

# SCS1312 Operating System Concepts

Dr. Chamath Keppitiyagama

University of Colombo School of Computing

```
int f()
{
// Some stuff here

    return 0;
}
```

f :

```
    movl $20, %eax
    movl $10, %ebx
    ...
    ...
    ret
```

# main.c

```
int main(void)
{
    // Some stuff here

    f();

    // Some other stuff here
    return 0;
}
```

## main.s

```
main:  
    movl $100, %eax  
    movl $125, %ebx  
    ...  
    ...  
    call _f  
    addl %eax, %ebx  
    ...  
    ...  
    ...
```

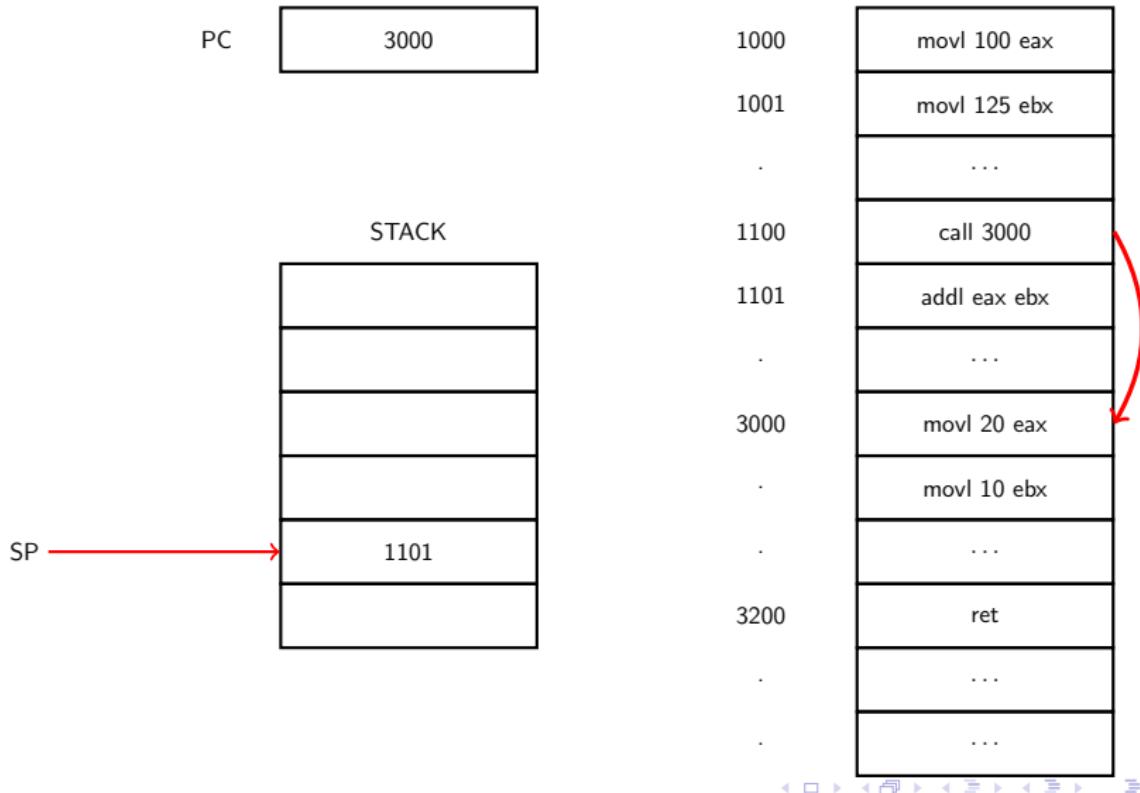
# Calling Functions

1000	movl 100 eax
1001	movl 125 ebx
.	...
1100	call 3000
1101	addl eax ebx
.	...
3000	movl 20 eax
.	movl 10 ebx
.	...
3200	ret
.	...
.	...

