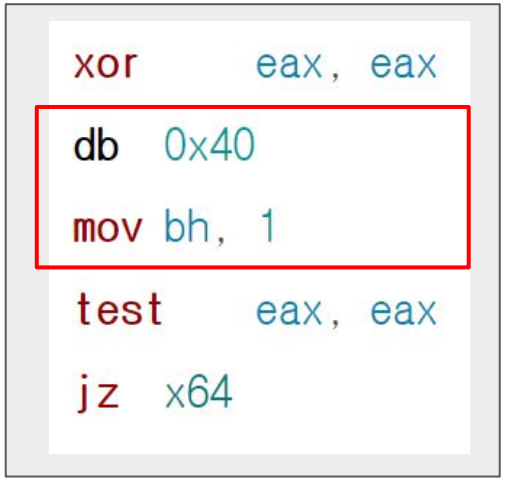
Observation: eax is modified by x32, whereas remains unchanged by x64

Idea from the article

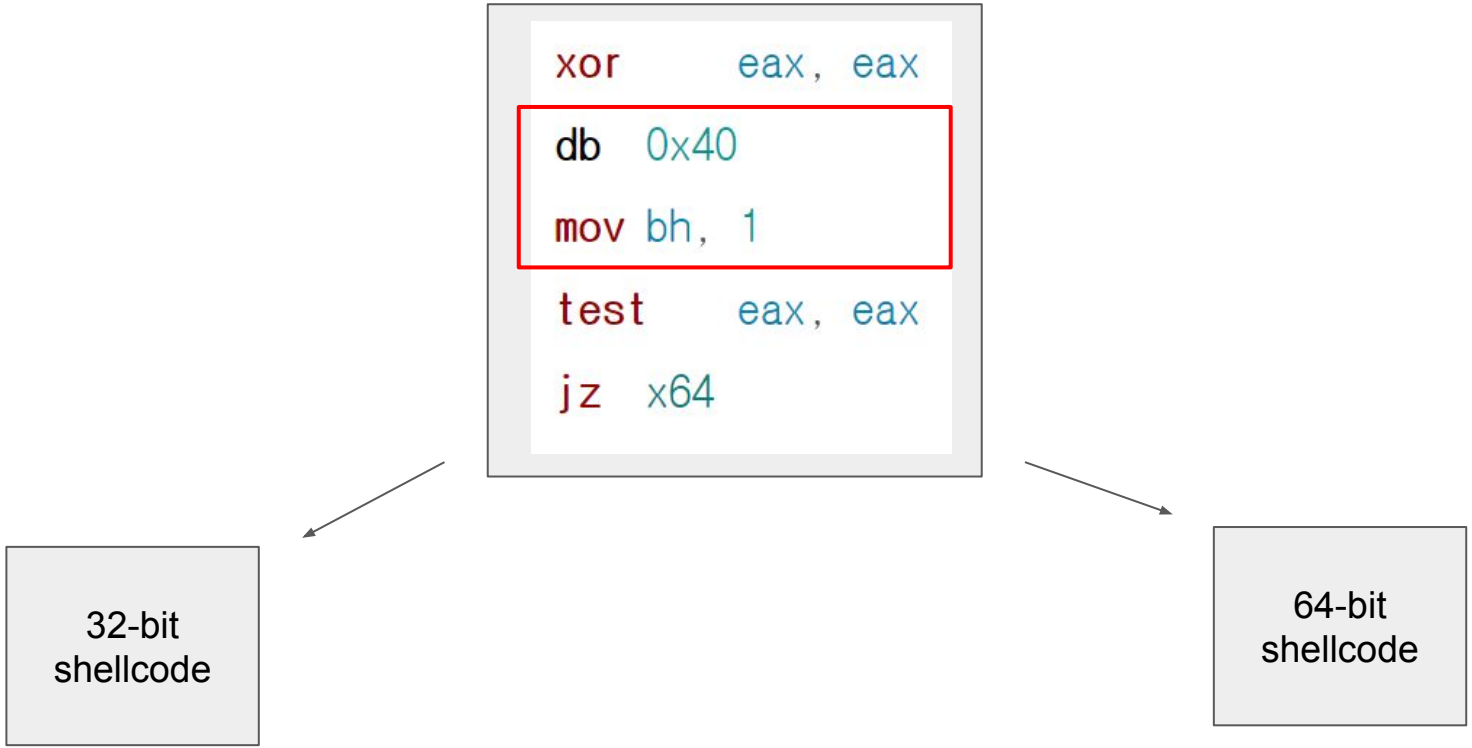


Idea: we can use this bit to construct a litmus test by observing the value of eax!

