Hibrid Politikalar

Yrd. Doç. Dr. Özgü Can

Chinese Wall (CW) Modeli

- **Bütünlük** ve **gizlilik** ile eşit olarak ilgilenen bir güvelik politikası modelidir.
- İşletmelerde meydana gelen **çıkar çatışmasına (*conflict of interest*)** yönelik politikaları tanımlar.

Chinese Wall Modeli

Amaç: İki müşteriyi temsil eden borsacının (trader) müşterileri arasında çıkar çatışmasını önlemektir.

Chinese Wall Modeli

Yatırım Şirketi

- Şirketlere ait yatırım kayıtları tutulmaktadır.
- Analistler, bu kayıtları kullanarak şirketlere danışmanlık yapmaktadır.
- Kerem → Analist
  - Müşterileri: İş Bankası ve Yapı Kredi Bankası

Her iki bankanın yatırımları çakışacağından, Kerem iki bankaya birlikte danışmanlık yapamaz.

Chinese Wall Modeli - Tanım

Tanım-1

Veritabanı nesneleri, şirket ile ilgili bilgi öğeleridir.

Tanım-2

Şirket veri kümesi (**CD** - **C**ompany **D**ataset) tek bir şirket ile ilgili nesneleri içerir.

Tanım-3

Çıkar çatışması (**COI** – **C**onflict **o**f **I**nterest) sınıfı , rekabet içindeki şirketlerin veri kümesini içerir.

Chinese Wall Modeli

- **COI(O)** → **O** nesnesini içeren **COI** sınıfıdır.
- **CD(O)** → **O** nesnesini içeren **şirket veri kümesi**dir.
- **Model** → **Her bir nesnenin tek** bir **COI sınıfına** ait olacağını varsayar.

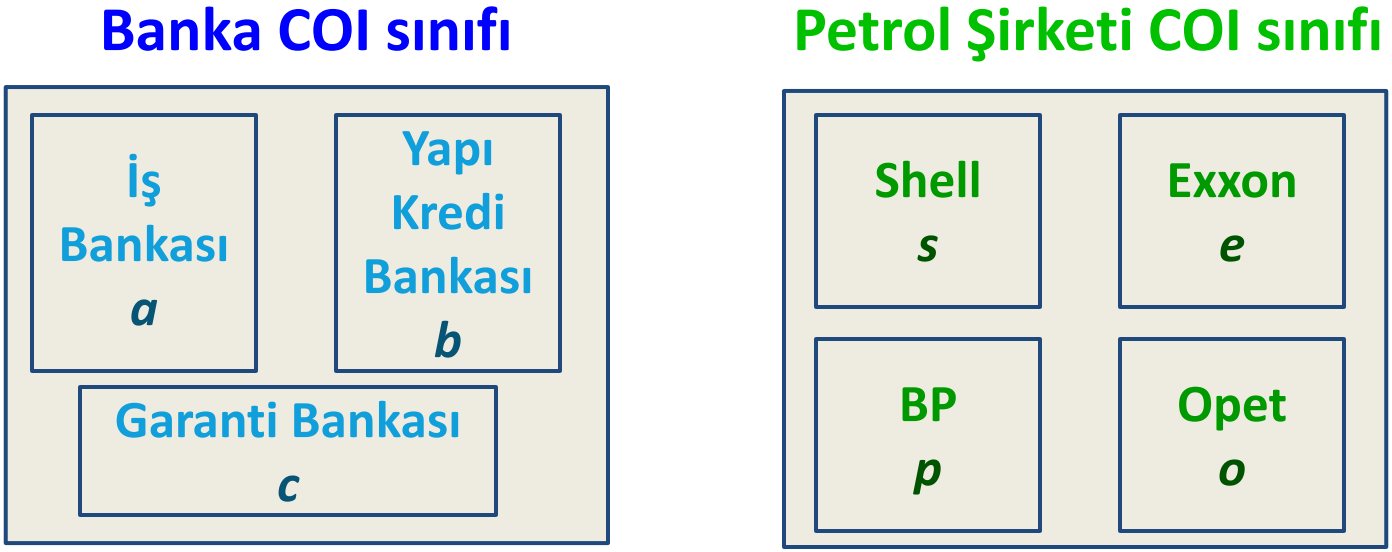
Chinese Wall Modeli

Kerem

- CD içerisindeki İş Bankası nesnelerine erişim yetkisi vardır.
- Yapı Kredi Bankası'nın CD'si İş Bankası ile ayni COI sınıfındadır.

