Bölüm 9: Güvenlik

İşletim Sistemleri

Güvenlik Hedefleri Ve Tehditler

- .

Goal	Threat
Data confidentiality	Exposure of data
Data integrity	Tampering with data
System availability	Denial of service
Exclusion of outsiders	System takeover by viruses

İzinsiz Kullanıcı

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

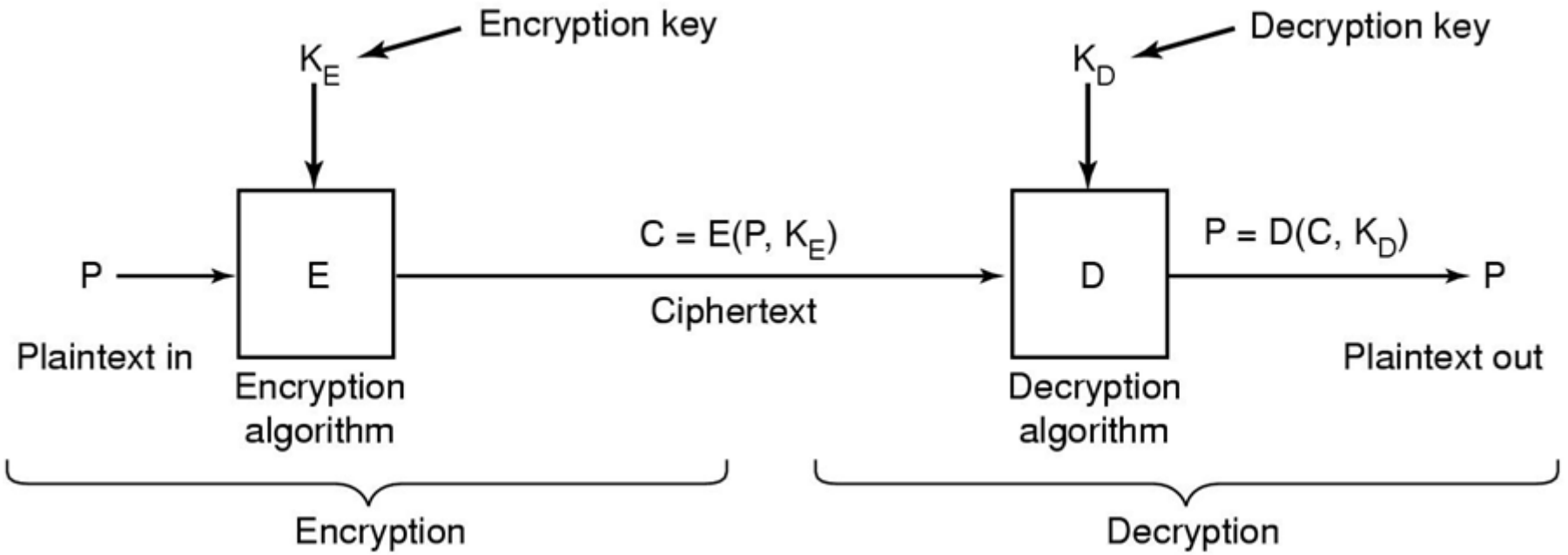
Kazayla Veri Kaybı

- 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.

Kriptografinin Temelleri

- Düz metin ve şifreli metin arasındaki ilişki.



Gizli Anahtarlı Kriptografi (secret key)

- Monoalfabetik ikame:

- Plaintext: ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Ciphertext: QWERTYUIOPASDFGHJKLZXCVBNM

