Erişim Denetim Modelleri

Yrd. Doç. Dr. Özgü Can

Erişim Denetim Modelleri

- Rol Tabanlı Erişim Denetimi
- Öznitelik Tabanlı Erişim Denetimi
- İçerik Tabanlı Erişim Denetimi
- Zaman Tabanlı Erişim Denetimi
- Konum Tabanlı Erişim Denetimi
- Amaç Tabanlı Erişim Denetimi
- Yaratıcı Kontrollü Erişim Denetimi

ROLE-BASSED ACCESS CONTROL (RBAC)

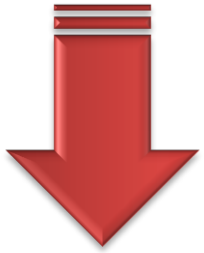
ROL TABANLI ERİŞİM DENETİMİ

Rol Tabanlı Erişim Denetimi

- **R**ole–**B**ased **A**ccess **C**ontrol (RBAC)
- **Yetkilendirme yönetimi maliyetlerinin** düşürülmesini amaçlamaktadır.
- Klasik erişim denetimlerinde **yetkilendirme sayısı** yüksek olmaktadır.
  - ÖR: 1,000 kullanıcı, 100,000 nesne ve 10 erişim hakkı olan bir sistemde → **10^9** olası yetkilendirme

Rol Tabanlı Erişim Denetimi

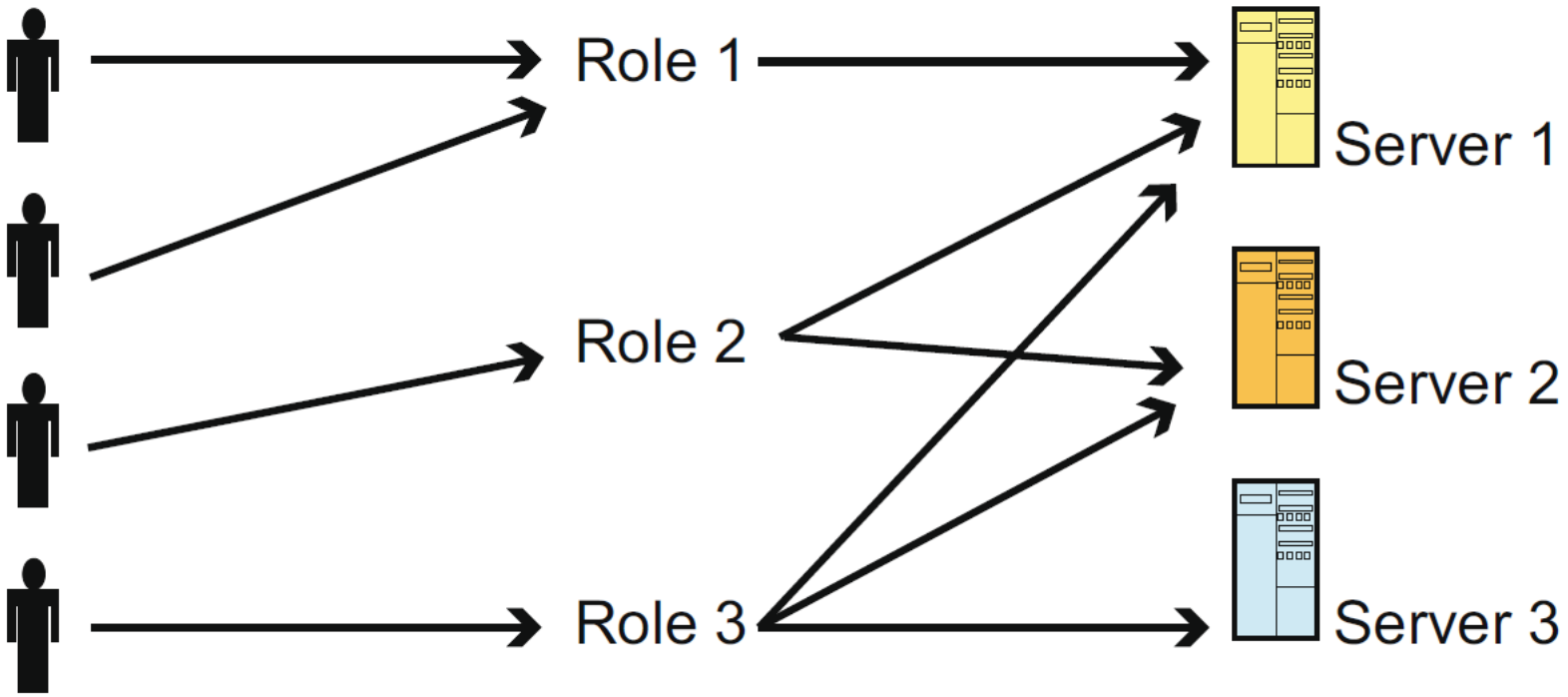
Kullanıcı topluluğu yapısı dinamik ise



Gerçekleştirilecek onay (grant) ve hakların geri alınması (revoke) işlemlerinin yönetimi zorlaşacaktır.

Rol Tabanlı Erişim Denetimi

- RBAC → **Rol** (role) kavramını kullanmaktadır.
- Rol, kullanıcılar ve izinler arasında aracı olarak davranmaktadır.



