MUH441 Bilişimde Güvenlik – 1

Prof. Dr. Hasan Hüseyin BALIK

(4. Hafta)

İçerik

- 2.Bilgisayar Güvenliği Teknolojisi ve İlkeleri
  - 2.1 Şifreleme Araçları
  - 2.2.Kullanıcı doğrulama
  - 2.3 Giriş/Erişim Kontrolu
  - 2.4 Veritabanı ve Veri Merkezi Güvenliği
  - 2.5 Kötü amaçlı yazılımlar
  - 2.6 Hizmet Reddi Saldırıları
  - 2.7 İzinsiz giriş tespiti
  - 2.8 Güvenlik Duvarları ve Saldırı Önleme Sistemleri

2.3.Giriş/Erişim Kontrolu

2.3.İçerik

- Giriş/Erişim Kontrol İlkeleri
- Özneler, Nesneler ve Erişim Hakları
- Isteğe bağlı erişim kontrolü
- Örnek: UNIX Dosya Erişim Kontrolü
- Rol Tabanlı Erişim Kontrolü
- Özniteliğe Dayalı Erişim Kontrolü
- Kimlik, Kimlik Bilgileri ve Erişim Yönetimi
- Güven Çerçeveleri

Erişim Kontrolü Tanımları1/2

NISTIR 7298 (*Temel Bilgi Güvenliği Terimleri Sözlüğü*, Mayıs 2013) erişim kontrolünü şu şekilde tanımlar:

"belirli talepleri kabul etme veya reddetme süreci: (1) bilgi ve ilgili bilgi işleme hizmetlerini elde etmek ve kullanmak; ve (2) belirli fiziksel tesislere girmek"

Erişim Kontrolü Tanımları2/2

RFC 4949 (*İnternet Güvenliği Sözlüğü*) erişim kontrolünü şu şekilde tanımlar:

"Sistem kaynaklarının kullanımının bir güvenlik politikasına göre düzenlendiği ve bu politikaya göre yalnızca yetkili kuruluşlar (kullanıcılar, programlar, süreçler veya diğer sistemler) tarafından izin verildiği bir süreç"

Temel Güvenlik Gereksinimleri	
1	Bilgi sistemi erişimini yetkili kullanıcılar, yetkili kullanıcılar adına hareket eden süreçler veya cihazlar (diğer bilgi sistemleri dahil) ile sınırlandırın.
2	Yetkili kullanıcıların yürütmesine izin verilen işlem türleri ve işlevlerle bilgi sistemi erişimini sınırlandırın.

Türetilmiş Güvenlik Gereksinimleri	
3	Onaylanmış yetkilendirmelere göre CUI akışını kontrol edin.
4	Gizli anlaşma olmadan kötü niyetli faaliyet riskini azaltmak için bireylerin görevlerini ayırın.
5	Belirli güvenlik işlevleri ve ayrıcalıklı hesaplar dahil olmak üzere en az ayrıcalık ilkesini kullanın.
6	Güvenlikle ilgili olmayan işlevlere erişirken ayrıcalıklı olmayan hesapları veya rolleri kullanın.
7	Ayrıcalıklı olmayan kullanıcıların ayrıcalıklı işlevleri yürütmesini önleyin ve bu tür işlevlerin yürütülmesini denetleyin.
8	Başarısız oturum açma girişimlerini sınırlayın.
9	Geçerli CUI kurallarıyla tutarlı gizlilik ve güvenlik bildirimleri sağlayın.
10	Hareketsizlik süresinden sonra verilere erişimi ve verilerin görüntülenmesini önlemek için desen gizleme ekranlarıyla oturum kilidini kullanın.
11	Tanımlanmış bir koşuldan sonra bir kullanıcı oturumunu (otomatik olarak) sonlandırın.
12	Uzaktan erişim oturumlarını izleyin ve kontrol edin.
13	Uzaktan erişim oturumlarının gizliliğini korumak için kriptografik mekanizmalar kullanın.
14	Yönetilen erişim kontrol noktaları aracılığıyla uzaktan erişimi yönlendirin.
15	Ayrıcalıklı komutların uzaktan yürütülmesine ve güvenlikle ilgili bilgilere uzaktan erişime izin verin.
16	Bu tür bağlantılara izin vermeden önce kablosuz erişimi yetkilendirin.
17	Kimlik doğrulama ve şifreleme kullanarak kablosuz erişimi koruyun.
18	Mobil cihazların bağlantısını kontrol edin.
19	Mobil cihazlarda CUI'yi şifreleyin.
20	Harici bilgi sistemlerine bağlantıları ve bunların kullanımını doğrulayın ve kontrol edin/sınırlayın.
21	Harici bilgi sistemlerinde kurumsal taşınabilir depolama cihazlarının kullanımını sınırlayın.
22	Kamuya açık bilgi sistemlerinde yayınlanan veya işlenen CUI'yi kontrol edin.

Erişim Kontrolü Güvenlik Gereksinimleri (SP 800-171)

Erişim Kontrol İlkeleri

- Geniş anlamda, bilgisayar güvenliğinin tamamı erişim kontrolü ile ilgilidir.

- RFC 4949, bilgisayar güvenliğini şu şekilde tanımlar:

"Bir bilgisayar sisteminde güvenlik hizmetlerini, özellikle erişim kontrol hizmetini sağlayanları uygulayan ve sağlayan önlemler"

