Bölüm 13: Güvenlik

İşletim Sistemleri

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Güvenlik Hedefleri

- **Gizlilik**: Hassas verilere yetkisiz erişimi önleyin
- **Bütünlük**: Verilerde veya sistemlerde yetkisiz değişikliklere karşı koruma sağlayın
- **Erişilebilirlik**: Yetkili kullanıcıların gerektiğinde verilere ve sistemlere erişebilmesini sağlayın

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Tehditler

- **Kötü Amaçlı Yazılım**: Virüs, Truva atı, solucan, casus yazılım, fidye yazılımı vb.
- **Yetkisiz Erişim**: Uygun yetkilendirme olmadan sistemlere veya verilere erişme girişimleri
- **Hizmet Reddi (DoS)**: Sistemlerin veya verilerin kullanılabilirliğini kesintiye uğratmak (denial of service)
- **Arabellek Taşmaları**: Bellekte bir arabellek taşması ve kötü amaçlı kod yürütme
- **Yarış Koşulları**: Beklenmeyen sonuçlara yol açabilecek kodun eşzamanlı yürütülmesi

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Savunma Mekanizmaları

- **Erişim Kontrolü**: Kimin hangi verilere veya sistemlere erişebileceğini tanımlayın
- **Güvenlik Duvarları**: Yetkisiz erişimi önlemek için ağ trafiğini filtreleyin
- **Bellek Koruması**: Arabellek taşmalarını ve diğer bellek tabanlı saldırıları önleyin
- **Sandboxing**: Birbirini engellemelerini önlemek için süreçleri izole edin
- Şifreleme: Aktarım halindeki veya atıl durumdaki hassas verileri koruyun

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Güvenlik İhlali Kategorileri

- **Breach of confidentiality**: Verilerin izinsiz okunması
- **Breach of integrity**: Verilerin izinsiz değiştirilmesi
- **Breach of availability**: Verilerin yetkisiz imhası
- **Theft of service**: Kaynakların yetkisiz kullanımı
- **Denial of service (DoS)**: Kullanımın önlenmesi
- **Masquerading**: Yetkili kullanıcı gibi davranmak
- **Replay attack**: Olduğu gibi veya mesaj değişikliği ile
- **Man-in-the-middle attack**: Alıcıya kendisini gönderici kılığında gösterir
- **Session hijacking**: Kimlik kontrolü yapılmış oturumu ele geçirmek
- **Privilege escalation**: Sahip olması gerekenden fazla erişime sahip olma

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

En İyi Uygulamalar (best practices)

- Güvenlik yamalarıyla yazılımı güncel tutun
- Güçlü kimlik doğrulama ve erişim kontrol mekanizmaları kullanın
- Güvenlik izleme ve günlük (log) kaydı tutma
- Düzenli güvenlik değerlendirmeleri ve sızma testleri gerçekleştirin
- Kullanıcıları en iyi güvenlik uygulamaları ve güvenlik tehditlerine ilişkin farkındalık konusunda eğitin.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

İzinsiz Kullanıcı

- Teknik olmayan kullanıcılar tarafından rastgele gözetleme.
- İçeridekiler tarafından gözetleme.
- Para kazanmak için kararlı girişimler.
- Ticari veya askeri casusluk.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Kazayla Veri Kaybı

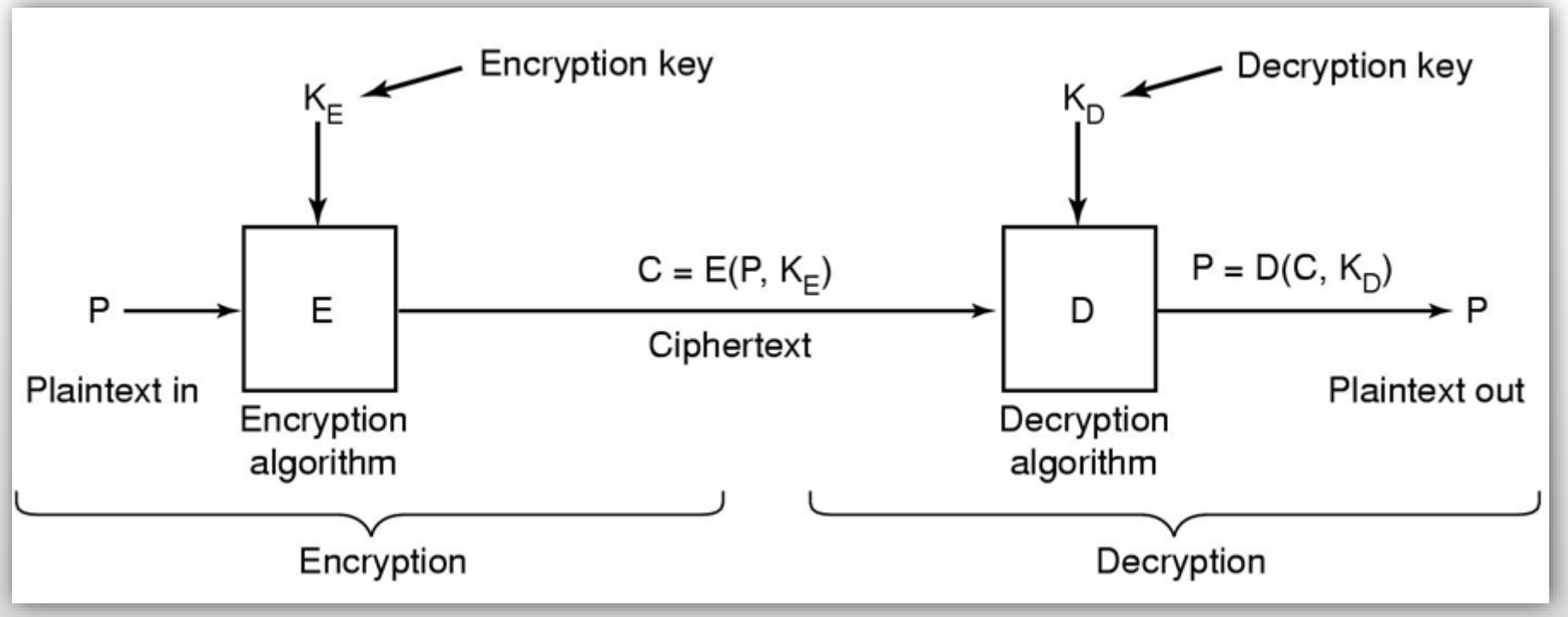
- Yanlışlıkla veri kaybının yaygın nedenleri:

- **Kader**: yangınlar, seller, depremler, savaşlar, isyanlar veya yedek bantları kemiren fareler.
- **Donanım veya yazılım hataları**: CPU arızaları, okunamayan diskler veya teypler, telekomünikasyon hataları, program hataları.
- **İnsan hataları**: yanlış veri girişi, yanlış teyp veya CD-ROM takma, yanlış program çalıştırma, kayıp disk veya teyp veya başka bir hata.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Şifrelemenin Temelleri

- Düz metin ve şifreli metin arasındaki ilişki.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Gizli Anahtarlı Şifreleme (secret key)

- Monoalfabetik ikame:

- Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Ciphertext: QWERTYUIOPASDFGHJKLZXCVBNM

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Açık Anahtarlı Şifreleme

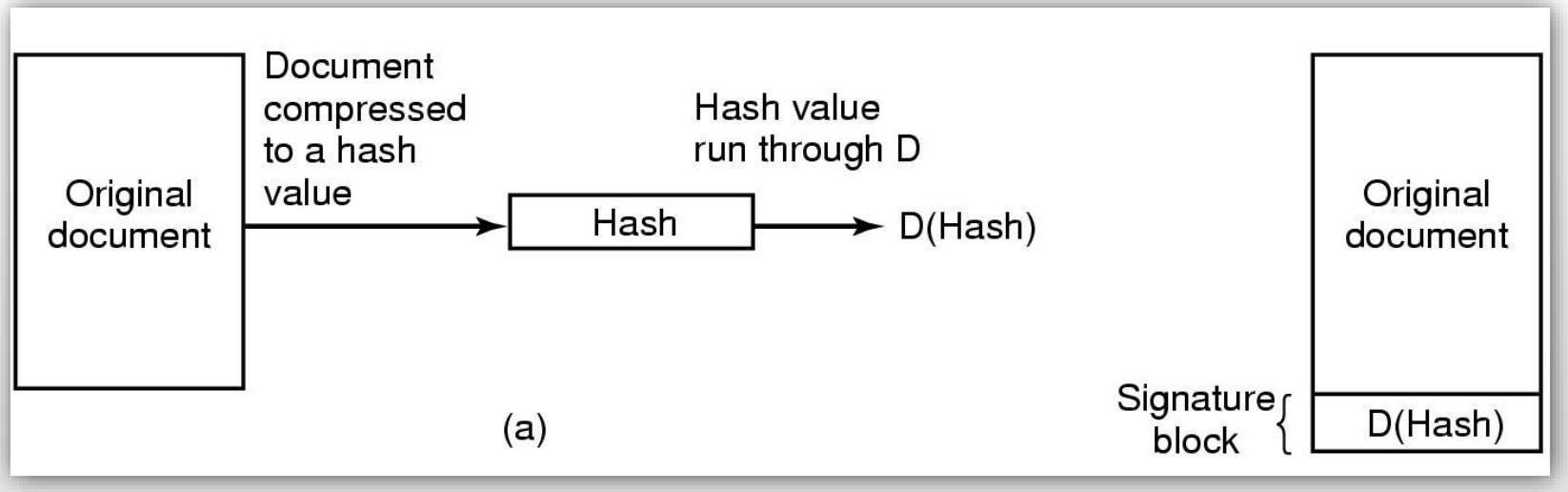
- Şifreleme, " 314159265358979 × 314159265358979 ne kadar" gibi "kolay" bir işlemden yararlanır?

- Anahtar olmadan şifre çözme, 391257150641938709059482850824 1'nin karekökü nedir gibi zor bir işlem yapmanızı gerektirir.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

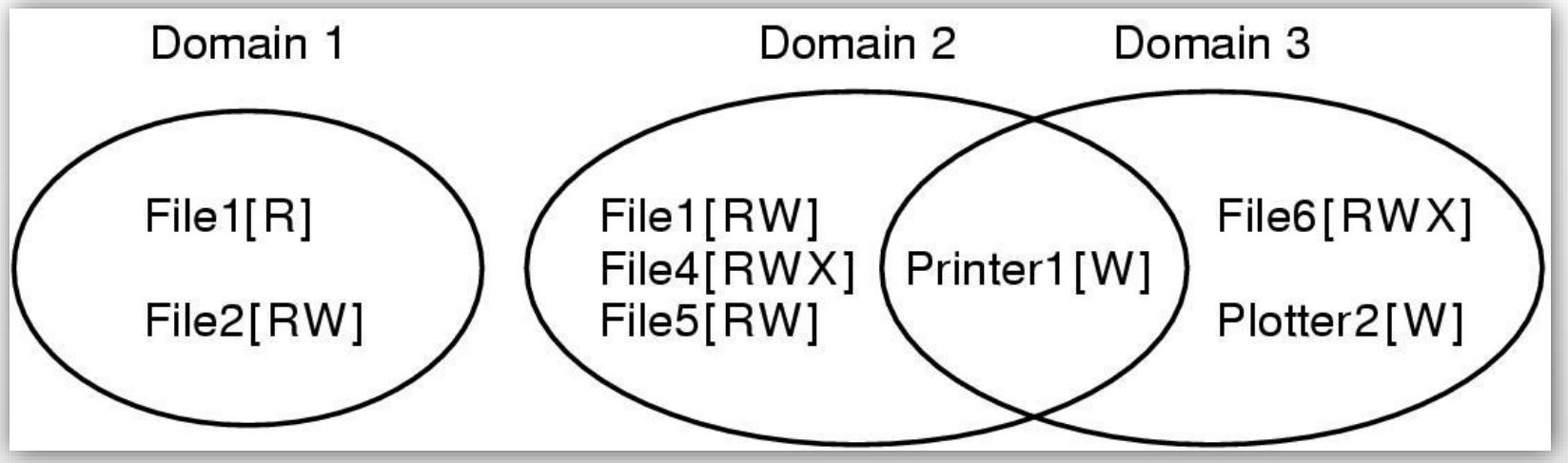
Dijital İmzalar

- (a) Bir imza bloğunun hesaplanması. (b) Alıcıya gelen şey.