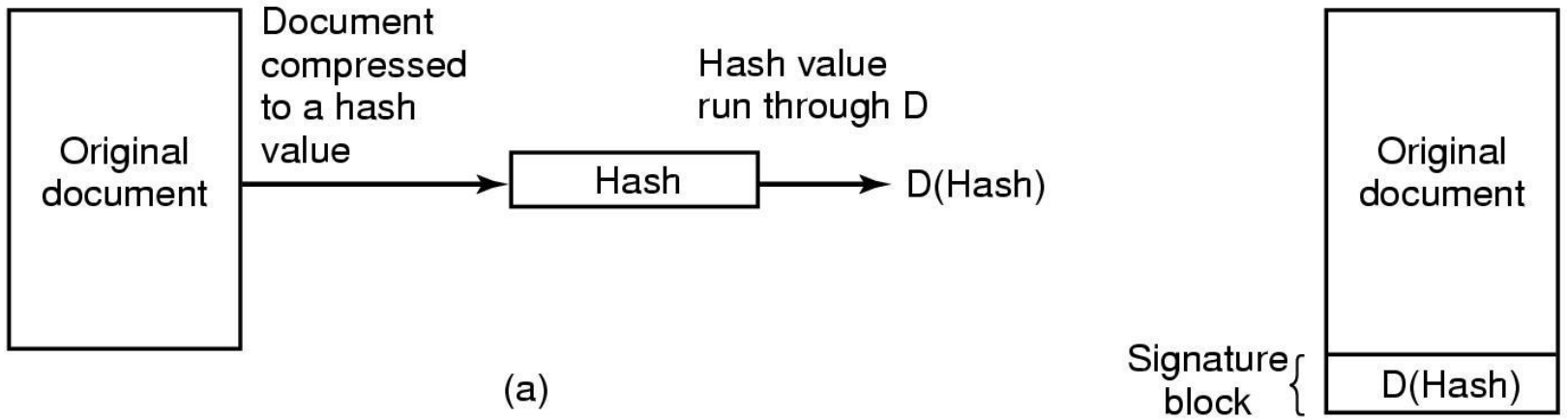
Açık Anahtarlı Kriptografi

- 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.

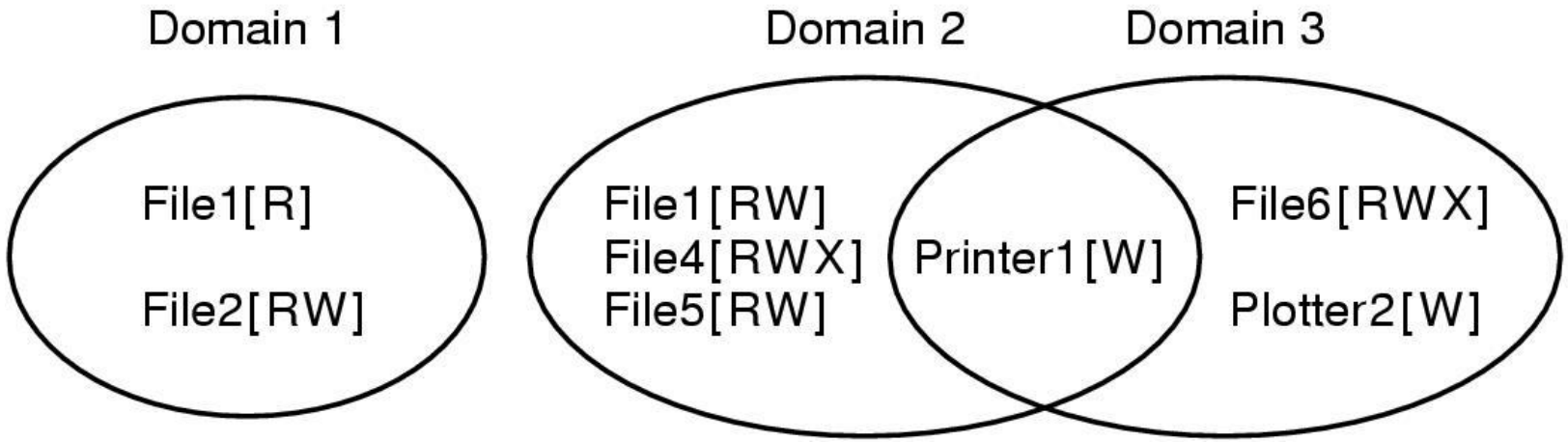
Dijital İmzalar

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



Koruma Etki Alanları

- Üç koruma alanı.