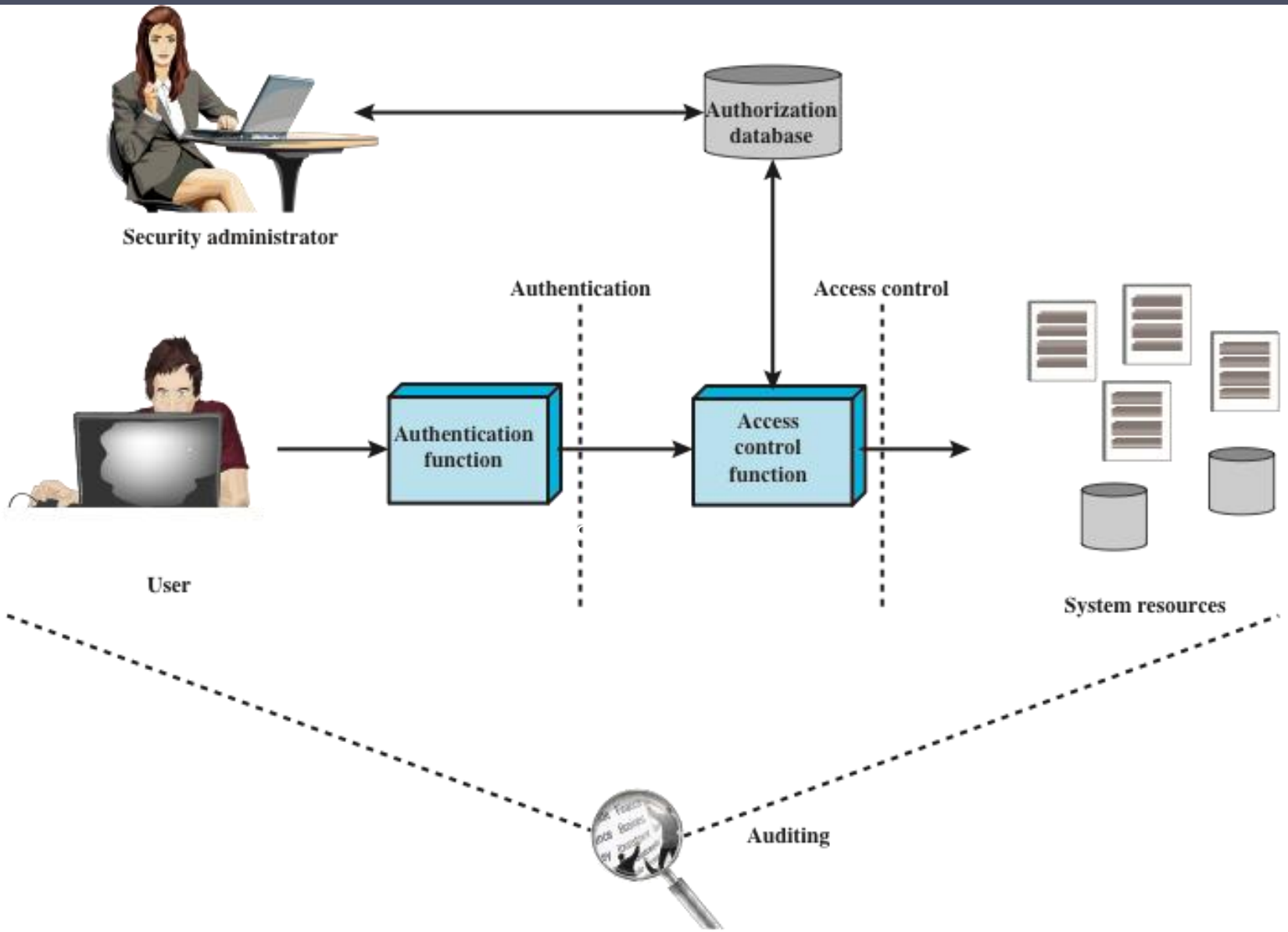


Figure 4.1 Relationship Among Access Control and Other Security Functions

Erişim Denetimi Politikaları

- İsteğe bağlı erişim denetimi (DAC)
  - İstekte bulunanın kimliğine ve istekte bulunanların ne yapmasına izin verildiğini (veya izin verilmediğini) belirten erişim kurallarına (yetkilere) dayalı olarak erişimi kontrol eder.
  - Bu politikanın adı*isteğe bağlı çünkü bir* varlık, kendi iradesiyle, varlığa izin veren erişim haklarına sahip olabilir. başka bir varlığın bazı kaynaklara erişmesini sağlar.
- Zorunlu erişim denetimi (MAC)
  - Güvenlik etiketlerini güvenlik izinleriyle karşılaştırarak erişimi kontrol eder
  - Bu politikanın adız*orunlu çünkü bir varlık* bir kaynağa erişim izni, yalnızca kendi iradesiyle başka bir kaynağa izin vermeyebilir. bu kaynağa erişmek için varlık
- Rol tabanlı erişim denetimi (RBAC)
  - Kullanıcıların sistem içinde sahip oldukları rollere ve verilen rollerde kullanıcılara hangi erişimlere izin verildiğini belirten kurallara dayalı olarak erişimi kontrol eder.
- Özniteliğe dayalı erişim denetimi (ABAC)
  - Kullanıcının özelliklerine, erişilecek kaynağa ve mevcut çevresel koşullara dayalı olarak erişimi kontrol eder.