Koruma Etki Alanları

- Üç koruma alanı.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Koruma Etki Alanları

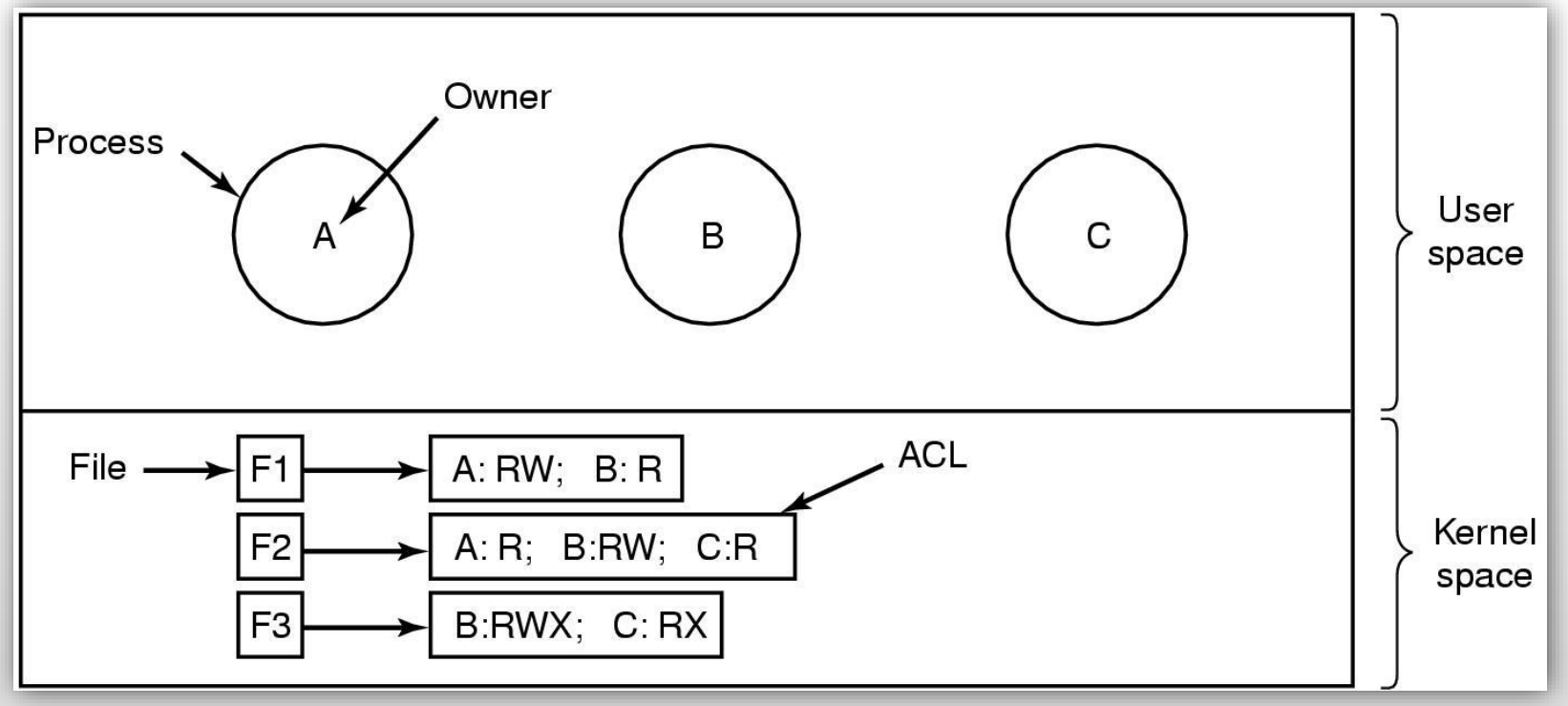
- Bir koruma matrisi.

Domain	Object: File1	File2	File3	File4	File5	File6	Printer1	Plotter2
1	Read	Read Write						
2			Read	Read Write Execute	Read Write		Write	
3						Read Write Execute	Write	Write

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Erişim Kontrol Listeleri

- Dosya erişimini yönetmek için erişim kontrol listelerinin kullanımı.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Erişim Kontrol Listeleri

- Erişim kontrol listesi (ACL), bir işletim sistemindeki (OS) dosya ve dizinler gibi sistem kaynaklarına erişim kontrolü sağlayan bir güvenlik mekanizmasıdır.
- Nesneye kimin erişmesine izin verildiğini ve hangi eylemleri gerçekleştirmesine izin verildiğini belirlemek için izinlerin listesi
- Kaynakları kısıtlı sistemlerde performansı etkileyebilecek ek işlem gücü ve depolama gerektirir.
- Yönetmek ve güncellemek, büyük ve karmaşık sistemlerde zor.
- Farklı işletim sistemleri ve uygulamalar arasında farklılık gösterebilir ve bu da uyumluluk ve birlikte çalışabilirlik sorunlarına yol açar.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

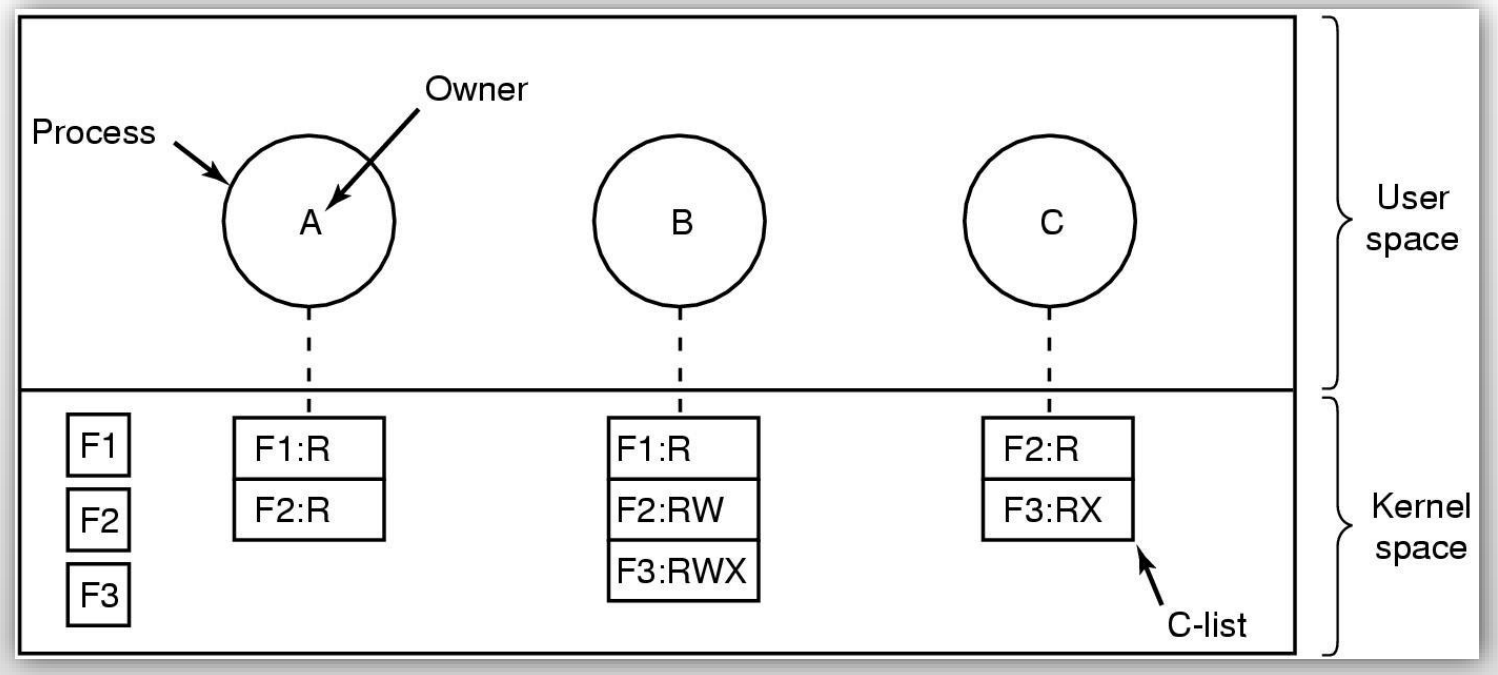
Erişim Kontrol Listeleri

- User Group 1: Read-only access to file A, full access to file B.
- User Group 2: Write access to file A, no access to file B.
- User Group 3: Execute access to file C, read access to file D.
- User Group 4: No access to files A, B, C, and D.
- Admin Group: Full access to all files.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Yetenekler

- Her sürecin bir yetenek listesi vardır.



Yetenekler

- Kriptografik olarak korunan bir yetenek.

Server	Object	Rights	f(Objects,Rights,Check)

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Yetenekler

- Genel haklara örnekler:
  - **Kopyalama yeteneği**: aynı nesne için yeni bir yetenek yaratır.
  - **Nesneyi kopyala**: yeni bir yeteneğe sahip yinelenen (duplicate) bir nesne oluşturur.
  - **Kaldırma yeteneği**: yetenek listesinden bir girdiyi siler; nesne etkilenmez.
  - **Nesneyi yok et**: bir nesneyi ve bir yeteneği kalıcı olarak kaldırır.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Güvenilir Sistemler

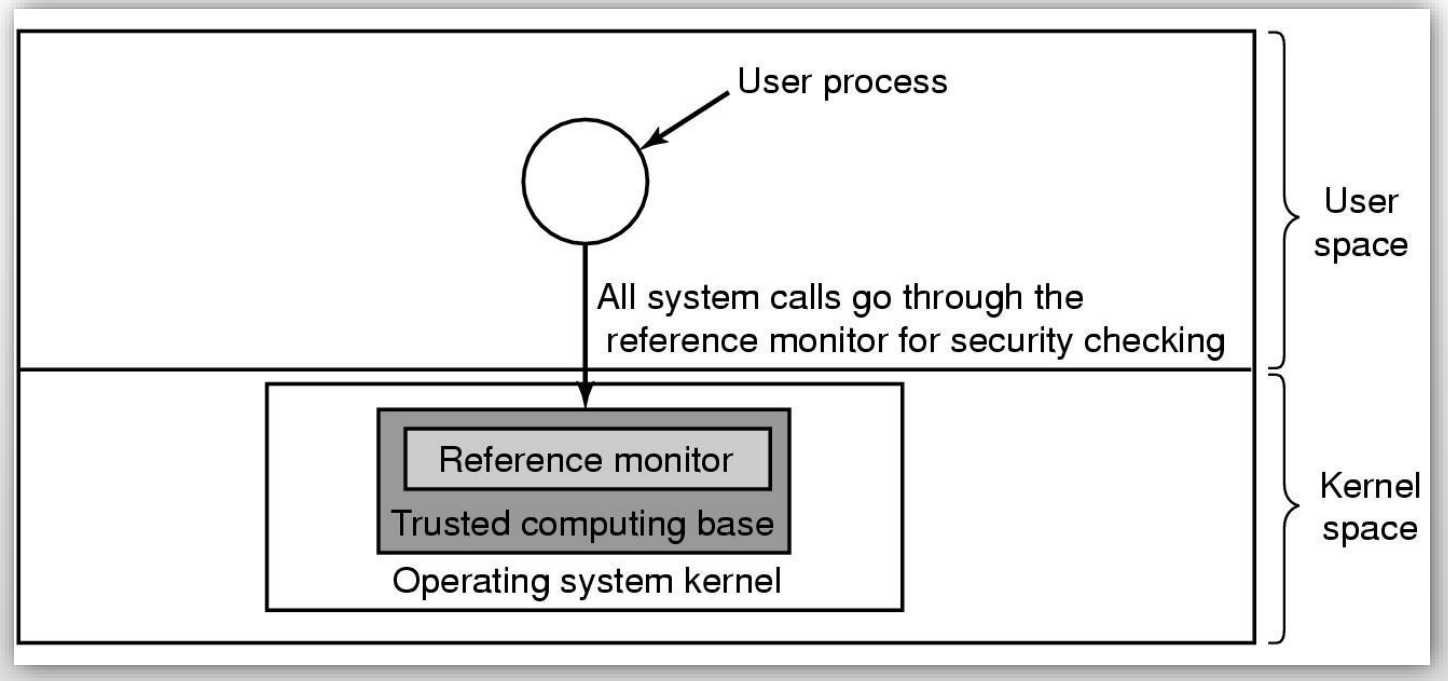
- Virüs, solucan vb. raporları dikkate alın.

