Bölüm 13: Güvenlik

İşletim Sistemleri

Güvenlik Hedefleri

- **Gizlilik**: (*privacy*)
  - Hassas verilere yetkisiz kullanıcılar *erişememeli*.
- **Bütünlük**: (*integrity*)
  - Yetkisiz kullanıcılar veri ve sistem üzerinde *değişiklik* yapamamalı.
- **Erişilebilirlik**: (accessibility)
  - Yetkili kullanıcılar *gerektiğinde* veri ve sistemlere erişebilmeli.

Tehditler

- **Kötü Amaçlı Yazılım**: (*malware*)
  - Virüs, Truva atı, solucan, casus yazılım, fidye yazılımı..
- **Yetkisiz Erişim**: (*unauthorized access*)
  - Uygun yetkilendirme olmadan verilere erişme girişimi.
- **Hizmet Reddi (DoS)**: (*denial of service*)
  - Sistemin kullanılabilirliğini kesintiye uğratmak.
- **Arabellek Taşmaları**: (*buffer overflow*)
  - Bellekte izin verilmeyen bir alana erişme girişimi.
- **Yarış Koşulları**: (*race condition*)
  - Kodun eşzamanlı yürütülmesi sonucu beklenmeyen durumlar.

Savunma Mekanizmaları

- **Erişim Kontrolü**: (*access control*)
  - Hangi kullanıcının hangi verilere erişebileceği tanımlanmalı.
- **Güvenlik Duvarı**: (*firewall*)
  - Yetkisiz erişimi önlemek amacıyla ağ trafiği filtrelenmeli.
- **Bellek Koruması**: (*memory protection*)
  - Arabellek taşması gibi bellek tabanlı saldırılar önlenmeli.
- **Kum Havuzu**: (sandboxing)
  - Süreçler izole edilerek birbirlerini engellemeleri önlenmeli.
- **Şifreleme:** (*encryption*)
  - Hassas veriler aktarım sırasında da korunmalı.

Güvenlik İhlali Kategorileri

- **Gizlilik İhlali:** *(Breach of confidentiality)*
  - Verilerin izinsiz okunması.
- **Bütünlük İhlali:** *(Breach of integrity)*
  - Verilerin izinsiz değiştirilmesi.
- **Erişilebilirlik İhlali:** *(Breach of availability)*
  - Verilerin yetkisiz imhası.
- **Hizmet Hırsızlığı:** *(Theft of service)*
  - Kaynakların yetkisiz kullanımı.
- **Hizmet Reddi:** *(Denial of service (DoS))*
  - Sistem kullanımının önlenmesi.

Güvenlik İhlali Kategorileri

- **Kimlik Değiştirme:** *(Masquerading)*
  - Yetkisiz bir kullanıcının yetkili gibi davranması.
- **Tekrar Saldırısı:** *(Replay attack)*
  - İzinsiz bir şekilde elde edilen mesajın tekrar kullanılması.
- **Ortadaki Adam Saldırısı:** *(Man-in-the-middle attack)*
  - Üçüncü tarafın kendisini alıcı sisteme gönderici kılığında göstermesi.
- **Oturum Kaçırma:** *(Session hijacking)*
  - Kimlik kontrolü yapılmış oturumun ele geçirilmesi.
- **Ayrıcalık Yükseltme:** *(Privilege escalation)*
  - Gerekenden daha fazla erişim hakkına sahip olunması.

İyi Uygulamalar (Best Practices)

- Güvenlik yamalarıyla (*security patch*) yazılım güncel tutulmalı.
- Güçlü kimlik doğrulama ve erişim kontrol mekanizmaları kullanılmalı.
- Güvenlik ile ilgili izleme ve günlük kaydı (*log*) tutulmalı.
- Düzenli olarak güvenlik ve sızma testleri gerçekleştirilmeli.
- Kullanıcılar güvenlik tehditlerine karşı farkındalık konusunda eğitilmeli.

Yetkisiz Kullanıcı

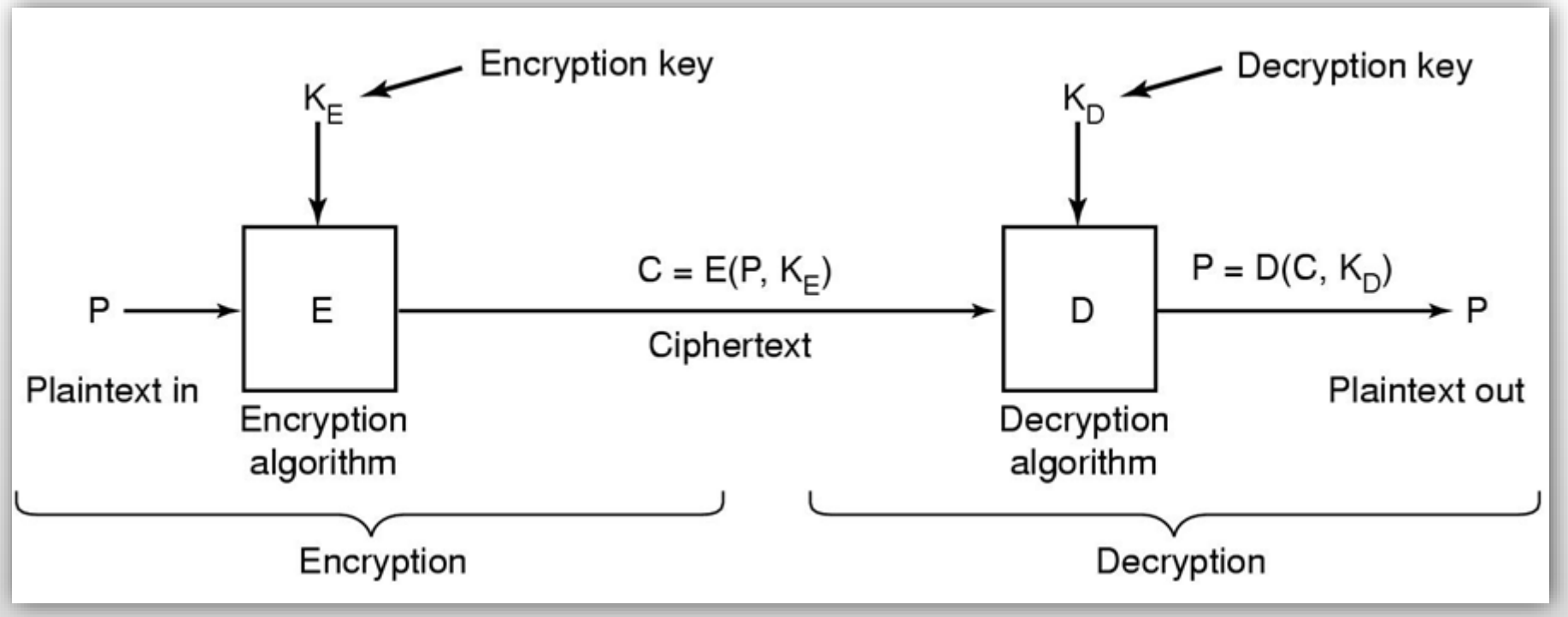
- Teknik olmayan kişiler tarafından,
  - bilgi veya eğlence amacıyla gerçekleştirilen rastgele gözlemleme.
  - kişisel gizliliği ihlal edebilir ve etik olmayan bir davranış.
- Organizasyonun kötü niyetli çalışanları tarafından,
  - gerçekleştirilen gözetleme faaliyetleri.
  - güvenlik ihlalleri ve hassas bilgilerin sızdırılmasına yol açar.
- Kar amacı güden bireyler tarafından,
  - gerçekleştirilen, kazanç sağlamayı amaçlayan casusluk gözetleme.
- Ticari casusluk, firmalar arasında rekabet avantajı elde etmeyi amaçlar.
- Askeri casusluk, devletler arasında stratejik avantaj sağlama amacı taşır.

Kazayla Veri Kaybı

- **Kader**:
  - yangın, sel, deprem, savaş veya yedek bantları kemiren fareler.☺
- **Donanım veya yazılım hataları**:
  - CPU arızaları, okunamayan diskler, program hataları.☹
- **İnsan kaynaklı hatalar**:
  - hatalı veri girişi, yanlış teyp veya CD-ROM takma, programın yanlış kullanımı, kayıp disk veya başka bir hata.

Şifrelemenin Temelleri

- Düz metin (*plain text*) ve şifreli metin (*ciphertext*).



Gizli Anahtarlı Şifreleme (Secret Key)

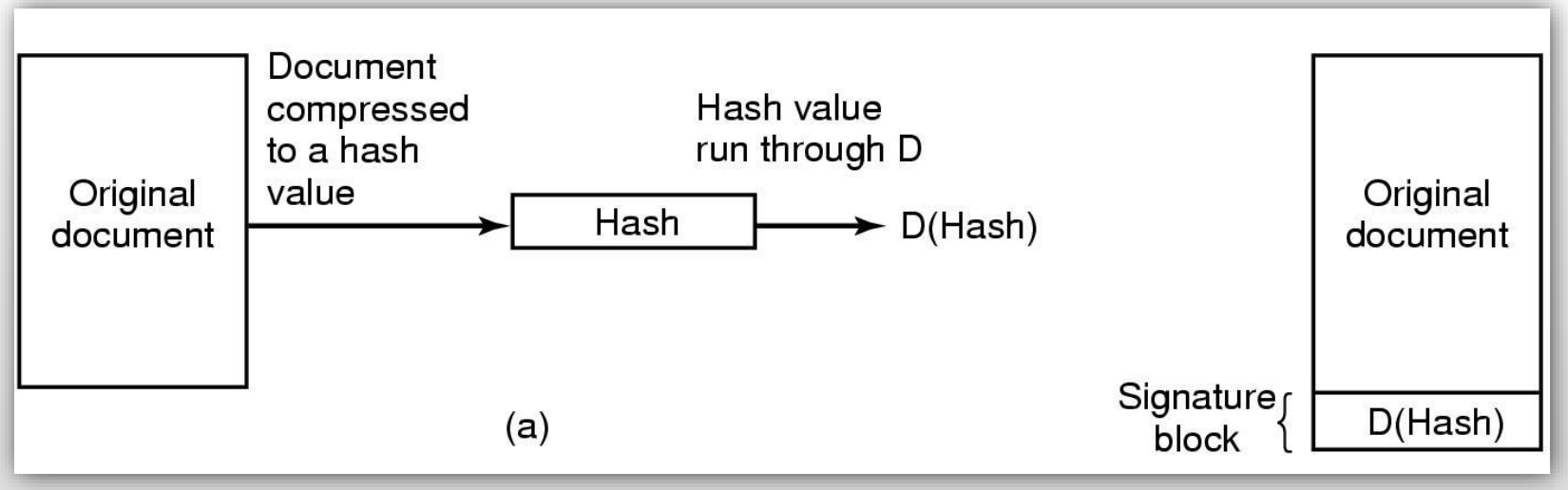
- Mono alfabetik ikame:
  - her karakter, sabit bir başka karaktere dönüştürülür.
- `Kaynak metin:  ABCDEFGHIJKLMNOPQRSTUVWXYZ`
- `Hedef metin:  QWERTYUIOPASDFGHJKLZXCVBNM`
- Örnek:
  - `Düz metin:  MERHABA`
  - `Şifreli metin: DTKIQWQ`

Açık Anahtarlı Şifreleme

- Şifreleme:
  - *11x11* gibi *kolay* bir işlem.
- Anahtar olmadan şifre çözme:
  - *121*'in *karekökü* gibi *zor* bir işlem gerektirir.