Özneler, Nesneler ve Erişim Hakları

Özne

Nesnelere erişebilen bir varlık

Üç Sınıfı vardır
- Sahip
- Grup
- Dünya

Nesne

Erişimin kontrol edildiği bir kaynak

Bilgi içeren ve/veya bilgi almak için kullanılan varlık

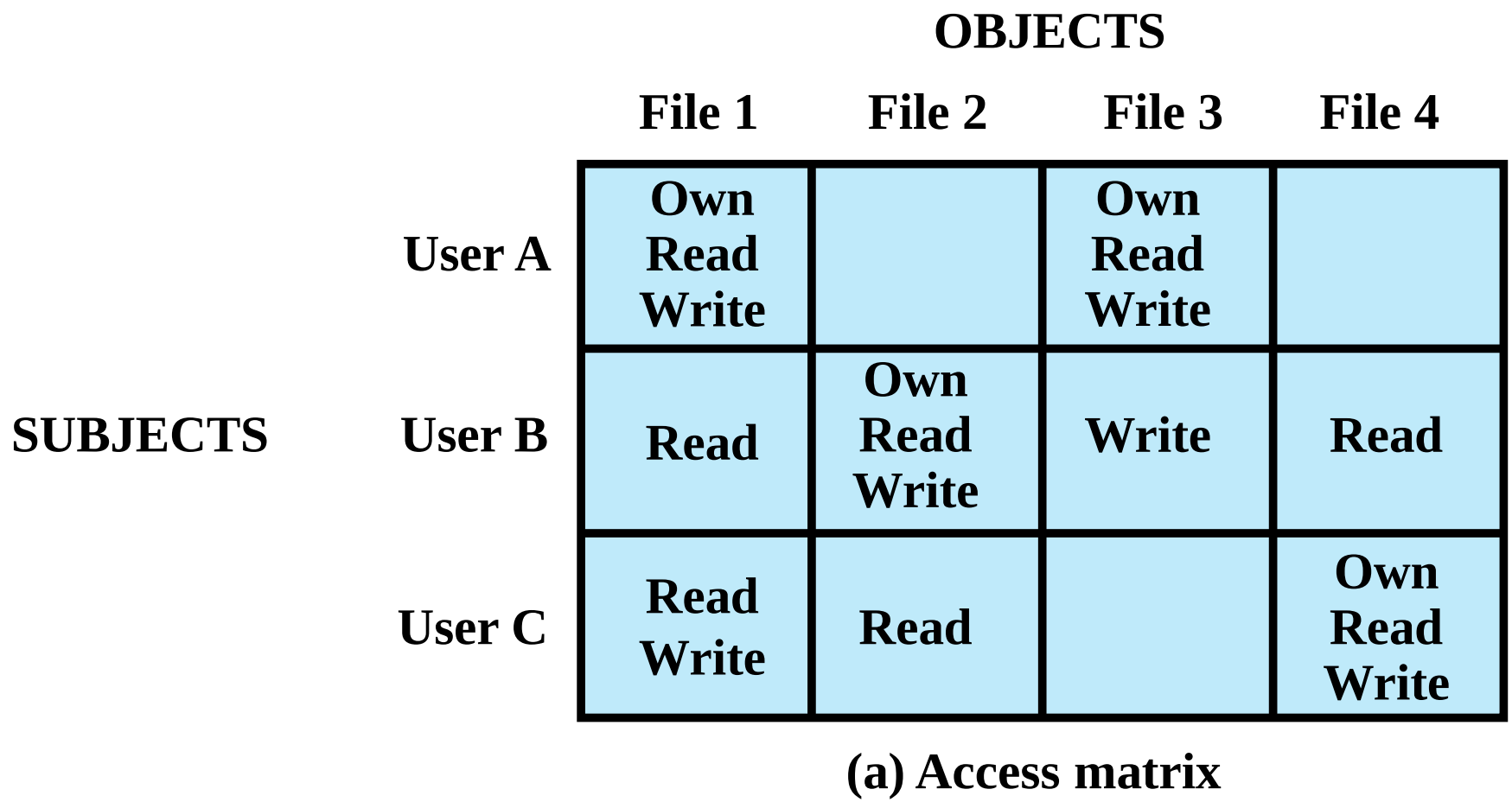
Erişim Hakkı

Bir öznenin bir nesneye nasıl erişebileceğini açıklar

Şunları içerebilir:
- Okuma
- Yazma
- Uygulama
- Silme
- Oluşturma
- Arama

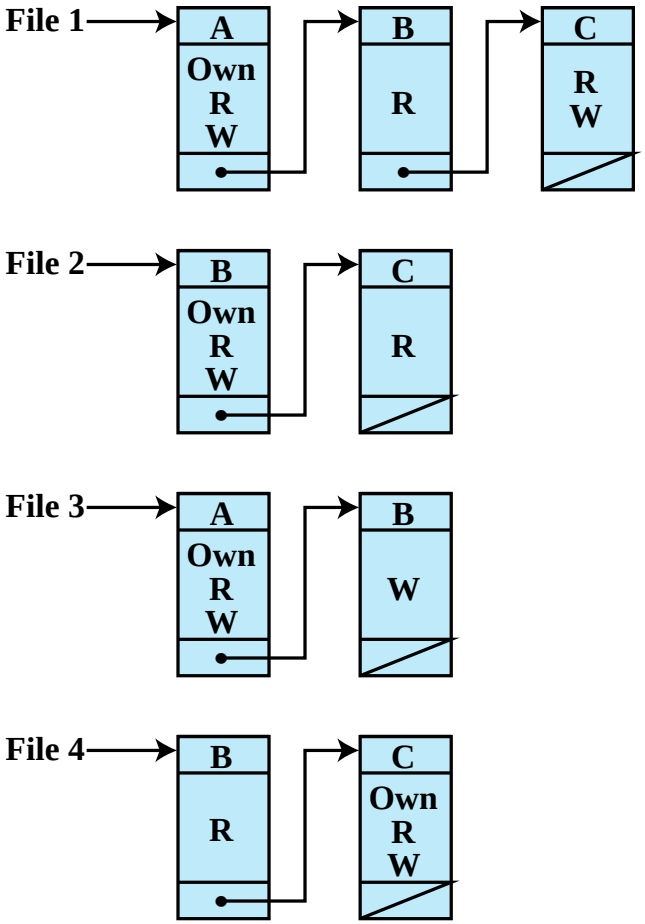
İsteğe Bağlı Erişim Kontrolü (DAC)

- Bir varlığa, kendi iradesiyle, başka bir varlığın bazı kaynaklara erişmesini sağlamak için varlığa izin veren erişim hakları verilebileceği şemadır
- Genellikle bir erişim matrisi kullanılarak sağlanır
  - Bir boyut, kaynaklara veri erişimi girişiminde bulunabilecek tanımlanmış öznelerden oluşur.
  - Diğer boyut, erişilebilecek nesneleri listeler.
- Matristeki her giriş, belirli bir nesne için belirli bir öznenin erişim haklarını gösterir.

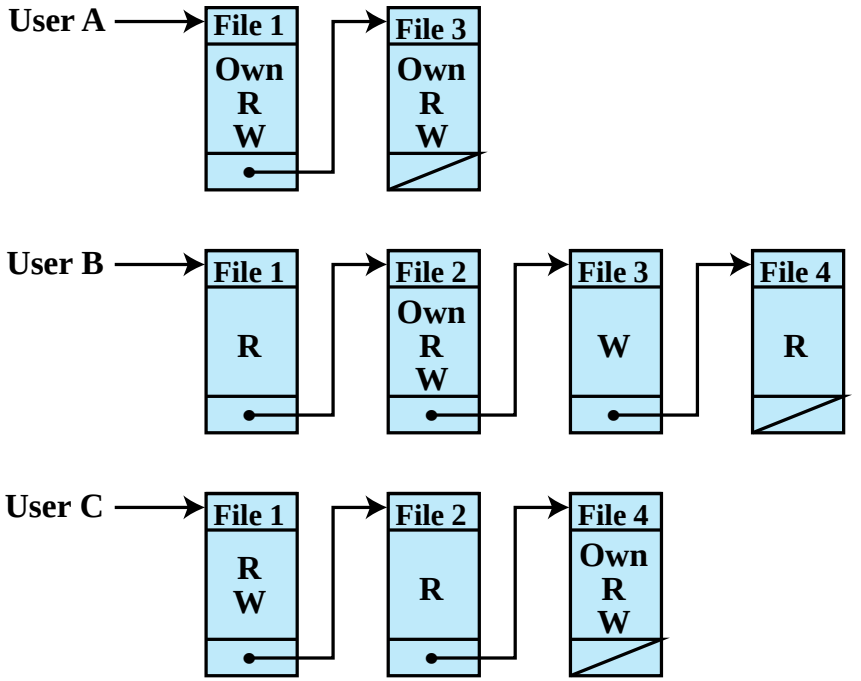


(a) Access matrix

Şekil 4.2 Erişim Kontrol Yapıları Örneği



(b) Access control lists for files of part (a)



(c) Capability lists for files of part (a)

Figure 4.2 Example of Access Control Structures

Özne	Giriş Modu	Nesne
A	Sahip olma	Dosya 1
A	Okuma	Dosya 1
A	Yazma	Dosya 1
A	Sahip olma	Dosya 3
A	Okuma	Dosya 3
A	Yazma	Dosya 3
B	Okuma	Dosya 1
B	Sahip olma	Dosya 2
B	Okuma	Dosya 2
B	Yazma	Dosya 2
B	Yazma	Dosya 3
B	Okuma	Dosya 4
C	Okuma	Dosya 1
C	Yazma	Dosya 1
C	Okuma	Dosya 2
C	Sahip olma	Dosya 4
C	Okuma	Dosya 4
C	Yazma	Dosya 4

Yetkilendirme Tablosu Şekil 4.2'deki Dosyalar için

Koruma Alanları

- Bu nesnelere erişim haklarıyla birlikte nesneler kümesi
- Yetenekleri koruma alanlarıyla ilişkilendirirken daha fazla esneklik
- Erişim matrisi açısından, bir satır bir koruma alanını tanımlar
- Kullanıcı, kullanıcının erişim haklarının bir alt kümesiyle süreçler oluşturabilir
- Bir süreç ve bir etki alanı arasındaki ilişki statik veya dinamik olabilir
- Kullanıcı modunda, belleğin belirli alanları kullanımdan korunur ve belirli komutlar yürütülmeyebilir.
- Çekirdek modunda ayrıcalıklı talimatlar yürütülebilir ve korunan bellek alanlarına erişilebilir