- İki saf (ama mantıklı) soru:
  - Güvenli bir bilgisayar sistemi kurmak mümkün mü?
  - Varsa neden yapılmıyor?

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Güvenilir Bilgi İşlem Tabanı

- Bir referans gözetleyici.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Güvenli Sistemlerin Biçimsel Modelleri

- (a) Yetkili bir durum. (b) Yetkisiz bir durum.

	Objects		
	Compiler	Mailbox 7	Secret
Eric	Read Execute		
Henry	Read Execute	Read Write	
Robert	Read Execute		Read Write

(a)

	Objects		
	Compiler	Mailbox 7	Secret
Eric	Read Execute		
Henry	Read Execute	Read Write	
Robert	Read Execute	Read	Read Write

(b)

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Bell-La Padula Modeli

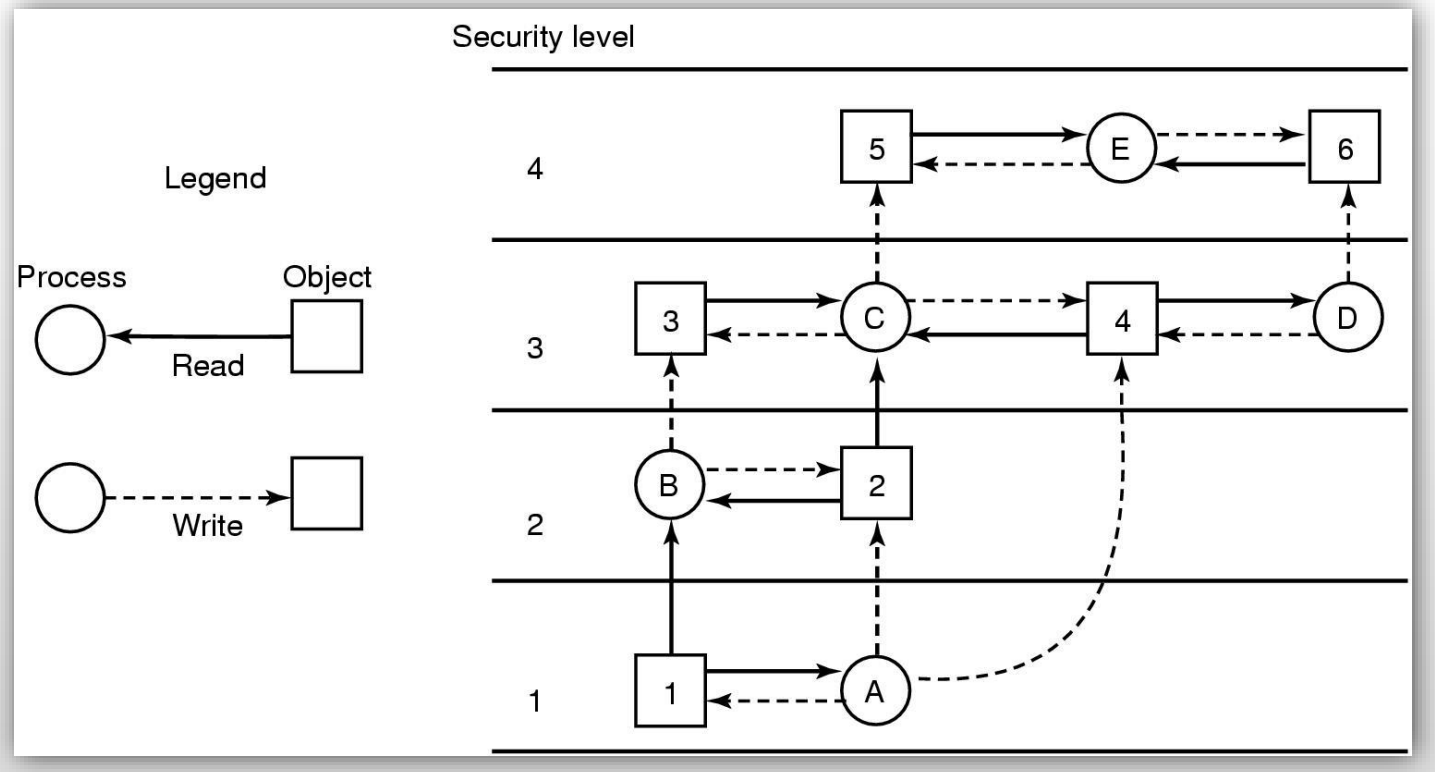
- Bell-La Padula modeli için kurallar:

- **Basit güvenlik özelliği**: k güvenlik düzeyinde çalışan bir işlem, yalnızca kendi düzeyindeki veya altındaki nesneleri okuyabilir.
- *** özelliği**: k güvenlik düzeyinde çalışan bir işlem, yalnızca kendi düzeyinde veya daha yüksek olan nesneleri yazabilir.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Bell-La Padula Modeli

- Bell-La Padula çok düzeyli güvenlik modeli.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Biba Modeli

- Biba modeli için kurallar:

- **Basit bütünlük ilkesi**: k güvenlik düzeyinde çalışan bir işlem, yalnızca kendi düzeyindeki veya altındaki nesneleri yazabilir.
- **Bütünlük * özelliği**: k güvenlik seviyesinde çalışan bir işlem, yalnızca kendi seviyesindeki veya daha yüksek seviyedeki nesneleri okuyabilir.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Bell-La Padula Modeli

- Gizli bilgilerin güvenliğini sağlamak amacıyla askeri kullanım için geliştirildi
- Gizliliğe odaklanır ve verilere yetkisiz erişime karşı koruma sağlar
- Öznelerin ve nesnelerin sınıflandırma seviyelerine göre erişim kontrolünü tanımlar
- Güvenliği sağlamak için "okuma yok" ve "yazma yok" ilkesini kullanır

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Biba Modeli

- Verilerde veya sistemlerde yetkisiz değişikliklere karşı koruma sağlamak için geliştirildi
- Bütünlüğe odaklanır ve verilerde veya sistemlerde yetkisiz değişiklikleri önler
- Öznelerin ve nesnelerin bütünlük düzeylerine göre erişim kontrolünü tanımlar
- Güvenliği sağlamak için "okuma yok" ve "yazma yok" ilkesini kullanır

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

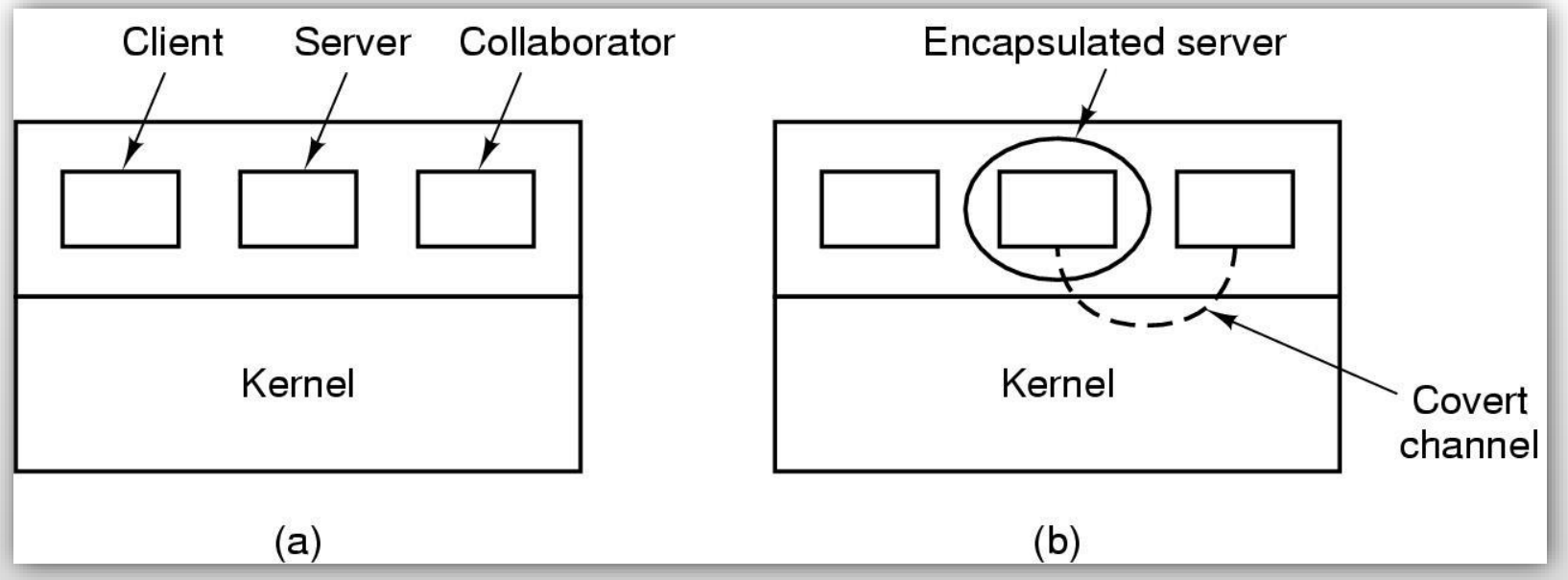
Covert Channel

- Normal güvenlik mekanizmalarını ve ilkelerini atlayarak bir bilgisayar sistemindeki süreçler arasında bilgi ileten bir mekanizmadır.
- **Gizli depolama kanalı**: Veriler, bilgilerin depolanmasındaki değişiklikler yoluyla iletilir.
- **Zamanlama gizli kanalı**: Veriler, olayların zamanlamasındaki değişiklikler yoluyla iletilir.
- **Gizli kaynak kanalı**: Veriler, sistem kaynaklarının kullanımı değiştirilerek iletilir.
- Gizli kanallar, verilerin gizliliğini ve/veya bütünlüğünü tehlikeye atarak güvenlik mekanizmalarından kaçmak için kullanılabilir.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Gizli Kanallar

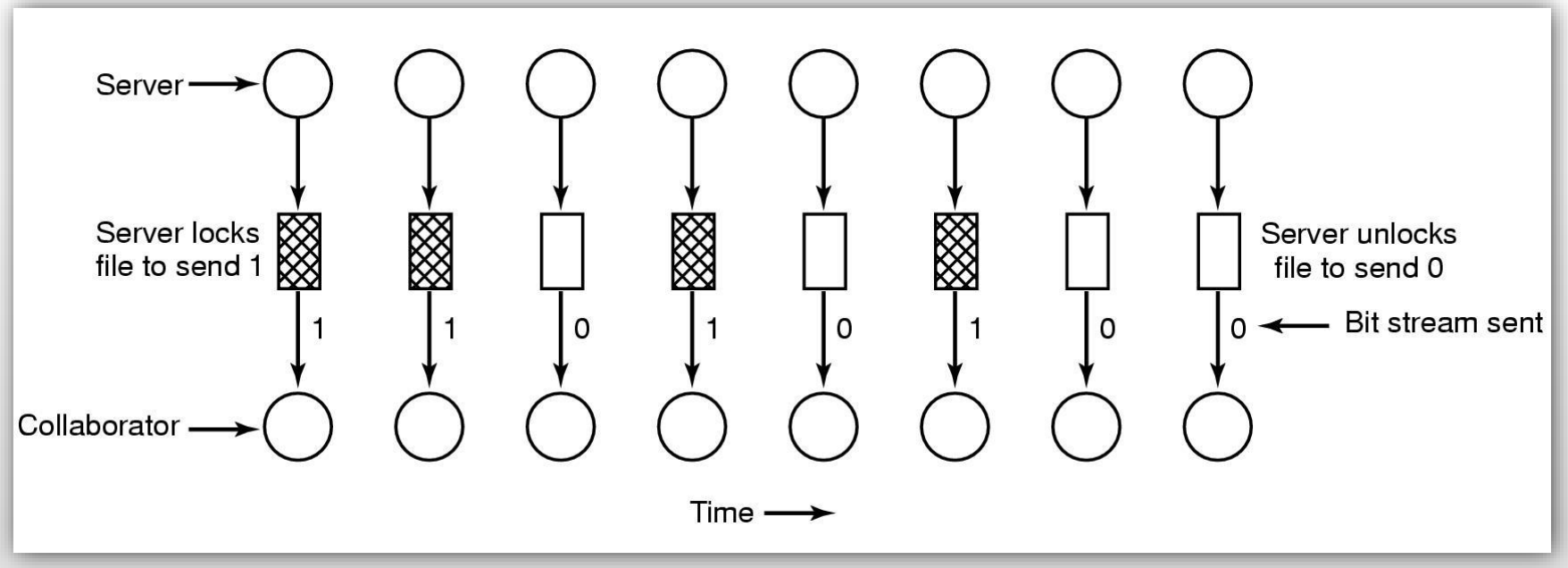
- (a) İstemci, sunucu ve ortak çalışan süreçleri. (b) Kapsüllenmiş sunucu, gizli kanallar aracılığıyla ortak çalışana yine de sızabilir.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Gizli Kanallar