Koruma Etki Alanları

- Bir 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

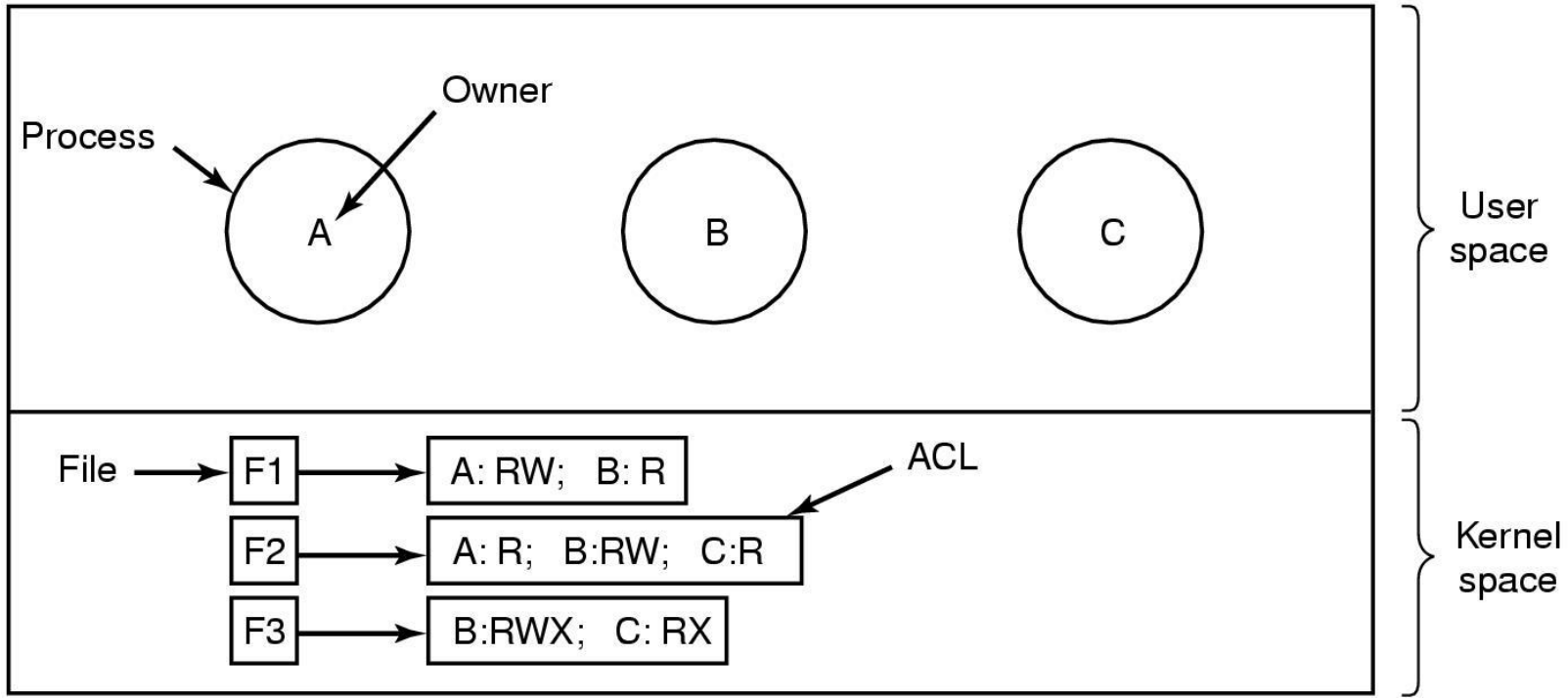
Koruma Etki Alanları

- Etki alanlarını nesne olarak içeren bir koruma matrisi.

	Object										
	File1	File2	File3	File4	File5	File6	Printer1	Plotter2	Domain1	Domain2	Domain3
Domain 1	Read	Read Write								Enter	
2			Read	Read Write Execute	Read Write		Write				
3						Read Write Execute	Write	Write			

Erişim Kontrol Listeleri

- Dosya erişimini yönetmek için erişim kontrol listelerinin kullanımı.