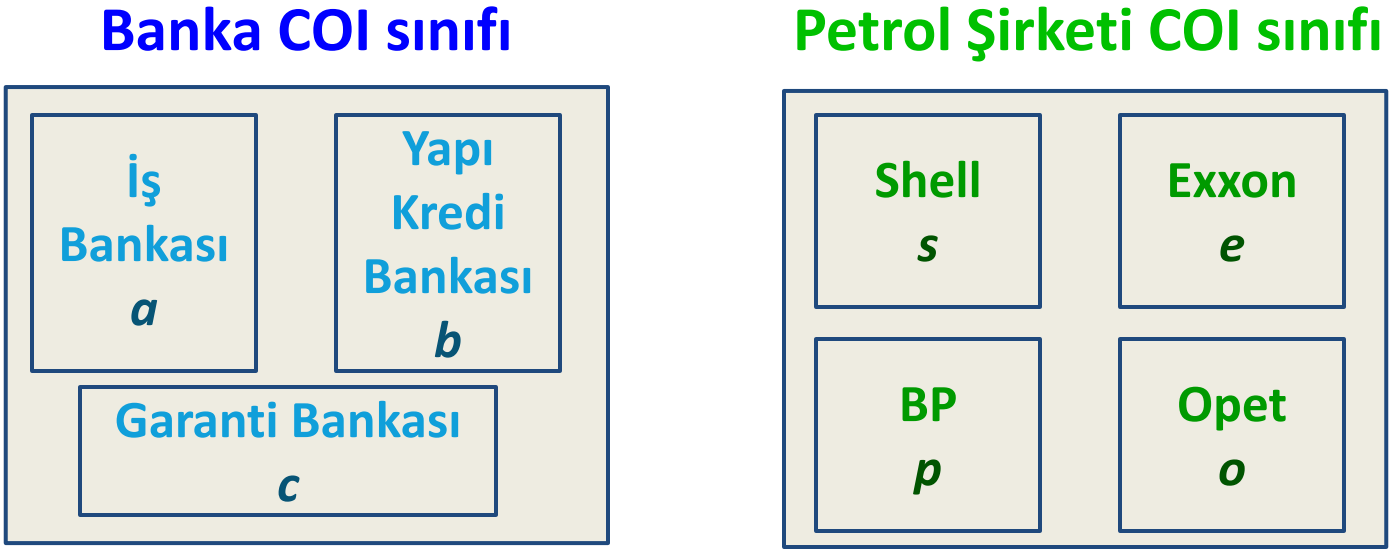
Kerem, Yapı Kredi Bankası'nın CD'si içerisindeki nesnelere **erişim hakkını** elde edemez.

Chinese Wall Modeli



- 2 **COI** sınıfı: Banka ve Petrol Şirketi
- **Banka** sınıfı → 3 CD içerir.
- **Petrol Şirketi** sınıfı → 4 CD içerir.
- Her **(COI, CD)** cifti bir küçük harf ile temsil edilir.
  - *(Banka COI, Garanti)* → *c*

Chinese Wall Modeli



- Aslı → Her bir COI için **birden fazla** CD'ye erişemez.
  - **İş Bankası CD** ve **Exxon CD**'ye ***erişebilir***.
  - **İş Bankası CD** ve **Garanti Bankası CD**'ye ***erişemez***.

Chinese Wall Modeli

- Kerem önce İş Bankası portföyü için, daha sonra Yapı Kredi Bankası portföyü için çalışmış olsun.
- Banka COI sınıfında sadece bir banka için çalışıyor olmasına rağmen, İş Bankası portföyünden öğrendiği bilgilerin bir çoğu hala geçerlidir.
- **Çıkar Çatışması** → İş Bankası portföyünden edindiği bilgileri kullanarak Yapı Kredi Bankası için yatırım yapmaktadır.

Chinese Wall Modeli

CW – Simple Security Condition (*Preliminary Version*)

PR(S) → ***S*** öznesinin okuduğu nesneler kümesi

S öznesi **O** nesnesini <u>sadece ve sadece</u> aşağıdaki kurallardan biri **doğru** ise okuyabilir:

1. **S** öznesinin eriştiği bir **O`** nesnesi vardır ve **CD(O`)=CD(O)**'dur.

2. Bütün **O`** nesneleri için, **O`∈ PR(S)⇒COI(O`)≠COI(O)**

Chinese Wall Modeli

(Chinese Wall) Simple Security Rule: S öznesinin **O** nesnesine erişimi sadece eğer nesne:

- **S** öznesi tarafından erişilmekte olan nesneler ile aynı şirket veri kümelerinde [**duvarın içinde (*within the wall*)**] ise

ya da

- farklı bir çıkar çatışması sınıfına ait ise

onaylanır.