UNIX Dosya Erişim Kontrolu

UNIX dosyaları inode'lar (dizin düğümleri) kullanılarak yönetilir

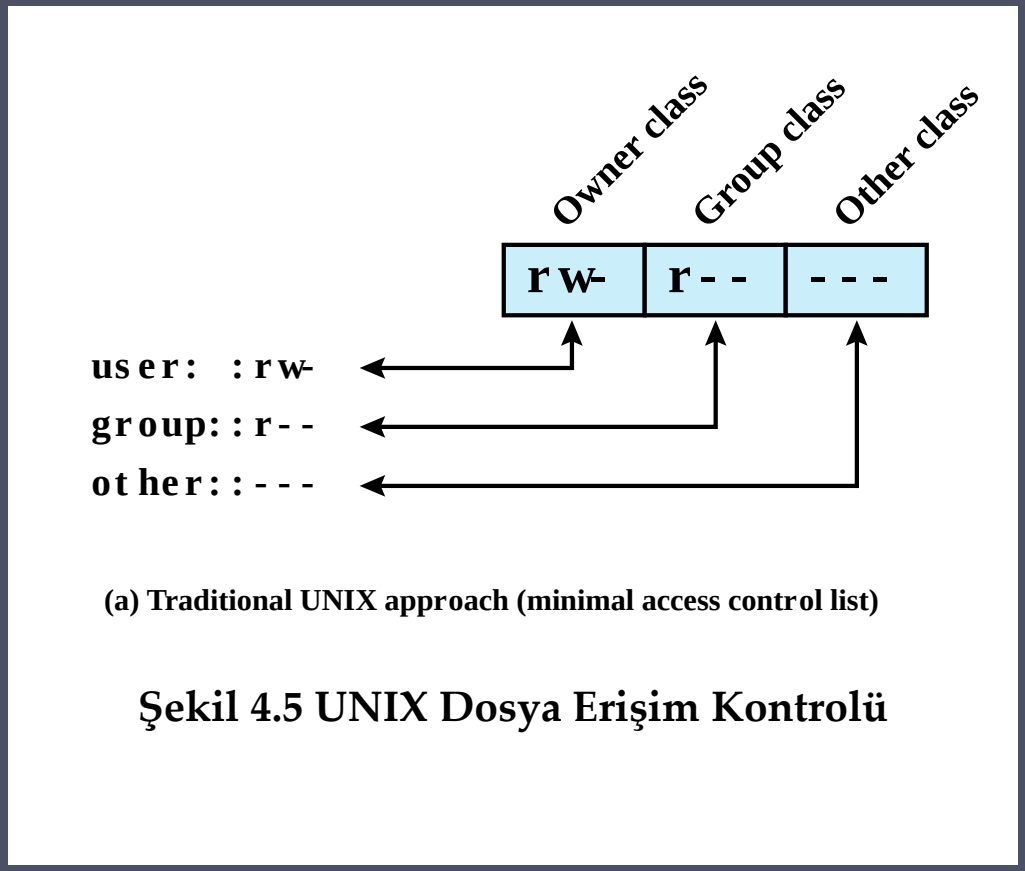
- Belirli bir dosya için gereken anahtar bilgileri içeren kontrol yapıları
- Birkaç dosya adı tek bir inode ile ilişkilendirilebilir
- Etkin bir inode, tam olarak bir dosyayla ilişkilendirilir
- Dosya öznitelikleri, izinler ve kontrol bilgileri inode'da sıralanır
- Diskte, dosya sistemindeki tüm dosyaların inode'larını içeren bir inode tablosu veya inode listesi vardır.
- Bir dosya açıldığında, inode'u ana belleğe getirilir ve bellekte yerleşik bir inode tablosunda saklanır.

Dizinler hiyerarşik bir ağaçta yapılandırılmıştır

- Dosyaları ve/veya diğer dizinleri içerebilir
- Dosya adları ve ilişkili inode'lara işaretçiler içerir

UNIX
Dosya Giriş kontrolu

- Tekil kullanıcı kimlik numarası (kullanıcı ID)
- Grup ID ile tanımlanan birincil grubun üyeliği
- Belirli bir gruba aidiyet
- 12 koruma biti
  - Dosyanın sahibi, grup üyeleri ve diğer tüm kullanıcılar için okuma, yazma ve yürütme izni belirtir
- Sahip kimliği, grup kimliği ve koruma bitleri, dosyanın idone'larının bir parçasıdır



(a) Traditional UNIX approach (minimal access control list)

Şekil 4.5 UNIX Dosya Erişim Kontrolü

Geleneksel UNIX Dosya Erişim Kontrolu

- "Kullanıcı kimliğini ayarla"(SetUID)
- "Grup kimliğini ayarla"(SetGID)
  - Sistem, erişim kontrol kararları verirken gerçek kullanıcı haklarına ek olarak dosya sahibinin/grubunun haklarını geçici olarak kullanır.
  - Ayrıcalıklı programların genel olarak erişilemeyen dosyalara/kaynaklara erişmesine olanak tanır
- yapışkan bit
  - Bir dizine uygulandığında, yalnızca dizindeki herhangi bir dosyanın sahibinin o dosyayı yeniden adlandırabileceğini, taşıyabileceğini veya silebileceğini belirtir.
- süper kullanıcı
  - Olağan erişim denetimi kısıtlamalarından muaftır
  - Sistem genelinde erişime sahiptir

UNIX'te Erişim Kontrol Listeleri (ACL'ler)

Modern UNIX sistemleri ACL'leri destekler

- FreeBSD, OpenBSD, Linux, Solaris

FreeBSD

- Setfacl komutu, UNIX kullanıcı kimliklerinin ve gruplarının bir listesini atar
- Herhangi bir sayıda kullanıcı ve grup bir dosyayla ilişkilendirilebilir
- Koruma bitlerini okuyun, yazın, yürütün
- Bir dosyanın bir ACL'ye sahip olması gerekmez

Bir işlem, bir dosya sistemi nesnesine erişim istediğinde iki adım gerçekleştirilir:

- 1. Adım en uygun ACL'yi seçer
- 2. Adım, eşleşen girişin yeterli izinleri içerip içermediğini kontrol eder