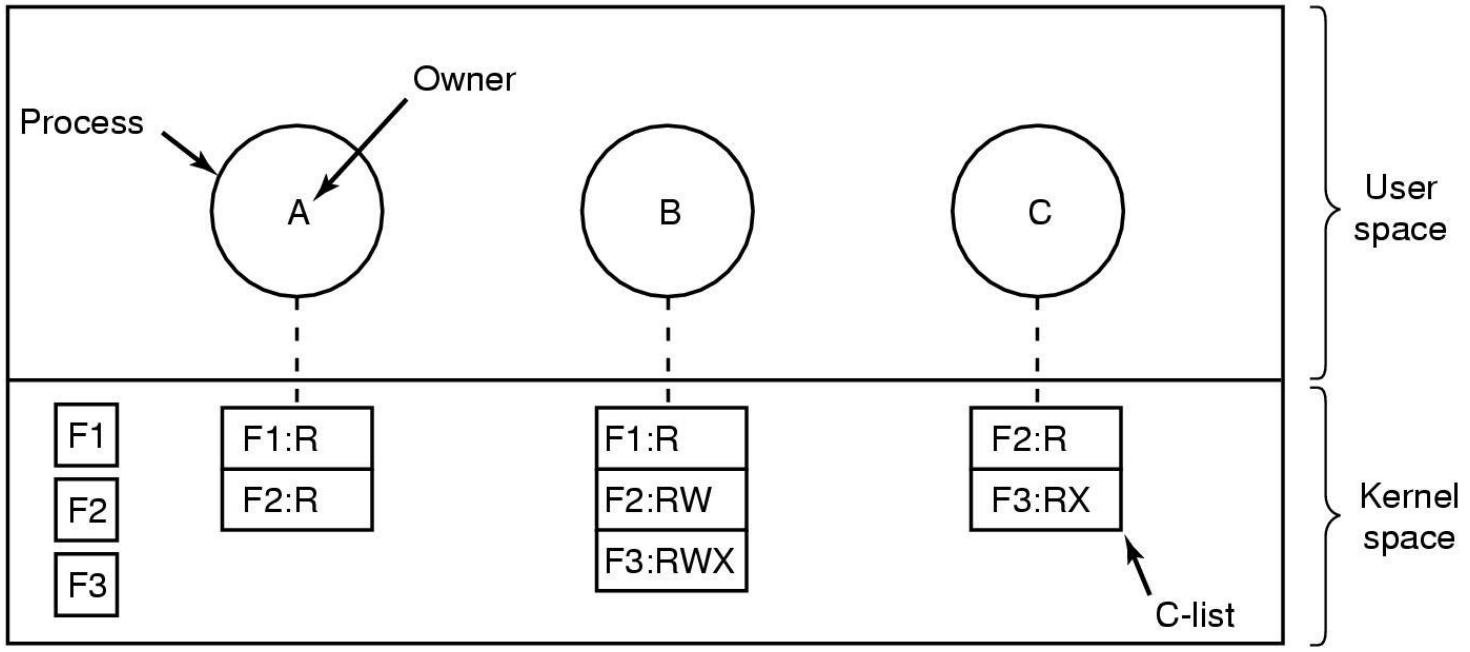
Erişim Kontrol Listeleri

- İki erişim kontrol listesi.

File	Access control list
Password	tana, sysadm: RW
Pigeon_data	bill, pigfan: RW; tana, pigfan: RW; ...

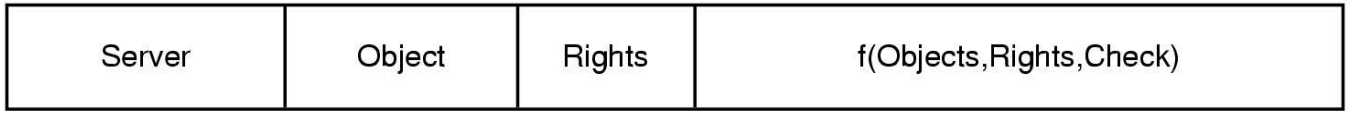
Yetenekler

- her sürecin bir yetenek listesi vardır.



Yetenekler

- Kriptografik olarak korunan bir yetenek.



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.