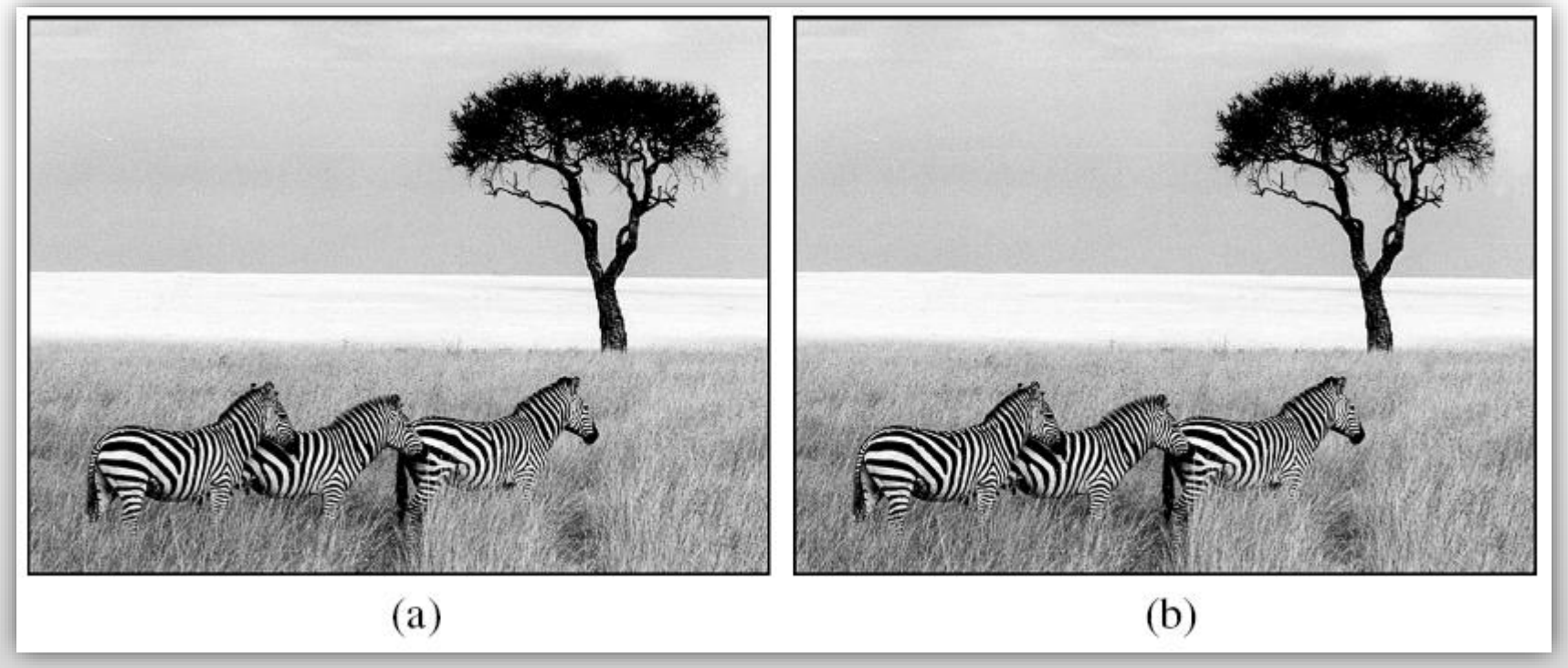
- Dosya kilitleme kullanan gizli bir kanal.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Gizli Kanallar

- (a) Üç zebra ve bir ağaç. (b) Üç zebra, bir ağaç ve William Shakespeare'in beş oyununun tam metni.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Kimlik Doğrulama

- Kullanıcıların kimliğini doğrulamanın genel ilkeleri:
  - Kullanıcının bildiği bir şey. (parola)
  - Kullanıcının sahip olduğu bir şey. (parmak izi, göz retina)
  - Kullanıcının olduğu bir şey. (kimlik kartı)

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Parola Kullanarak Kimlik Doğrulama

- (a) Başarılı bir oturum açma. (b) Ad girildikten sonra oturum açma reddedildi. (c) Ad ve parola yazıldıktan sonra oturum açma reddedildi.

(a)	(b)	(c)
LOGIN: mitch	LOGIN: carol	LOGIN: carol
PASSWORD: FooBar!-7	INVALID LOGIN NAME	PASSWORD: Idunno
SUCCESSFUL LOGIN	LOGIN:	INVALID LOGIN
		LOGIN:

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Bilgisayar Korsanları Nasıl İçeri Girer?

- .

```
LBL> telnet elxsi
ELXSI AT LBL
LOGIN: root
PASSWORD: root
INCORRECT PASSWORD, TRY AGAIN
LOGIN: guest
PASSWORD: guest
INCORRECT PASSWORD, TRY AGAIN
LOGIN: uucp
PASSWORD: uucp
WELCOME TO THE ELXSI COMPUTER AT LBL
```


Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

UNIX Parola Güvenliği

- Şifreli parolaların ön hesaplamasını (precomputation) önlemek (defeat) için tuz (salt) kullanılır. Tuz aynı şifrelerin üretilmesini önler.

Bobbie, 4238, e(Dog, 4238)
Tony, 2918, e(6%%TaeFF, 2918)
Laura, 6902, e(Shakespeare, 6902)
Mark, 1694, e(XaB#Bwcz, 1694)
Deborah, 1092, e(LordByron,1092)

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Sorgu-Yanıt Kimlik Doğrulaması

- Sorular, kullanıcının yazmasını gerektirmeyecek şekilde seçilmelidir.

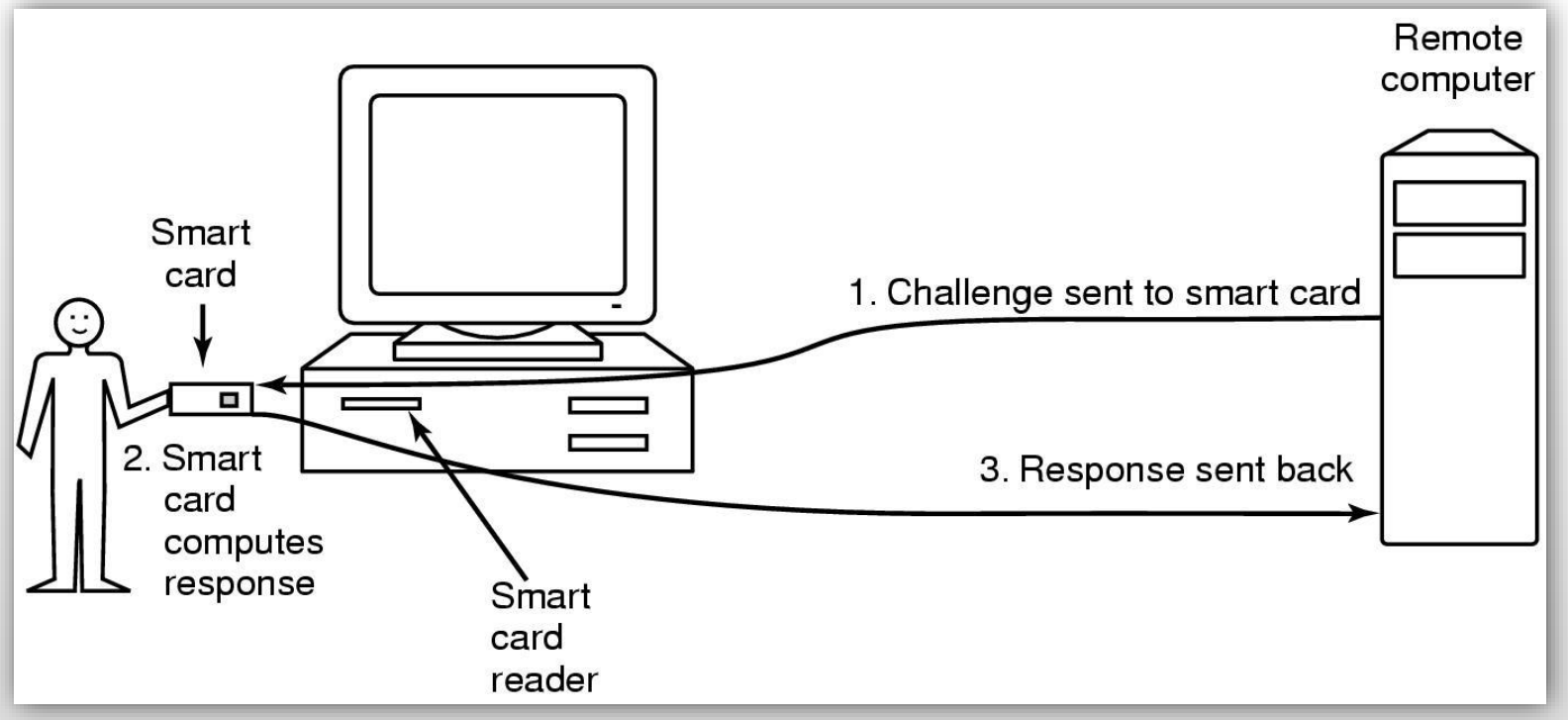
Örnekler:

- Marjolein'in kız kardeşi kimdir?
- İlkokulunuz hangi sokaktaydı?
- Bayan Woroboff ne öğretti?

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Fiziksel Nesne Kullanarak Kimlik Doğrulama

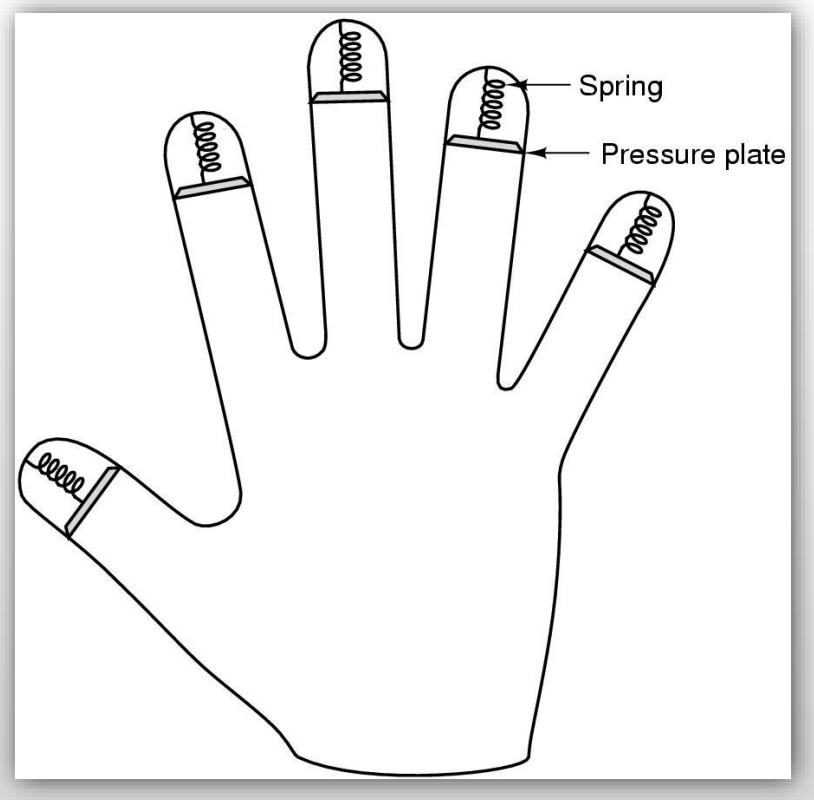
- Kimlik doğrulama için akıllı kart kullanımı.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Biyometri Kullanarak Kimlik Doğrulama

- Parmak uzunluğunu ölçmek için bir cihaz.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Tuzak Kapısı

- (a) Normal kod. (b) Tuzak kapılı kod.

```
while (TRUE) {
        printf("login: ");
        get_string(name);
        disable_echoing( );
        printf("password: ");
        get_string(password);
        enable_echoing( );
        v = check_validity(name, password);
        if (v) break;
}
execute_shell(name);
```

(a)

```
while (TRUE) {
        printf("login: ");
        get_string(name);
        disable_echoing( );
        printf("password: ");
        get_string(password);
        enable_echoing( );
        v = check_validity(name, password);
        if (v || strcmp(name, "zzzzz") == 0) break;
}
execute_shell(name);
```

(b)

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Giriş Sayfası Kandırma Saldırısı

- (a) Doğru oturum açma ekranı. (b) Sahte oturum açma ekranı.