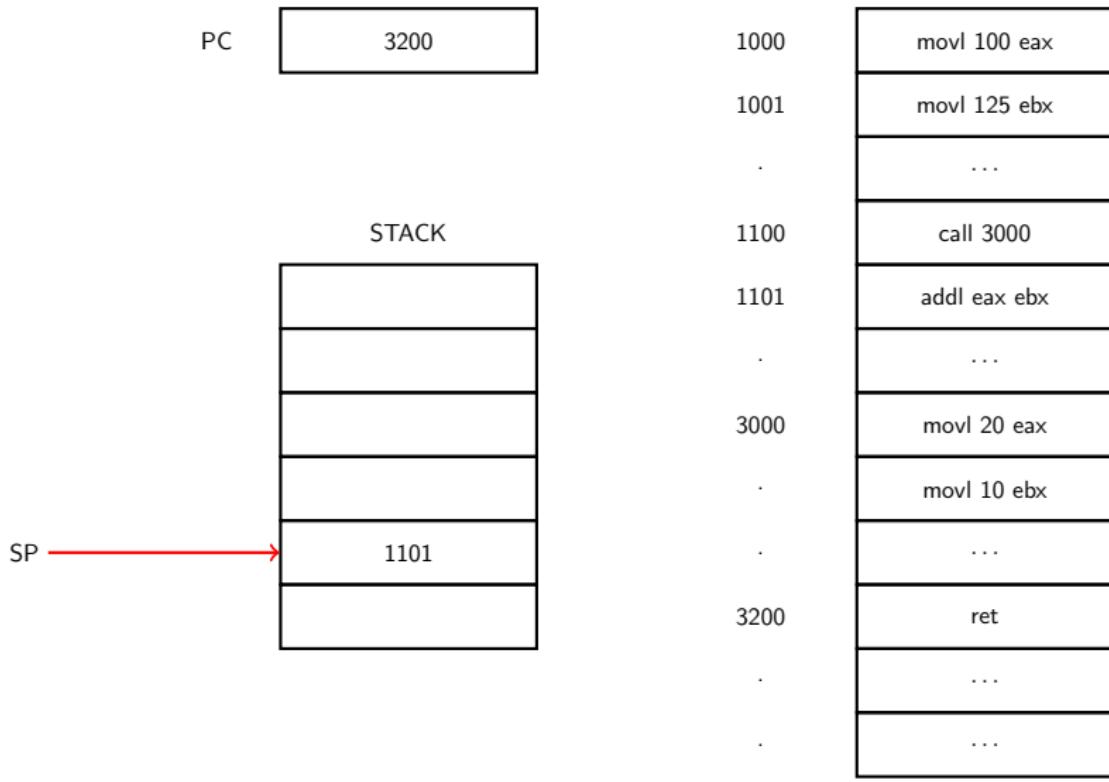
# Calling Functions

PC	1100	1000	movl 100 eax
		1001	movl 125 ebx
		.	...
	1100	1100	call 3000
		1101	addl eax ebx
		.	...
	3000	3000	movl 20 eax
		3001	movl 10 ebx
		.	...
	3200	3200	ret
		.	...
		3201	...

