# IS|WEC

iSecur1ty Windows Exploitation Course

Mahmoud Reda


m.reda@isecur1ty.org

Contact:FB.com/mahmoud.reda.vet

# متطلبات الدورة

- معرفة بلغة السى
- معرفة بلغة الأسمبلى

الأدوات :


- المنقح «GDB»
- توزيعة كالى لينكس

# اساسيات مهمة

- البفر buffer هو جزء من الذاكرة لحمل البيانات بشكل مؤقت وله حجم ثابت

- الهيب heap هو جزء من الذاكرة وحجمه يتغير بحسب متطلبات وعمليات البرنامج.


- Buffer Overflow:

تحدث ثغرات الفيض عندما يتم كتابة بيانات زائدة فى البفر اكثر مما ينبغى وتحدث نتيجة عدم التحقق من مدخلات المستخدم الذى استطاع ان يضيف بيانات اكثر مما يحمله البفر

- مثال :

```
char buffer[4];
buffer[4] = ‘a’;
```

# اساسيات مهمة

- Stack

المكدس هو جزء من الذاكرة لحفظ البيانات

عبارة عن مجموعة مرتبة من العناصر


PUSH

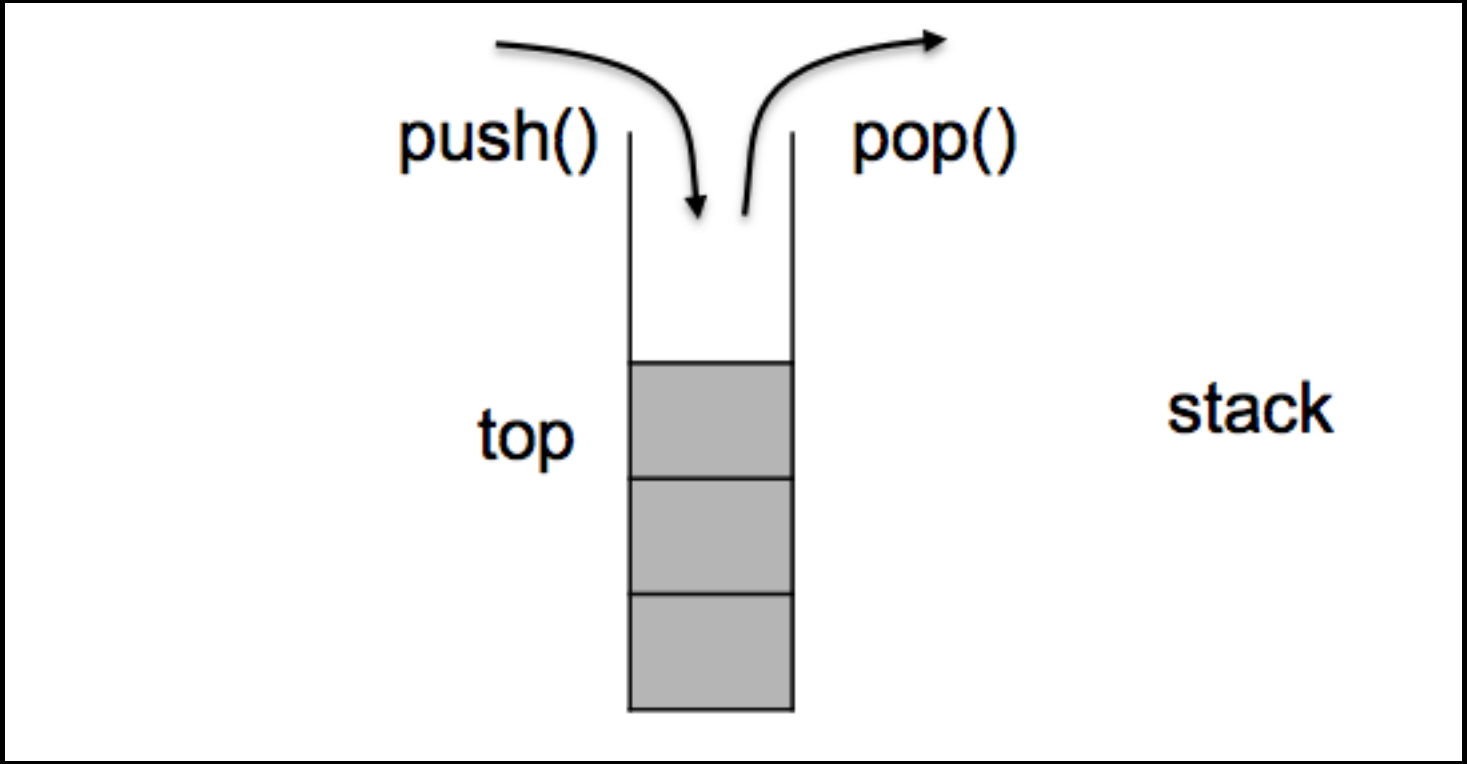
تضيف بيانات الى stack

POP

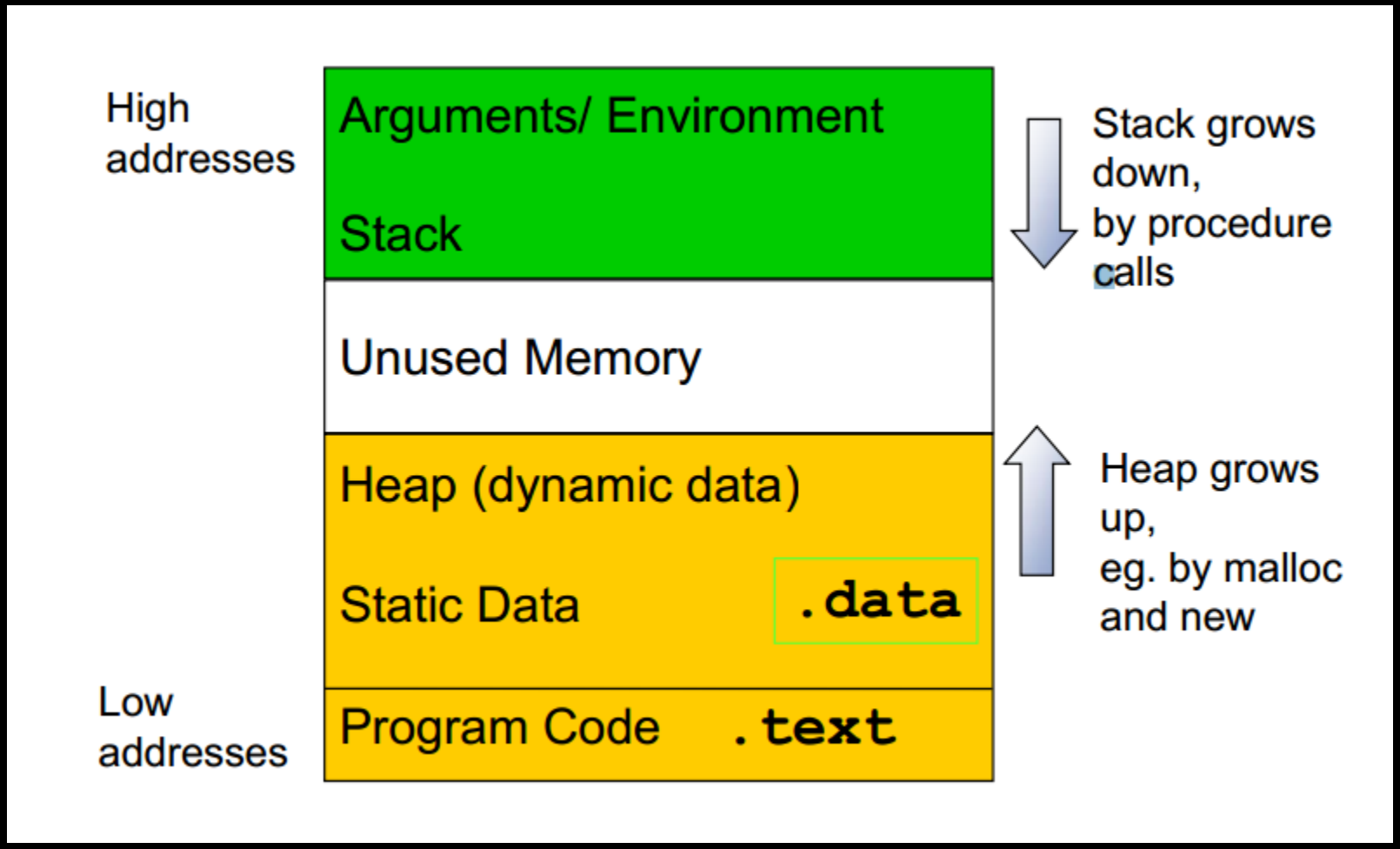
تحذف بيانات من stack

# stack

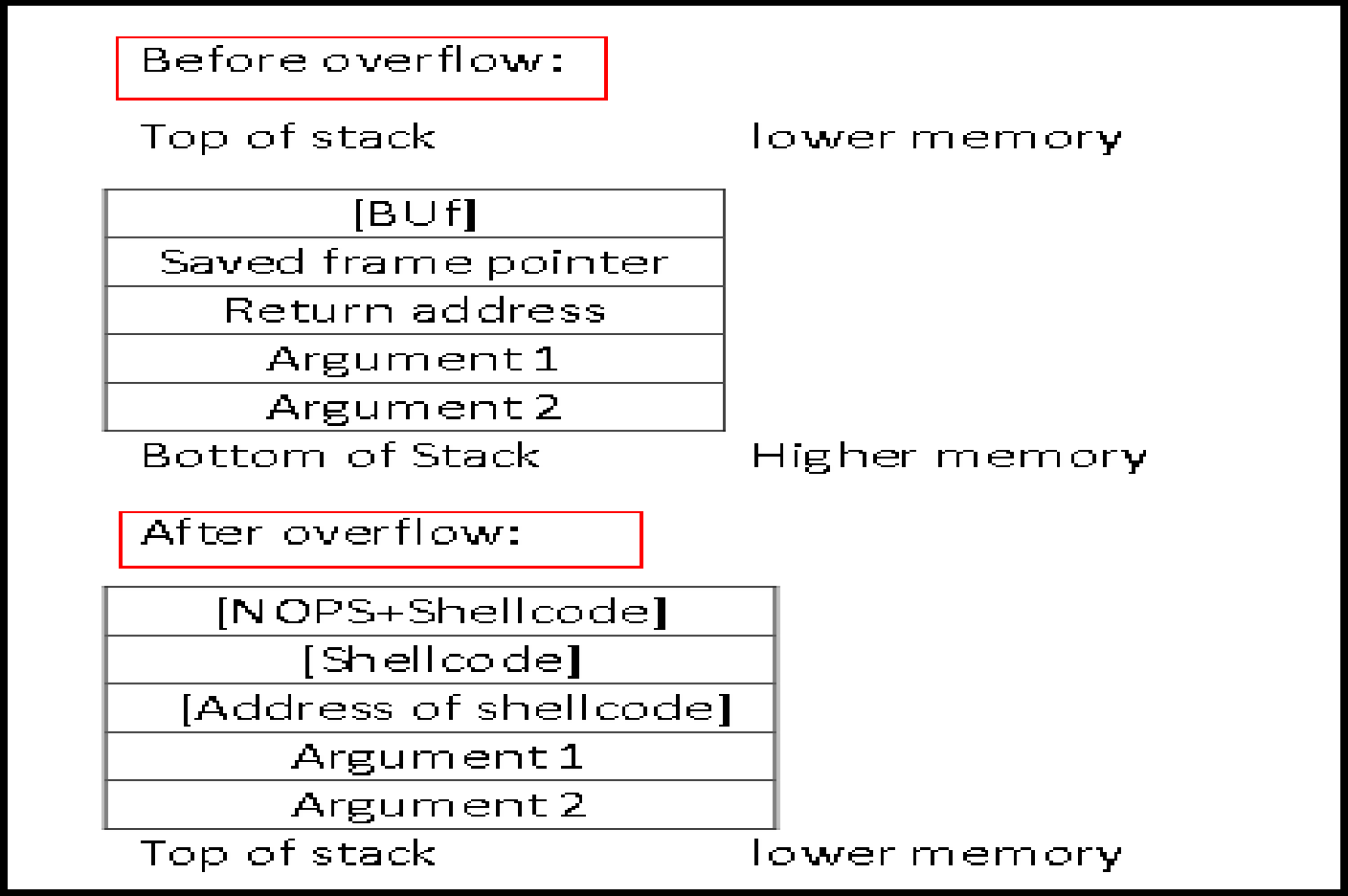
**LIFO**



# Process memory



# استغلال ثغرات الفيض



# دوال مصابة

- gets()