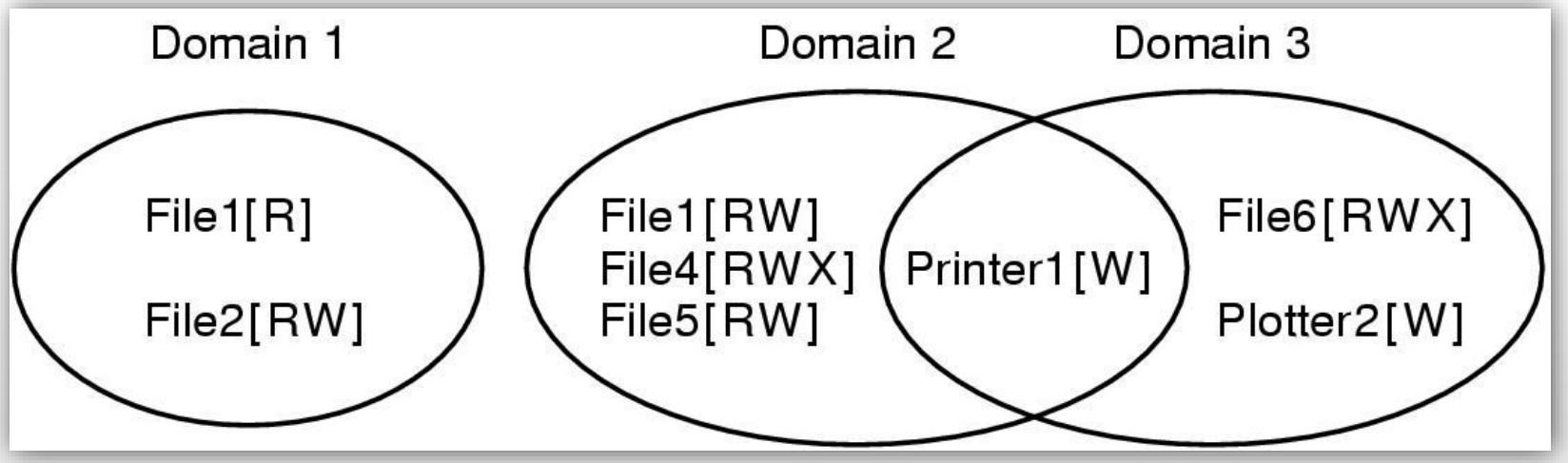
Dijital İmzalar

- (a) Belge sıkıştırılarak bir değer (*hash*) hesaplanır.
- (b) Alıcıya belge ile beraber hash değeri gönderilir.



Koruma Etki Alanları

- Üç farklı koruma alanı.



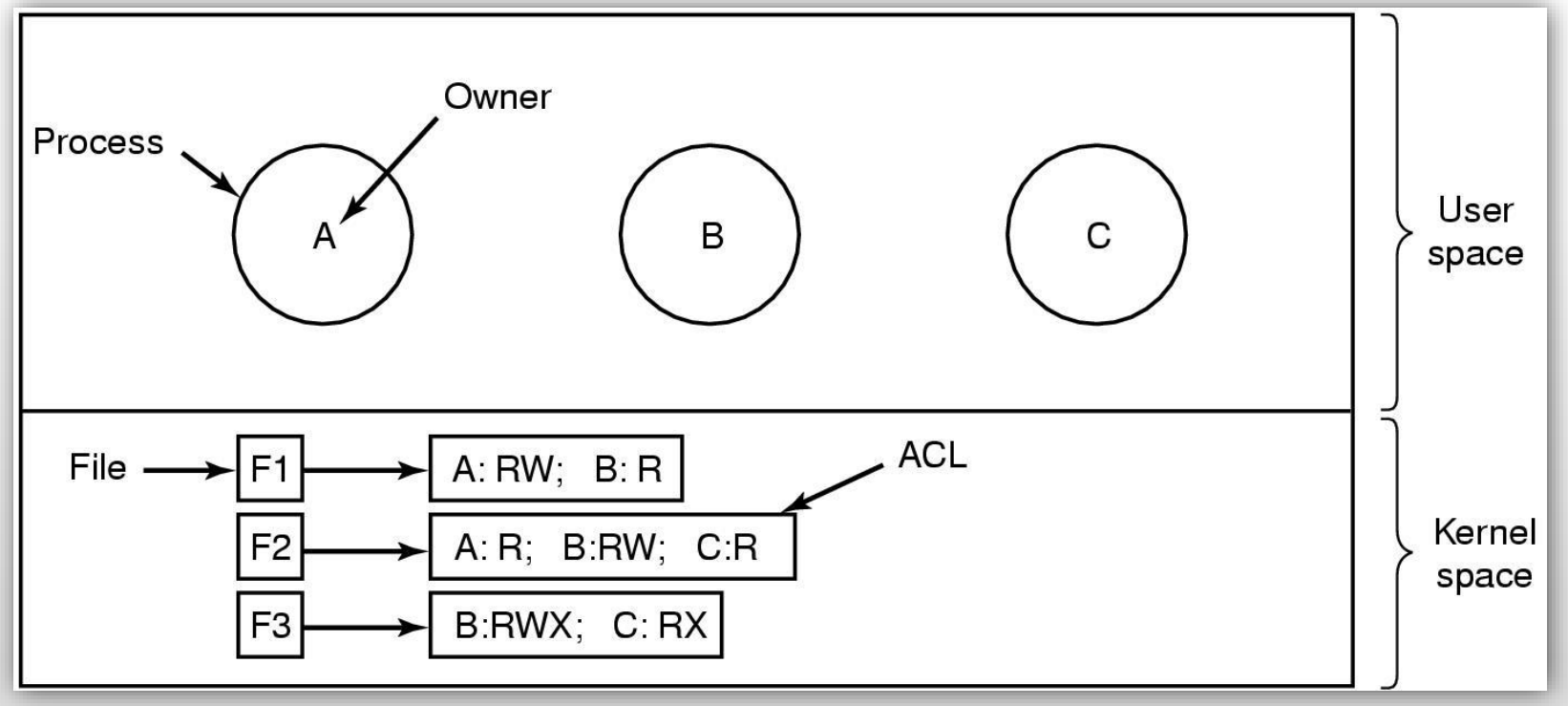
Koruma Etki Alanları

- koruma matrisi.

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

Erişim Kontrol Listeleri

- Dosya erişimini yönetmek için erişim kontrol listeleri.



Erişim Kontrol Listeleri

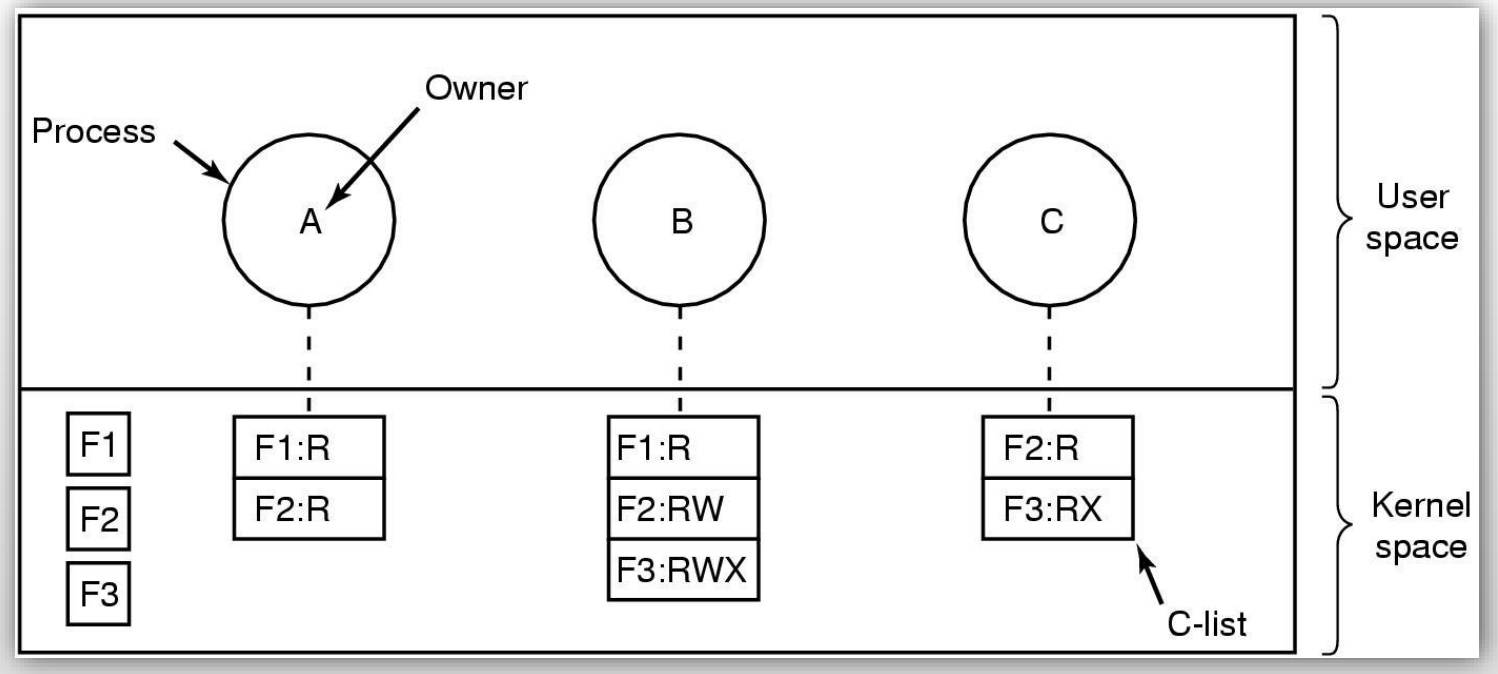
- *Access control list.*
- Sistem kaynaklarına erişim kontrolü sağlayan güvenlik mekanizması.
- Hangi kaynağa, kim erişebilir, neler yapabilir?
- Kısıtlı kaynak sistemlerde performansı olumsuz etkiler.
- Büyük ve karmaşık sistemlerde yönetimi zor.
- Farklı işletim sistemlerinde,
  - Uyumluluk ve birlikte çalışabilirlik sorunlarına yol açabilir.

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.

Yetenek Listesi

- Her sürecin bir yetenek (*capability*) listesi var.



Yetenek Listesi

- Şifreli olarak korunan bir yetenek.

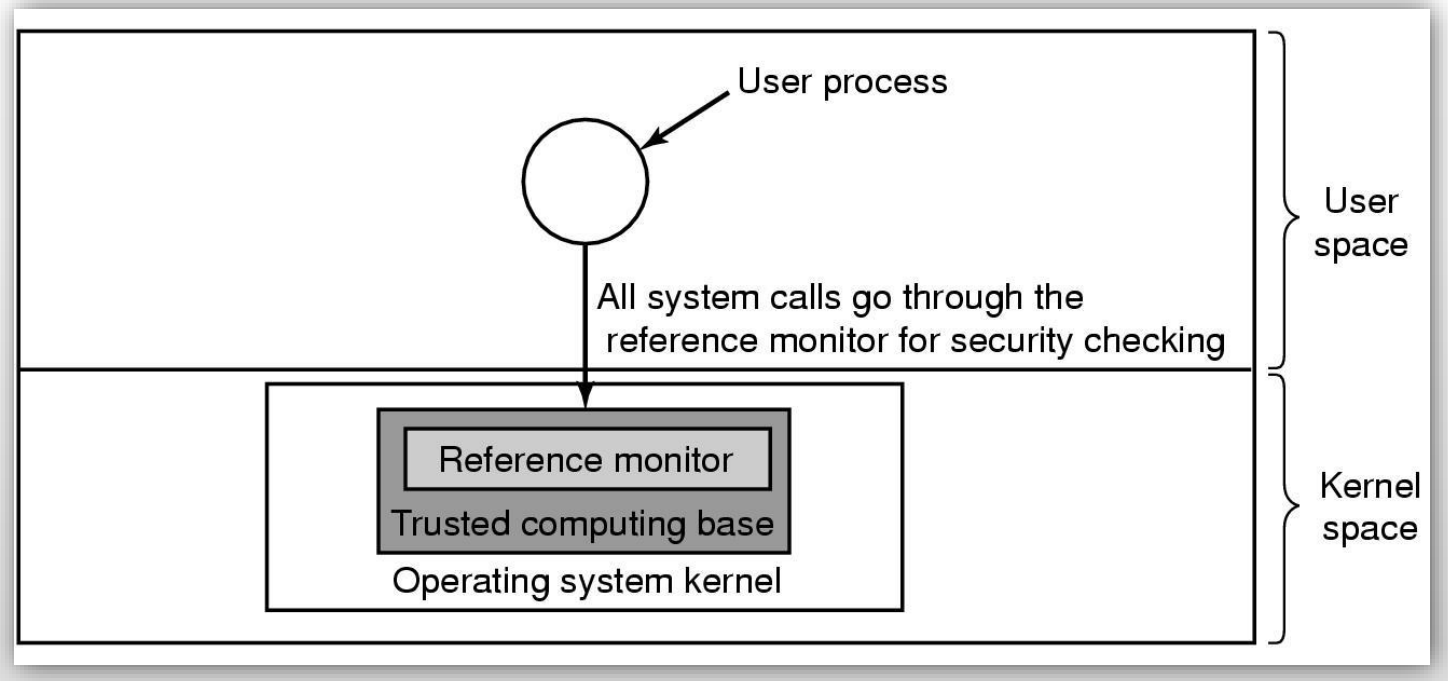
Sunucu	Nesne - Kaynak	Haklar - Yetenekler	f(nesne,haklar,kontrol)