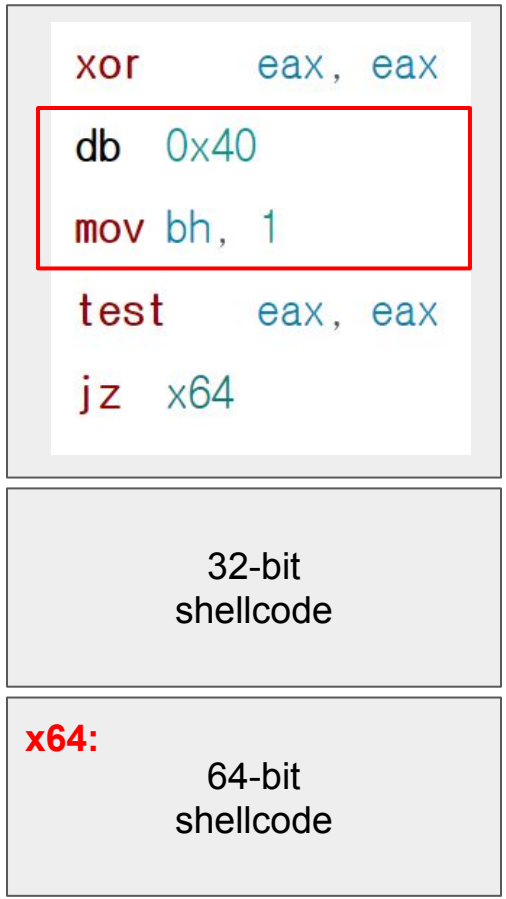
A litmus test



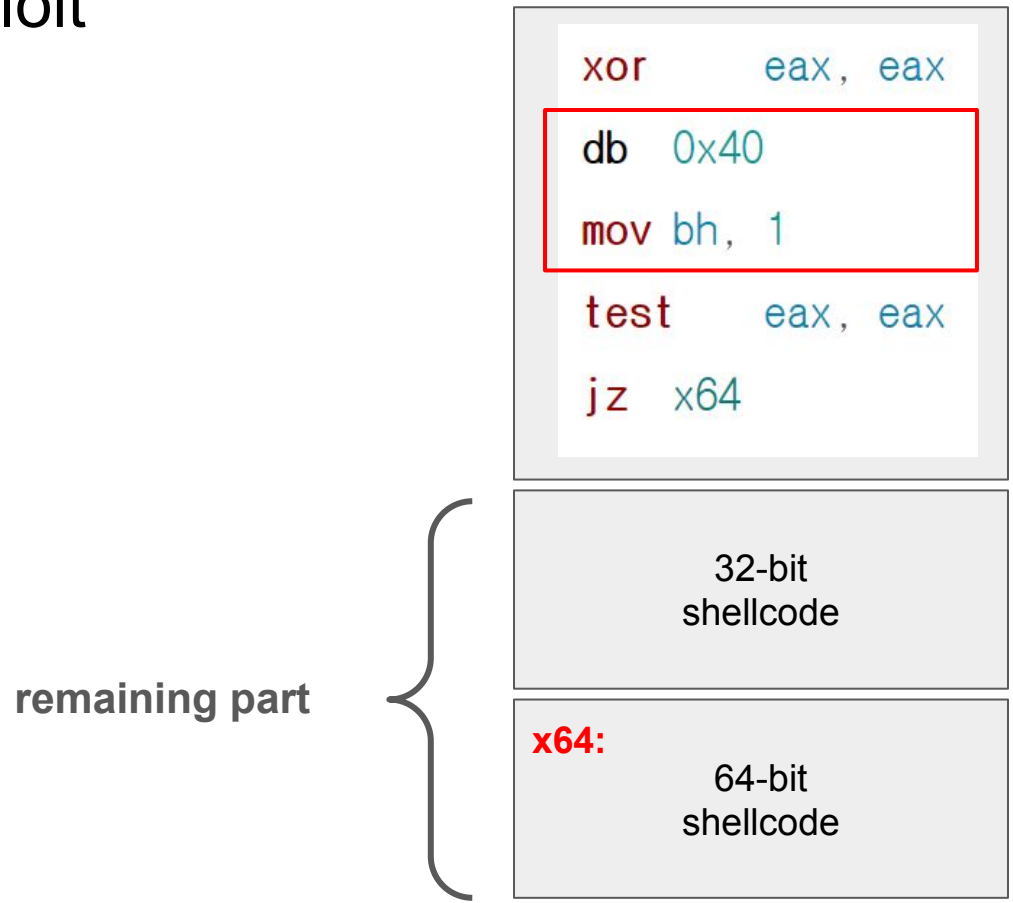
Exploit


xor eax, eax
db 0x40
mov bh, 1
test eax, eax
jz x64
32-bit shellcode
64-bit shellcode