- strcpy(,)
- scanf
- realpath


هذا الدوال لا تتحقق من القيم !!!

# خطورة ثغرات الفيض

- اخطر ثغرة امنية موجودة حاليا
- تؤدى الى اختراق كامل للشبكة الداخلية
- تستخدم ايضا فى هجمات حرمان الخدمة dos attack على المواقع.

# انواع ثغرات الفيض

- Stack Overflow
- Heap Overflow
- Format String Overflow

# انواع ثغرات الفيض

| Remote | Local |
| --- | --- |
| • خارج الشبكة المحلية<br>• الإختراق عن طريق Ip | • داخل الشبكة المحلية |

# انواع المعالجات

## معالج ٣٢ بت

- x86
- اقل فى السرعة
- اقل فى الحماية

## معالج ٦٤ بت

- x64
- السرعة اعلى
- الحماية اقوى

- NX

تقوم بتحزين البيانات وبالتالى تمنع تنفيذ اى كود

- AVP

# انواع المعالجات

| معالج ٣٢ بت | معالج ٦٤ بت |
| --- | --- |
| • esp = Stack Pointer<br>• ebp = Base Pointer<br>• eip= instruction Pointer | • rsp = Stack Pointer<br>• rbp = Base Pointer<br>• **rip** = instruction Pointer |
| | memory addresses are 64 bits long but user space only uses the first 47 bits. |

# اساسيات لغة الأسمبلى

- برنامج الأسمبلى يتكون من ٤ اجزاء رئيسية :