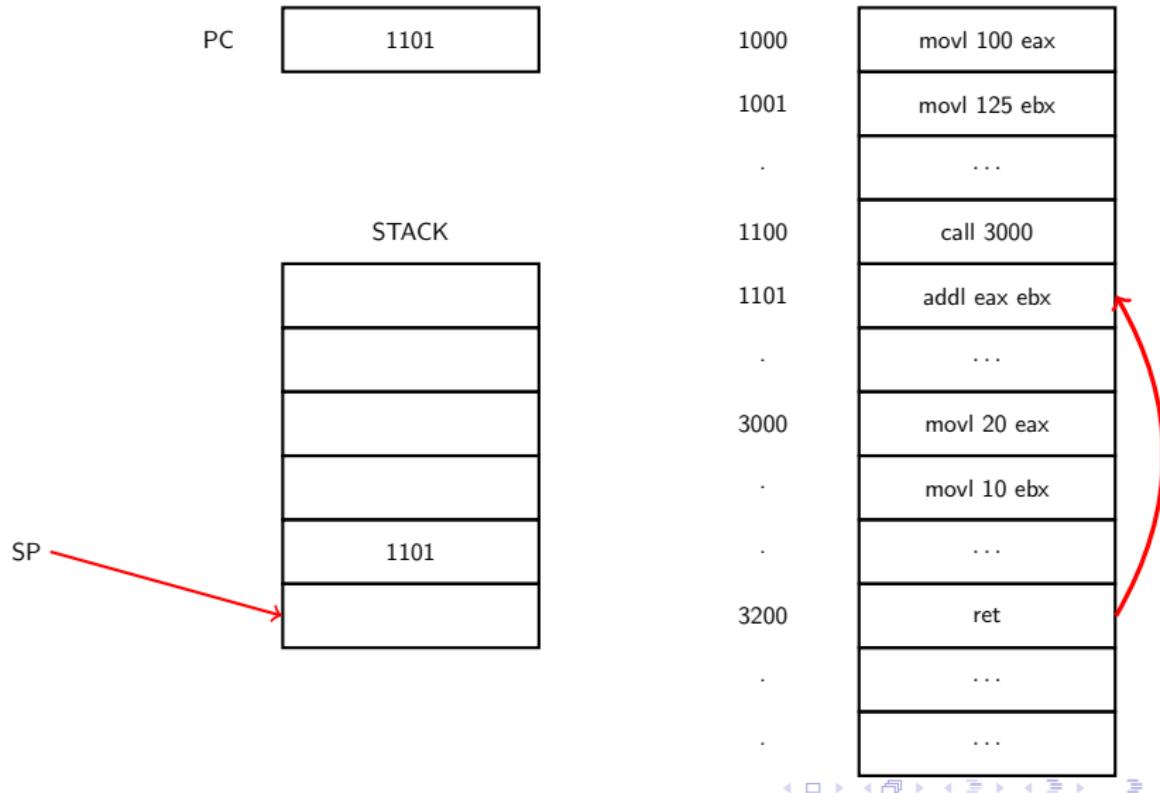
# Calling Functions



# Returning



# Returning



# Registers - Just before calling f()

PC	1100
eax	100
ebx	125

1000	movl 100 eax
1001	movl 125 ebx
.	...
1100	call 3000
1101	addl eax ebx
.	...
3000	movl 20 eax
.	movl 10 ebx
.	...
3200	ret
.	...
.	...

# Registers - Just after returning from f()

PC	1101		
eax	20	1000	movl 100 eax
ebx	10	1001	movl 125 ebx
	.	.	...
		1100	call 3000
		1101	addl eax ebx
	.	.	...
		3000	movl 20 eax
		.	movl 10 ebx
	.	.	...
		3200	ret
		.	...
		.	...

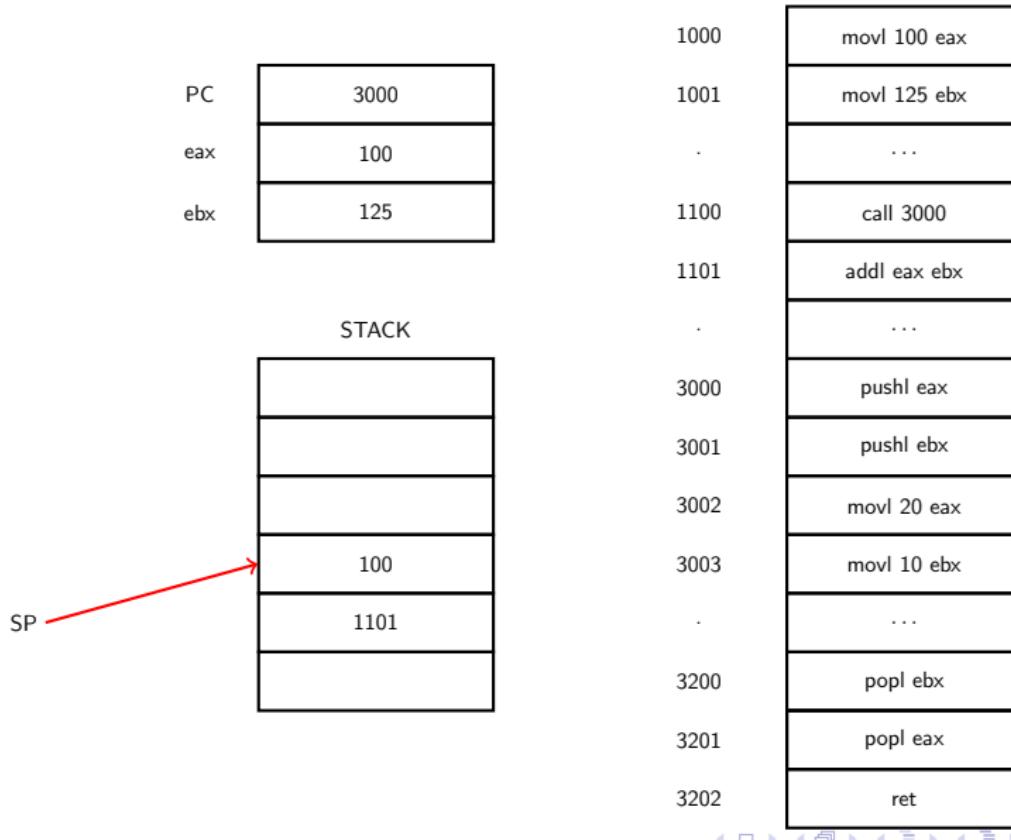
f :

```
pushl %eax
pushl %ebx
movl $20, %eax
movl $10, %ebx
.....
.....
popl %ebx
popl %eax
ret
```