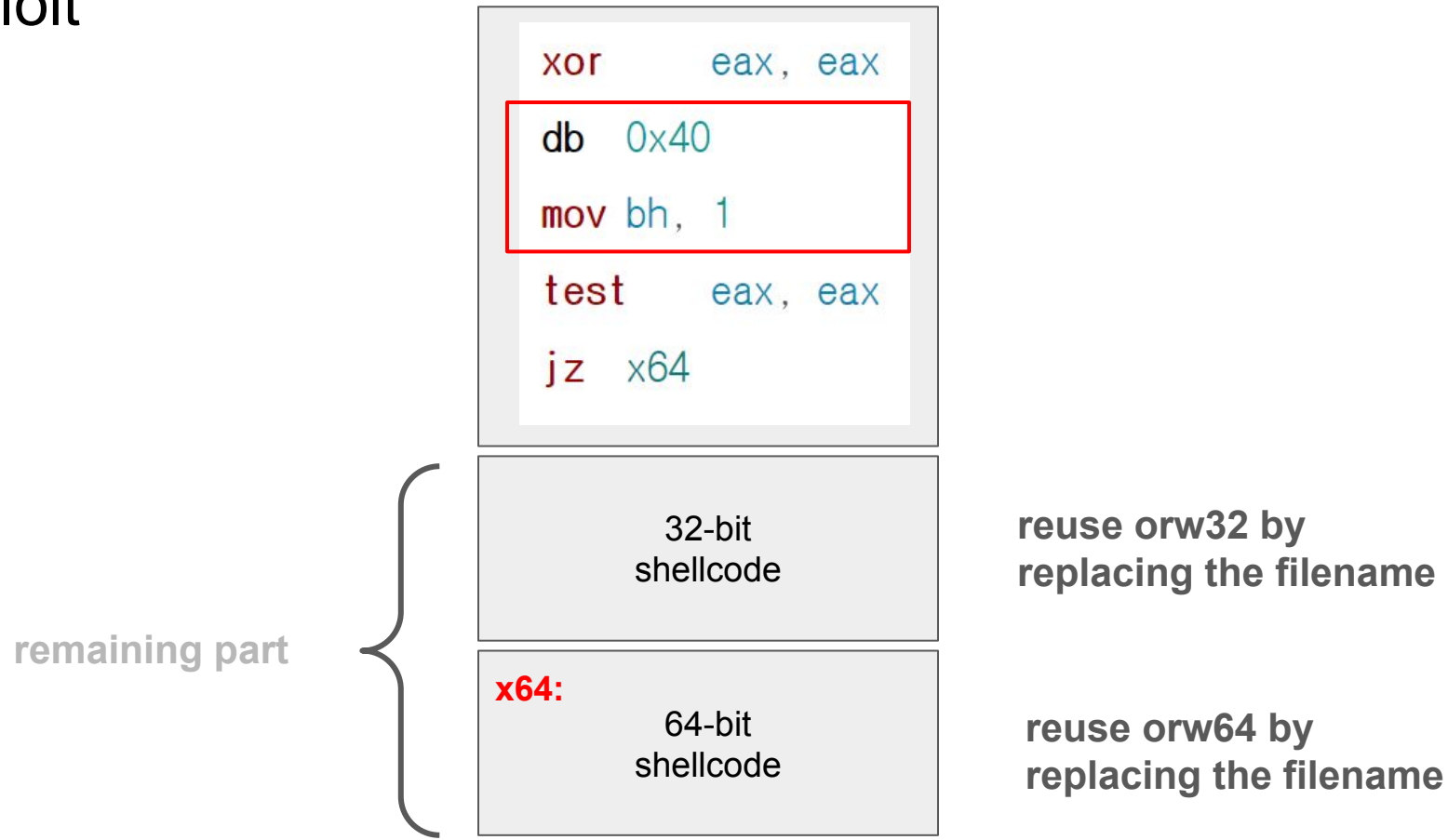
Exploit


xor eax, eax
db 0x40
mov bh, 1
test eax, eax
jz x64
32-bit
shellcode
x64:
64-bit
shellcode

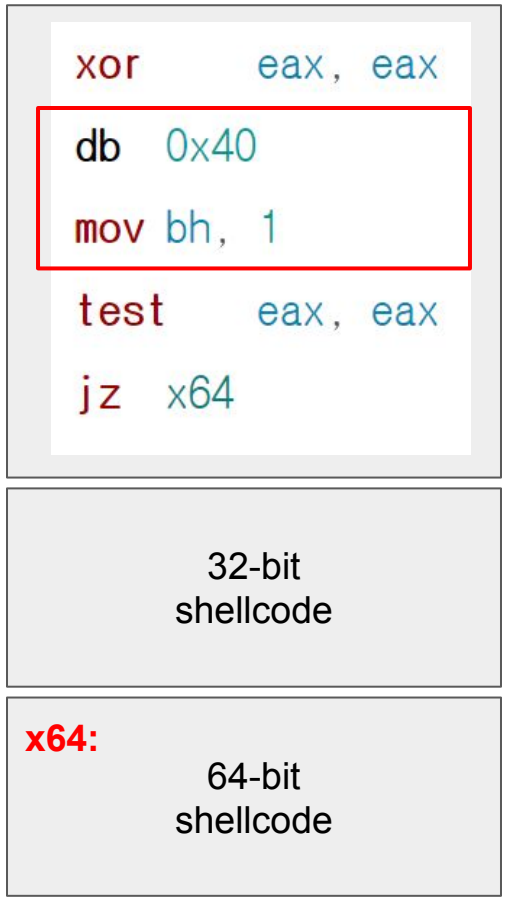
Exploit


xor eax, eax
db 0x40
mov bh, 1
test eax, eax
jz x64
32-bit
shellcode
remaining part
x64:
64-bit
shellcode

Exploit


xor eax, eax
db 0x40
mov bh, 1
test eax, eax
jz x64
32-bit
shellcode
x64:
64-bit
shellcode
remaining part
reuse orw32 by
replacing the filename
reuse orw64 by
replacing the filename

