İşletim Sistemleri

Güvenlik

İşletim sistemleri

Güvenlik

- Birçok şeyin dijital olarak saklanması
- Önemli veri miktarının artışı
- Çok kullanıcılı bilgisayarlarda kullanıcı izolasyonu hedefi
- Ayrıca dosya tabanlı güvenlik mekanizması ihtiyacı
  - Askeri dosyalar için farklı gizlilik seviyeleri işaretlemeleri
- Güvenlik açıkları
  - Vulnerability

İşletim sistemleri

Güvenlik

- Bug tetikleyen girdiler
  - Exploit
- Bu exploit'ler ile çalıştırılan zararlı yazılımlar
  - Malware
- Diğer çalıştırılabilen dosyalara eklenen malware
  - Virus
- Bilinen bir yazılım ile gelen zararsız gözüken zararlı yazılımlar
  - Trojan

İşletim sistemleri

Güvenlik

- İşletim sistemleri sistem güvenliği
- CIA
  - Confidentiality (Güvenilirlik)
  - Integrity (Bütünlük)
  - Availability (Erişilebilirlik)

İşletim sistemleri

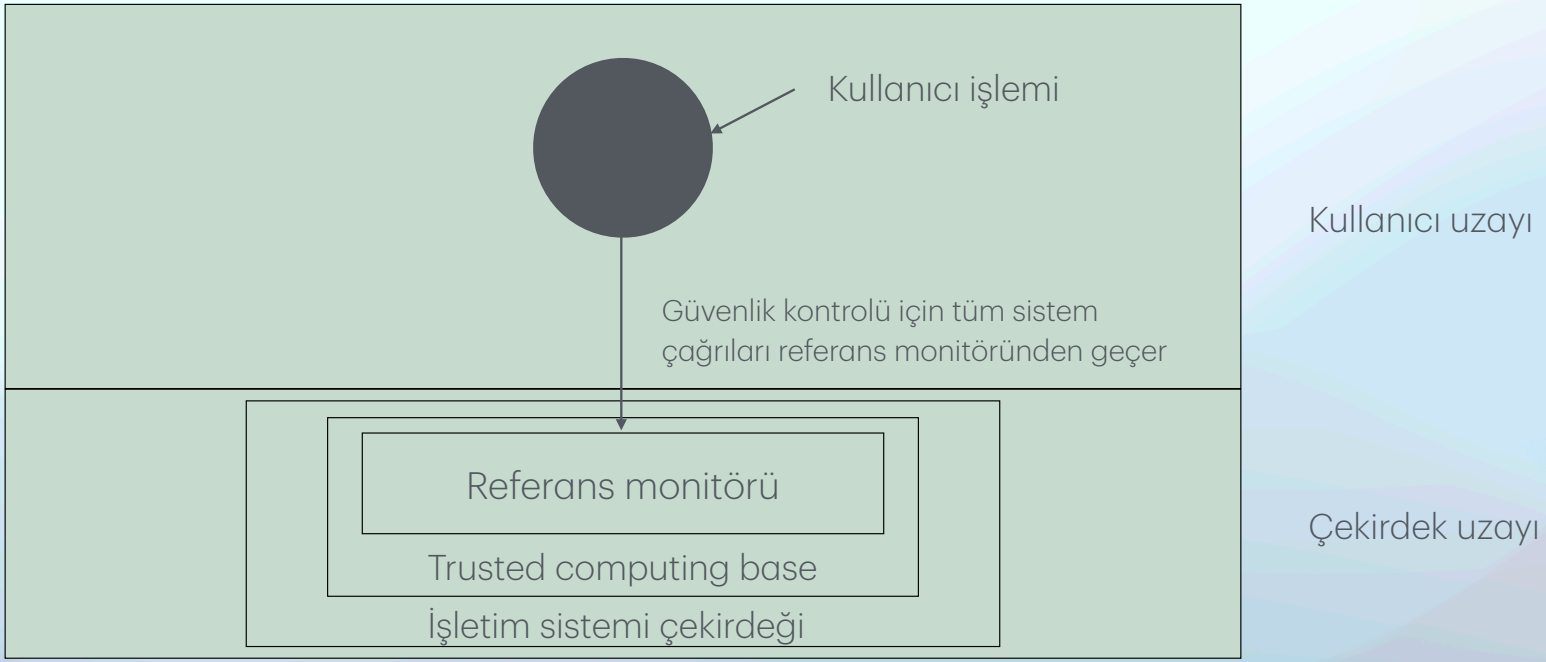
Güvenlik

- Güvenlik prensipleri
  - Sistemin karmaşıklığı
  - Erişimin varsayılan davranışları
  - Eksiksiz tahkim
  - Olabilecek en az yetki prensibi
  - Önceliklerin ayrılma prensibi
  - Ortak mekanizmaların minimizasyon prensibi
  - Açık dizayn prensibi
    - Kerckhoff