Kod Hatalarından Yararlanma

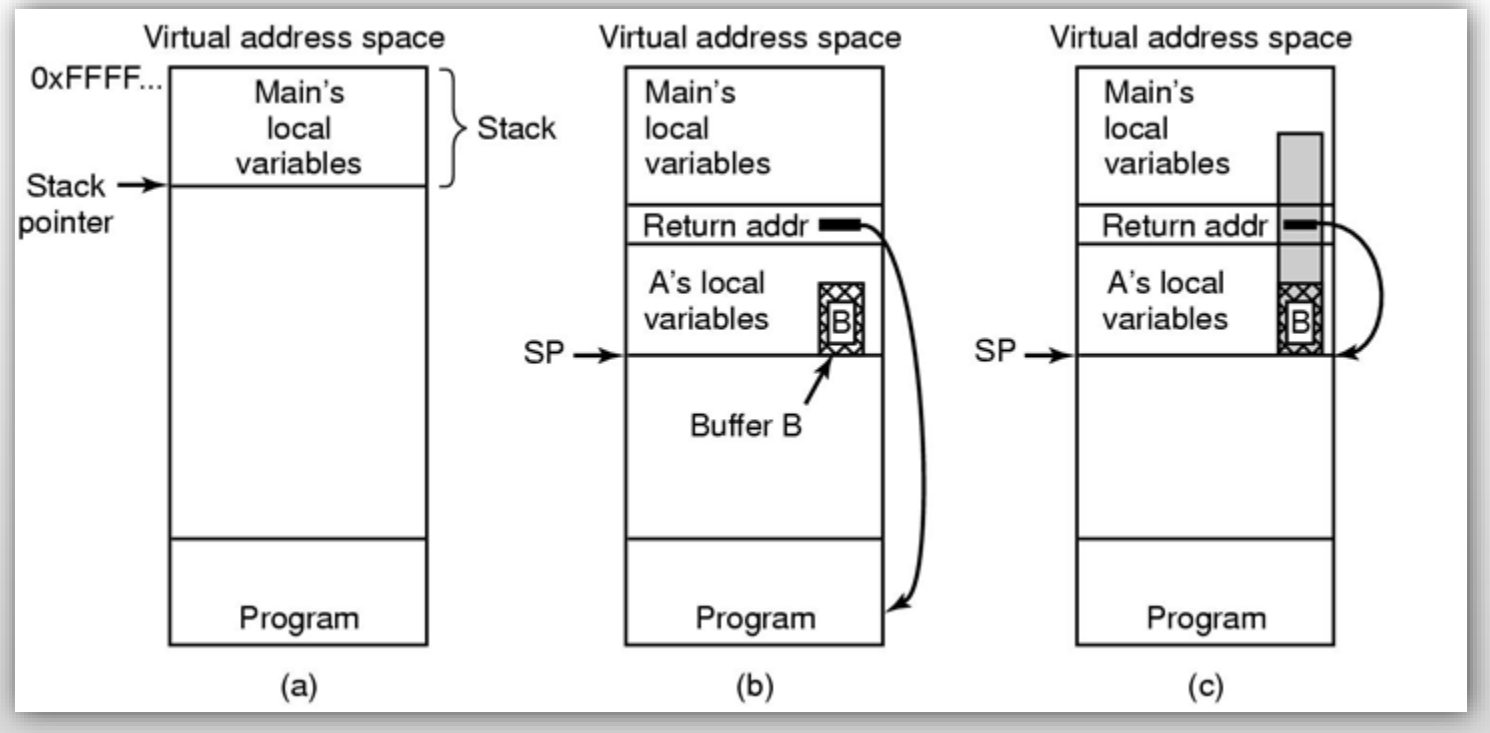
- Bir hatadan yararlanmak için örnek adımlar:

- Telnet bağlantılarını kabul eden makineleri bulmak için bağlantı noktası taramasını (scan port) çalıştır.
- Kullanıcı adı, şifre kombinasyonları tahmin ederek giriş yapmayı dene.
- Girişten sonra, hatayı tetikleyen girdiyle hatalı programı çalıştır.
- Hatalı program SETUID kökü ise, bir SETUID kök kabuğu (root shell) oluştur.
- Cmds için IP port dinleyen bir zombi programı getir (fetch) ve başlat.
- Sistem yeniden başlatıldığında zombi programının başlatılmasını sağla.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Tampon Taşma Saldırıları

- (a) Ana programın çalıştığı durum. (b) Prosedür A çağrıldıktan sonra. (c) Gri renkle gösterilen arabellek taşması.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

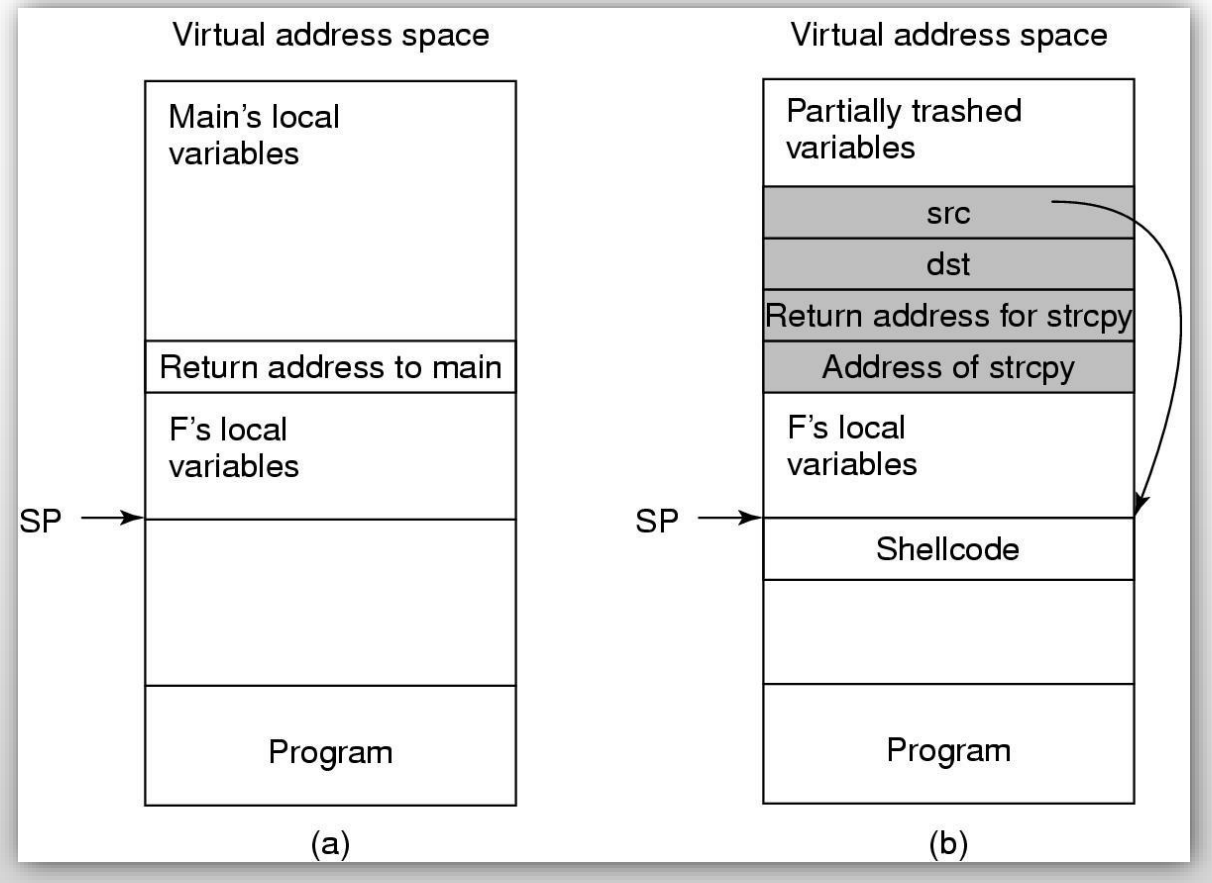
Tampon Taşma Saldırıları

```
#include <stdio.h>
#define BUFFER SIZE 256
int main(int argc, char *argv[])
{
      char buffer[BUFFER SIZE];
      if (argc < 2)
            return -1;
      else {
            strcpy(buffer,argv[1]);
            return 0;
      }
}
```


Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

libc Saldırıları

- (a) Saldırıdan önceki yığın. (b) Yığın üzerine yazıldıktan sonra.



Kod Enjeksiyon Saldırıları

- Kod enjeksiyon saldırısına yol açabilecek kod.

```
int main(int argc, char *argv[])
{
  char src[100], dst[100], cmd[205] = "cp ";          /* declare 3 strings */
  printf("Please enter name of source file: ");       /* ask for source file */
  gets(src);                                          /* get input from the keyboard */
  strcat(cmd, src);                                   /* concatenate src after cp */
  strcat(cmd, " ");                                   /* add a space to the end of cmd */
  printf("Please enter name of destination file: ");  /* ask for output file name */
  gets(dst);                                          /* get input from the keyboard */
  strcat(cmd, dst);                                   /* complete the commands string */
  system(cmd);                                        /* execute the cp command */
}
```


Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Kötü Amaçlı Yazılım (malware)

- Bir tür şantaj için kullanılabilir.
- Örnek: Kurban diskindeki dosyaları şifreler, ardından şu mesajı görüntüler…

Greetings from General Encryption

To purchase a decryption key for your hard disk, please send $100 in small unmarked bills to Box 2154, Panama City, Panama.
Thank you. We appreciate your business.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

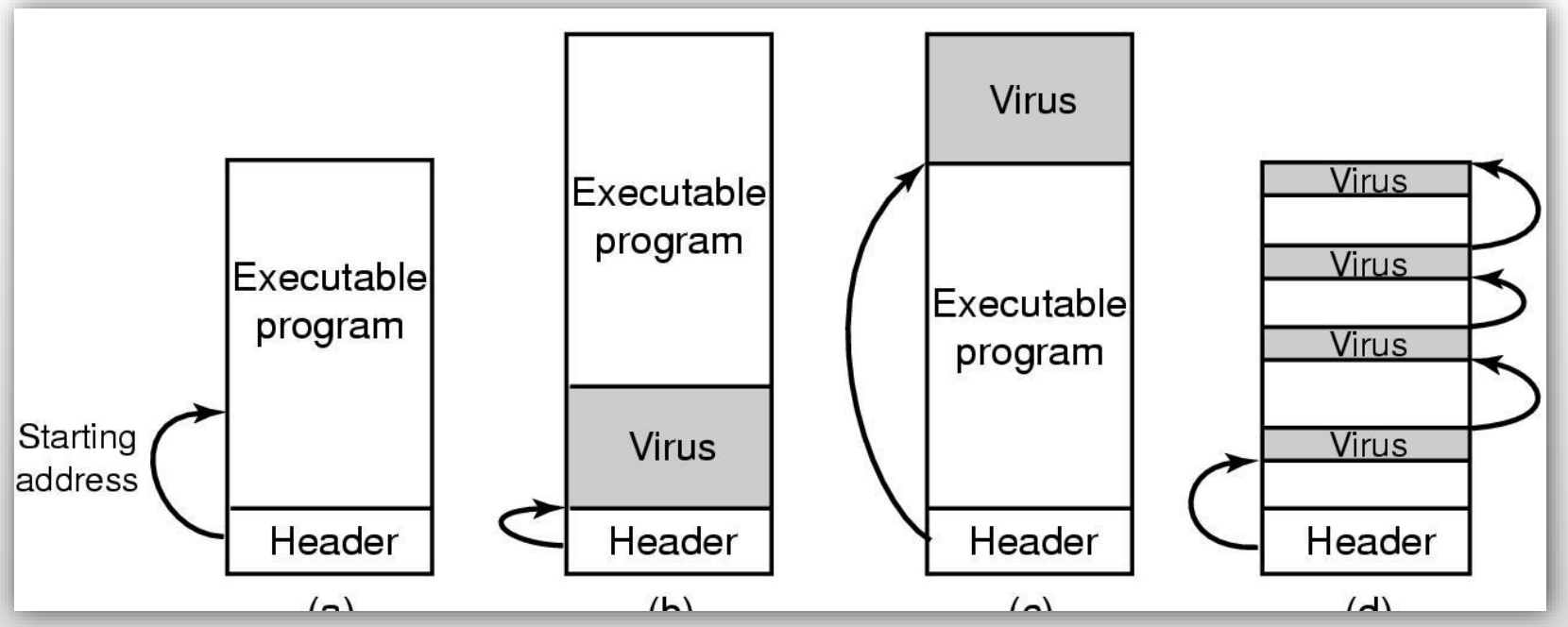
Virüs Çeşitleri

- Eşlik eden virüs (companion)
- Yürütülebilir program virüsü (executable)
- Parazitik virüs (parasitic)
- Bellekte yerleşik virüs (memory resident)
- Önyükleme sektörü virüsü (boot sector)
- Aygıt sürücüsü virüsü (device driver)
- Makro virüs (macro)
- Kaynak kodu virüsü (source code)