Rol Tabanlı Erişim Denetimi

- Amaç:
  - Kullanıcı sayısından daha az *rol* olması
  - Organizasyondaki kullanıcı kümesinden daha statik bir *rol kümesinin* olması

Rol Tabanlı Erişim Denetimi

- **İzinler** kullanıcılar yerine **rollere** atanmaktadır.
- Erişim denetim politikalarının *tanımlanması*, *analizi* ve *yönetimi* kolaylaşmaktadır.
- Organizasyonun **erişim denetim durumunun doğrulanması süreci** iyileştirilmektedir.
- Bu nedenle, birçok sistemde kullanılmaktadır.
  - İşletim Sistemleri
  - DBMS
  - Kimlik Yönetim Sistemleri

Rol Tabanlı Erişim Denetimi

- RBAC terimleri:
  - **U** : Kullanıcı (user) kümesi
  - **P** : İzinler (permissions) kümesi
  - **R** : Roller (roles) kümesi

Rol Tabanlı Erişim Denetimi

Kullanıcı

- Organizasyon içerisinde bir iş ünvanını temsil eden bir roldür.
- ÖR: Akademik roller
  - Bölüm Başkanı
  - Profesör
  - Memur
  - Öğrenci

Rol Tabanlı Erişim Denetimi

İzin

- Genellikle **nesne-eylem** çifti olarak kabul edilir.
- İznin türü ve biçimi, RBAC'in kullanıldığı sisteme göre belirlenir.

Rol Tabanlı Erişim Denetimi

İzin

- ÖR: İlişkisel SQL veritabanı
  - **Nesneler:** İlişkiler ve veritabanı nesneleri
  - **Eylemler:** SQL komutları (SELECT, INSERT, vs..)

Rol Tabanlı Erişim Denetimi

Rol

- Kullanıcılar, roller ile ilişkilendirilir.
- Kullanıcı-rol ataması için **UA ilişkisi** kullanılır.
- UA İlişkisi → **(u,r)** formundadır.
  - ***u*** kullanıcısı ***r*** rolüne atanmaktadır.

Rol Tabanlı Erişim Denetimi

- İzinler rollere atanır ve rollerden geri alınır.
- İzin-Rol ataması → **PA ilişkisi**
  - Hangi iznin hangi role atandığını belirtir.
- Kullanıcı, kendisine atanan role verilmiş olan bütün izinlere sahiptir.

Rol Tabanlı Erişim Denetimi

- Kullanıcılar, RBAC sistemi ile bir oturumu etkinleştirerek etkileşimde bulunmaktadır.
- **Oturum (Session)** → Kullanıcı ve kullanıcıya atanmış etkinleştirilmiş rol alt kümesi arasındaki eşlemedir.
- Oturumun gerçekleştirimi genellikle RBAC'in bulunduğu sisteme bağlı olduğundan, birçok RBAC gerçekleştirimi oturumu desteklemez.

Rol Tabanlı Erişim Denetimi

ÖR:

- Kullanıcı, DBMS'de kimliğini doğrular.
- Kendisine atanan rollerden birini ya da birkaçını seçer.
- Eğer *s* oturumu *P* izni için bir istekte bulunursa, oturum rolleri ile ilgili izinler değerlendirilir.
- Eğer istenilen izin varsa, erişim isteği onaylanır.

Rol Tabanlı Erişim Denetimi

- RBAC, **role hiyerarşisi** kavramını kullanarak yönetimsel masrafları düşürmektedir.
- Role hiyerarşisi, yönlü düz ağaçtır (Directed Acyclic Graph - DAC) ve düğümler (node) rolleri temsil eder.
- Hiyerarşide üst seviyede olan rol, izinlerin atanmasına gerek olmadan alt seviyedeki rollerin izinlerini kalıt alır (inherit).