Yetenek Listesi

- **Yetenek kopyalama**:
  - aynı nesne için yeni bir yetenek oluşturur.
- **Nesne kopyalama**:
  - yeni bir yeteneğe sahip yinelenen (*duplicate*) bir nesne oluşturur.
- **Yetenek kaldırma**:
  - yetenek listesinden bir öğeyi siler; nesne etkilenmez.
- **Nesneyi yok etme**:
  - bir nesne ve bir yeteneği kalıcı olarak siler.

Güvenilir Bilgi İşleme Tabanı

- Güvenlik kontrolü için bir referans gözetleyici.



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

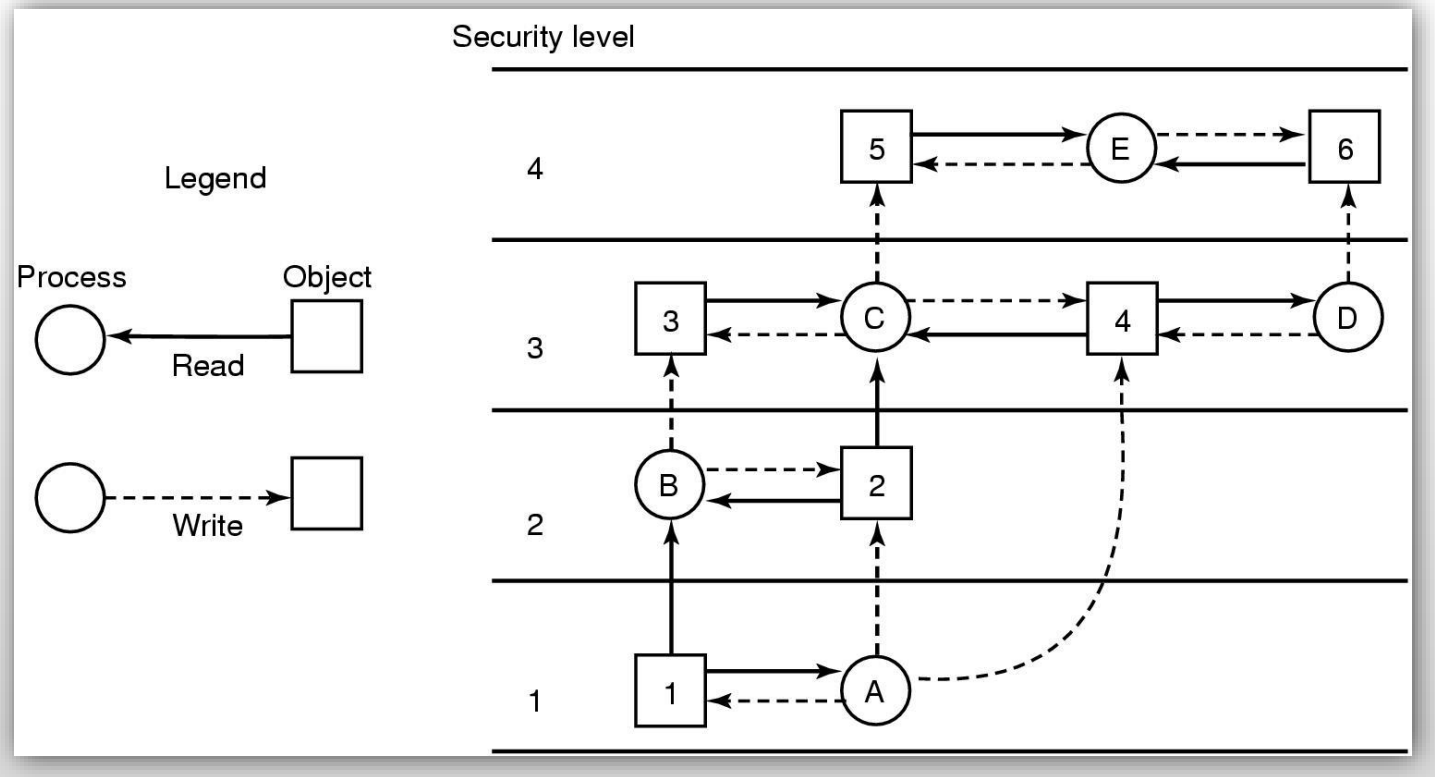
(b)

Bell-La Padula Modeli

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

Bell-La Padula Modeli

- Çok düzeyli güvenlik modeli.



Bell-La Padula Modeli

- Gizli bilgilerin güvenliğini sağlamak amacıyla geliştirildi.
- Gizliliğe odaklanır ve verilere yetkisiz erişime karşı koruma sağlar.
- Süreç ve nesnelerin düzeylerine göre erişim kontrolü tanımlar.
- Güvenliği sağlamak için *okuma yok* ve *yazma yok* ilkesini kullanır.

Biba Modeli

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

Biba Modeli

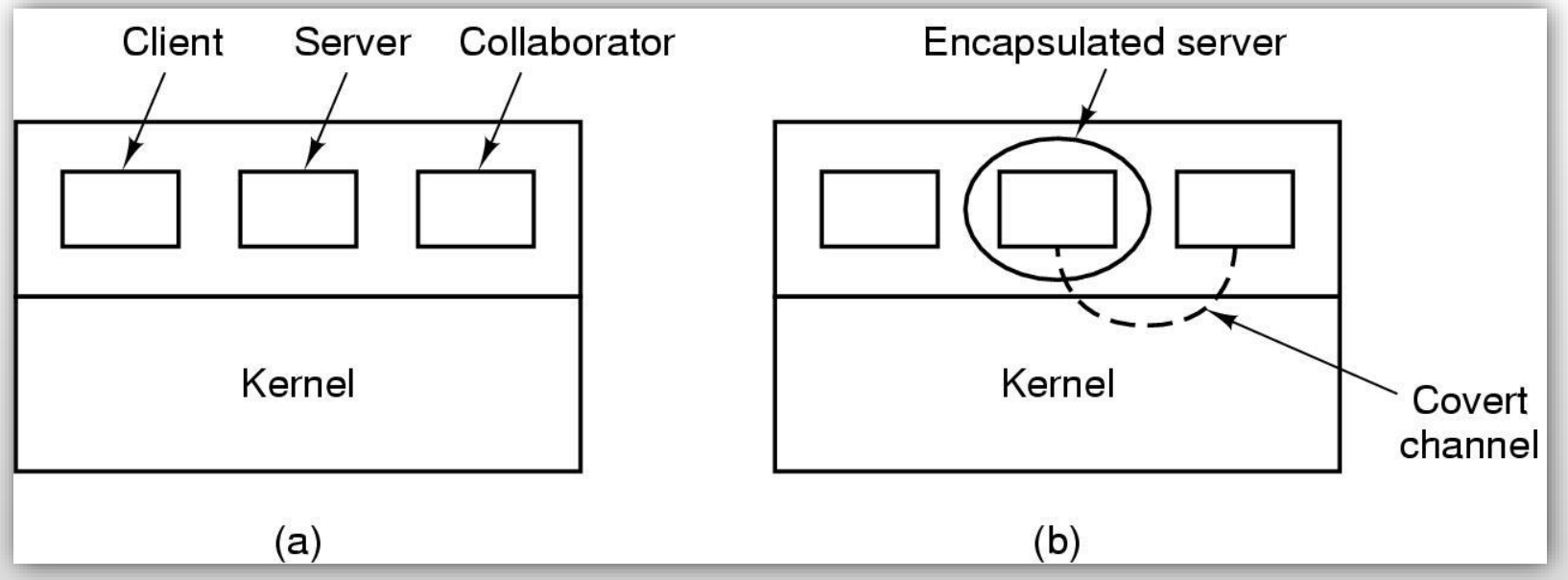
- Verileri yetkisiz değişikliklere karşı koruma sağlamak için geliştirildi.
- Bütünlüğe odaklanır ve veriler üzerinde yetkisiz değişiklikleri önler.
- Süreç ve nesnelerin bütünlük düzeylerine göre erişim kontrolü tanımlar.
- Güvenliği sağlamak için *okuma yok* ve *yazma yok* ilkesini kullanır.

Gizli Kanal (Covert Channel)

- Verilerin gizliliğini ve/veya bütünlüğünü tehlikeye atarak,
- Güvenlik mekanizmaları ve ilkelerini atlayarak,
- Süreçler arasında bilgi iletir.
- **Saklama gizli kanalı**:
  - Veriler, bilgilerin saklanmasındaki değişiklikler yoluyla iletilir.
- **Zamanlama gizli kanalı**:
  - Veriler, olayların zamanlamasındaki değişiklikler yoluyla iletilir.
- **Kaynak gizli kanalı**:
  - Veriler, sistem kaynaklarının kullanımındaki değişiklikler yoluyla iletilir.

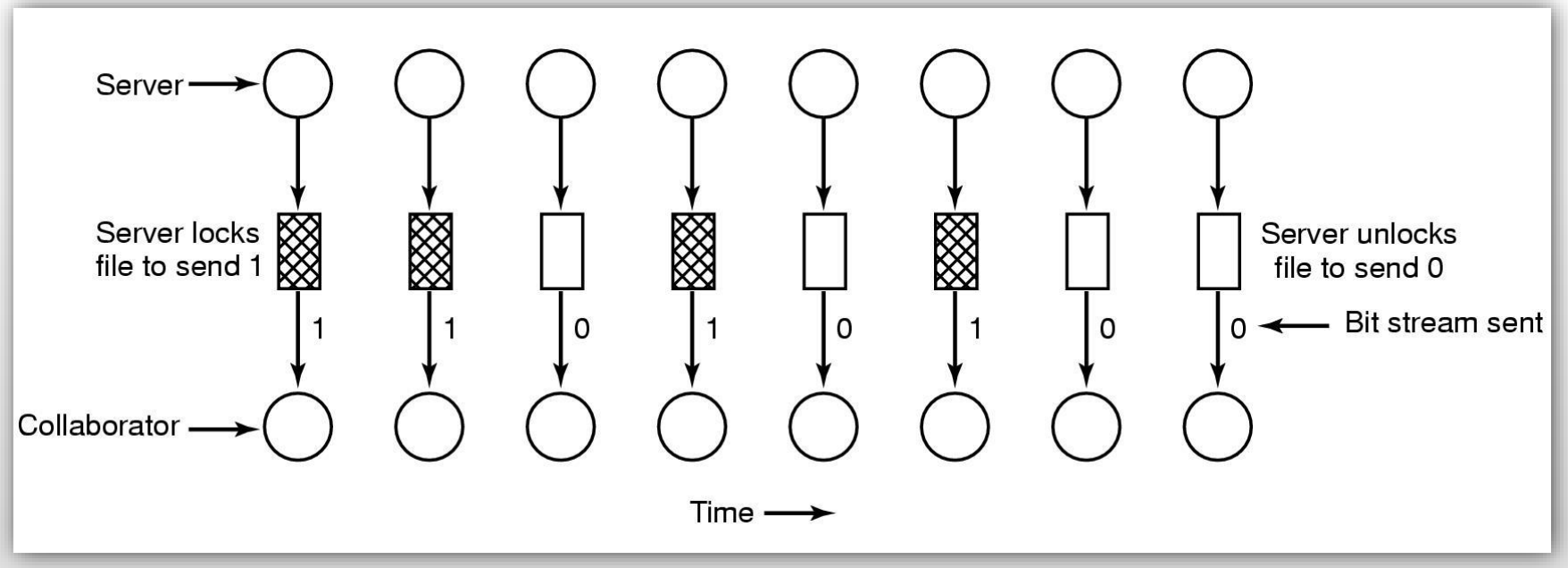
Gizli Kanallar

- (a) İstemci, sunucu ve işbirlikçi süreç.
- (b) Kapsüllenmiş sunucu, gizli kanal ile işbirlikçi sürece sızabilir.