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

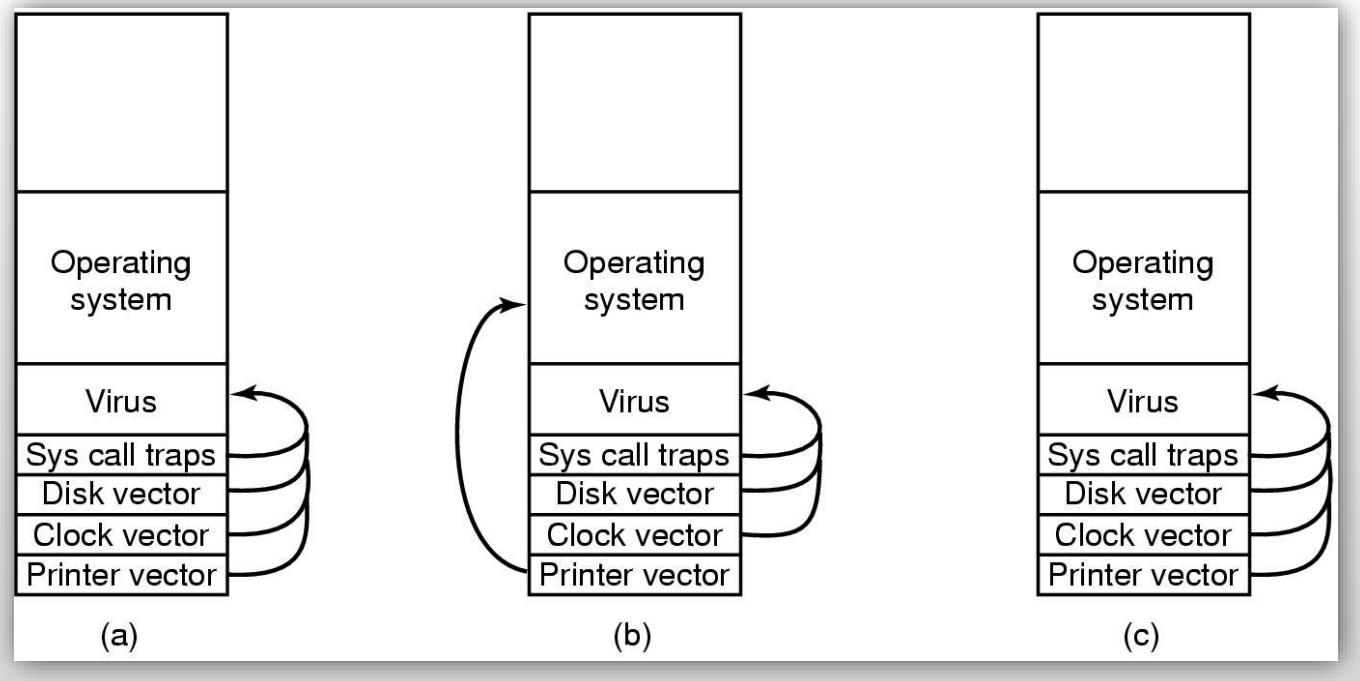
Parazitik Virüsler

- (a) Yürütülebilir bir program (b) Önünde yerleşik bir virüs (c) Sonunda yerleşik bir virüs (d) Program içindeki boş alana yayılmış bir virüs ile.



Önyükleme Sektörü Virüsleri

- (a) Virüs tüm kesme ve tuzak vektörlerini yakaladıktan sonra. (b) İşletim sistemi yazıcı kesme vektörünü yeniden aldıktan sonra. (c) Virüs, yazıcı kesme vektörünü yeniden yakaladıktan sonra.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Casus Yazılım

- Sahibinin bilgisi dışında gizlice bir PC'ye yüklenir
- Arka planda çalışır
- Gizlenir, kurban kolayca bulamaz
- Kullanıcı hakkında veri toplar
- Toplanan bilgileri uzakta bir bilgisayara iletir
- Onu ortadan kaldırmak için kararlı girişimlerde hayatta kalmaya çalışır

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Casus Yazılım Nasıl Yayılır

- Olası yollar:

- Kötü amaçlı yazılımla aynı, Truva atı
- İndirme, virüslü bir web sitesini ziyaret etme
- Web sayfaları bir .exe dosyası çalıştırmayı dener
- Şüphelenilmeyen kullanıcı virüslü bir araç çubuğu yükler
- Kötü amaçlı activeX denetimleri yüklenir

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Casus Yazılım Gerçekleştirdiği Eylemler

- Tarayıcının ana sayfasını değiştirme.
- Tarayıcının favori (yer imi eklenmiş) sayfalar listesini değiştirme.
- Tarayıcıya yeni araç çubukları ekleme.
- Varsayılan medya yürütücüsünü değiştirme.
- Varsayılan arama motorunu değiştirme.
- Windows masaüstüne yeni simgeler ekleme.
- Web sayfalarındaki banner reklamları, casus yazılımın seçtikleriyle değiştirme.
- Reklamları standart Windows iletişim kutularına yerleştirme
- Sürekli ve durdurulamaz bir pop-up reklam akışı oluşturma.

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

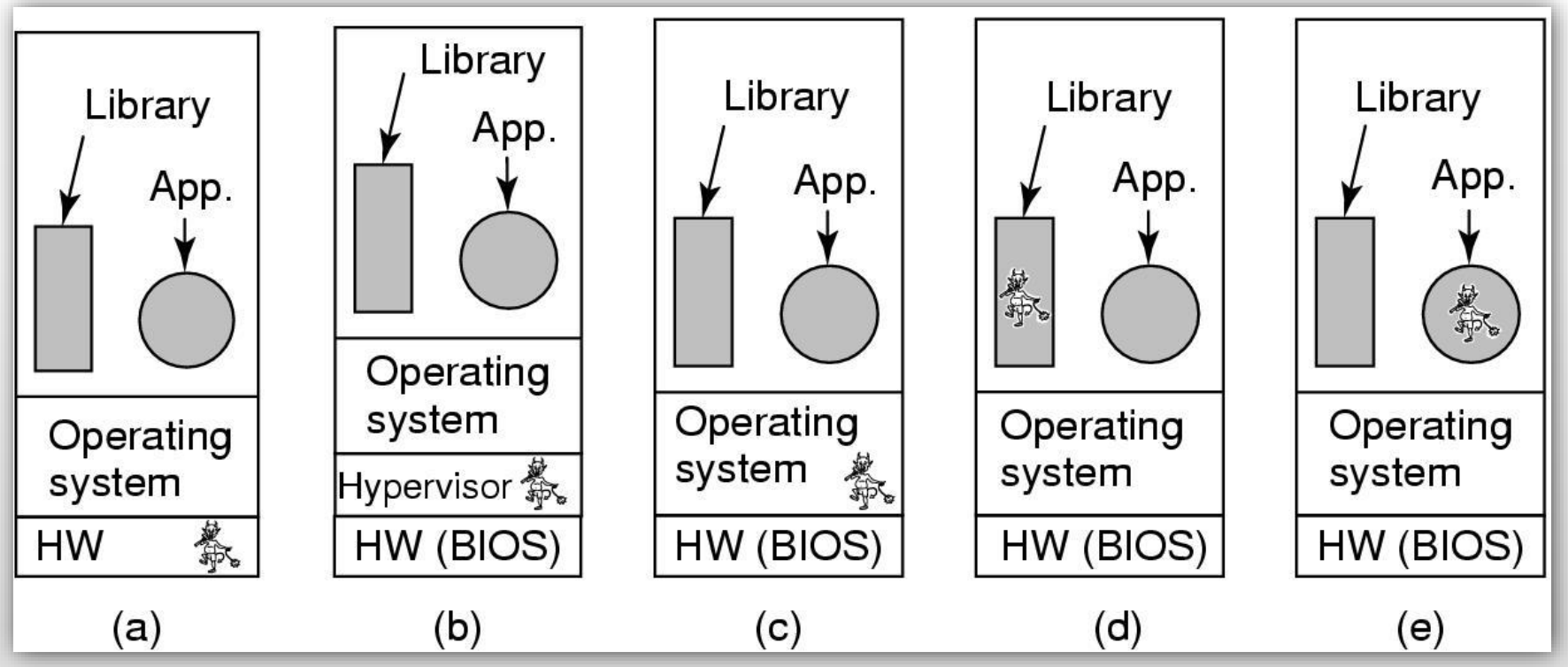
Rootkit Türleri

- Bellenim rootkit'leri (firmware)
- Hipervizör rootkit'leri
- Çekirdek rootkit'leri (kernel)
- Kütüphane rootkit'leri
- Uygulama rootkit'leri

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Bir Rootkit'in Saklanabileceği Beş Yer

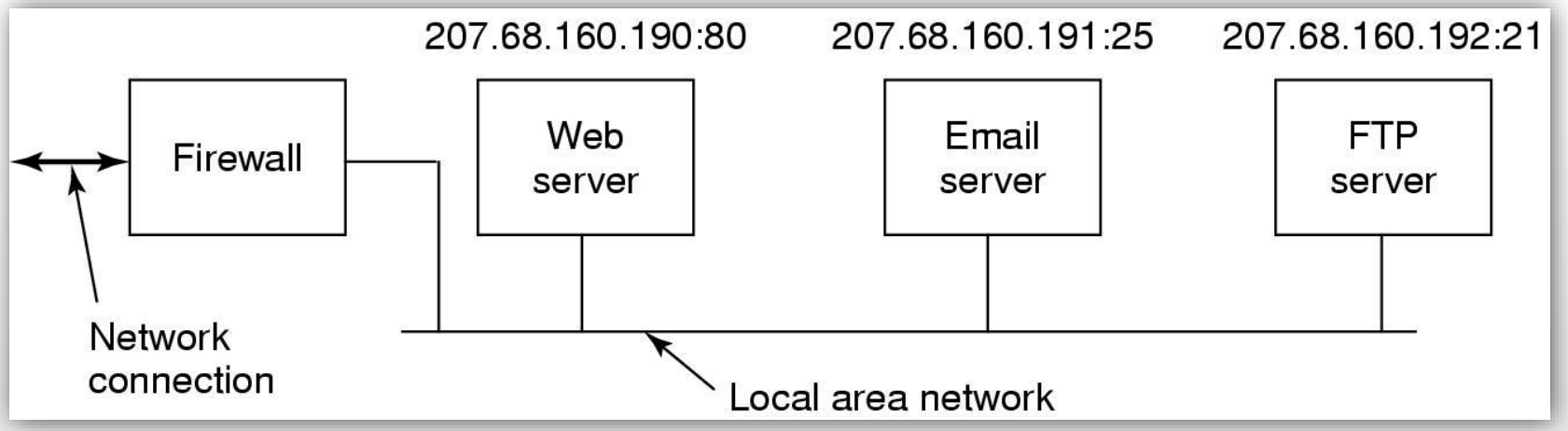
- .