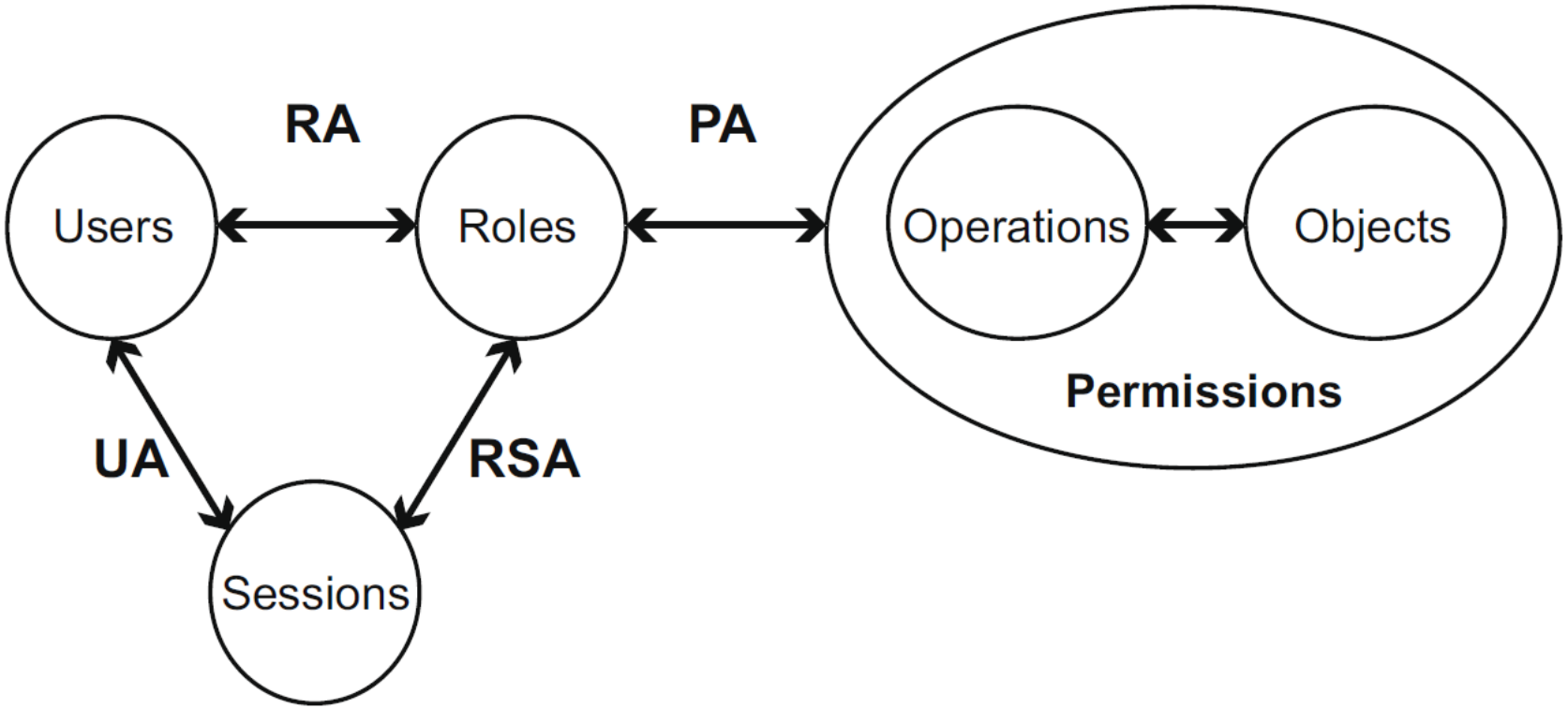
Rol Tabanlı Erişim Denetimi

Böylece, kıdemli rollere atanması gereken **izinlerin sayısı azalır**.

Yönetimsel yükler azalır.

Erişim denetim kararı verilirken bütün alt rollerin izinleri dikkate alınacağından, **erişim denetim kontrolü algoritmasının yükü artar**.

Rol Tabanlı Erişim Denetimi



RBAC ve SQL

- Günümüzde birçok veri yönetim sisteminde RBAC desteği bulunmaktadır.

- SQL standardı rol yönetimi ile ilgili olarak RBAC'i destekleyen komutlar sunmaktadır.

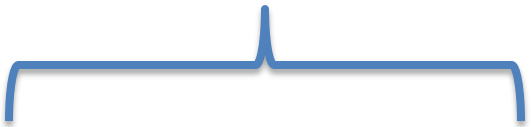
RBAC ve SQL

- Rol yaratma:

```
CREATE ROLE <role_name>
```

- Rol silme:

Yaratılacak/Silinecek rol adı



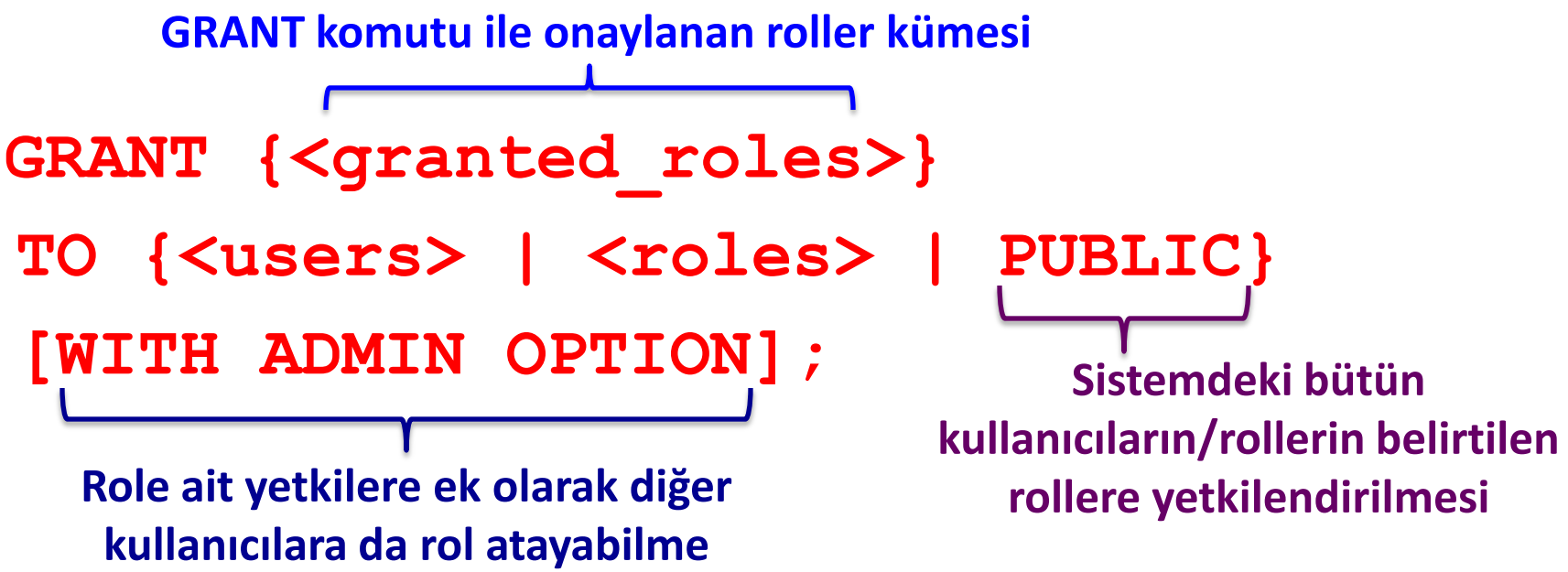
```
DROP ROLE <role_name>
```

RBAC ve SQL

- Yetkilerin tanımlanması:

RBAC ve SQL

- Kullanıcılara rol tanımlanması:



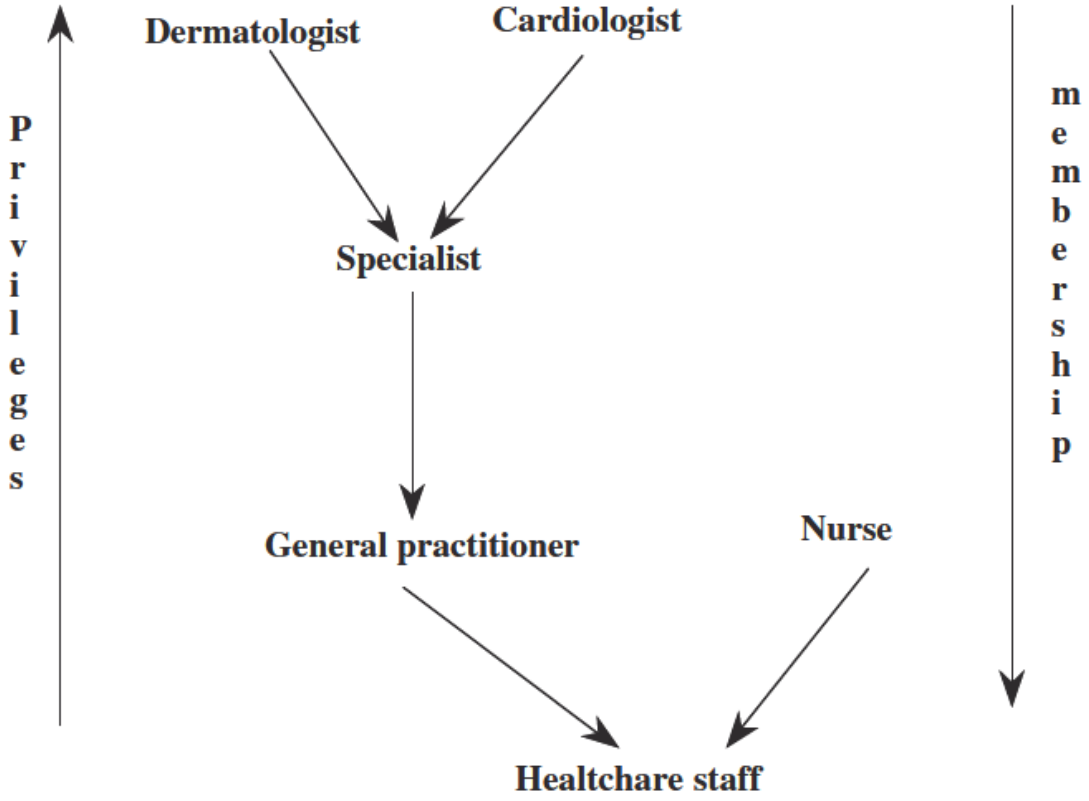
RBAC ve SQL

- Rolün aktive edilmesi: **SET ROLE**

- Rollerin silinmesi:

RBAC ve SQL

- Sağlık alanı rol hiyerarşisi örneği:



RBAC ve SQL

```
CREATE ROLE Nurse;
CREATE ROLE Cardiologist;
CREATE ROLE Healthcare_staff;
GRANT select(name, address) ON Patients TO Healthcare_staff;
GRANT Nurse TO John WITH ADMIN OPTION;
GRANT Cardiologist TO Ann;
GRANT Healthcare_staff TO Nurse;
```

`Healthcare_staff`'in hasta kayıtlarında isim ve adres sorgusu yapabilmesi için yetkilendirilmesi

Nurse ≥ Healthcare_staff

John, `Patients` üzerinde `isim` ve `adres` sorgusu gerçekleştirme yetkisine sahiptir.

RBAC ve SQL

```
REVOKE ADMIN OPTION FOR Nurse FROM John;
REVOKE select ON Patients FROM Healthcare_staff;
REVOKE Cardiologist FROM Ann;
```

John, Nurse rolünde olmasına rağmen diğer kullanıcılara rol ataması yapamamaktadır.

Healthcare_staff'ın Patients üzerinde isim ve adres sorgusu yapma izni silinmektedir.