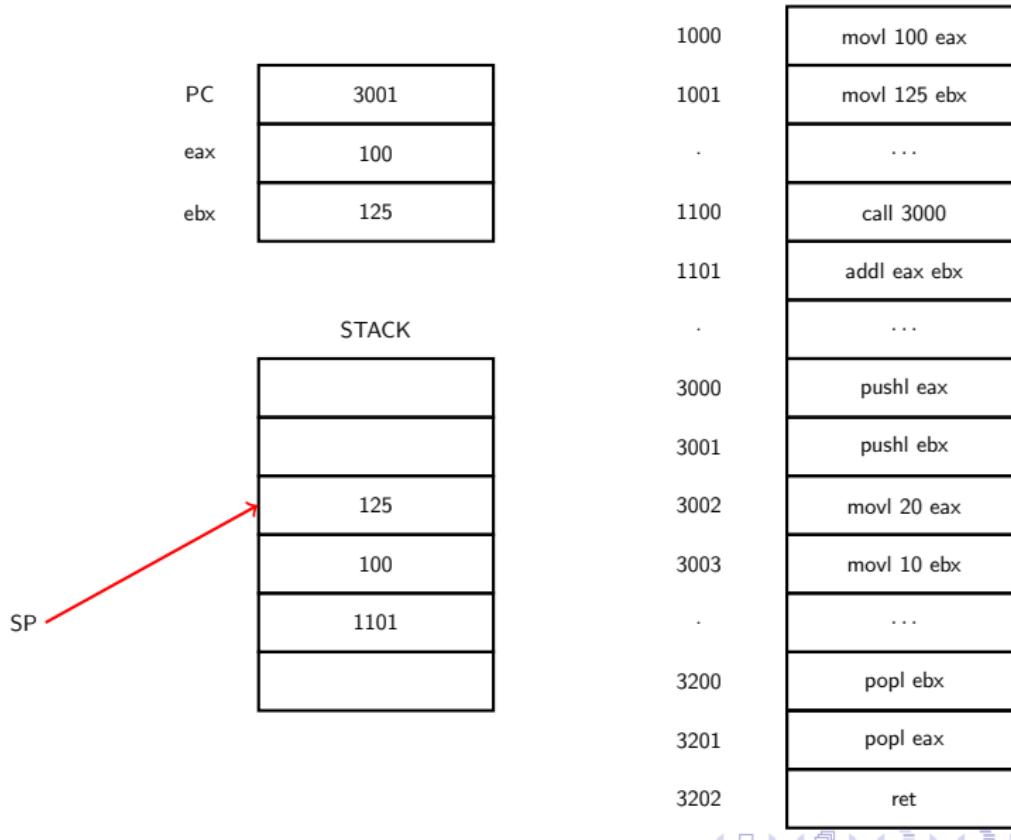
# Registers - Just before calling f()

PC	1100	1000	movl 100 eax
eax	100	1001	movl 125 ebx
ebx	125	.	...
		1100	call 3000
		1101	addl eax ebx
		.	...
		3000	pushl eax
		3001	pushl ebx
		3002	movl 20 eax
		3003	movl 10 ebx
		.	...
		3200	popl ebx
		3201	popl eax
		3202	ret