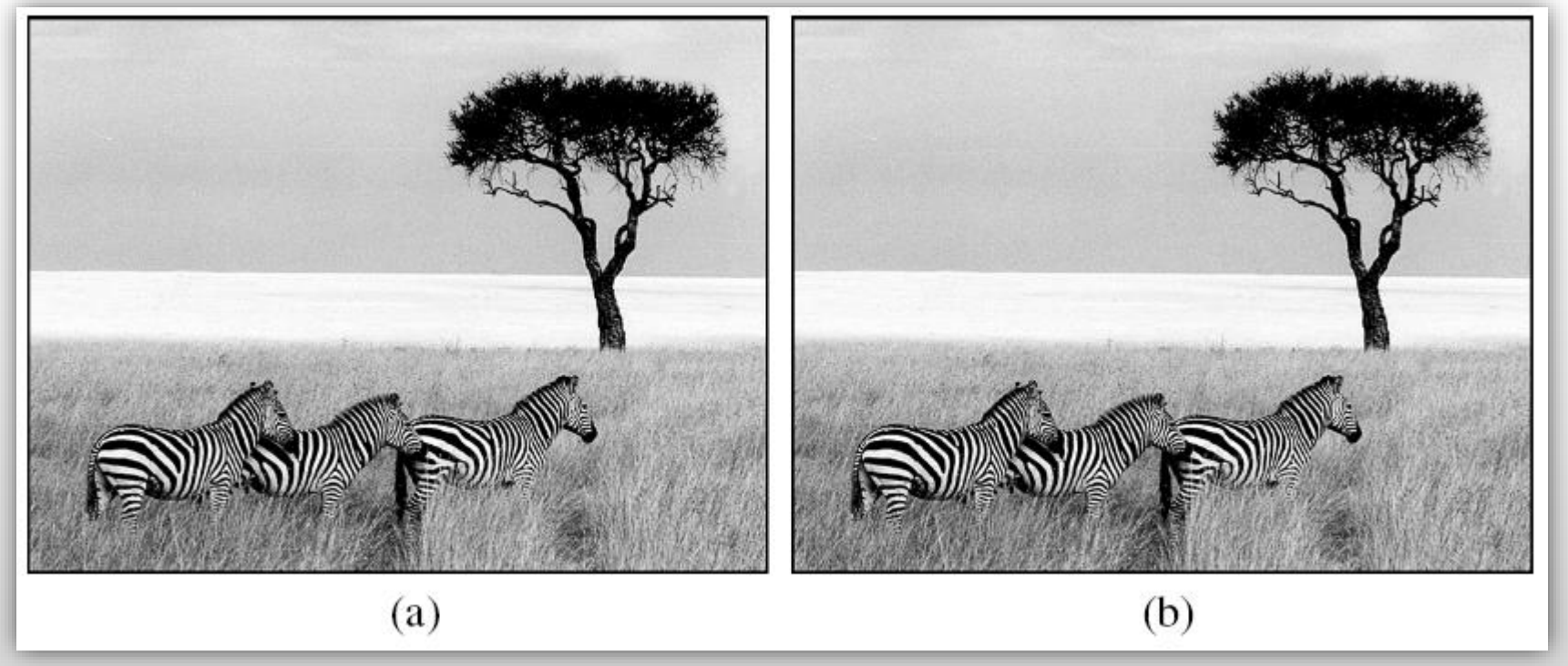
Gizli Kanallar

- Dosya kilitleme işlemi kullanan gizli bir kanal.



Gizli Kanallar

- (a) Üç zebra, bir ağaç.
- (b) Üç zebra, bir ağaç ve görünmeyen bir metin.



Kimlik Doğrulama (Authentication)

- Kullanıcı kimliğini doğrulamak için:
  - Kullanıcının bildiği bir şey. (*parola*)
  - Kullanıcının sahip olduğu bir şey. (*parmak izi, göz retina*)
  - Kullanıcının kim olduğunu belirten bir şey. (*kimlik kartı*)

- something the user *knows*.
- something the user *has*.
- something the user *is*.

Parola Kullanarak Kimlik Doğrulama

- (a) Başarılı bir oturum açma.
- (b) Ad girildikten sonra *geçersiz kullanıcı adı* ile başarısız oturum açma.
- (c) Ad ve parola girildikten sonra *yanlış şifre* ile başarısız oturum açma.