ATTRIBUTE-BASED ACCESS CONTROL (ABAC)

ÖZNİTELİK TABANLI ERİŞİM DENETİMİ

Öznitelik Tabanlı Erişim Denetimi

- **A**ttribute-**B**ased **A**ccess **C**ontrol (ABAC)
  - Öznelerin ve nesnelerin öznitelikler kümesi ile tanımlanması,
  - Öznelerin ve nesnelerin güvenlik ile ilgili özelliklerinin kodlanması,
  - Yetkilendirmedeki öznelerin ve nesnelerin özniteliklerin koşulları ile ifade edilmesidir.

Öznitelik Tabanlı Erişim Denetimi

Bir özne, bir nesneye eğer;

- öznenin *A* yetkilendirmesinde yer alan özne koşullarını doğruladığı

ve

- nesnenin *A* yetkilendirmesinde yer alan nesne koşullarını doğruladığı

bir ***A* yetkilendirmesi** bulunuyorsa erişebilir.

Öznitelik Tabanlı Erişim Denetimi

- ÖR: *Yetişkinlere yönelik MPEG filmler sadece 18 yaşında olan ya da 18 yaşından büyük olan kişiler tarafından indirilebilir.*

- Bu kuralda herhangi bir **kullanıcı kimliği belirleyicisi** (kullanıcı adı gibi) belirtilmemektedir.
  - Yaşı 18 ve üstü olan bütün kullanıcılar koşulu doğrulamaktadır.
- Korunan nesneler için bir **belirleyici** (dosya adı gibi) belirtilmemektedir.
  - *"kategori = yetişkinlere yönelik"*

Öznitelik Tabanlı Erişim Denetimi

- ABAC → Özneleri ve korunan nesneleri tanımlayan **öznitelikleri kullanımını** temel almaktadır.
- Kurumsal güvenlik politikalarından **yetkilendirmelerin elde edilmesini** kolaylaştırmaktadır.
  - İçerden gelebilecek tehditlere (insider threats) yönelik korunmayı sağlayacak yetkilendirmeyi kolaylaştırmaktadır.

Öznitelik Tabanlı Erişim Denetimi

- En bilinen ABAC modeli → XACML (e**X**tensible **A**ccess **C**ontrol **M**arkup **L**anguage)

- Farklı kurum etki alanları arasında **işbirliği verisinin paylaşım ihtiyacı** sonucunda geliştirilmiştir.

XACML

XACML;

- Genişleyebilen,
- XML olarak kodlanmış
- Erişim denetim **politikalarının**, erişim **isteklerinin** ve erişim denetim **kararlarının**

tanımlandığı bir dildir.

XACML

- Yetkilendirmeler üçlü (triple) formunda ifade edilmektedir:

<Kaynak, Özne, Eylem>

- Kaynak → Korunan nesne

XACML

- Erişim denetim politikalarının **yapısal** (structured) bir düzenlemesidir.
- Bir XACML politikasının en üst elemanı **politikalar kümesidir**.
- Her bir politika kümesi diğer politika kümelerini ya da **politika elemanlarını** bir araya getirmektedir.
- Bir politika elemanının temel bileşeni **kural kümesidir** (rule set).
- Kural kümesi, birçok kuraldan oluşur.
- Her bir kural, üçlü-tabanlı yetkilendirmedir.

XACML

- Negatif yetkilendirmeyi desteklemektedir.
  - Negatif yetkilendirme → “**Deny**”
  - Pozitif yetkilendirme → “**Permit**”
- Farklı kurallar nedeni ile erişim denetim kararlarında meydana gelen **çelişmeleri çözmek için** farklı algoritmaları desteklemektedir.

XACML

```
<Policy ID = P1>
<Target>
      <Subjects> <Subject> GroupName = IBMOpenCollaboration </Subject>
</Subjects>
      </Target>
<Rule ID = R11 Effect = Permit>
      <Target>
            <Subjects> <Subject> Designation = Professor </Subject>
</Subjects>
            <Resources> <Resource> FileType = Source </Resource>
</Resources>
            <Actions> <Action> Type = Read </Action> </Actions>
            <Environments> <Environment> Time = (8AM, 6PM)
</Environment> </Environments>
      </Target>
      <Condition> (FileSize < 100MB) </Condition>
</Rule>
<Rule ID = R12 ..> ... . </Rule>
```

Kuralın uygulanacağı hedef

Kuralın etkisi: Permit ya da Deny

Politika, kurallar kümesi ile ifade edilir.

XACML Politika Örneği

XACML

- Bir **istek**;
  - istek ile ilgili **öznenin**,
  - istekte yer alan **kaynağın**,
  - yerine getirilen **eylemin**

  ve
  - **çevrenin**

  ilişkili olduğu ***öznitelikleri*** içerir.

XACML

- **Yanıt** ise dört karardan birini içerir:
  - **İzin (Permit)**
  - **Red (Deny)**
  - **Uygulanamaz (Not Applicable)**
    - Uygulanabilecek politikaların ya da kuralların bulunamadığı durumu belirtir.
  - **Belirsiz (Indeterminate)**
    - Erişim denetim işlemi sırasında bazı hataların meydana geldiğini belirtir.

XACML

- Yanıt, **zorunlulukları** (obligations) da içerebilir.
- Zorunluluk → Veriye erişim olduğunda gerçekleştirilmesi gereken eylemlerdir.
- ÖR: *Veriye erişildiğinde kullanıcının verisine bir erişim gerçekleştirildiğinden haberdar edilmesi.*

XACML

Bir istek, bir politika ve ilgili yanıt

XACML bağlamını (XACML context) oluşturur.