Chinese Wall Modeli

- Başlangıç olarak; **PR(S)= Ø** ve başlangıç okuma isteğinin onaylandığı varsayılır.

- Bu varsayımlar doğrultusunda;
  - İş Bankası COI sınıfı ve Yapı Kredi Bankası COI sınıfı aynıdır. [**Banka COI sınıfı**]

*Bütün **O`** nesneleri için, **O`∈ PR(S)⇒COI(O`)≠COI(O)***
kuralı işleyeceğinden

Kerem, İş Bankası portföyünde daha önce çalıştığı için, Yapı Kredi Bankası portföyüne erişemeyecektir.

Chinese Wall Modeli

- *CW- Simple Security Condition* kuralının sonuçları öznenin haklarını (rights) etkilemektedir.

  1. Özne COI sınıfında bir CD'yi okumuş ise, bundan sonra öznenin COI sınıfında okuyabileceği diğer bütün nesneler aynı CD içerisindedir.

     - *Kerem, İş Bankası CD'sine eriştiği için Yapı Kredi Bankası CD'sine erişemeyecektir.*

Chinese Wall Modeli

- *CW- Simple Security Condition* kuralının sonuçları öznenin haklarını (rights) etkilemektedir.

  2. COI sınıfındaki her nesneye erişecek *min.* özne sayısı COI sınıfındaki CD'lerin sayısına eşittir.

*Petrol Şirketi COI sınıfında **4 CD** yer almaktadır.*

*COI sınıfındaki bilgiye erişim için **en az 4 analiste** ihtiyaç vardır.*

Herhangi bir yatırım şirketi, çıkar çatışması olmadan bu COI sınıfındaki bilgiye erişecek en az 4 analiste sahip olmalıdır.

Chinese Wall Modeli

- Pratikte;
  - Şirketlerin halka açıkladıkları bilgiler (ÖR: *raporlar, devlet komisyonlarına iletilen dosyalar, vb.*) Chinese Wall modeli tarafından dikkate alınmamaktadır.

Veri herkese açıktır.

Chinese Wall Modeli

- CW Modeli, "**sanitized**" ve "**unsanitized**" veri ile ilgilenmektedir.
- *CW-Simple Security Condition* → "**unsanitized**" veriyi kapsamaktadır.
- *CW-Simple Security Condition* → "**sanitized**" veriyi kapsamamaktadır.

CW-Simple Security Condition (Preliminary Version) **yeniden düzenlenmelidir**.

Chinese Wall Modeli

CW – Simple Security Condition

S öznesi **O** nesnesini sadece ve sadece aşağıdaki kurallarından birini sağlarsa **okuyabilir**:

1. **S** öznesinin eriştiği bir **O`** nesnesi vardır ve **CD(O`)=CD(O)**'dur.
2. Bütün **O`** nesneleri için, **O`∈ PR(S)⇒COI(O`)≠COI(O)**
3. **O** nesnesi "**sanitized**" bir nesnedir.

- **Kerem** ve **Aslı** aynı yatırım şirketinde çalışıyor.
- **Kerem** → **İş Bankası CD** içerisindeki nesneleri **oku**yabilmektedir.
- **Aslı** → **Yapı Kredi Bankası CD** içerisindeki nesneleri **oku**yabilmektedir.
- **Kerem** ve **Aslı** → Her ikisi de **Exxon CD** içerisindeki nesneleri **oku**yabilmektedir.
  - **Kerem** → **Exxon CD** içerisine **yaz**abilmektedir.

Kerem → **İş Bankası CD** içerisindeki nesneleri **oku**yarak, **Exxon CD** içerisindeki nesnelere **yaz**abilir.

Aslı → Bu bilgileri **oku**yabilir.

Çıkar Çatışması

Chinese Wall Modeli

CW – * Property

S öznesi **O** nesnesine sadece ve sadece aşağıdaki kuralları sağlarsa **yazabilir**:

1. CW-Simple Security Condition, **S** öznesinin **O** nesnesini okumasına izin verir.
2. **S** öznesi, farklı veri kümesinde (**CD(O`) ≠ CD(O)**) ve "**unsanitized**" olan **O`** nesnesini okuyamıyorsa

Chinese Wall Modeli

(Chinese Wall) *-property: Yazma izni sadece eğer:

– Erişim, *simple security* kuralı tarafından onaylanıyorsa

ve

– aşağıdaki kuralları sağlayan nesne okunamıyorsa:

- Yazma izni istenen nesne ile *farklı* veri kümesinde ise

ve

- "**unsanitized**" bilgi içeriyorsa

onaylanır.