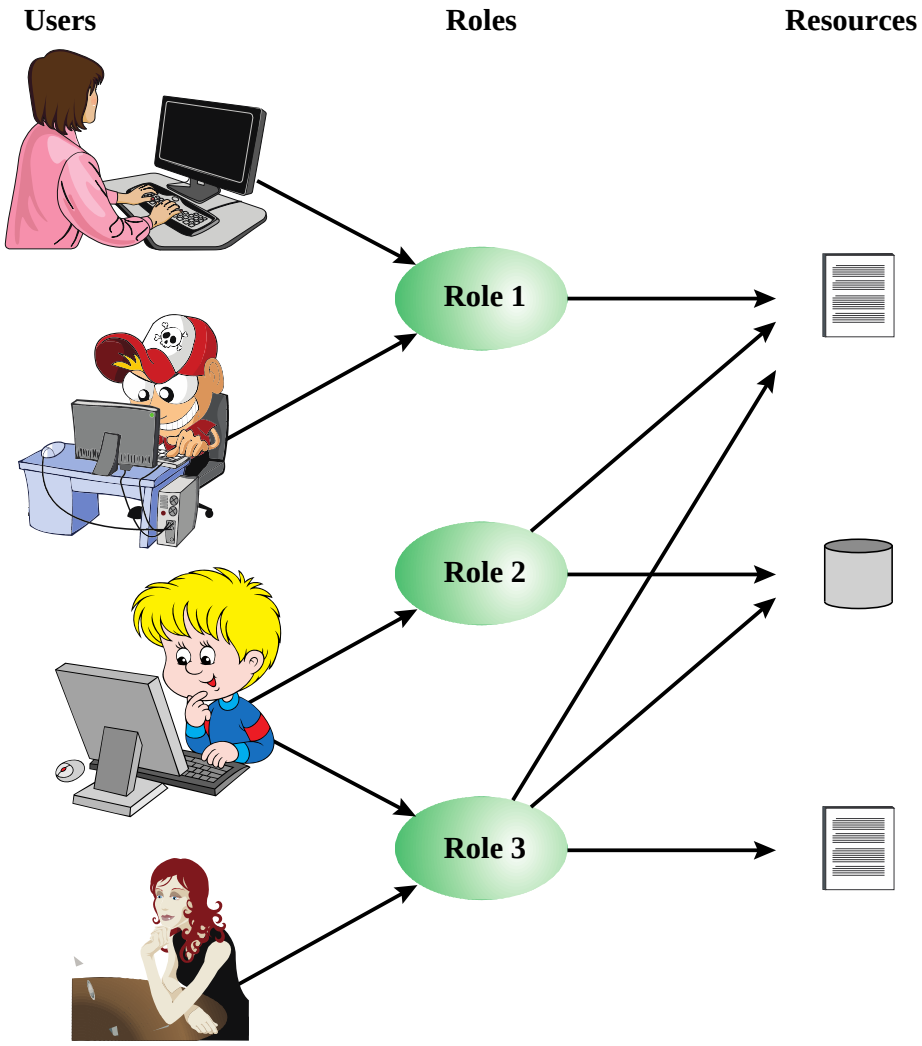
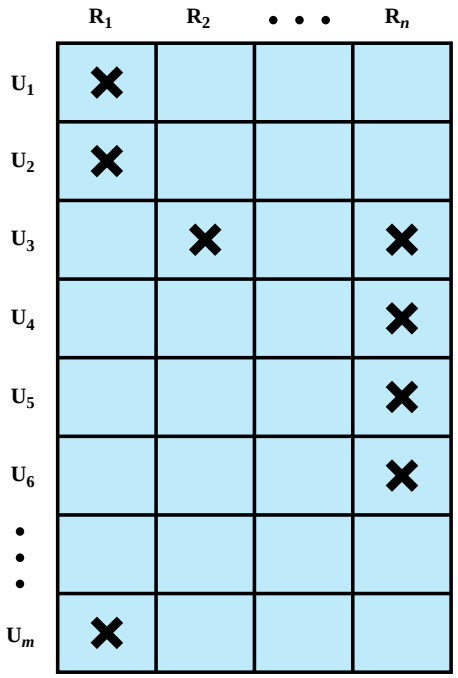


Figure 4.6 Users, Roles, and Resources



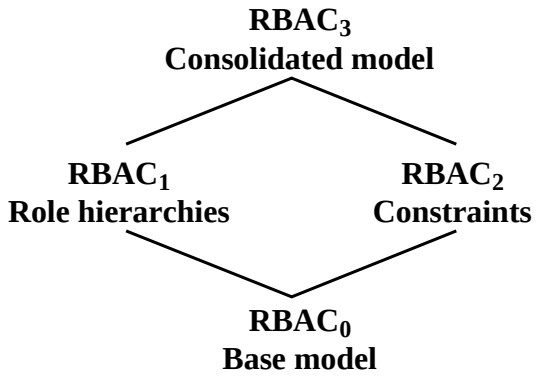
OBJECTS

ROLES	R_1	R_2	R_n	F_1	F_1	P_1	P_2	D_1	D_2
R_1	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R_2		control		write *	execute			owner	seek *
• • •									
R_n			control		write	stop			

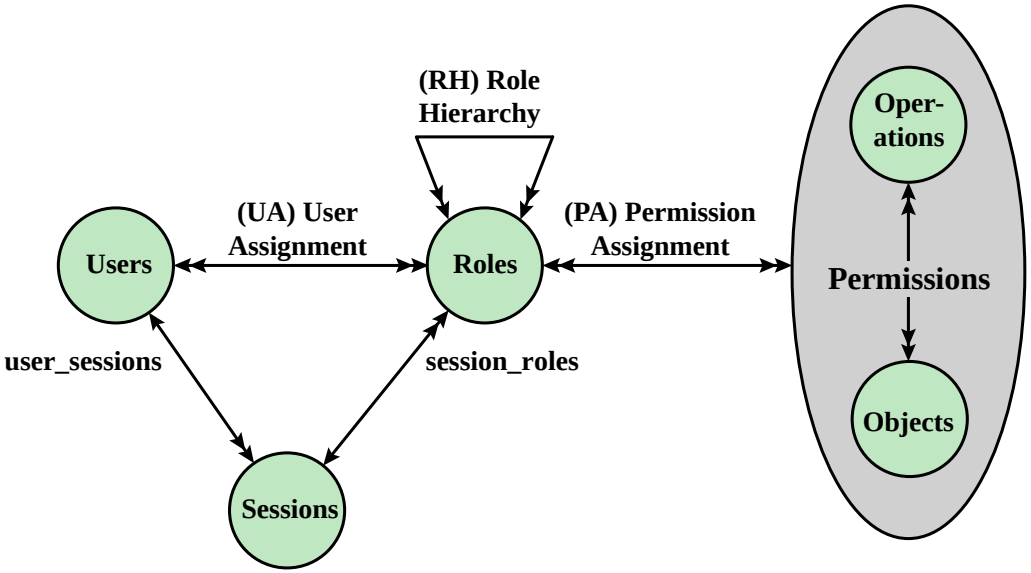
Figure 4.7 Access Control Matrix Representation of RBAC

Kapsam RBAC Modelleri

Models	Hierarchies	Constraints
$RBAC_0$	No	No
$RBAC_1$	Yes	No
$RBAC_2$	No	Yes
$RBAC_3$	Yes	Yes



(a) Relationship among RBAC models



(b) RBAC models

Figure 4.8 A Family of Role-Based Access Control Models.