Exploit

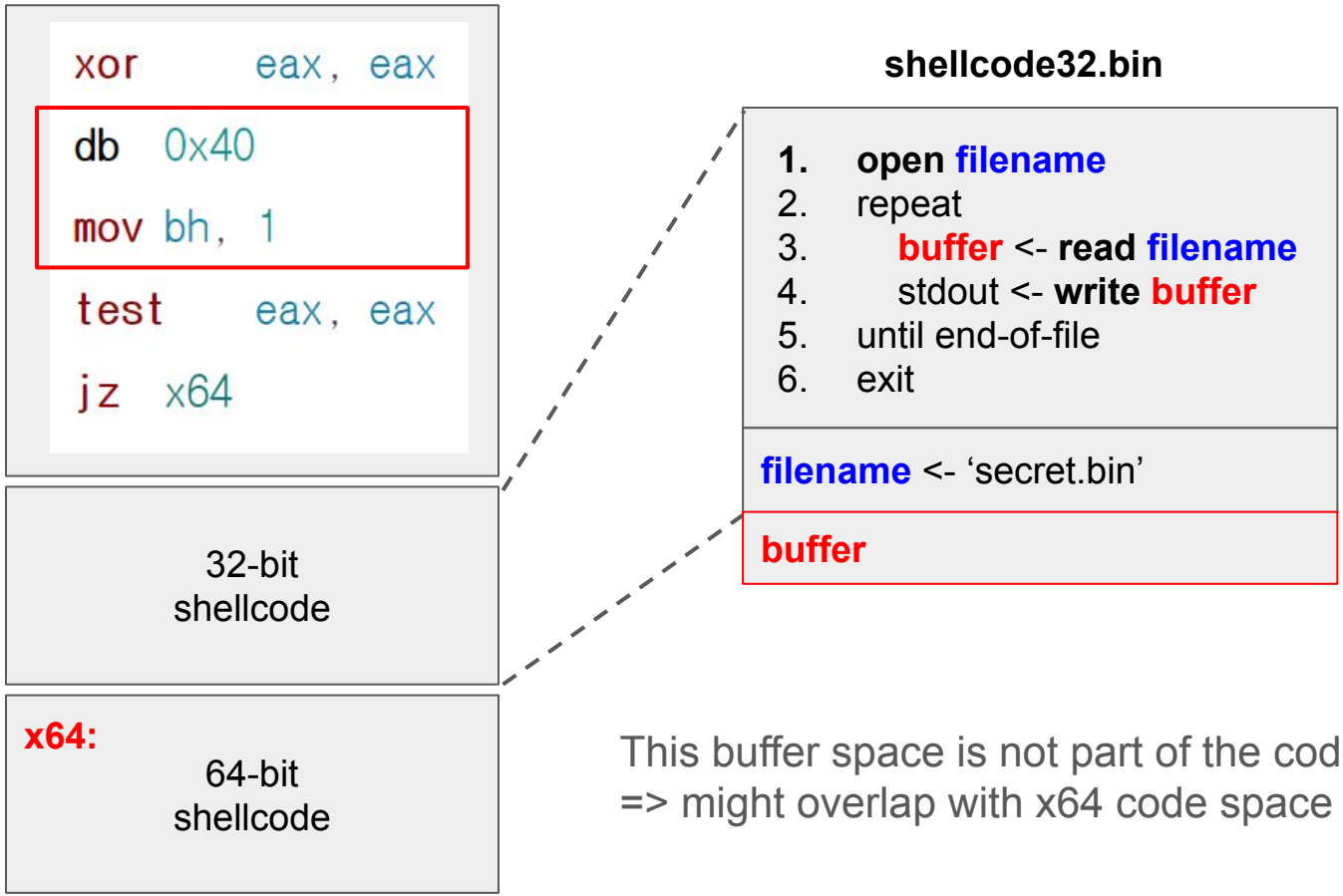


can we just naively concatenate them?