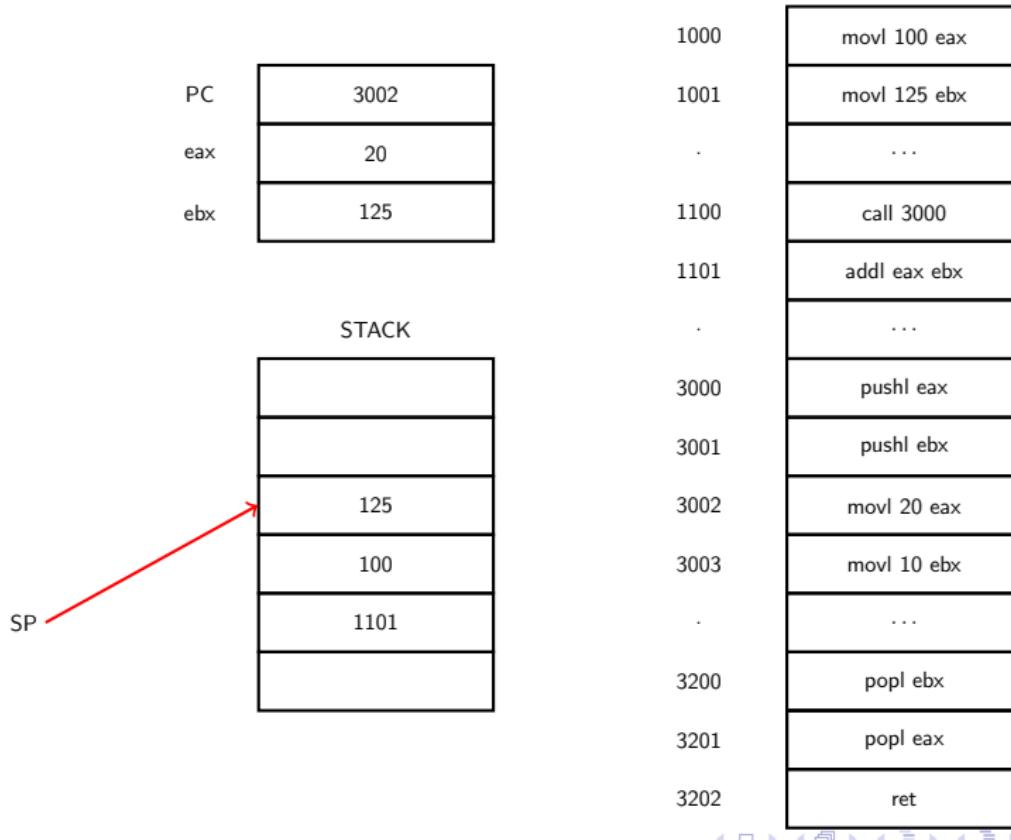
# Registers - In f()