İşletim sistemleri

Güvenlik

- Trusted Computing Base



İşletim sistemleri

Güvenlik

- %100 güvenli bir sistem geliştirmek mümkün müdür?
- Güvensiz sistemlerin terkedilmemesi
- Her eklenen özelliğin güvenlik açığı ihtimali oluşturması

İşletim sistemleri

Güvenlik

- Dosya sistemi güvenliği
- İzinler
  - RWX
- UID
- GID
- Erişim matrisi
- Erişim listeleri

İşletim sistemleri

Güvenlik

- Çok seviyeli güvenlik
  - Bell-LaPadula Modeli
    - Okuma yalnızca aşağı doğru (basit güvenlik özelliği)
    - Yazma yalnızca yukarı doğru (* özelliği)
  - Biba Modeli
    - Yazma yalnızca aşağı doğru (basit bütünlük özelliği)
    - Okuma yalnızca yukarı doğru (bütünlük * özelliği)

İşletim sistemleri

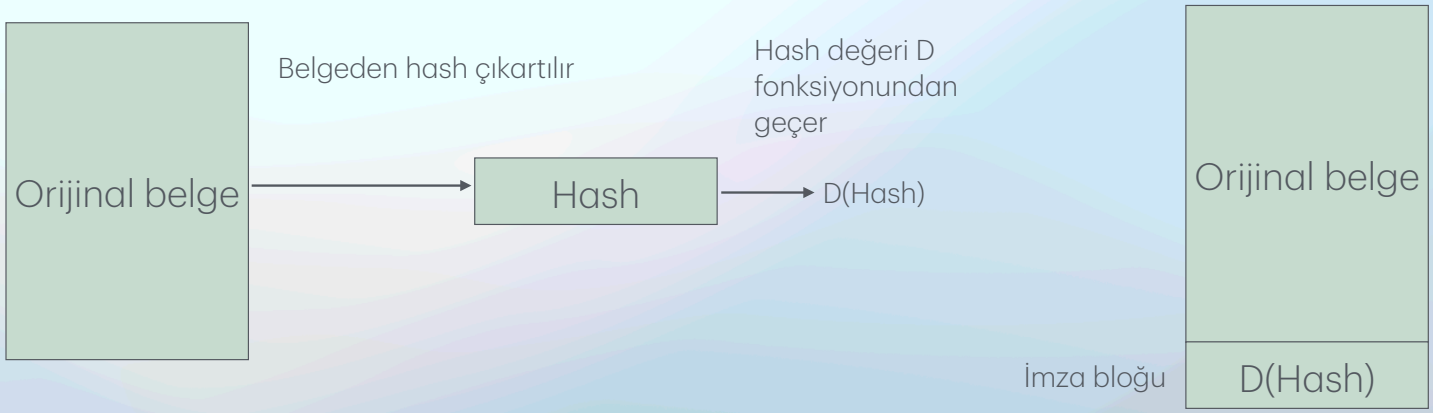
Kriptografi

- Açık metin
- Şifreli metin
- Fonksiyonlar açık olmalı
- Anahtar planlama
- Gizli anahtar ile şifreleme
  - Simetrik anahtarlı şifreleme
- Açık anahtar ile şifreleme
  - Gizli anahtar açma
  - Açık anahtar şifreleme

İşletim sistemleri

Dijital imzalar

- Kriptografik hash fonksiyonu
- Belgenin sonuna eklenebilir



İşletim sistemleri

Trusted Platform Module

- TPM
- Donanımsal şifreleme
- Şifreleme - açma işlemlerini yapabilir
- Anahtarlar için alana sahiptir
- Bitlocker

İşletim sistemleri

Kimlik doğrulama

- Authentication
  - Şifreler
    - Zayıf şifre
    - Güçlü şifre
  - Şifrelerin saklanması
    - Açık text
    - Hash
    - Salt