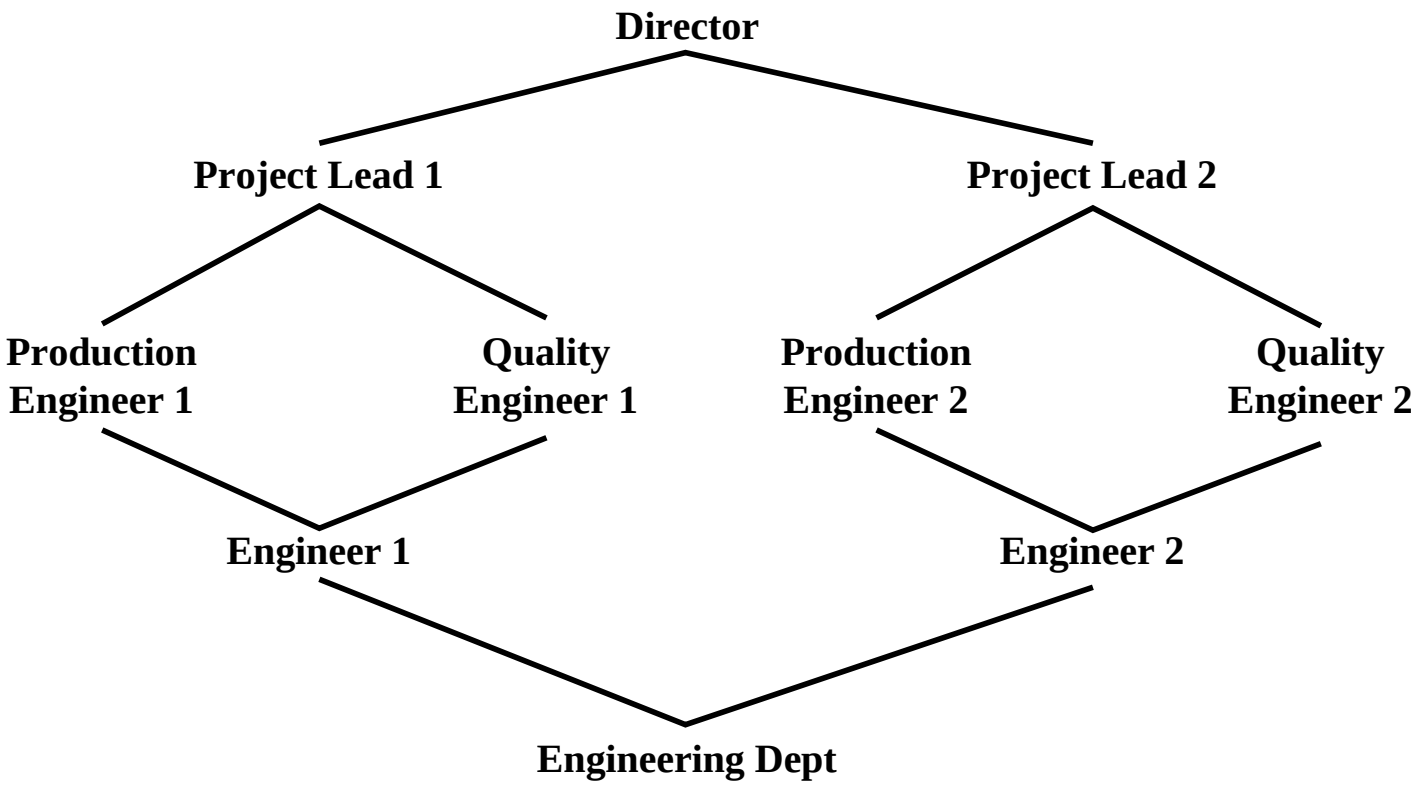


Figure 4.9 Example of Role Hierarchy

Kısıtlamalar - RBAC

- RBAC'yi bir kuruluşun idari ve güvenlik politikalarının özelliklerine uyarlamak için bir araç sağlar
- Roller arasında tanımlanmış bir ilişki veya rollerle ilgili bir koşuldur
- Türleri:

Birbirini dışlayan roller

- Bir kullanıcı, kümede yalnızca bir role atanabilir (oturum sırasında veya statik olarak)
- Sette yalnızca bir role herhangi bir izin (erişim hakkı) verilebilir.

Kardinalite

- Rollere göre maksimum sayı belirleme

Önkuşullu Roller

- Bir kullanıcının yalnızca belirli bir role eğer önceden belirlenmiş başka bir role atanmışsa atanabileceğini belirtir,

Öznitelik Tabanlı Erişim Kontrolü (ABAC)

Hem kaynağın hem de öznenin özelliklerine ilişkin koşulları ifade eden yetkileri tanımlar

Kuvvetli yönü esnekliği ve ifade gücüdür

Gerçek sistemlerde benimsenmesinin önündeki ana engel, her erişim için hem kaynak hem de kullanıcı özellikleri üzerindeki tahminlerin değerlendirilmesi nin performans etkisi ile ilgili endişe dir

Web hizmetleri, Genişletilebilir Erişim Denetimi İşaretleme Dili (XACML'nin tanıtılmasıyla öncü teknolojiler olmuştur.

Modelin bulut hizmetlerine uygulanmasına büyük ilgi vardır

ABAC Modeli: Öznitelikler

Özne öznitelikleri

- Özne, nesneler arasında bilgi akışına neden olan veya sistem durumunu değiştiren aktif bir varlıktır.
- Öznitelikler öznenin kimliğini ve özelliklerini tanımlar
- Bir öznenin rolü de bir nitelik olarak görülebilir.

Nesne öznitelikleri

- Bir nesne (veya kaynak), bilgi içeren veya alan pasif bir bilgi sistemi ile ilgili varlıktır.
- Nesneler, erişim kontrolü kararları vermek için kullanılabilecek özniteliklere sahiptir.

Ortam öznitelikleri

- Bilgi erişiminin gerçekleştiği operasyonel, teknik ve hatta durumsal ortamı veya bağlamı tanımlar
- Bu nitelikler şimdiye kadar çoğu erişim kontrol politikasında büyük ölçüde göz ardı edilmiştir.

ABAC

Bir istekle ilgili varlıkların, işlemlerin ve ortamın özniteliklerine karşı kuralları değerlendirerek nesnelere erişimi kontrol ettiği için ayırt edilebilir

Öznenin özniteliklerinin, nesnenin özniteliklerinin ve belirli bir ortamda özne-nesne öznitelik kombinasyonları için izin verilen işlemleri tanımlayan resmi bir ilişki veya erişim denetimi kuralının değerlendirilmesine dayanır.

Sistemler DAC, RBAC ve MAC kavramlarını uygulayabilir

Herhangi bir erişim kontrol kuralını karşılamak için sınırsız sayıda özniteliğin birleştirilmesine izin verir