**.data**

تحتوى على البيانات والقيم

**.bss**

تحتوى على البيانات الغير جاهزة للإستخدام

**.text**

تحتوى على اكواد البرنامج والتعليمات التى سيتم تنفيذها

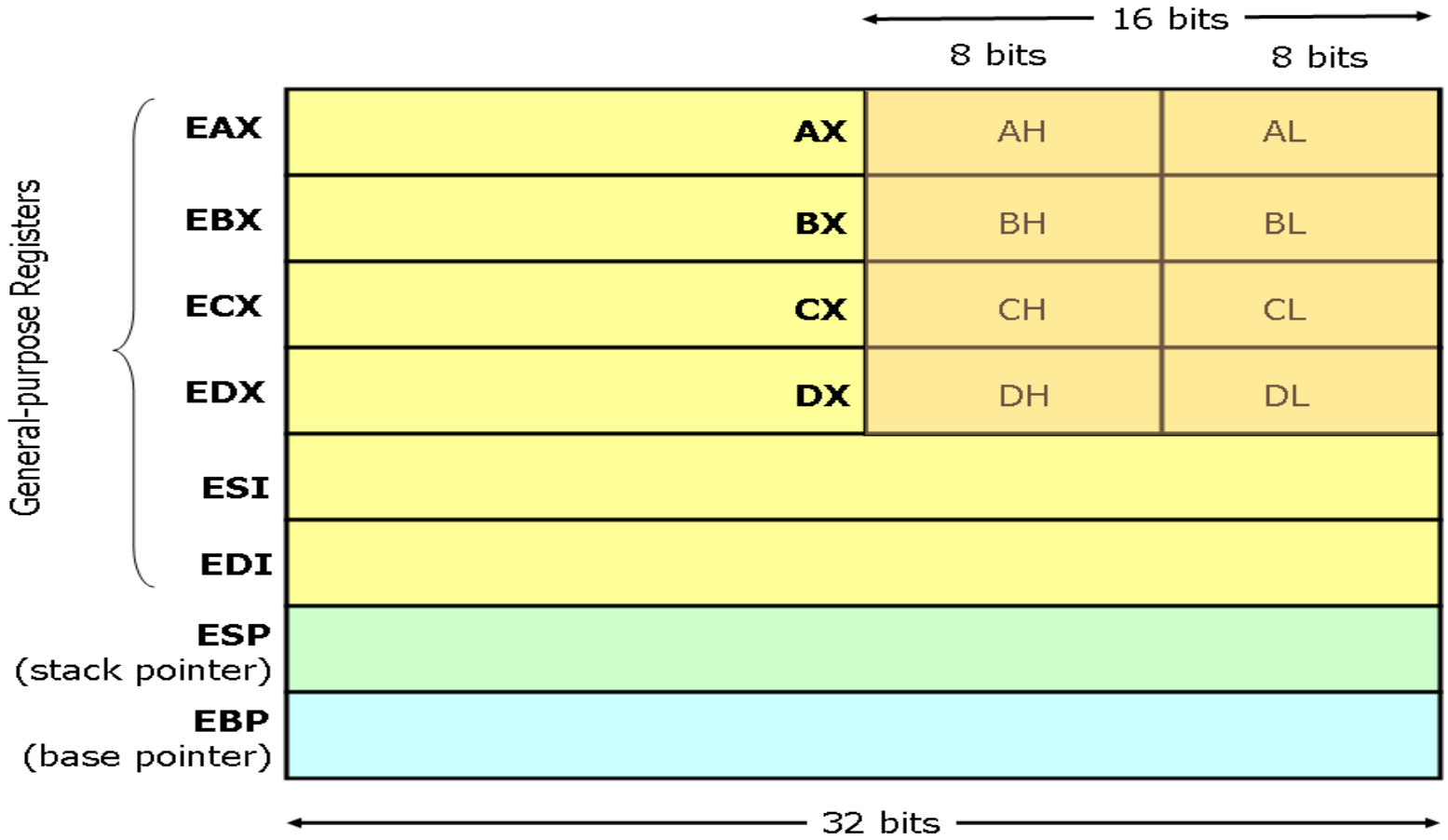
**_start()**

يشير الى بداية الأكواد والتعليمات التى سيتم تنفيذها

# اساسيات لغة الأسمبلى

- المسجلات Registers:

تستخدم لتخزين البيانات .



# اساسيات لغة الأسمبلى

- المسجلات Registers:

تستخدم لتخزين البيانات .