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

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
```

UNIX Parola Güvenliği

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

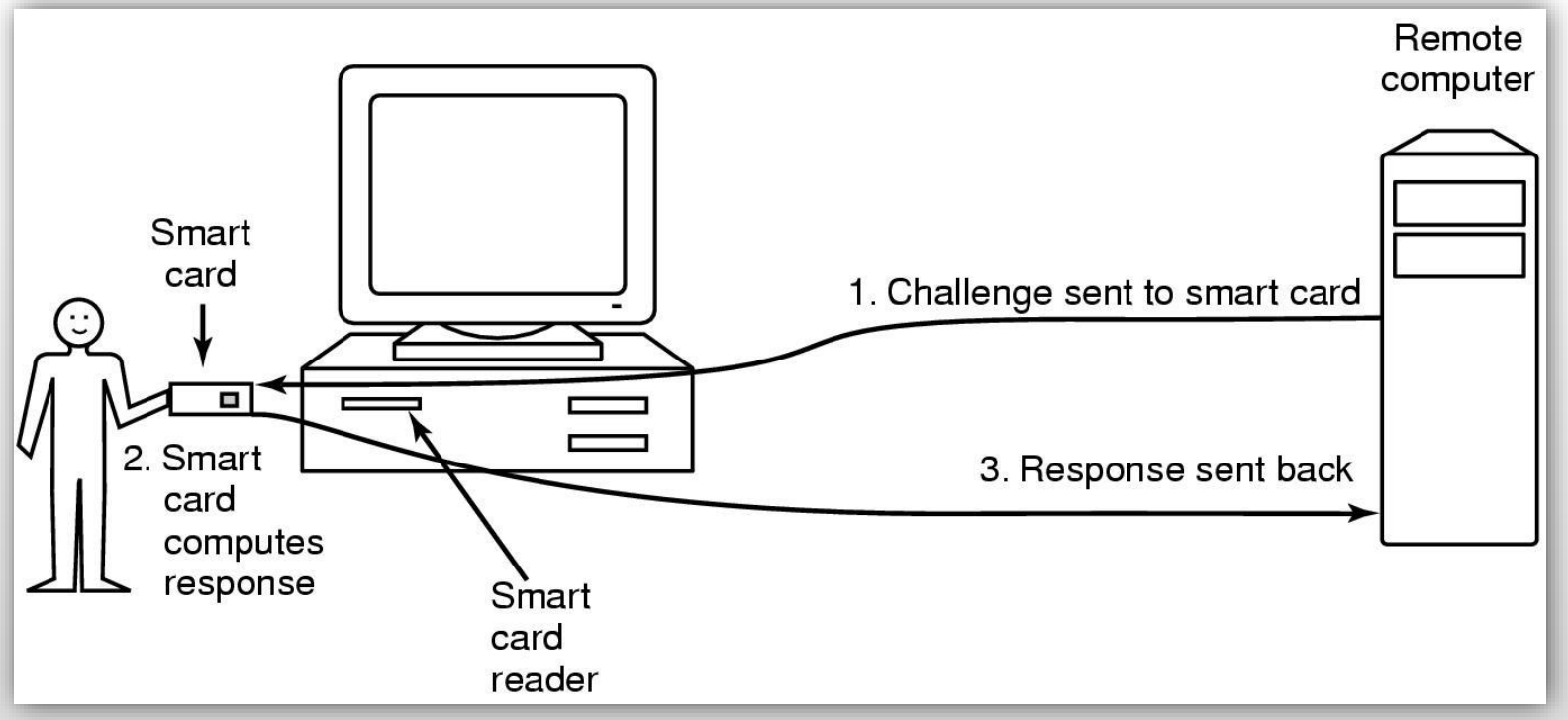
Bobbie, 4238, e(Dog, 4238)
Tony, 2918, e(6%%TaeFF, 2918)
Laura, 6902, e(Shakespeare, 6902)
Mark, 1694, e(XaB#Bwcz, 1694)
Deborah, 1092, e(LordByron,1092)

Sorgu-Yanıt Kimlik Doğrulaması

- Sorular, kullanıcının yazmasını gerektirmeyecek şekilde seçilmelidir.
- Örnekler:
  - Kız kardeşinin adı?
  - İlkokulunuz hangi sokaktaydı?
  - İlk evcil hayvanınız ne?

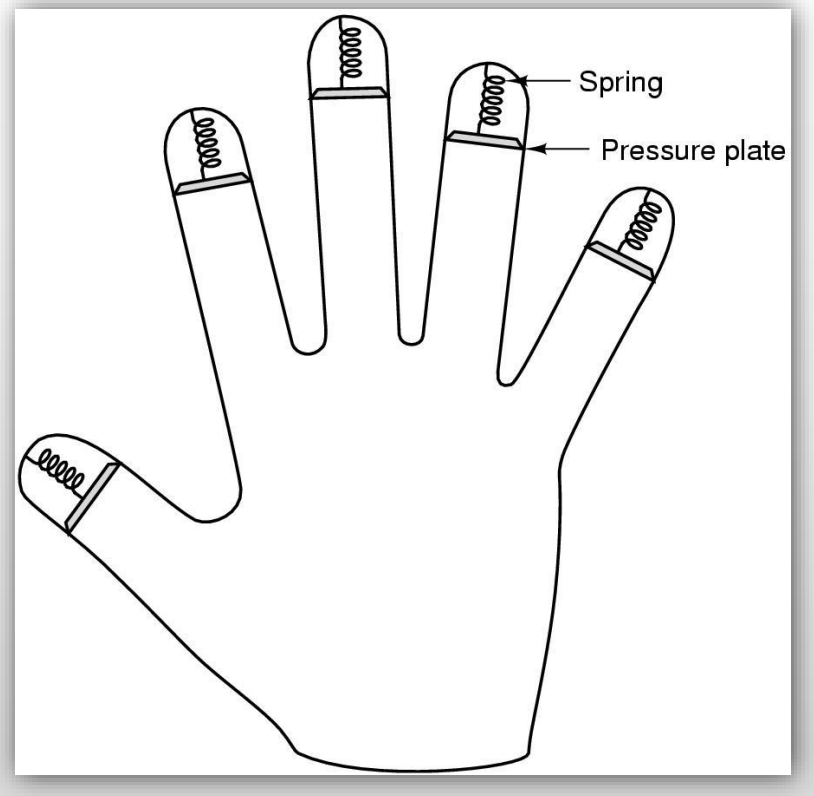
Fiziksel Nesne Kullanarak Kimlik Doğrulama

- Kimlik doğrulama için akıllı kart kullanımı.



Biyometri Kullanarak Kimlik Doğrulama

- Parmak uzunluğunu ölçmek için bir cihaz.



Tuzak Kapısı (Trap Doors)

- (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)

Giriş Sayfası Kandırma Saldırısı

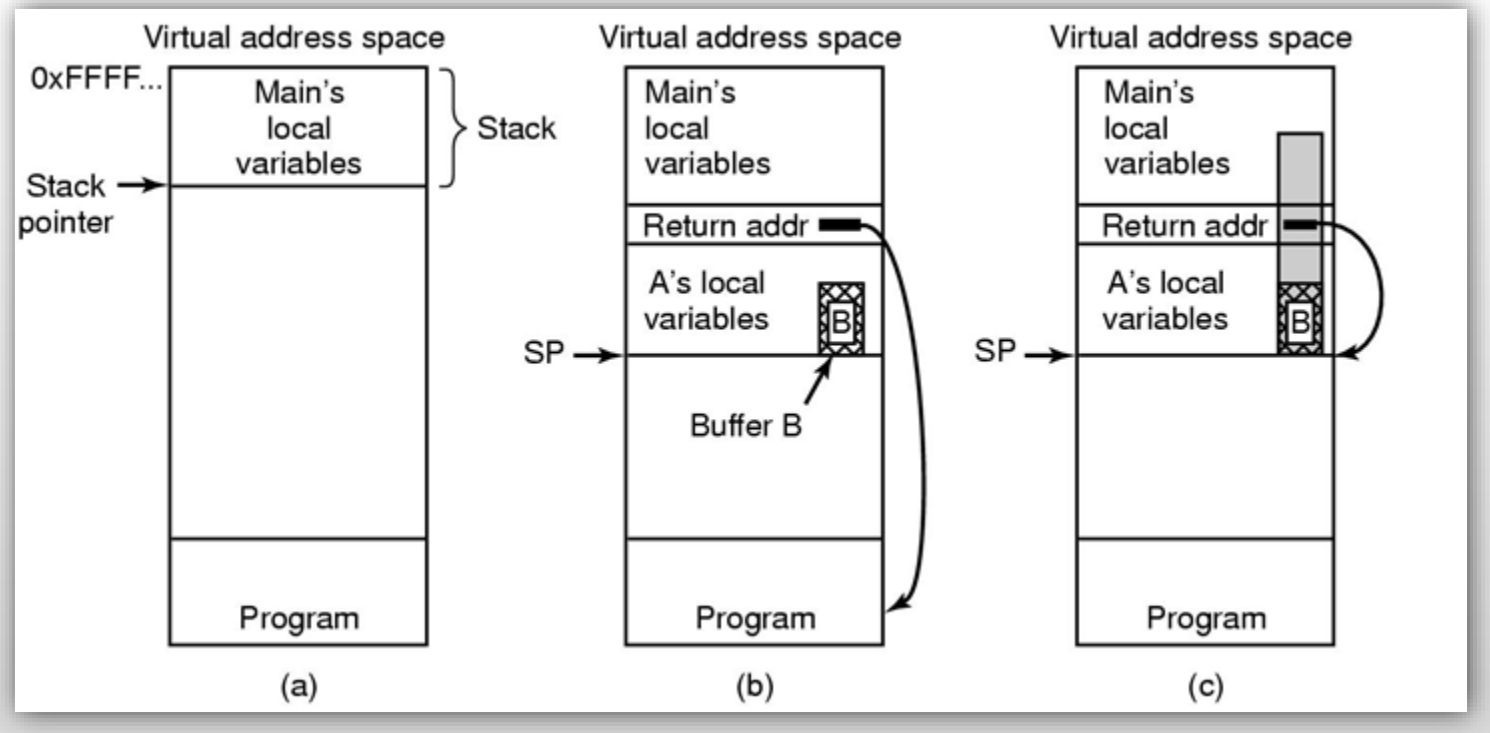
- *Login Spoofing.*
- (a) Doğru oturum açma ekranı. (b) Sahte oturum açma ekranı.

Kod Hatalarından Yararlanma

- Telnet bağlantılarını kabul eden makineleri bulmak için,
  - bağlantı noktası taraması (*scan port*) çalıştır.
- Kullanıcı adı, şifre kombinasyonları tahmin ederek giriş yapmayı dene.
- Girişten sonra, hatayı tetikleyen girdiyle (*input*) programı çalıştır.
- Hatalı program SETUID kökü ise, SETUID kök kabuğu (*root shell*) oluştur.
- CMDS (*Computer Misuse Detection System*) için,
  - *IP*:*port* dinleyen bir zombi programı başlat.
  - Zombi programının sistem başlangıcında çalışmasını sağla.

Ara Bellek Taşma Saldırıları

- (a) Normal durum. (b) *A* prosedürü çağrıldıktan sonra.
- (c) Gri renkle gösterilen tampon bellek (*buffer*) taşması.

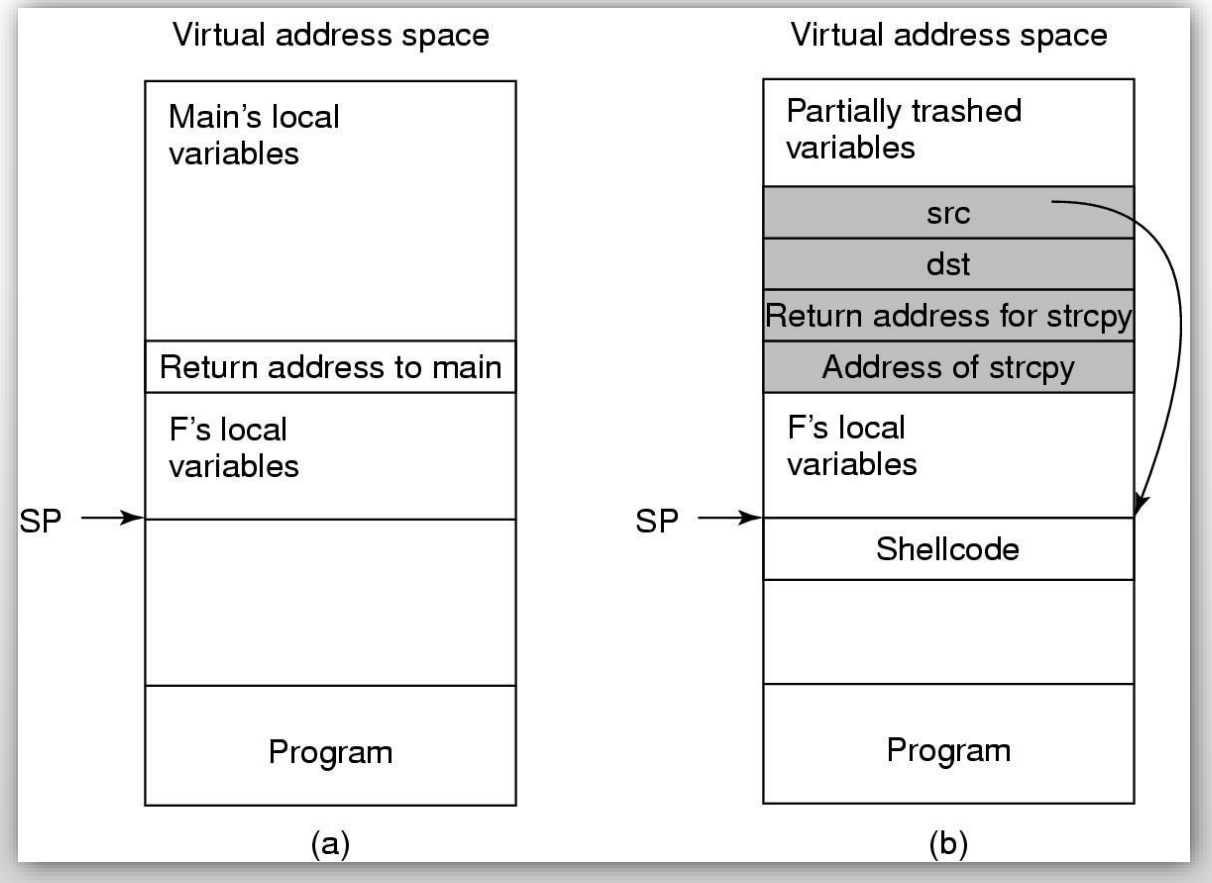


Tampon Taşma Saldırıları

```
#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;
      }
}
```

libc Saldırıları

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



Kod Enjeksiyon Saldırıları

- Kod enjeksiyon (*code injection*) 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 */
}
```

Kötü Amaçlı Yazılım (Malware)

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

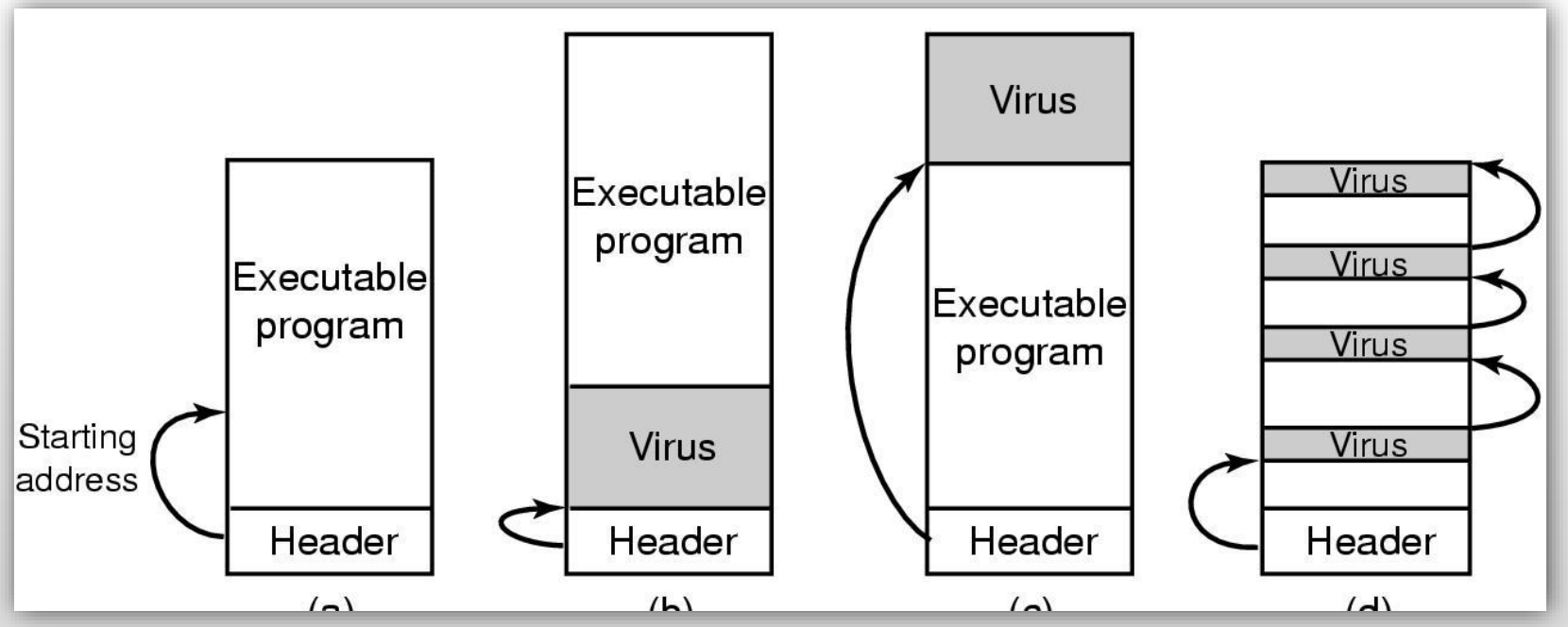
> Greetings from General Encryption
>
> To purchase a decryption key for your hard disk, please send $100 in small unmarked bills to Box 2154, Panama City, Panama.
> Thank you. We appreciate your business.