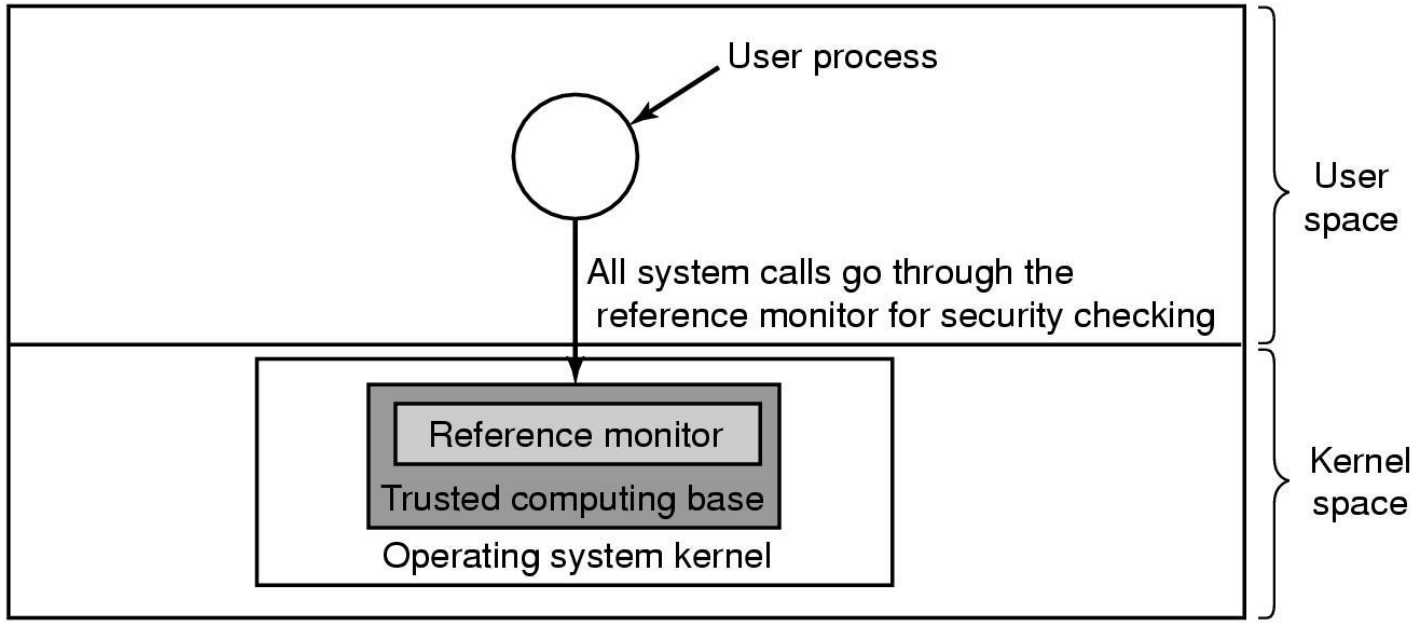
Güvenilir Sistemler

- Virüs, solucan vb. raporları dikkate alın.

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

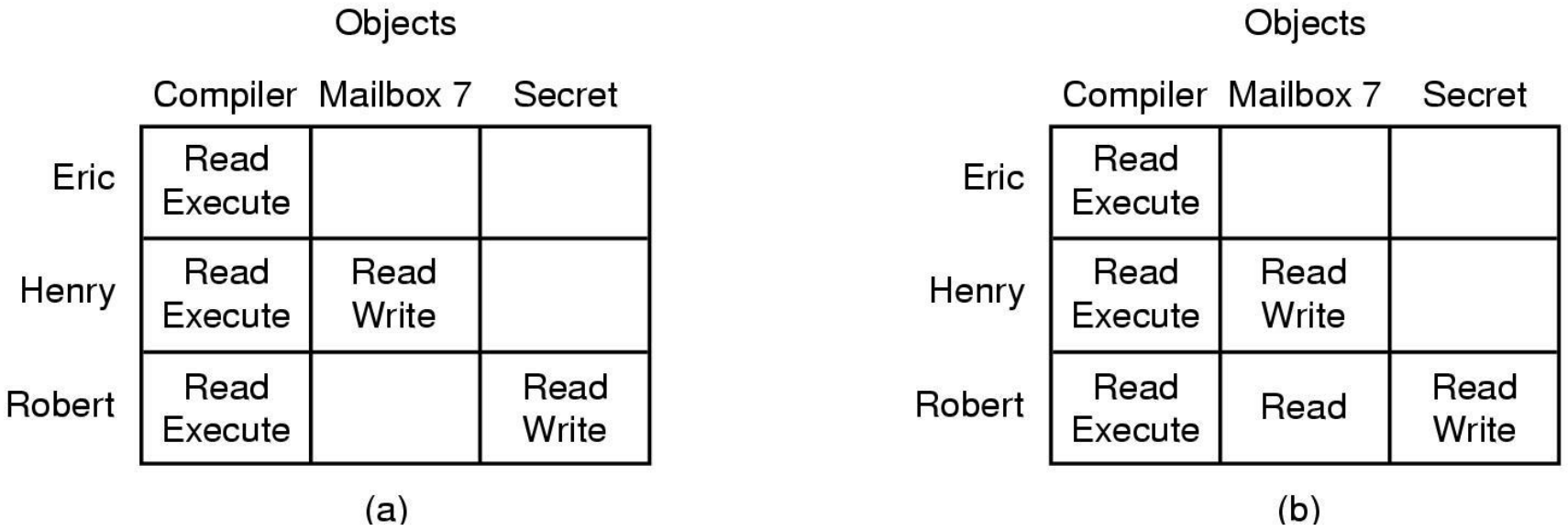
Güvenilir Bilgi İşlem Tabanı

- Bir referans gözleyici.



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)

SON