Eax

تحتوى على نتائج العمليات الحسابية



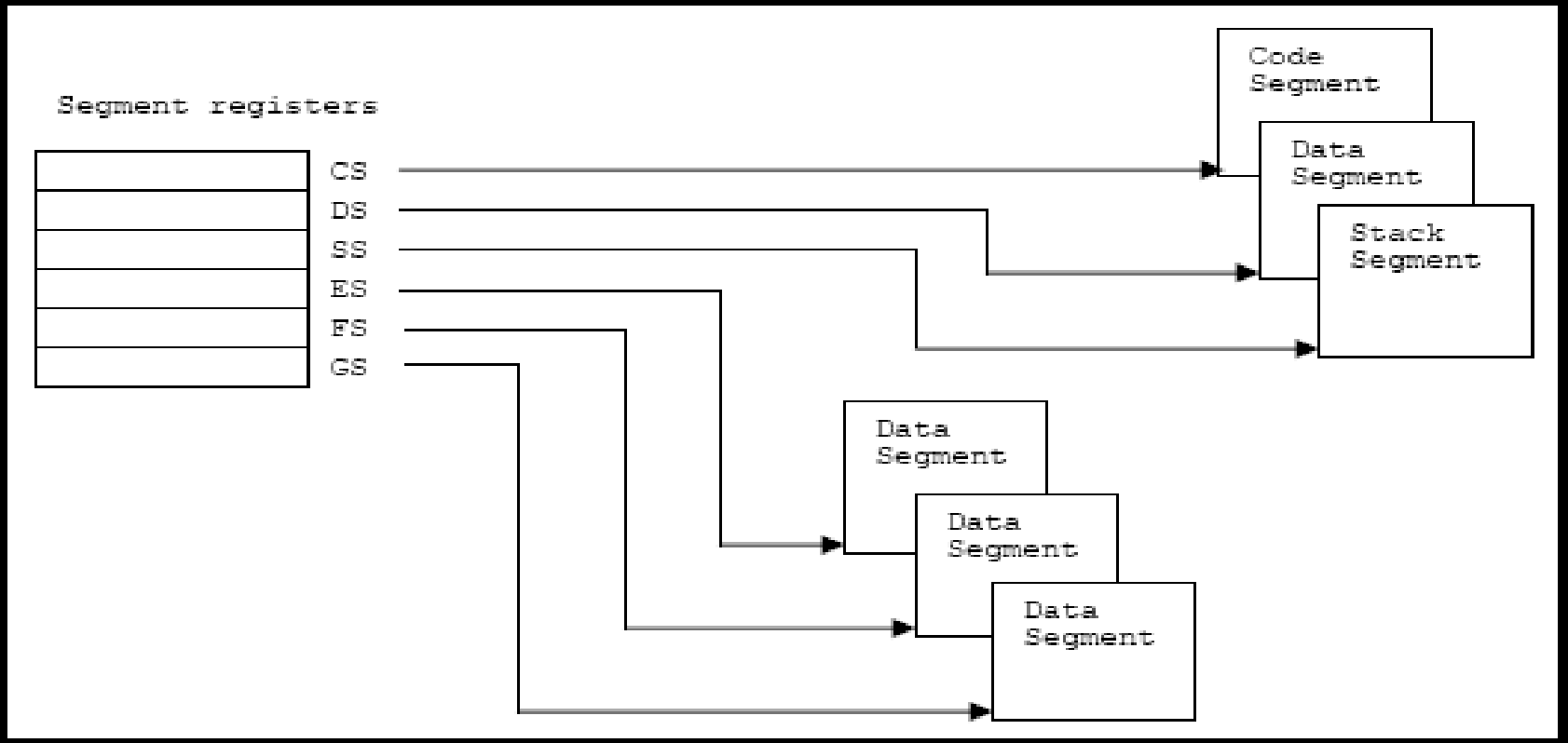
Ecx

يستخدم فى الحلقات التكرارية

# اساسيات لغة الأسمبلى

- المسجلات Registers:

تستخدم لتخزين البيانات .



# اساسيات لغة الأسمبلى

- المسجلات Registers:

تستخدم لتخزين البيانات .

- EIP

هو instruction pointer register

يشير الى التعليمية التى يقوم بها المعالج فى هذه النقطة .

# اساسيات لغة الأسمبلى

- اهم التعليمات بين المسجلات :

MOV

CALL

JMP



- التعليمات للعمليات الحسابية :

ADD

SUB

MUL

DIV

- العمليات المنطقية:

AND OR XOR

نـهاية الدرس الأول شكرا لكم .

Mahmoud Reda

iSecur1ty
www.isecur1ty.org

m.reda@isecur1ty.org

Contact:FB.com/mahmoud.reda.vet