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*)

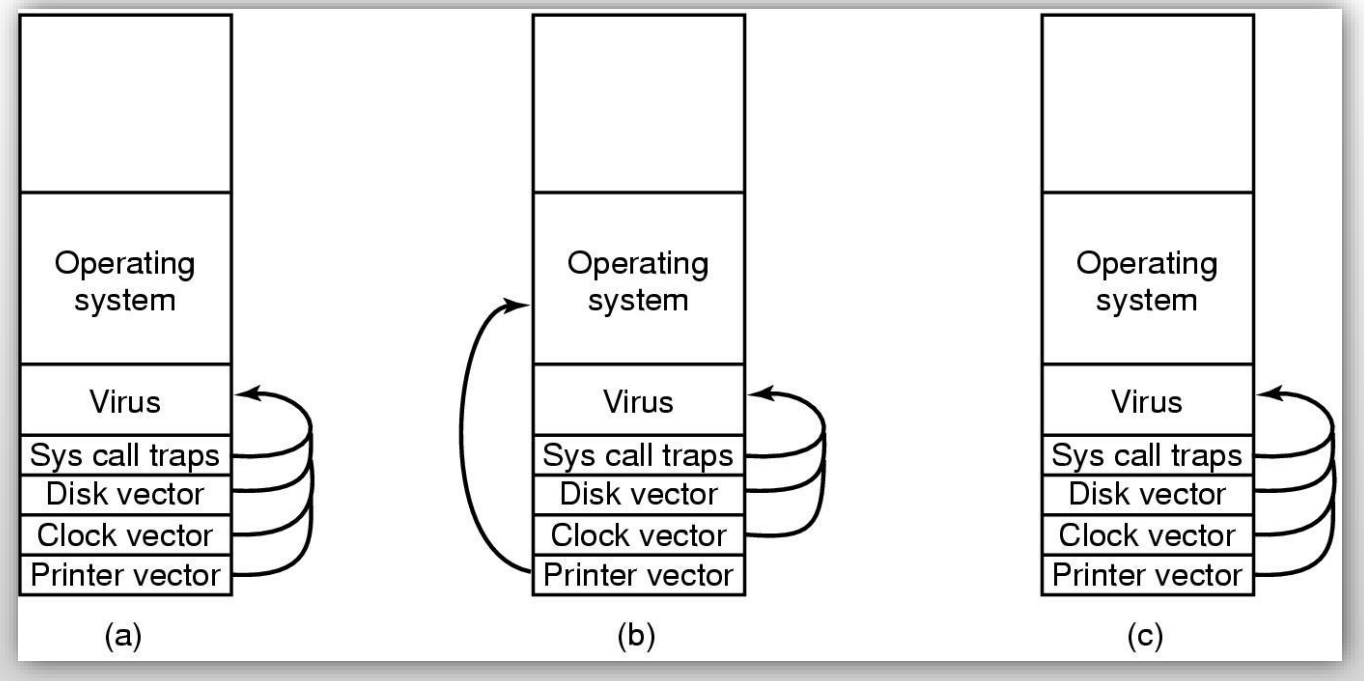
Parazitik Virüsler

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



Önyükleme Sektörü Virüsleri

- (a) Virüs, tüm kesme (*interrupt*) ve tuzak (*trap*) vektörlerini ele geçirmiş.
- (b) İşletim sistemi, yazıcı (*printer*) kesme vektörünü yeniden almış.
- (c) Virüs, yazıcı kesme vektörünü yeniden ele geçirmiş.



Casus Yazılım (Spyware)

- Bilgisayara gizlice yüklenir.
- Arka planda çalışır.
- Gizlenir, kurban (*victim*) tarafındana kolayca bulunamaz.
- Kullanıcı hakkında veri toplar.
- Toplanan bilgileri uzakta bir bilgisayara iletir.

Casus Yazılım Nasıl Yayılır

- Truva atı (*Trojan horse*) ile.
- İndirme (*download*),
  - Virüslü bir web sitesini ziyaret etme.
  - Web sayfaları bir *.exe* dosyası çalıştırmayı dener.
  - Şüphelenilmeyen bir kullanıcı virüslü bir araç çubuğu (*toolbar*) yükler.
  - Kötü amaçlı *activeX* denetimleri yüklenir.

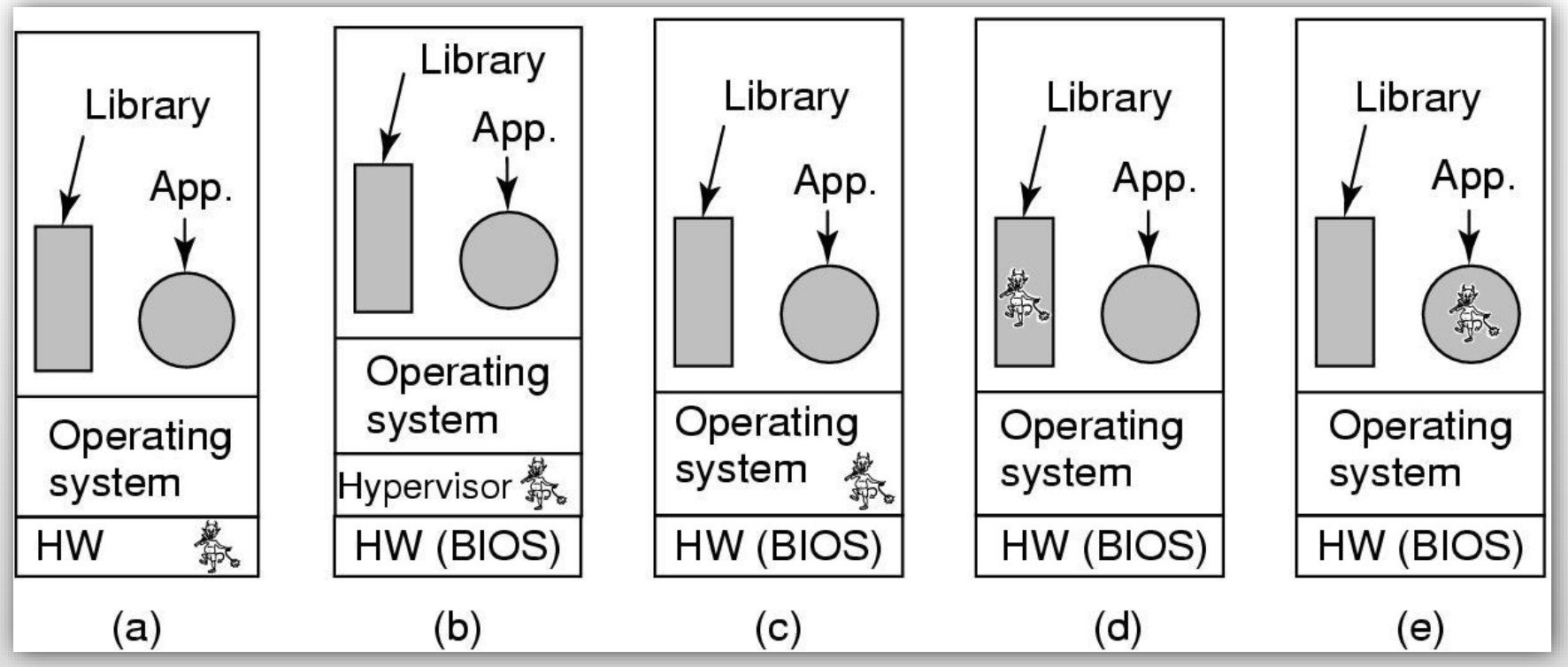
Casus Yazılım Gerçekleştirdiği Eylemler

- Tarayıcı ana sayfasını (*homepage*) değiştirme.
- Tarayıcının *yer imi (bookmark)* eklenmiş sayfalar listesini değiştirme.
- Tarayıcıya yeni araç çubukları (*toolbar*) ekleme.
- Varsayılan medya yürütücüsünü (*media player*) değiştirme.
- Varsayılan arama motorunu (*search engine*) değiştirme.
- Masaüstüne (*desktop*) yeni simgeler ekleme.
- Web sayfasındaki reklamları, casus yazılımın seçtikleriyle değiştirme.
- Reklamları standart Windows iletişim kutularına yerleştirme.
- Sürekli ve durdurulamaz bir *pop-up* reklam akışı oluşturma.

Kök Kullanıcı Takımı (Rootkit) Türleri

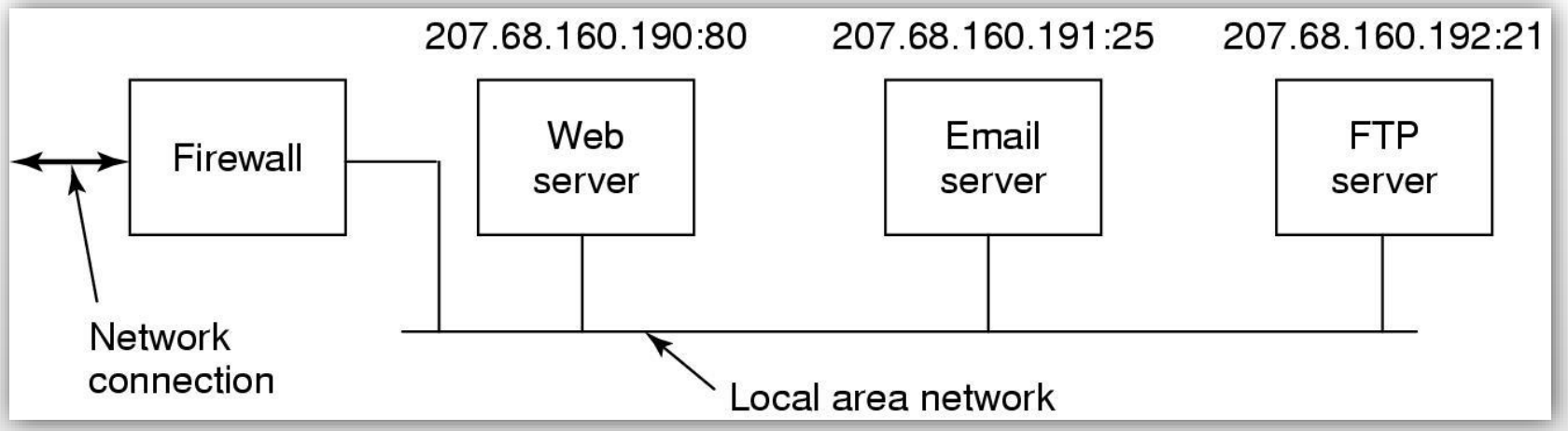
- Bellenim (*firmware*).
- Hipervizör (*hypervisor*).
- Çekirdek (*kernel*).
- Kütüphane (*library*).
- Uygulama (*application*).

Kök Kullanıcı Takımının Saklanabileceği Yerler



Güvenlik Duvarı (Firewall)

- Üç bilgisayarlı bir yerel ağı *koruyan* donanım güvenlik duvarı.

