STACK OVERFLOW

By Mustafa Onur Parlak

- **Buffer Overflow**
  - **Buffer,** hafızada veri tiplerini depolayan hafıza bloğudur.
  - Fonksiyonlarda yazılan değişkenlere, saklama kapasitesinden fazla veri yüklenirse **crash** hatası verir.
- **Stack Nedir?**
  - İşletim sisteminde oluşturulan **thread**'ler (Bir process'in multitask iş yapabilmesini sağlayan yapıdır); fonksiyon parametreleri, lokal değişkenler ve fonksiyonların çalışması duraklatıldığı veya bitirildi durumda **stack** (yığın) denilen alanlar oluşur ve burada depolanır.
  - Gecici hafıza bölümüdür.
- **Stack vs Heap?**
  - Program esnasında boyutları bildirilmiş değişmez bir değer kullanıyorsak, **STACK** denmektedir.
  - Eğer değişebilecek bir değer kullanıyorsak **HEAP** olarak adlandırılır.

```
int32_t *pNumbers;

// STACK olarak yazım
pNumbers[10];

// HEAP olarak yazım
pNumbers = new int [];
```

- **Function Prologue (Fonksiyon Girişi)?**
  - **Fonksiyon Çağırma**
    - Fonksiyon çağrılmadan önce, fonksiyon içindeki parametrelerin saklandığı **EIP (Instruction Pointer)** ve **EBP (Base Pointer)** register'ları stack üzerinden kopyalanır.
    - Fonksiyon işleri tamamlandıktan sonra, **EIP** register'ı **EBP**'ye kopyalanır.
    - Program akışı kaldığı yerden devam eder.
  - **Function Prologue :** Programa işlenen bir verinin, daha sonrasında fonksiyon içinde işlem görüp çıkışta farklı bir değer alma olayıdır.
  - **Function Prologue Adımları**
    - **ESP (stack pointer)**'in değeri **EBP** olarak kopyalanıp **stack**'e pushlanır
    - Bir sonraki **Instruction** adresi **stack**'e puslanır
    - Fonksiyon için **call komutu** aktif edilir.
  - **Function Epilogue BU ADIMLARIN TAM TERSİ İŞLEMEKTEDİR.**

- **Stack Overflow Nedir?**
  - Programın tanımlanmış **stack memory** sınırının ötesinde erişim sağlandığı durumlarda taşma (overflow) oluşur. Diğer bir deyiş ile; Call stack pointer'ı, stack sınırını aşarsa **stack overflow** olur.
  - **Program çökmesi gözlemlenebilir**
  - **Segmentation fault** hatası da denmektedir.

- **Kitabi Anlatım ile Stack Overflow Nasıl Oluşur?**
  - **Stack** depolama alanı dolup taştığı durumda,
  - **EIP register'**ının değeri değiştirilerek program akış yönü değişir.
  - **EIP,** program çalıştırıldıktan bir sonraki kodun adresini tutar. Bu **adresin** değiştiği durumda program akışı değişmektedir.
  - **Base Pointer stack**'in başlangıcını gösterir.
  - **Stack Pointer** ise yapılan büyüme-küçülme (pop-push) işlemlerine göre değişir.

- **Stack Overflow Sebepleri?**
  - Başta, derleyiciden kaynaklı memory sıkışması olmaktadır.
  - **Recursive** fonksiyonların yanlış kullanılması
  - Fonksiyona çok fazla argüman gönderilmesi
  - Fonksiyona doğrudan **struct** gönderilmesi
  - **İç içe** fonksiyon çağrıları
  - Büyük boyutlarda **local** dizi oluşturmak