reuse orw32 by replacing the filename

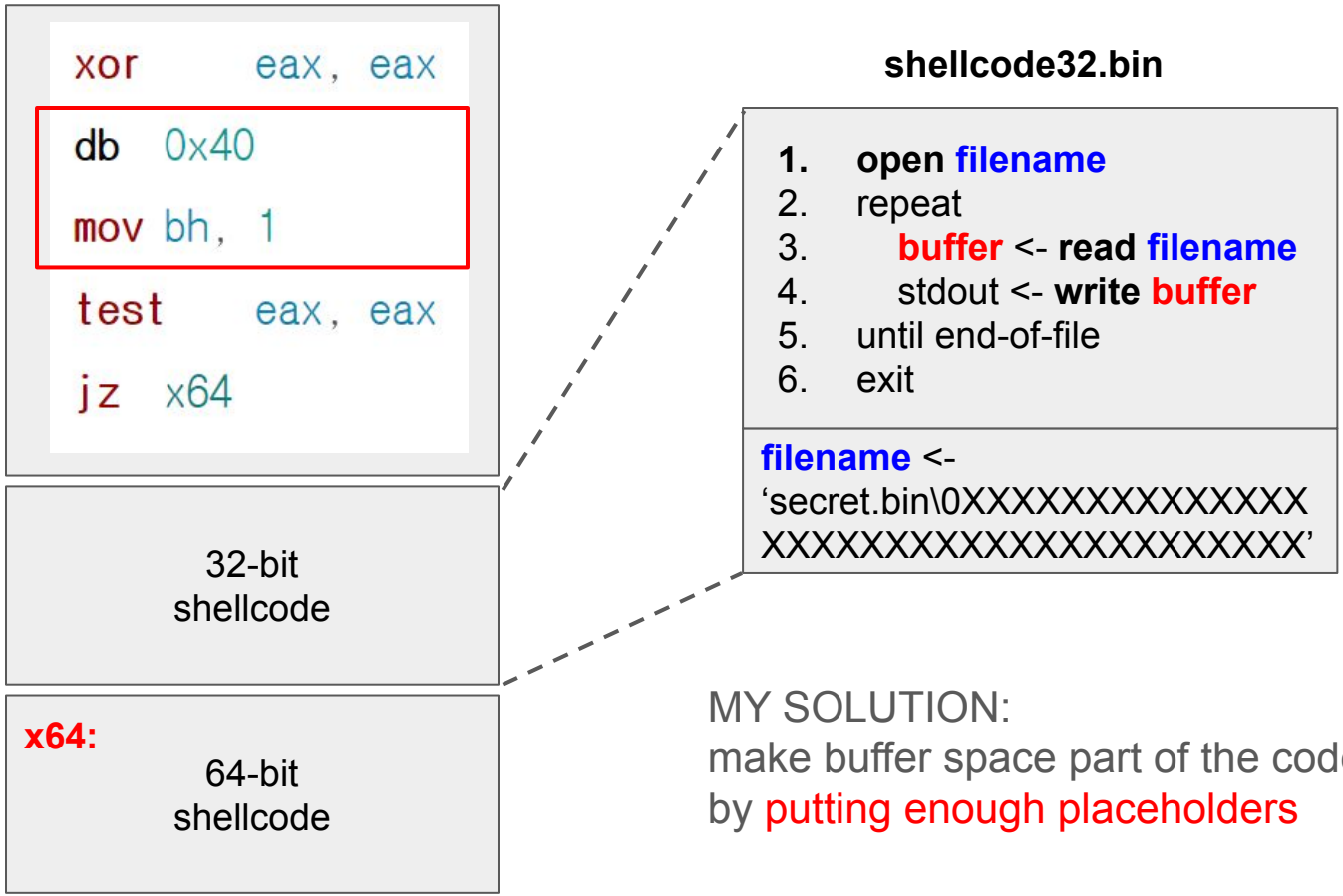
reuse orw64 by replacing the filename

Exploit



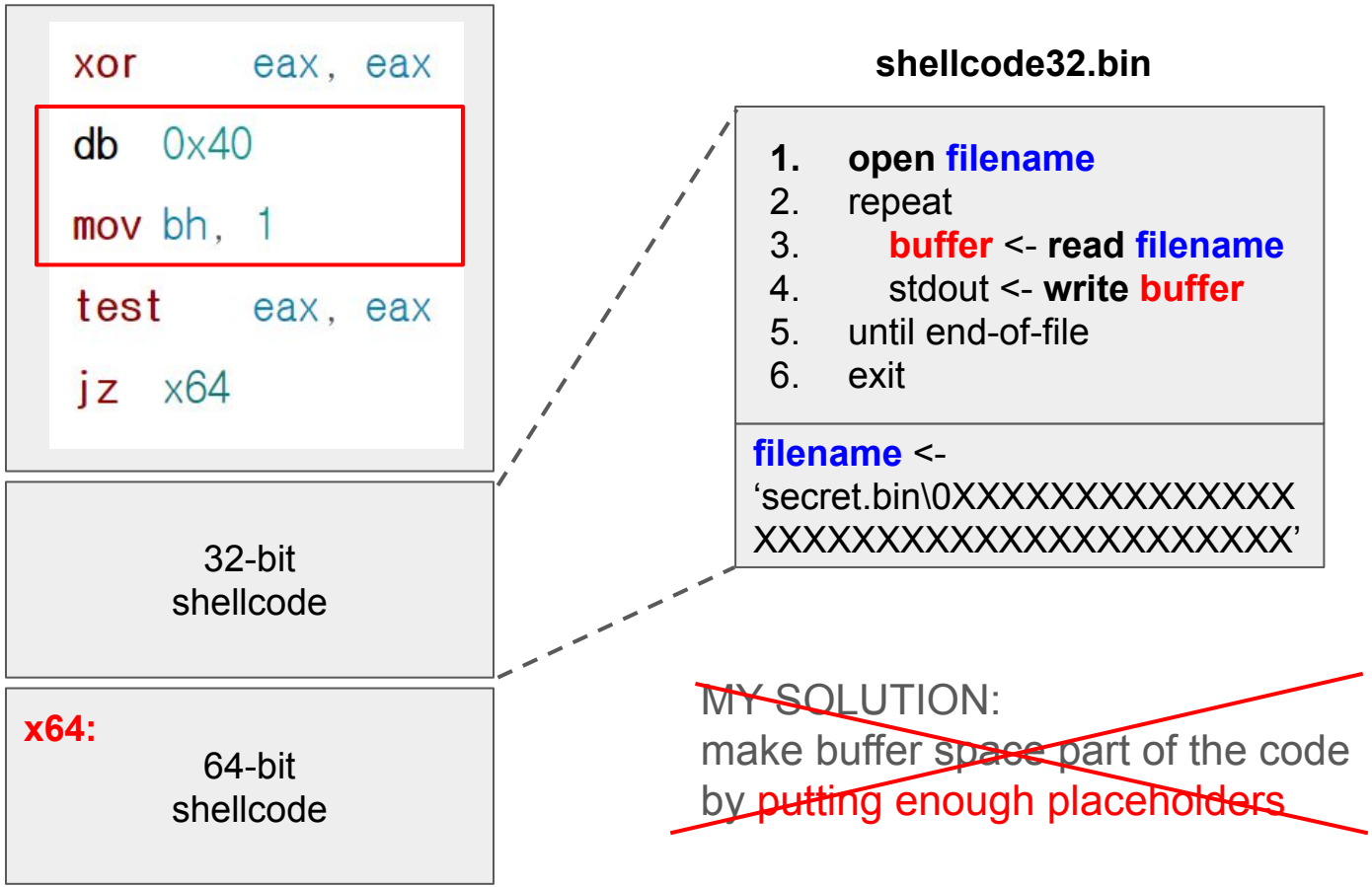
This buffer space is not part of the code
=> might overlap with x64 code space

Exploit



MY SOLUTION:
make buffer space part of the code
by putting enough placeholders

Exploit


xor eax, eax
db 0x40
mov bh, 1
test eax, eax
jz x64
32-bit
shellcode
x64:
64-bit
shellcode
shellcode32.bin
1. open filename
2. repeat
3. buffer <- read filename
4. stdout <- write buffer
5. until end-of-file
6. exit
filename <-
'secret.bin\0XXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXX'
MY SOLUTION:
make buffer space part of the code
by putting enough placeholders

Thank you!