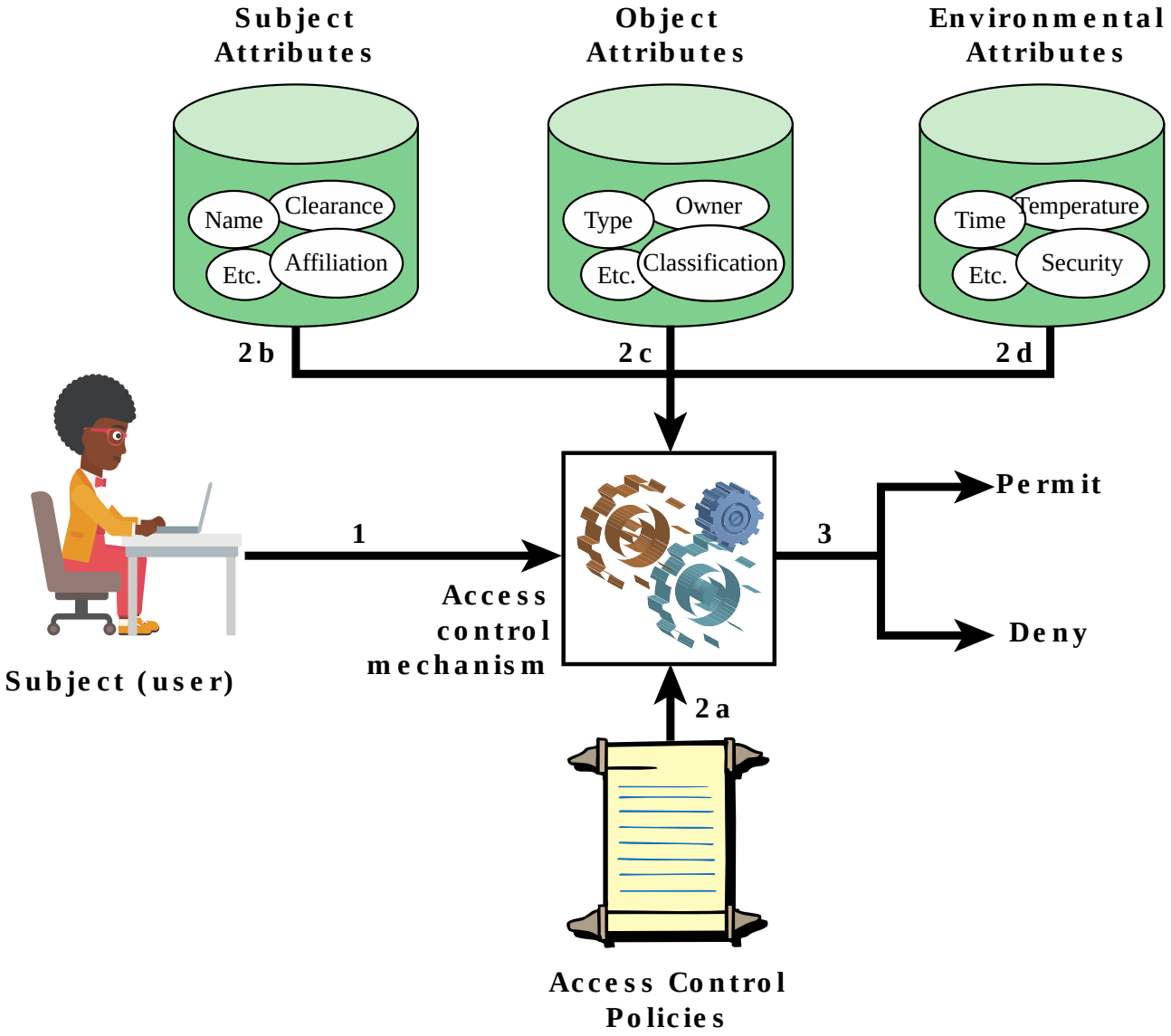


Figure 4.10 ABAC Scenario

ABAC Politikaları

Politika, öznelerin ayrıcalıklarına ve kaynakların veya nesnelerin hangi ortam koşullarında nasıl korunacağına bağlı olarak, bir kuruluş içinde izin verilen davranışları yöneten bir dizi kural ve ilişki olarak tanımlanır.

Tipik olarak, korunması gereken nesne ve öznelere sunulan ayrıcalıklar açısından yazılır.

Ayrıcalıklar, bir öznenin yetkili davranışını temsil eder ve bir otorite tarafından tanımlanır ve bir politikada somutlaşır.

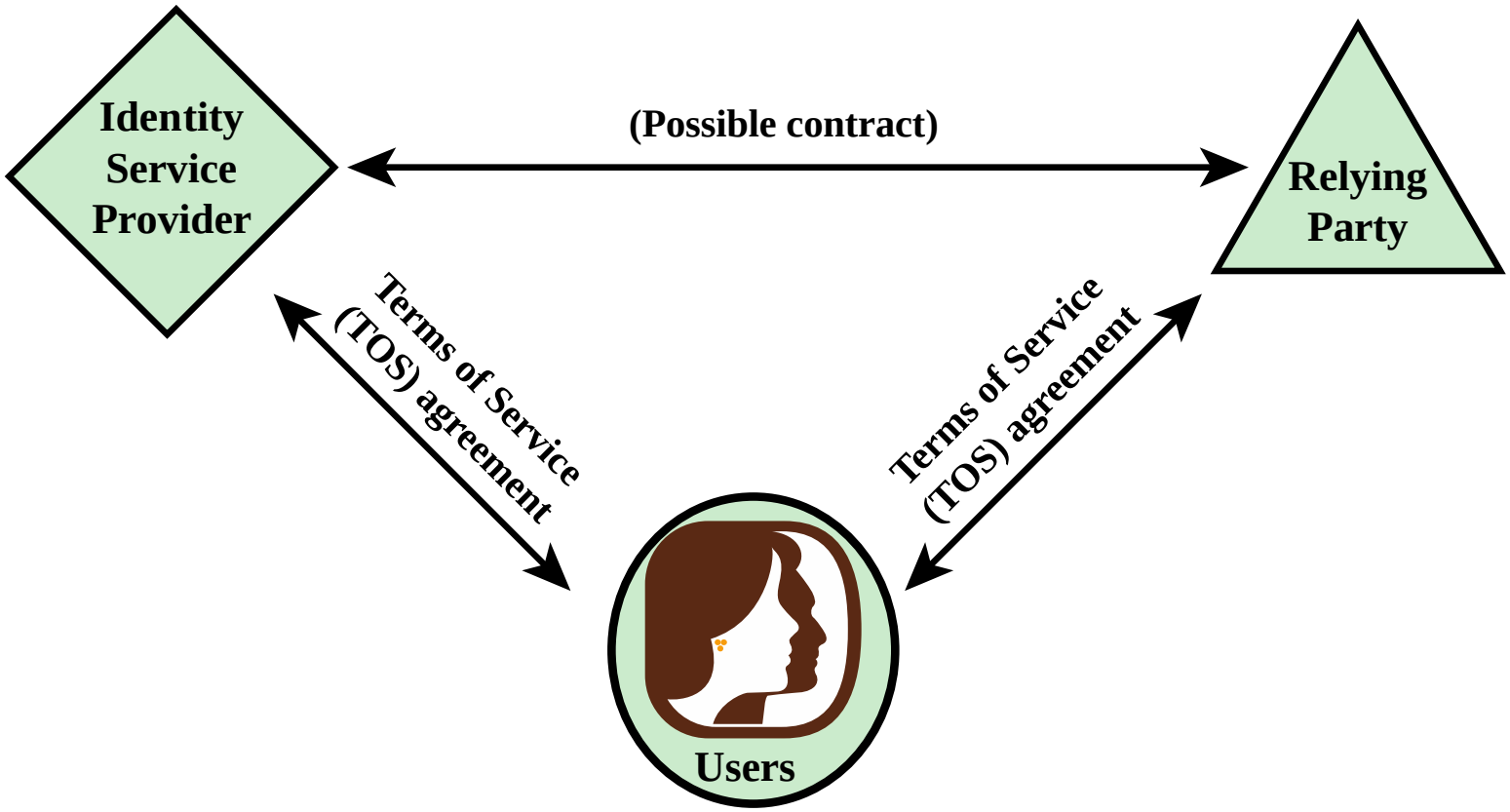
Ayrıcalıklar yerine yaygın olarak kullanılan diğer terimler şunlardır: haklar ve yetkiler