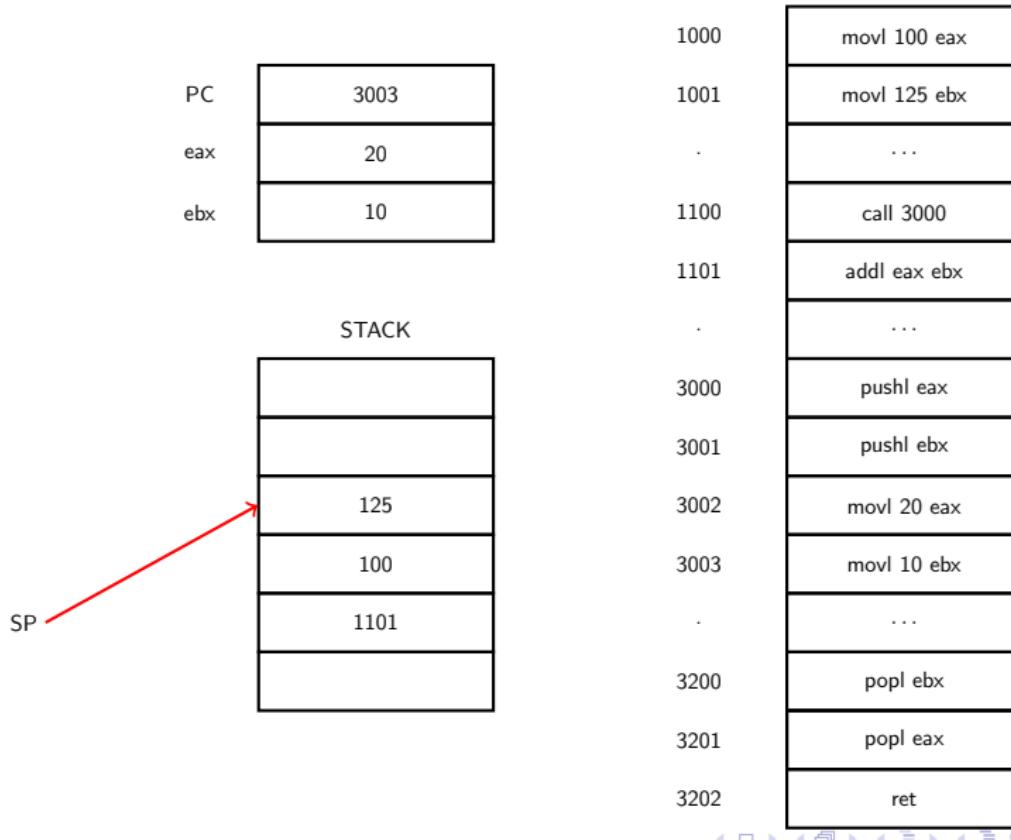
# Registers - In f()



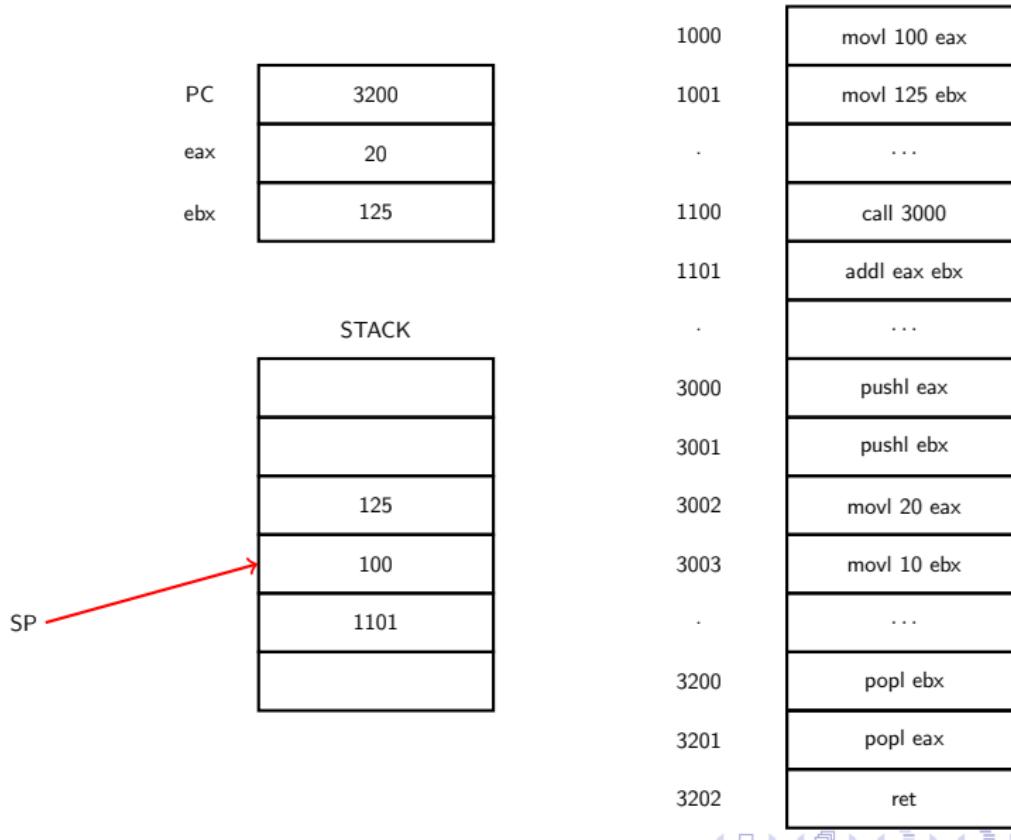
# Registers - In f()