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Güvenlik Duvarı

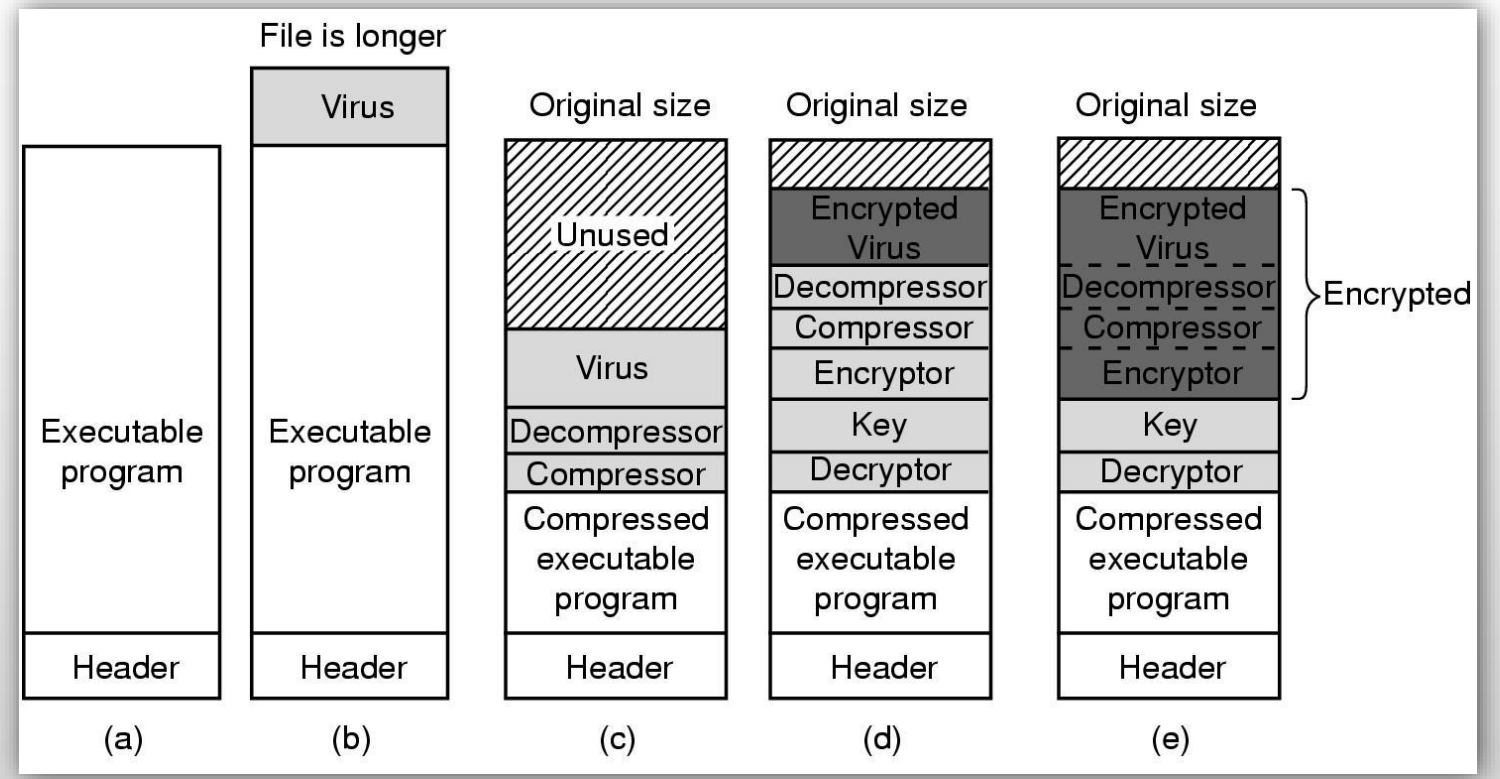
- Üç bilgisayarlı bir LAN'ı koruyan donanım güvenlik duvarı



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Virüs Tarayıcıları

- (a) Bir program. (b) Virüslü program. (c) Sıkıştırılmış virüslü program. (d) Şifrelenmiş bir virüs. (e) Şifrelenmiş sıkıştırma ile sıkıştırılmış virüs.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Virüs Tarayıcıları

- Polimorfik virüs örnekleri.

(a)	(b)	(c)	(d)	(e)
MOV A,R1	MOV A,R1	MOV A,R1	MOV A,R1	MOV A,R1
ADD B,R1	NOP	ADD #0,R1	OR R1,R1	TST R1
ADD C,R1	ADD B,R1	ADD B,R1	ADD B,R1	ADD C,R1
SUB #4,R1	NOP	OR R1,R1	MOV R1,R5	MOV R1,R5
MOV R1,X	ADD C,R1	ADD C,R1	ADD C,R1	ADD B,R1
	NOP	SHL #0,R1	SHL R1,0	CMP R2,R5
	SUB #4,R1	SUB #4,R1	SUB #4,R1	SUB #4,R1
	NOP	JMP .+1	ADD R5,R5	JMP .+1
	MOV R1,X	MOV R1,X	MOV R1,X	MOV R1,X
			MOV R5,Y	MOV R5,Y

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

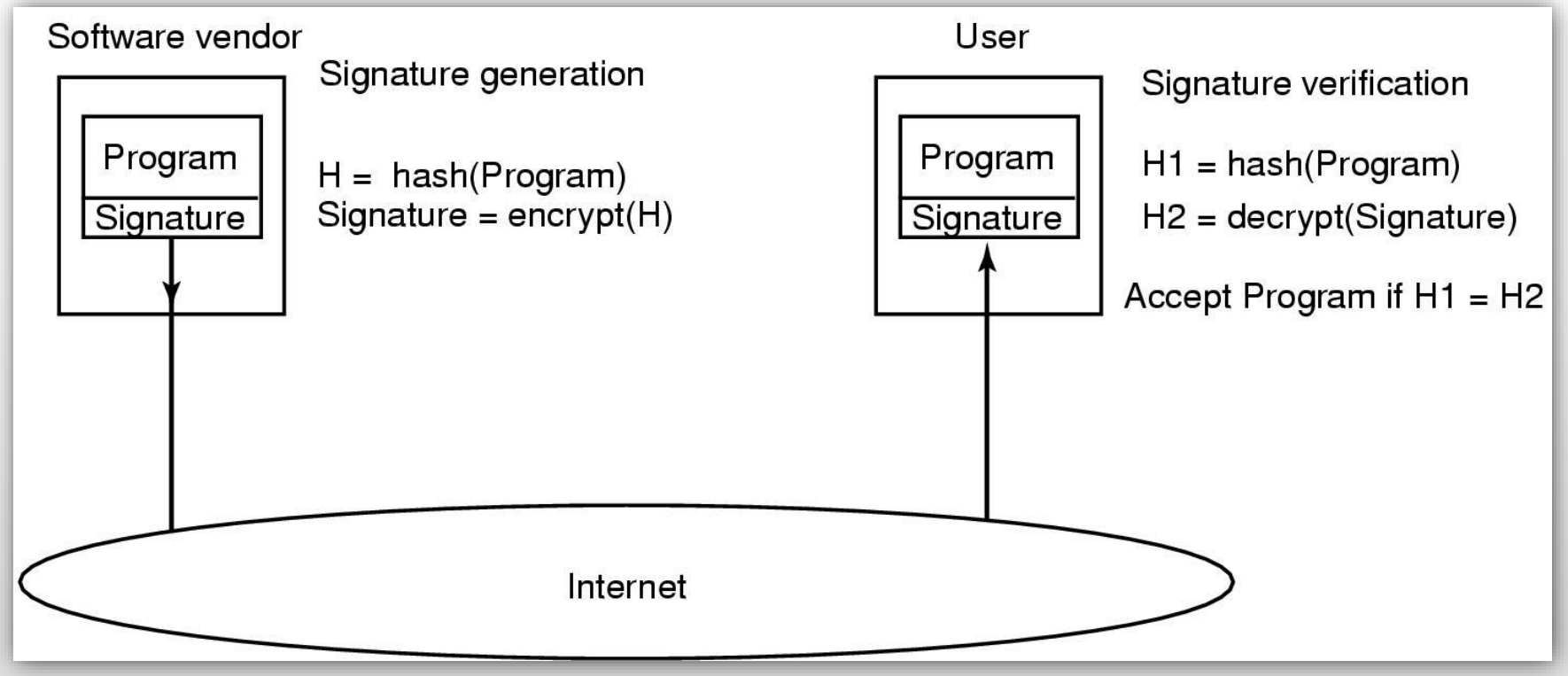
Antivirüs ve Anti-Antivirüs Teknikleri

- Virüs tarayıcıları
- Bütünlük denetleyicileri (integrity)
- Davranışsal denetleyiciler
- Virüsten kaçınma

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Kod İmzalama Nasıl Çalışır?

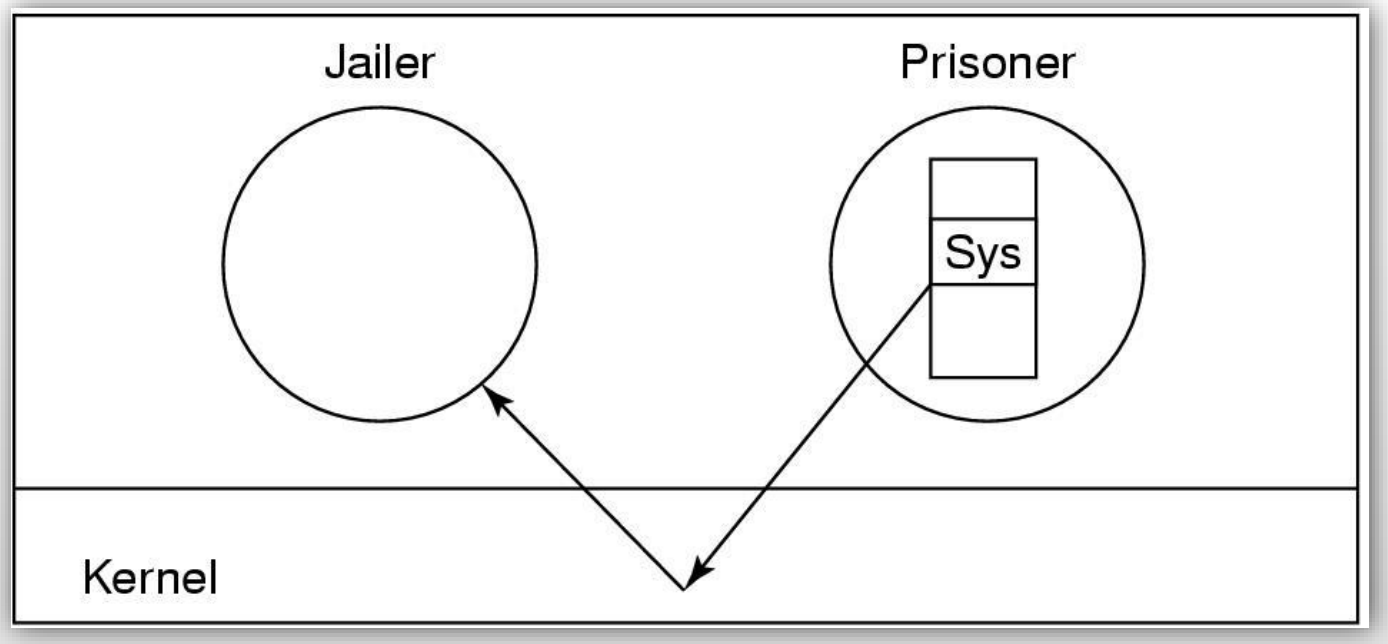
- .



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Hapse Atmak (jailing)

- .