İşletim sistemleri

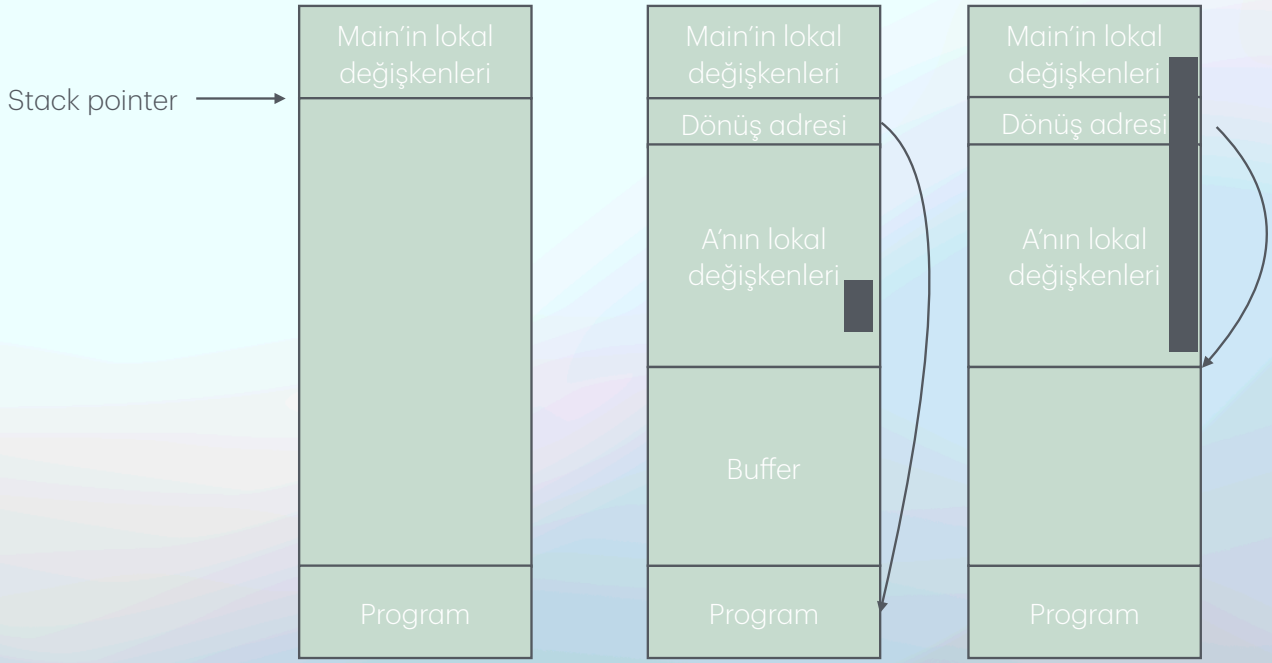
Kimlik doğrulama

- Tek seferlik şifreler
  - Tek yönlü hash zinciri
- Fiziksel nesneler ile kimlik doğrulama
- Biyometri
- Passkeys