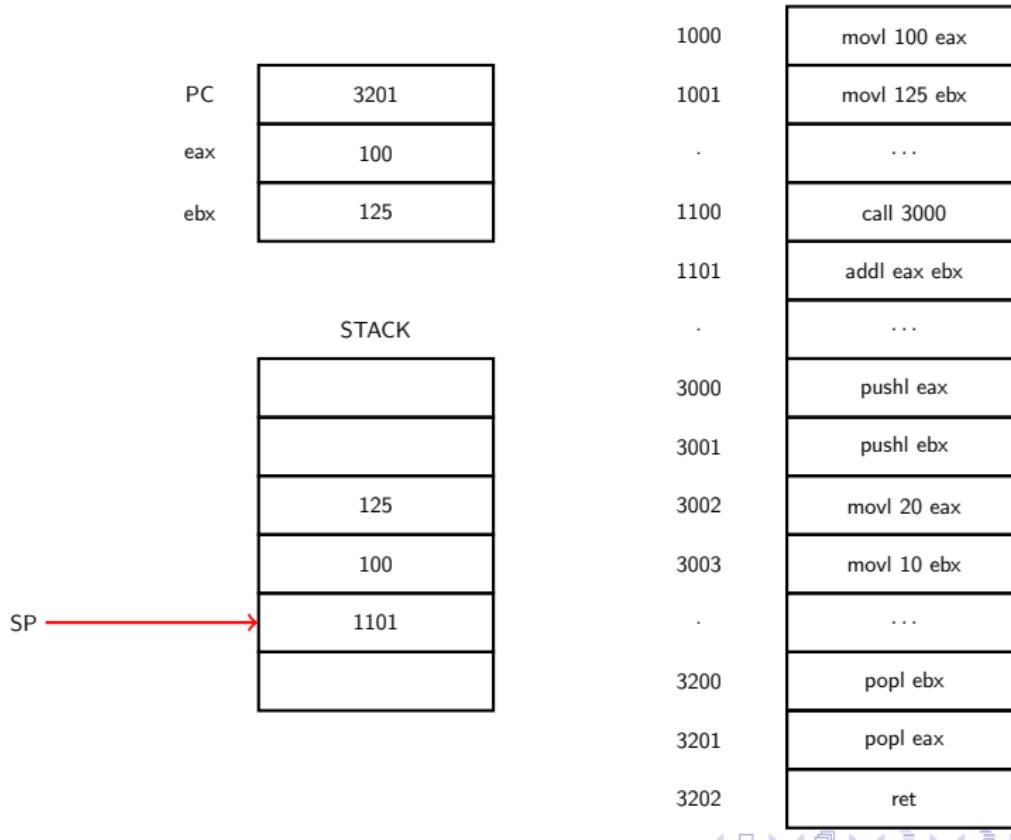
# Registers - In f()