Kimlik, Kimlik Bilgileri ve Erişim Yönetimi (ICAM)

- Dijital kimlikleri, kimlik bilgilerini ve erişim kontrolünü yönetmeye ve uygulamaya yönelik kapsamlı bir yaklaşımdır
- ABD hükümeti tarafından geliştirilmiştir
- …. İçin tasarlanmış:
  - Bireylerin ve kişi olmayan varlıkların (NPE'ler) güvenilir dijital kimlik temsillerini oluşturmak
  - Bu kimlikleri, erişim işlemlerinde NPE'nin bireyi için bir vekil görevi görebilecek kimlik bilgilerine bağlamak
    - Kimlik bilgisi, bir kimliği bir abonenin sahip olduğu ve kontrol ettiği bir simgeye yetkili olarak bağlayan bir nesne veya veri yapısıdır.
  - Bir ajansın kaynaklarına yetkili erişim sağlamak için kimlik bilgileri kullanılır

Kimlik Kuruluşu

- Bir kuruluşun dijital kimliklere, kimlik niteliklerine ve başka bir kuruluş tarafından oluşturulan ve verilen kimlik bilgilerine güvenmesine olanak tanıyan teknolojiyi, standartları, politikaları ve süreçleri tanımlamak için kullanılan terimdir
- İki soruyu ele alıyor:
  - Sistemlerinize erişmesi gereken harici kuruluşlardan kişilerin kimliklerine nasıl güveniyorsunuz?
  - Dış kuruluşlarla işbirliği yapmaları gerektiğinde kuruluşunuzdaki bireylerin kimlikleri için nasıl kefil olursunuz?



(a) Traditional triangle of parties involved in an exchange of identity information

Figure 4.13 Identity Information Exchange Approaches

Açık Kimlik Güven Çerçevesi

OpenID

- Kullanıcıların bir üçüncü taraf hizmeti kullanarak işbirliği yapan belirli siteler tarafından kimliklerinin doğrulanmasına olanak tanıyan açık bir standartdır.

OIDF

- OpenID Kuruluşu, OpenID teknolojilerini etkinleştirmeyi, teşvik etmeyi ve korumayı taahhüt eden kişi ve şirketlerden oluşan, kar amacı gütmeyen uluslararası bir kuruluştur.

ICF

- Bilgi Kartı Kuruluşu, bilgi kartı ekosistemini geliştirmek için birlikte çalışan şirketler ve bireylerden oluşan kar amacı gütmeyen bir topluluktur.

OITF

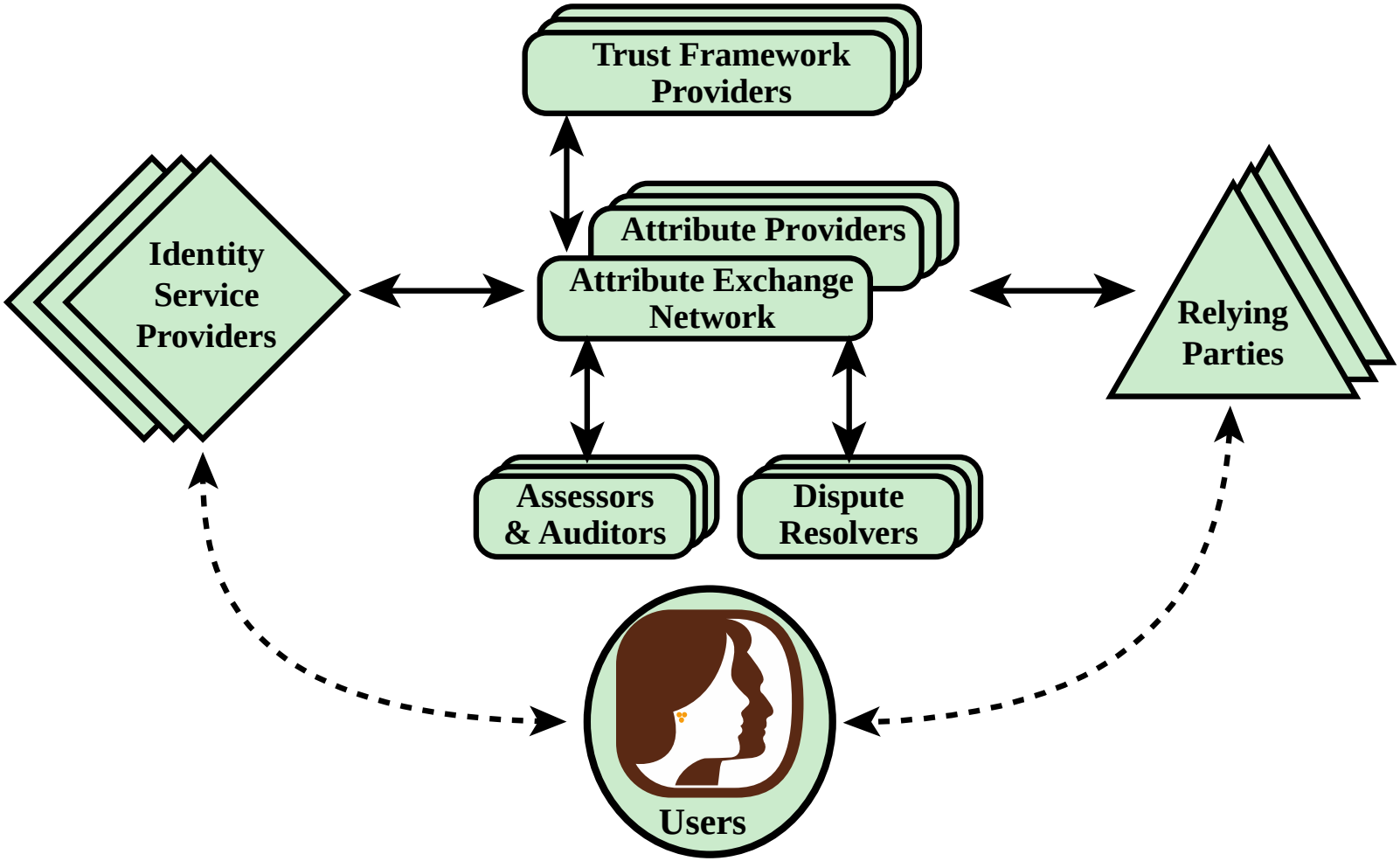
- Açık Kimlik Güven Çerçevesi, OIDF ve ICF tarafından ortaklaşa geliştirilen, kimlik ve öznitelik değişimi için bir güven çerçevesinin standart, açık bir özelliğidir.

OIX

- Açık Kimlik Değişimi Şirketi, OITF modeline uygun bağımsız, tarafsız, uluslararası bir sertifika güven çerçeveleri sağlayıcısıdır.

AXN

- Öznitelik Değişim Ağı, kimlik hizmeti sağlayıcıları ve bağlı taraflar için, kullanıcı tarafından iddia edilen, izin verilen ve doğrulanan çevrimiçi kimlik özelliklerine yüksek hacimlerde uygun maliyetlerle verimli bir şekilde erişmeleri için çevrimiçi İnternet ölçeğinde bir ağ geçididir.



(B) Identity attribute exchange elements

Figure 4.13 Identity Information Exchange Approaches