İşletim sistemleri

Yazılım saldırı türleri

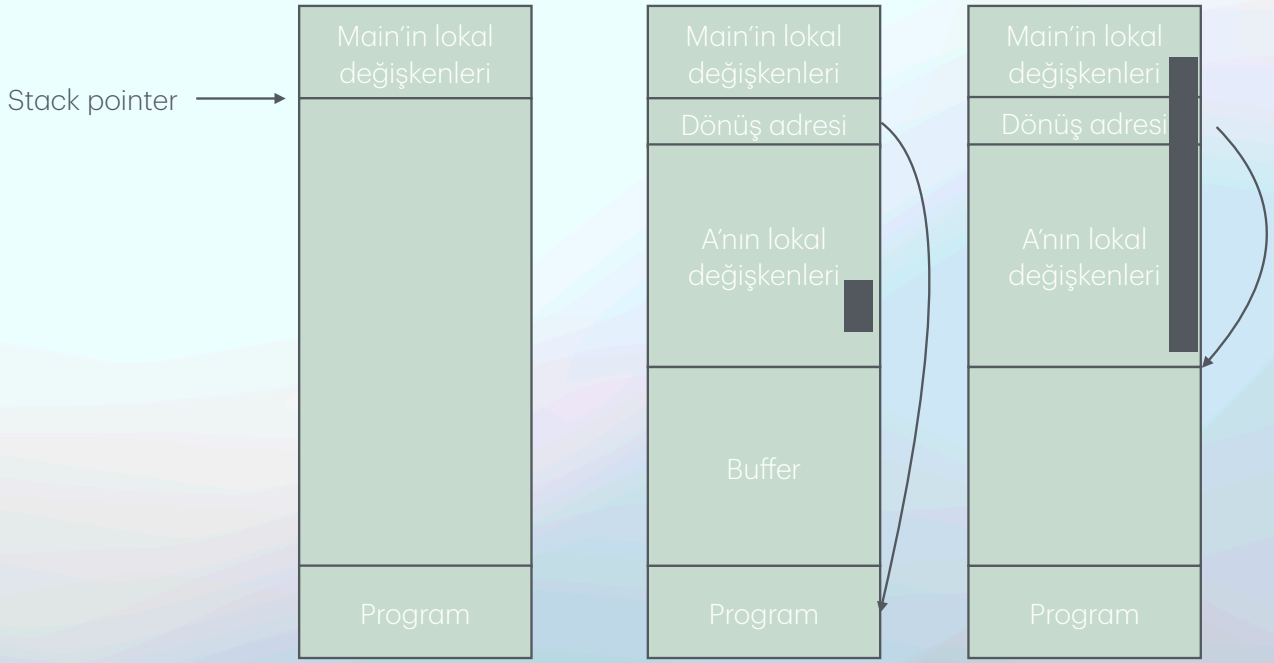
- Buffer overflow attack



İşletim sistemleri

Yazılım saldırı türleri

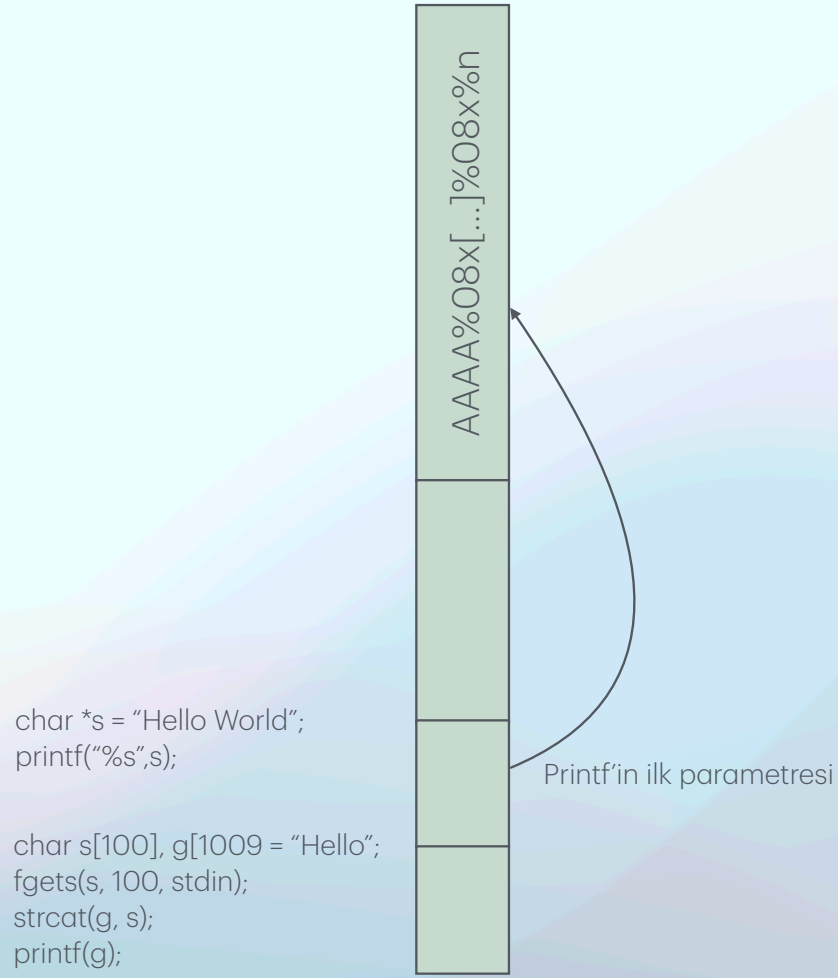
- Buffer overflow attack
- Shellcode
- Stack canaries
- Data execution prevention
- Code reuse
- Address-Space Layout randomization



İşletim sistemleri

Yazılım saldırı türleri

- Format string attack



İşletim sistemleri

Yazılım saldırı türleri

- Use after free attack
  - Malloc
  - Free
  - Double free attack
- Null pointer dereference attack
- Integer overflow attack

İşletim sistemleri

İşletim sistemlerinin korunması

- Randomizasyonun tahmin edilemeyecek hale getirilmesi
- Kontrol akışının kısıtlanması
- Erişim kısıtlamaları
- Kod ve veri bütünlüğü kontrolleri
- Güvensiz kodun sarmalanması
    - Sandboxing