Content-Based Access Control

İÇERİK TABANLI ERİŞİM DENETİMİ

İçerik Tabanlı Erişim Denetimi

- Korunan veri nesnelerine erişim, nesnelerin içeriklerini temel almaktadır.

ÖR:

- *Maaş verisi 5000TL ve üzerinde olan verilere, sadece insan kaynakları yöneticisi tarafından erişilebilir.*
- *Maaş verisi 5000TL'nin altında olan verilere, insan kaynakları yöneticisi ya da yardımcısı tarafından erişilebilir.*

İçerik Tabanlı Erişim Denetimi

İçerik Tabanlı Erişim Denetimi

İçeriden gelen tehditlere (insider threats) yönelik korunma için önemlidir.

İçeriği nedeni ile **hassas (sensitive) verinin** açık bir şekilde **belirtilmesine izin verir**.

Veriye erişim **kısıtlanır**.

İçerik Tabanlı Erişim Denetimi

- İlişkisel veritabanında → Verinin içeriği değiştiğinde, eğer verinin *yeni versiyonları* erişim denetim politikasının koşullarını sağlıyorsa

Sistem, politikayı otomatik olarak uygular.

İçerik Tabanlı Erişim Denetimi

İlişkisel veritabanında içerik tabanlı erişim denetimi için geliştirilen yaklaşım

View Düzeneği

View definition sorguları kullanılarak sütun alt kümelerini ve/veya relation üçlülerini içeren "*virtual relations*"ların tanımlanması

İçerik Tabanlı Erişim Denetimi

- ÖR: Sadece maaşı 5000TL'nin altında olan üçlüleri listeleyen bir *view* tanımlanabilir.

- Sorgu işlemi sırasında → DBMS, *view* üzerinde gerçekleştirilen sorgudaki koşullar ile *view* sorgu tanımındaki koşulları birleştirmektedir.

Kullanıcılar, bir *view*'a erişim yetkisine sahip ise

View'u sorgularken *view* tarafından filtrelenen veriye hiçbir zaman **erişemezler**.

İçerik Tabanlı Erişim Denetimi

Aynı tablo için farklı kullanıcılara farklı içerik tabanlı erişim denetim politikası uygulanması gerektiğinde

1. Erişim denetim politikası kadar *view* yaratılmalıdır.
2. Her kullanıcının doğru *view* ile yetkilendirilmesi gerekmektedir.

İçerik Tabanlı Erişim Denetimi

- Oracle DBMS → **Transparent query-rewriting**'ı temel alır.
- Kullanıcı, verilen tabloda sorgu gerçekleştirdiğinde;
  - DBMS, sorguya ek koşullar uygulayarak kullanıcının görmemesi gereken veriyi filtreleyerek sorguyu (kullanıcıya) *transparent* bir şekilde tekrar yazar.
  - Bu koşulların nasıl tanımlanacağı → **Virtual Private Mechanism (PVD)** ile gerçekleştirilir.

TIME-BASED ACCESS CONTROL

ZAMAN TABANLI ERİŞİM DENETİMİ

Zaman Tabanlı Erişim Denetimi

- Erişim denetim düzeneğindeki en önemli ihtiyaçlardan biri korunmada izinlerin zaman boyutudur.
- Kullanıcılara verilen yetkilendirmeler, kullanıcıların kurum içerisindeki etkinliklerine bağlı olmalıdır.

Kullanıcı veriye, sadece *ihtiyacı olduğu*

zaman periyodunda erişmelidir.

Zaman Tabanlı Erişim Denetimi

ÖR:

Proje dosyalarını yedeklemekle görevli olan sistem yöneticisi, dosyalara sadece Cuma günleri saat 3 pm ve 6 pm arasında erişebilir.

- Bu politika ile, sistem yöneticisinin veriye erişimi kısıtlandırılmakta ve veriyi çalması ihtimali azaltılmaktadır.

Zaman Tabanlı Erişim Denetimi

Yetkilendirme

- **U** : Kullanıcı kümesi
- **O** : Korunan nesneler kümesi
- **M**: Nesneler üzerinde gerçekleştirilebilecek eylemler kümesi

Yetkilendirme → **<s, o, m, pn, g>**

s, g ∈ U, o ∈ O, m ∈ M, pn ∈ {+, -}

- **s** : Yetkilendirilen kullanıcı
- **g** : *s*'yi yetkilendiren kullanıcı
- **+** : Pozitif yetkilendirme
- **-** : Negatif yetkilendirme

Zaman Tabanlı Erişim Denetimi

Periyodik Yetkilendirme

<[begin, end], P, auth>

- **begin** : Gün ifadesi
- **end** : Sabit (∞) ya da **begin**'e eşit ya da **begin**'den büyük bir gün ifadesi
- **P** : Periyodik zaman ifadesi (**begin**'den büyük ya da eşit, **end**'den küçük ya da eşit)
- **auth** : Yetkilendirme (authorization)

<[begin, end], P, (s, o, m, pn, g)>

Zaman Tabanlı Erişim Denetimi

Periyodik Yetkilendirme

`([1/1/2014, 31/12/2016]), Pazartesi, (Can, o1, read, +, Burak)`

- **Burak** tarafından onaylanan ve **Can**'ın **o1** nesnesini **1/1/2014-31/12/2016** tarihleri arasında her **Pazartesi okuma** hakkına sahip olduğunu belirten periyodik yetkilendirme