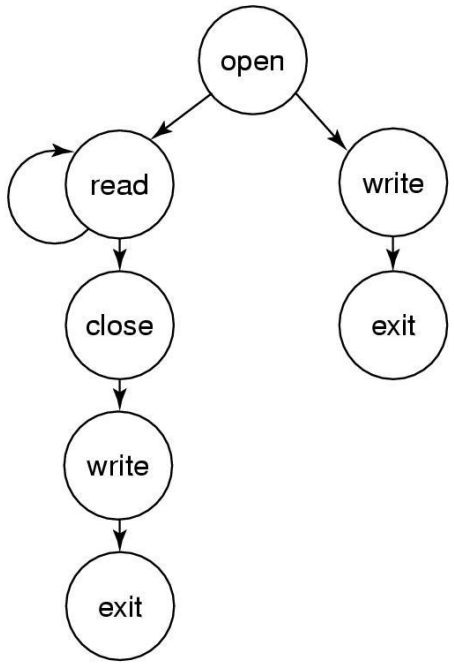
Model Tabanlı Saldırı Tespiti

- (a) Bir program. (b) (a) için sistem çağrıları çizgesi.

```
int main(int argc *char argv[])
{
  int fd, n = 0;
  char buf[1];

  fd = open("data", 0);
  if (fd < 0) {
      printf("Bad data file\n");
      exit(1);
  } else {
      while (1) {
          read(fd, buf, 1);
          if (buf[0] == 0) {
            close(fd);
            printf("n = %d\n", n);
            exit(0);
        }
        n = n + 1;
      }
  }
}
```

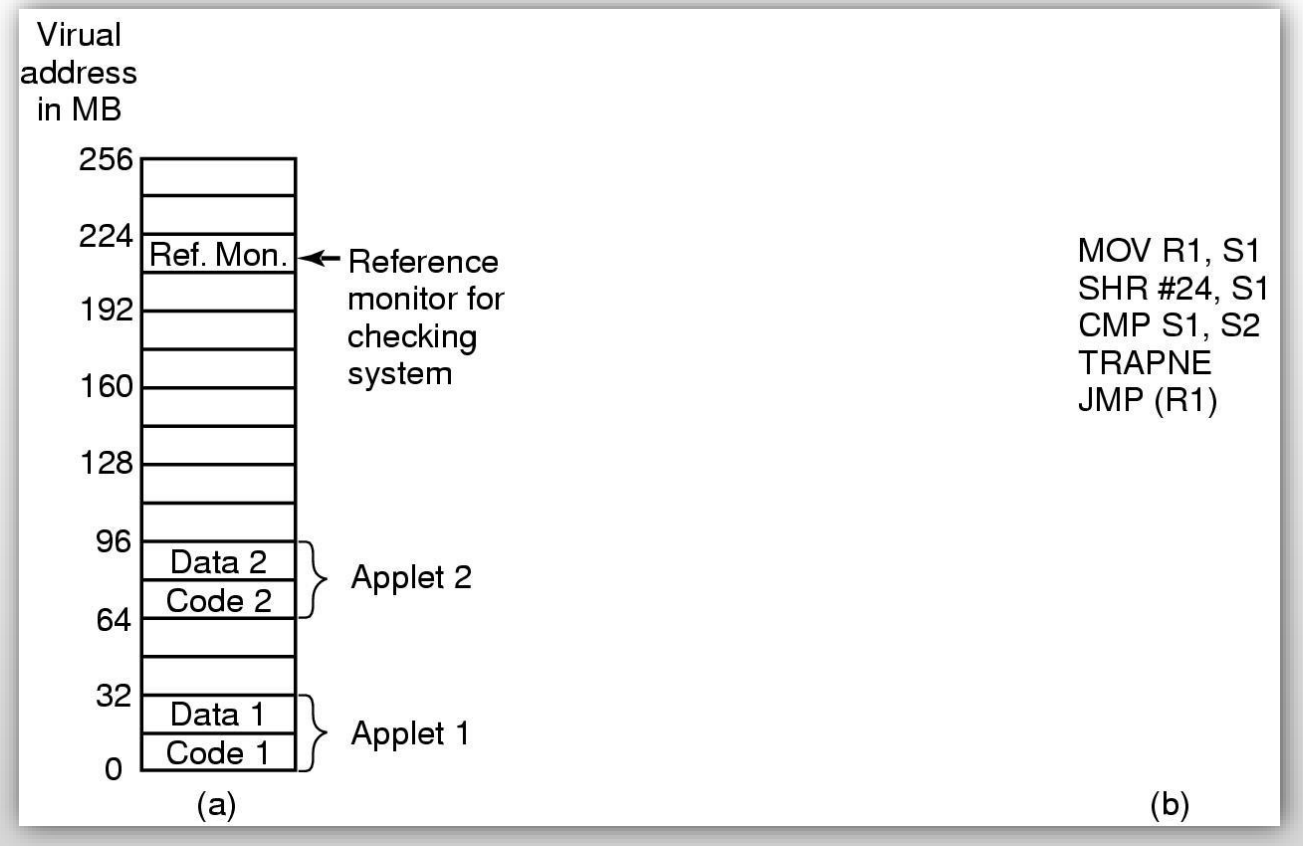
(a)



(b)

Korumalı Alan (sandboxing)

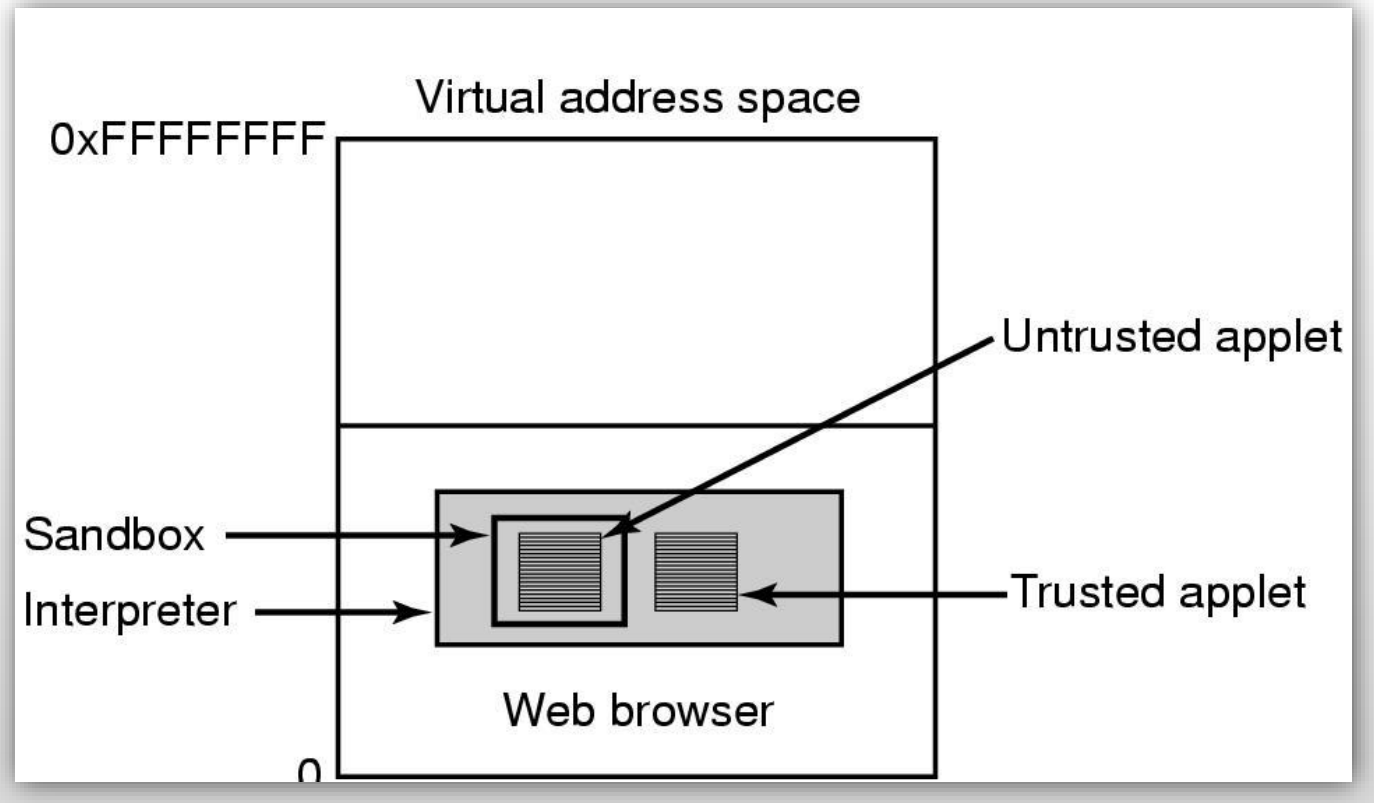
- (a) 16 MB sanal alanlara bölünmüş bellek. (b) Bir talimatın geçerliliğini kontrol etmenin yolu.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Yorumlamalı Dil (interpreter)

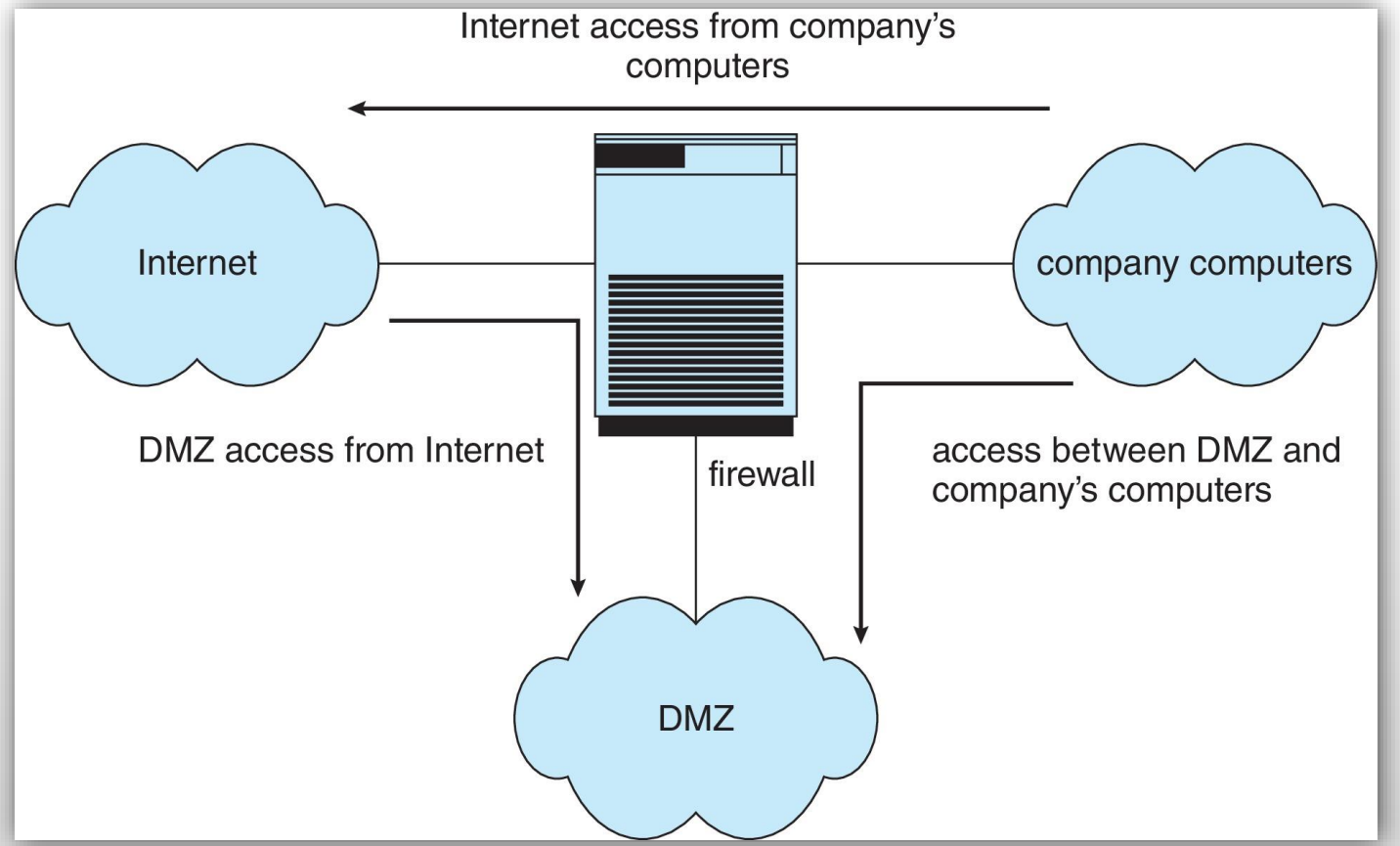
- Applet'ler bir Web tarayıcısı tarafından yorumlanabilir.



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Ateş Duvarı (Firewall)

- .



Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

Java Güvenlik

- JVM bayt kodu doğrulayıcı, uygulamanın belirli kurallara uyup uymadığını kontrol eder:
- Uygulama, işaretçiler oluşturmaya çalışıyor mu?
- Özel sınıf üyeleri üzerindeki erişim kısıtlamalarını ihlal ediyor mu?
- Bir tür değişkeni başka bir tür olarak kullanmaya çalışıyor mu?
- Yığın taşmaları oluşturuyor mu? (stack overflows, underflows)
- Bir türdeki değişkenleri yasa dışı bir şekilde diğerine dönüştürüyor mu?

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.

SON

Sercan KÜLCÜ, Tanenbaum, Modern Operating Systems 3e kitabından faydalanılmıştır. Tüm hakları saklıdır.