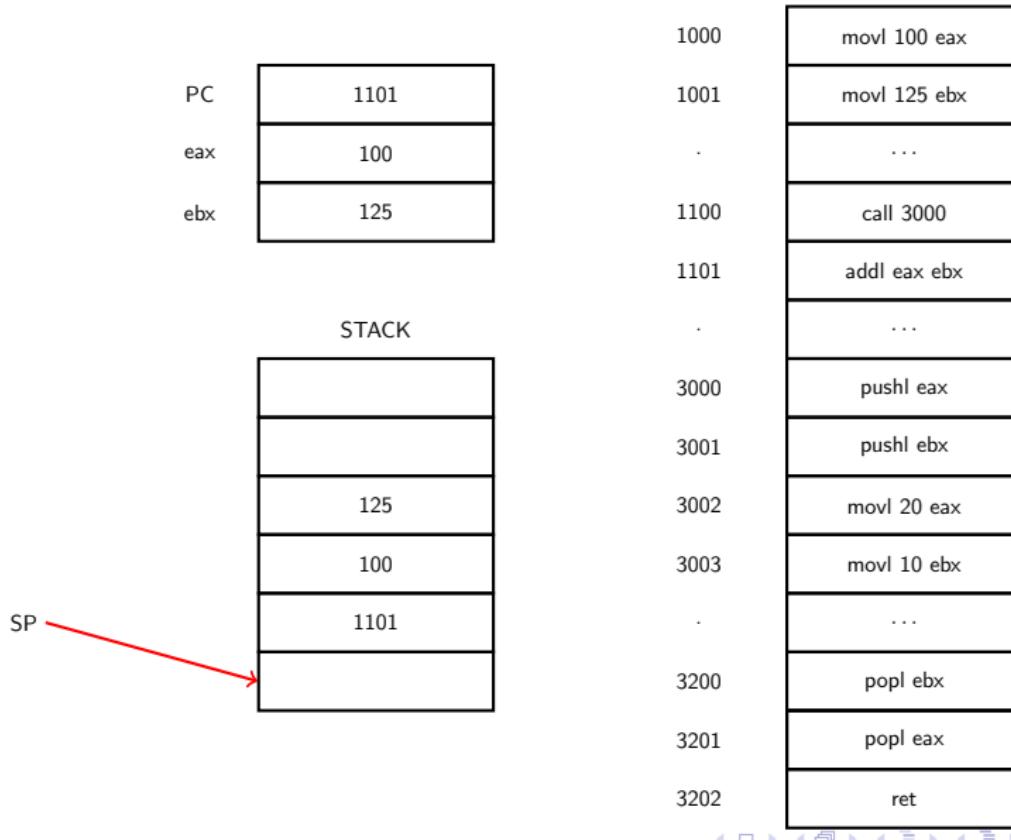
# Registers - In f()



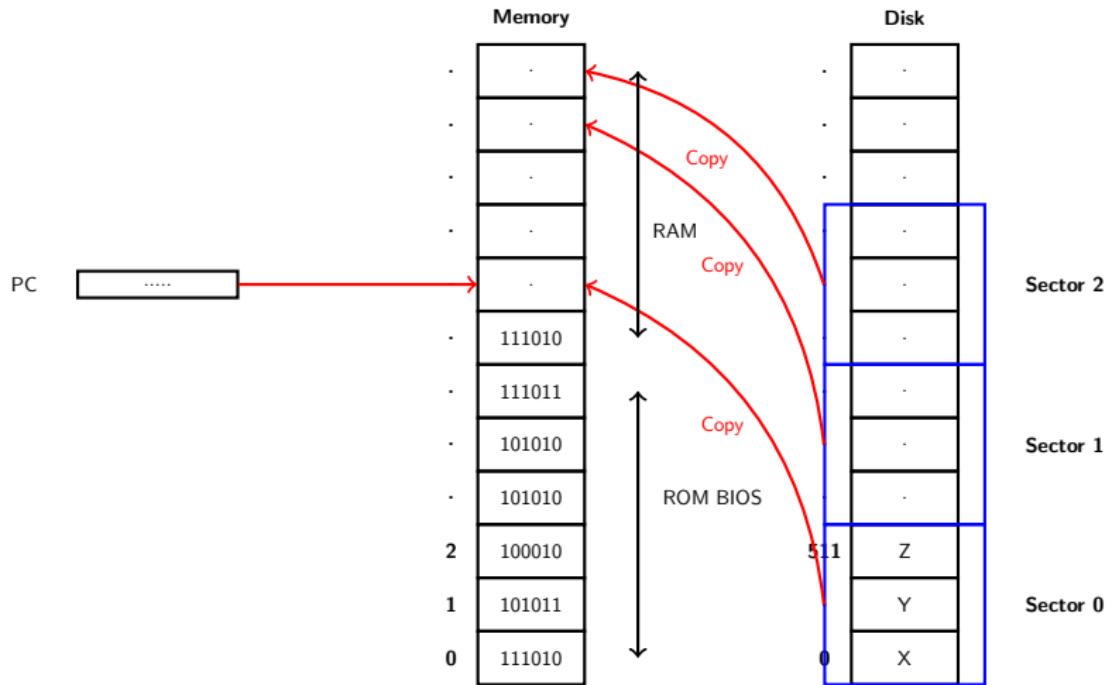
# Registers - In f()



# Registers - In f()



# *init/systemd* First Userland Process - PID 1



## Program Vs Process