Zaman Tabanlı Erişim Denetimi

Periyodik Olmayan Yetkilendirme

- **P** periyodik zaman ifadesi olmayan yetkilendirmedir.

```
([1/1/2014, 31/12/2016]), (Can, o1, read, +, Burak)
```

- **Burak** tarafından onaylanan ve **Can**'ın **o1** nesnesini **1/1/2014-31/12/2016** tarihleri arasında **her an okuma** hakkına sahip olduğunu belirten periyodik yetkilendirme

Zaman Tabanlı Erişim Denetimi

Türetme (Derivation) Kuralı

([begin, end], P, A, <OP> $\mathcal{A}$)

- **begin** : Gün ifadesi
- **end** : Sabit (∞) ya da **begin**'e eşit ya da **begin**'den büyük bir gün ifadesi
- **P** : Periyodik zaman ifadesi
- **A** : Yetkilendirme
- **<OP>**: *WHENEVER*, *ASLONGAS*, *UPON* ifadelerinden biri
- $\mathcal{A}$: Boolean yetkilendirme ifadesi

Zaman Tabanlı Erişim Denetimi

```
([2014, 2015], Çalışma-günleri, (part-time-staff,*,read,+,Can)
  WHENEVER (staff,*,*,+,Can)∨(temporary-staff,*,read,+,Can))
```

- **part-time-staff**, **[2014, 2015]** tarihleri arasında herhangi bir **çalışma gününde herhangi bir nesneyi (*)**, aynı nesne için **staff herhangi bir hakka** ya da **temporary-staff okuma** hakkına sahip olduğunda **okuyabilir**.

Zaman Tabanlı Erişim Denetimi

```
([2014, 2015],Çalışma-günleri,(temporary-staff,doc,read,+,Can)
   ASLONGAS (summer-staff,doc,read,+,Can)
```

- **temporary-staff**, dokümanı **[2014, 2015]** tarihleri arasında herhangi bir **çalışma gününde**, aynı nesne için **summer-staff okuma** hakkına sahip olduğu sürece **okuyabilir**.

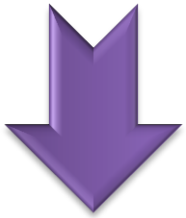
Zaman Tabanlı Erişim Denetimi

```
([2014, 2015],Çalışma-günleri,(Canan,fatura-ödeme,read,+,Can)
   UPON (Burak,fatura-ödeme,write,+,Can)
```

- **Canan**, **fatura-ödeme** nesnesini **[2014, 2015]** tarihleri arasında herhangi bir **çalışma gününde**, **Burak** **fatura-ödeme** nesnesine **yazması** üzerine **okuyabilir**.

Zaman Tabanlı Erişim Denetimi

RBAC modeline zaman boyutunun uygulanması ile



Temporal RBAC (TRBAC) modeli geliştirilmiştir.

Rollere atanan izinler, belirli zaman periyodları için geçerlidir.

Zaman Tabanlı Erişim Denetimi

- Kullanıcı, bir role sahip olmasına rağmen, role atanan bütün **izinlerin kullanımı** belirli bir zaman aralığı için geçerlidir.

- TRBAC → RBAC'i rollere atanan zaman aralığı ile genişletmektedir.

Zaman Tabanlı Erişim Denetimi

- TRBAC → Rollerin iki durumu olabilir:
  - **Aktif durum**
    - Rolün kullanılabildiği durum
  - **Aktif olmayan durum**
    - Rolün kullanılamadığı durum
    - Zaman aralığı dışında, rol her zaman aktif olmayan durumdadır.

LOCATION-BASED ACCESS CONTROL

KONUM TABANLI ERİŞİM DENETİMİ

Konum Tabanlı Erişim Denetimi

- Verinin güvenli kullanımı için konum önemli bir boyuttur.
- Kurumlar hassas veriye sadece kurum içinden ulaşılmasını istemektedir.
  - Fiziksel ve cyber güvenlik dikkate alındığında hassas veriye sadece **kurum içinden** ulaşılmalıdır.

Konum Tabanlı Erişim Denetimi

ÖR:

- *Kullanıcıların işlemlerini kaydeden video kayıtları* → Kullanıcının ekrandan verinin fotoğrafını çekip çekmediğinin kontrol edilmesi

- *Bir başka kullanıcıyı taklit ederek işlem yapmaya çalışan kötü niyetli kullanıcı* → Kullanıcıya konuma göre erişim denetim izni verilmesi durumunda, işlem sadece ofisten gerçekleştirilebilecektir.

Konum Tabanlı Erişim Denetimi

Konum tabanlı erişim denetimi

Yetkilendirmeler, erişimin onaylanacağı **konumu** belirten **ek parametre** içermektedir.

Yetkilendirme,

kullanıcı yetkilendirmede belirtilen konumda

*bulunmadığı sürece **aktif değildir**.*

Konum Tabanlı Erişim Denetimi

- İki ihtiyaç bulunmaktadır:

  1. Konumun ifade edilmesi için bir model
  2. Kullanıcı konumunu tespit edecek bir düzeneğin tanımlanması ve geliştirilmesi

Erişim denetimi kararının verilmesi kullanıcı konumuna bağlı olduğundan

Konum bilgisinin **güvenilir** olması önemlidir.