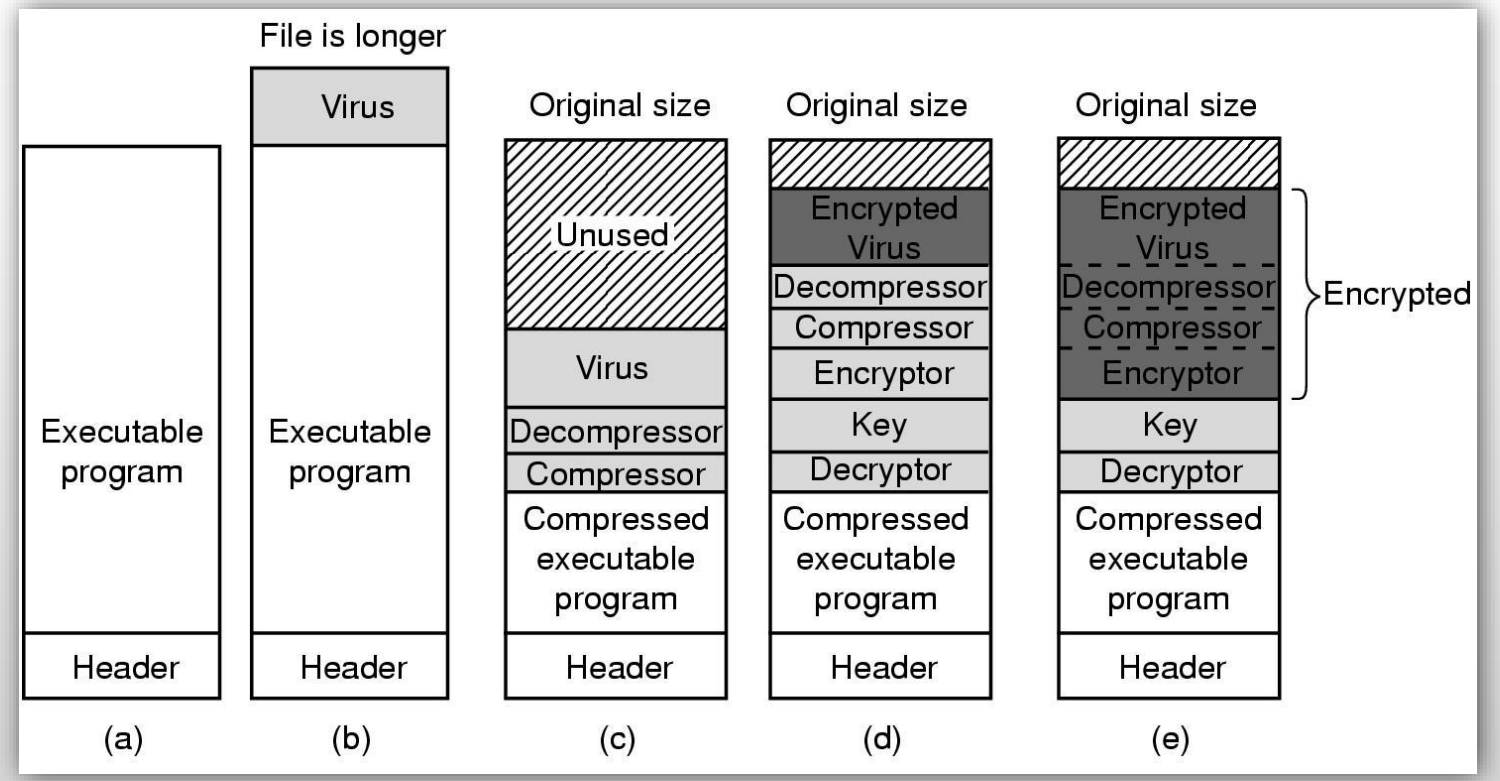


Antivirüs ve Anti-Antivirüs Teknikleri

- Virüs tarayıcıları (*virus scanner*).
- Bütünlük denetleyicileri (*integrity checker*).
- Davranışsal denetleyiciler (*behavioral checker*).
- Virüsten kaçınma (*virus avoidance*).

Virüs Tarayıcıları

- (a) Yürütülebilir program. (b) Virüslü program. (c) Sıkıştırılmış virüslü program. (d) Şifrelenmiş virüs. (e) Şifrelenmiş ve sıkıştırılmış virüs.



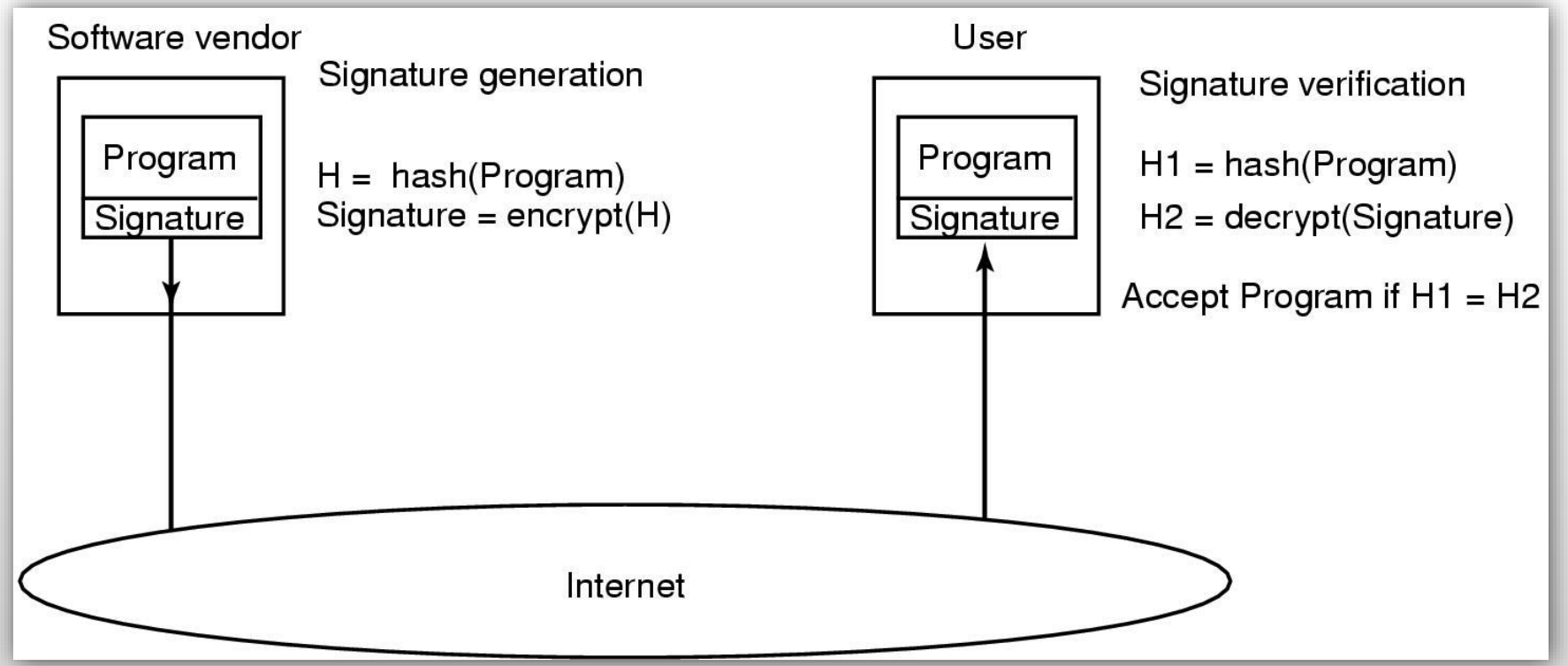
Virüs Tarayıcıları

- Çok şekilli (polimorphic) virüs örnekleri.

```
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
   (a)               (b)               (c)               (d)               (e)
```

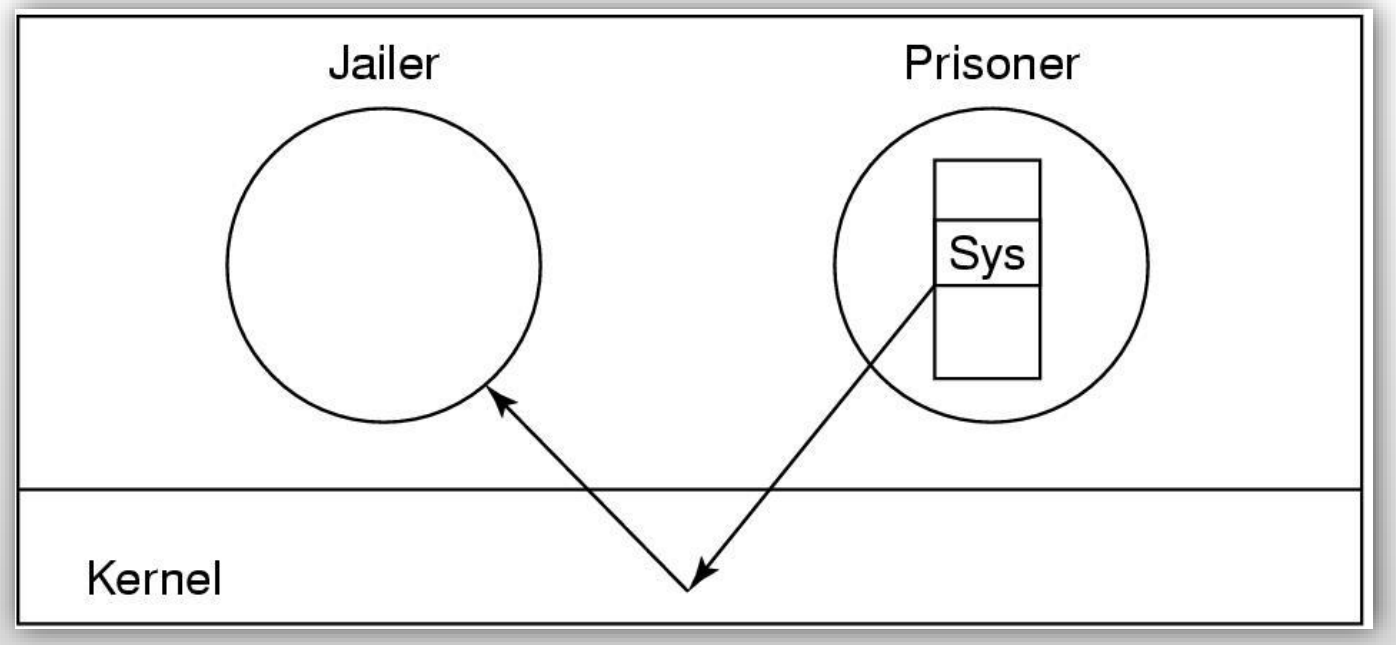
Kod İmzalama

- Dijital imza'ya benzer şekilde, kod okunarak bir *hash* değeri üretilir.
- Kullanıcı tarafında üretilen ve alınan *hash* değerleri karşılaştırılır.



Hapse Atmak (Jailing)

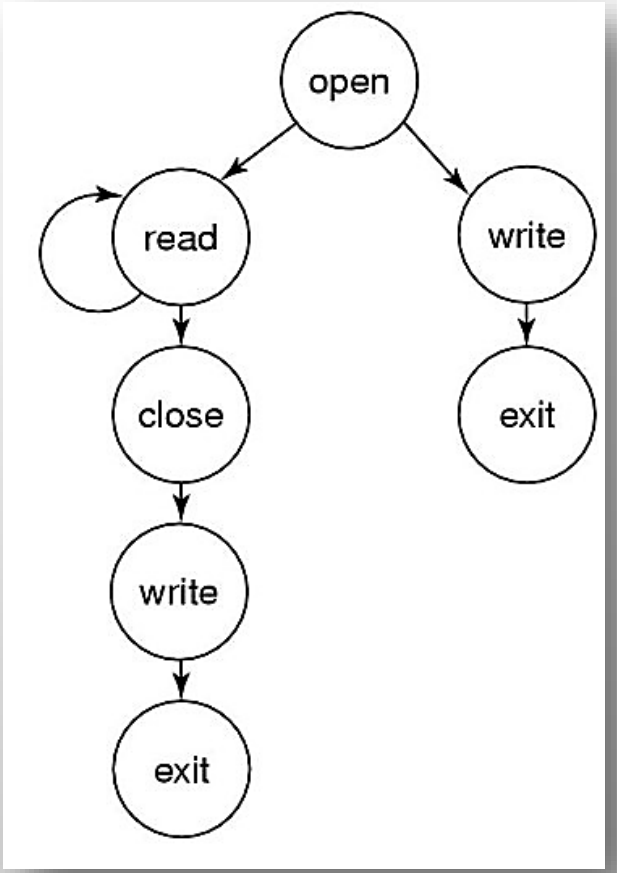
- Mahkum (*prisoner*) programın yaptığı tüm sistem çağrıları (*system call*), gardiyan (*jailer*) program tarafından kontrol edilir.