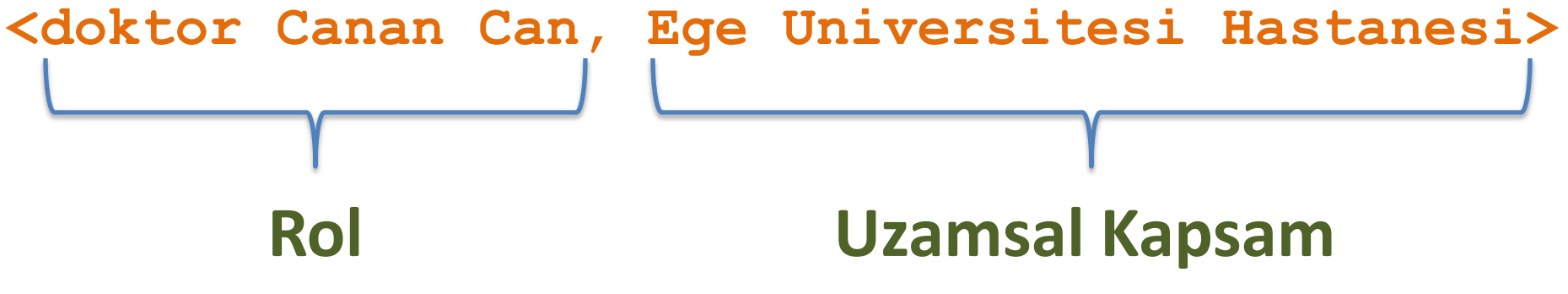
Konum Tabanlı Erişim Denetimi

- **GEO-RBAC** → Konumun ifade edilmesi için bir modeldir.
- Model **uzamsal rol** (spatial role) kavramını temel almaktadır.
- **Uzamsal kaplam/kapsam** (spatial extent)
  - Rolün tanımlandığı sınır (yol, şehir, kurum, vs.)
  - Kullanıcının, rolünü kullanabilmesi için konumlanabileceği bölge

Konum Tabanlı Erişim Denetimi

- Uzamsal rol **<r, e>** çifti ile tanımlanmaktadır.
  - r: Rol adı
  - e: Rolün uzamsal kapsamı

ÖR:



Konum Tabanlı Erişim Denetimi

- Geo-RBAC → Genel politikaların tanımlanabilmesi için **rol şeması (role schema)** kavramını sağlamaktadır.

- *Bir hastane ile ilişkilendirilmiş bir doktor, hastanede olduğu zaman tıbbi veriler üzerinde yetkilendirmeye sahiptir.*

<Doktor, Hastane>

Konum Tabanlı Erişim Denetimi

GEO-RBAC

Open GeoSpatial Consortium

(OGC, http://www.opengeospatial.org)

(Coğrafi Bilgi Sistemi Standardı) modeli ile uyumludur.

Konum Tabanlı Erişim Denetimi

- **Near Field Communication (NFC)** → Kullanıcı konumunu tespit edecek bir düzeneğin tanımlanmasına ve geliştirilmesine yönelik bir modeldir.
- RFID tabanlı yakınlık-kısıtlı (proximity-constrained) bir teknolojidir.
- Cihaz ve kullanıcı arasında temassız bir iletişim sağlamaktadır.

PURPOSE-BASED ACCESS CONTROL

AMAÇ TABANLI ERİŞİM DENETİMİ

Amaç Tabanlı Erişim Denetimi

- Mahremiyet-hassas verinin korunması için **verinin kullanım amacını** belirten erişim denetim politikaları önem kazanmaktadır.

Politikalar, **kişisel verinin toplanmasındaki amacı** belirtmelidir.

Belirtilen amacın dışındaki kullanımlar **anomali** olarak işaretlenir ve ek kontroller tetiklenir.

Amaç Tabanlı Erişim Denetimi

- Modelin temel aldığı kavramlar:
  - Verinin planlanan kullanım amacı
  - Erişim amaçları
- Amaçlar, **amaç ağacı (purpose tree)** içerisinde düzenlenmektedir.

Amaçların tanımlandığı hiyerarşik yapı

ORIGINATOR CONTROLLED ACCESS CONTROL – ORGCON/ORCON

YARATICI KONTROLLÜ ERİŞİM DENETİMİ

Yaratıcı Kontrollü Erişim Denetimi

- **ORi**nator **CON**trolled Access Control (ORGCON/ORCON)

- Özne diğer özneye, sadece nesnenin yaratıcısının izni ile nesneye erişim için haklar vermektedir.

Yaratıcı Kontrollü Erişim Denetimi

- Avrupa Birliği Komisyonu sekreteri hazırladığı dokümanları yorumlamaları için yardımcılarına gönderir.
- Yardımcılar dokümanı sekreterin izni olmadan **dağıtamaz**.
- Sekreter, **dağıtımı** kontrol etmektedir.

Yaratıcı Kontrollü Erişim Denetimi

- ORCON, erişim denetimin **dağıtılmış (decentralized)** bir sistemidir.
- Her yaratıcı, veriye kimin ihtiyacı olduğunu belirler.
- Veriye erişimi merkezi kurallar kümesi denetlemez.
- Erişim tamamen yaratıcının kontrolündedir.