Model Tabanlı Saldırı Tespiti

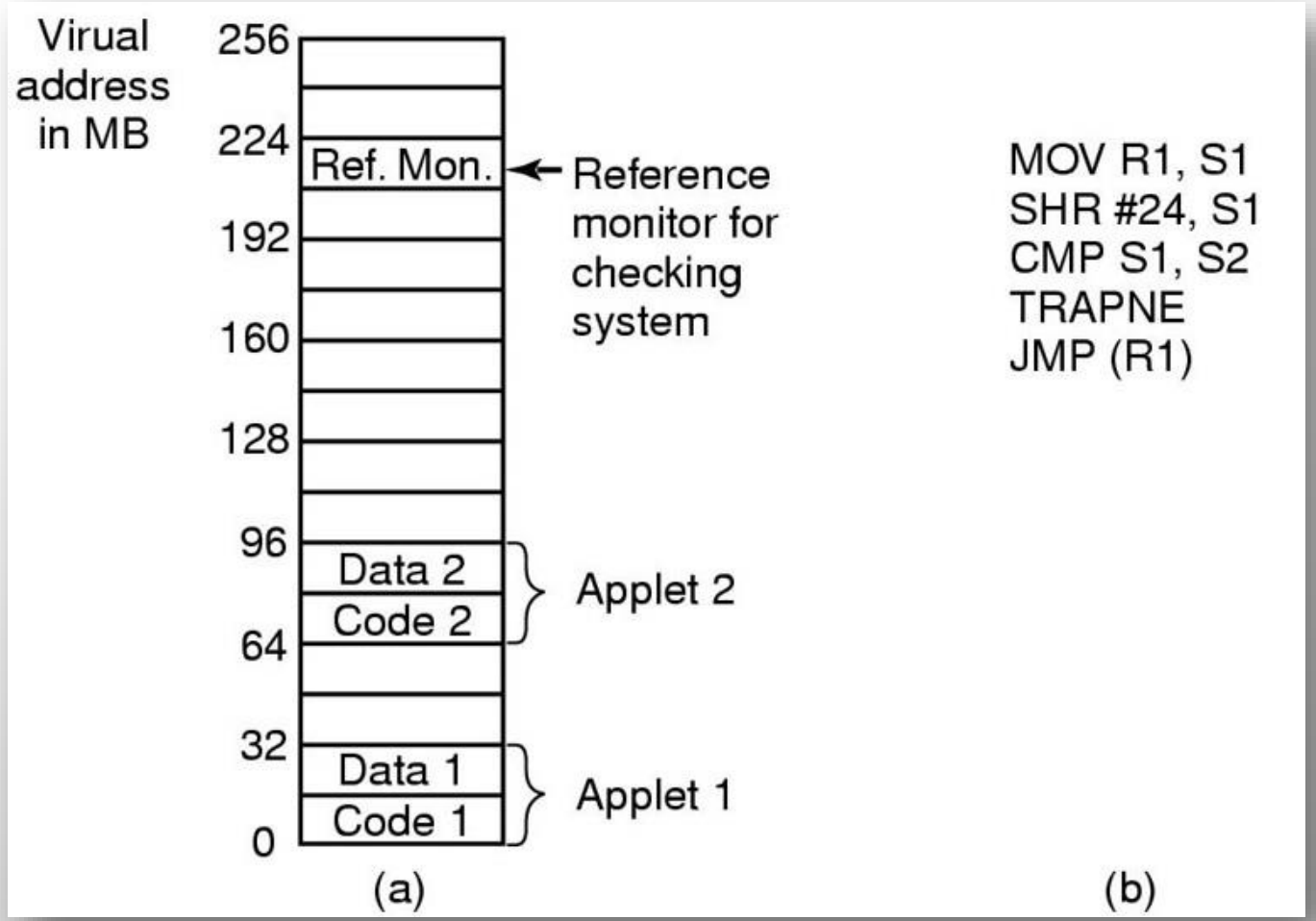
- Bir program ve yaptığı sistem çağrıları (*system call*) çizgesi.

```
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;
    }
  }
}
```



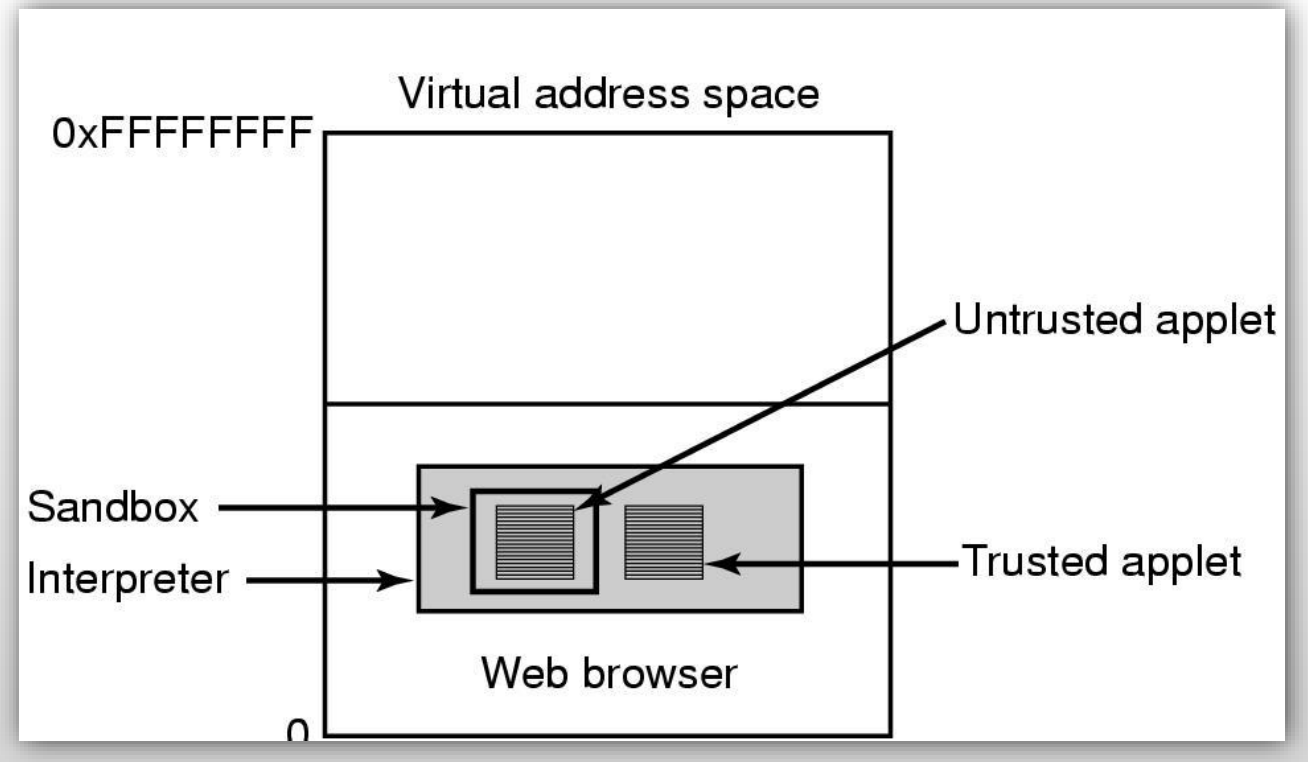
Korumalı Alan (Sandboxing)

- (a) 16 MB alanlara bölünmüş sanal bellek.
- (b) Bir komutun geçerliliğini kontrol etme.
- Programın kendi kendini değiştirememesi için, kod ve veri *ayrı* tutulur.



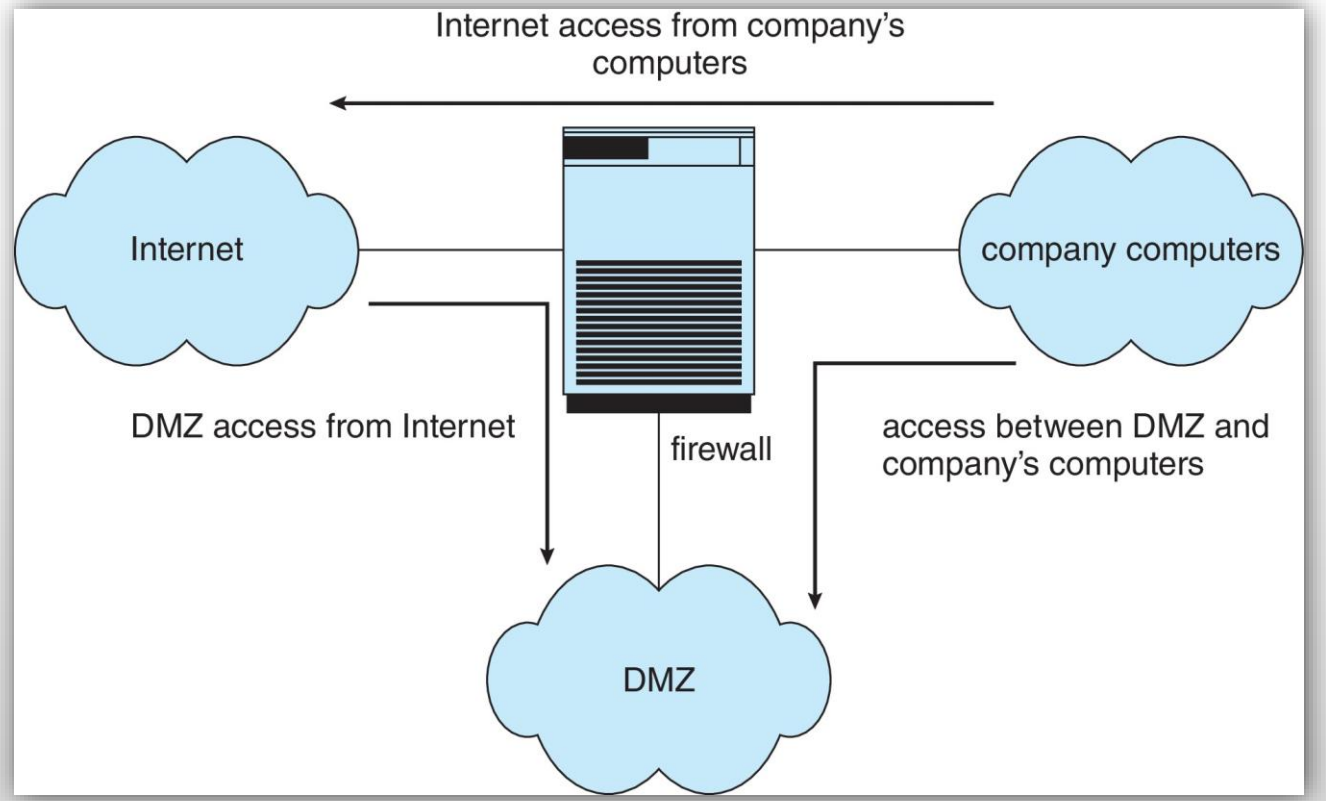
Yorumlamalı Dil (Interpreter)

- Donanıma doğrudan erişime izin verilmez.
- *Applet* bir Web tarayıcısı tarafından yorumlanabilir.



Güvenlik Duvarı (Firewall)

- İnternet üzerinden gelen verileri filtreleyip inceleyen *yazılım veya donanım*.



Java Güvenlik

- *JVM bayt kodu doğrulayıcı*,
  - uygulamanın kurallara uyup uymadığını kontrol eder.
- Uygulama, işaretçi (*pointer*) oluşturmaya çalışıyor mu?
- Gizli (*private*) sınıf üyelerine erişim kısıtlamalarını ihlal ediyor mu?
- Bir tür değişkeni başka bir tür olarak kullanmaya çalışıyor mu?
- Yığın taşmaları oluşturuyor mu? (*stack overflows, underflows*)

SON