Chinese Wall Modeli

- **Kerem** → **İş Bankası CD** içerisindeki nesneleri **oku**yabilmektedir. [**Kural 1**] ✓

- **İş Bankası CD** içerisindeki nesnelerin "**unsanitized**" olduğu varsayıldığında → [**Kural2**] ✗

Kerem → **Exxon CD** içerisine **yazamaz.**

- Eğer **S** öznesinin okuduğu bütün "**unsanitized**" (ayıklanmamış) nesneler aynı veri kümesinde yer alıyorsa **S** öznesi **O** nesnesine yazabilir.

Bell LaPadula & Chinese Wall

Bell LaPadula ve Chinese Wall modelleri birbirinden farklıdır.

CW

- Özneler herhangi bir **güvenlik etiketi** (security label) ile ilişkilendirilmemektedir.
- **Geçmiş erişimler** CW modelinin kontrollerinin temelini oluşturmaktadır.

BLP

- Özneler **güvenlik etiketleri** ile ilişkilendirilmektedir.
- **Geçmiş erişimler** ile ilgilenilmemektedir.

Bell LaPadula & Chinese Wall

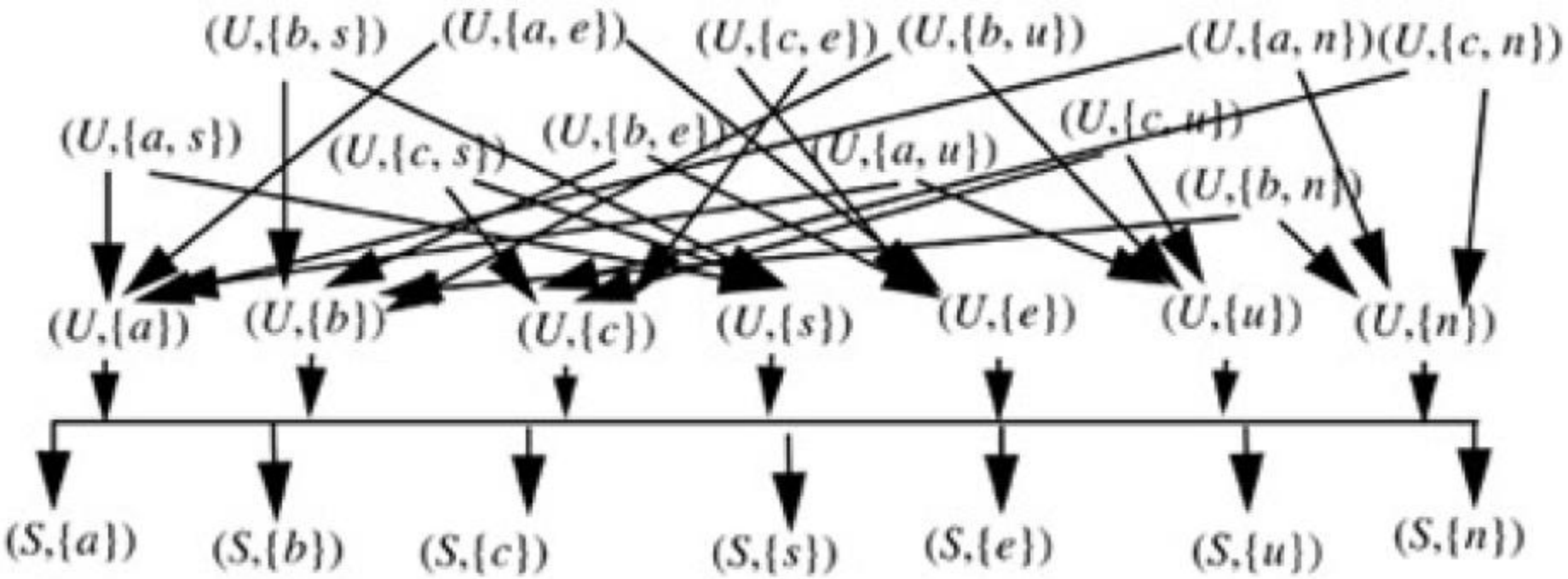
- CW modelinin, BLP modeline benzemesi için:
  - (COI, CD) çiftine bir güvenlik kategorisi atanmalıdır.

İki güvenlik seviyesi tanımlanır.

Sanitized (S) ve **Unsanitized (U)**

S dom U

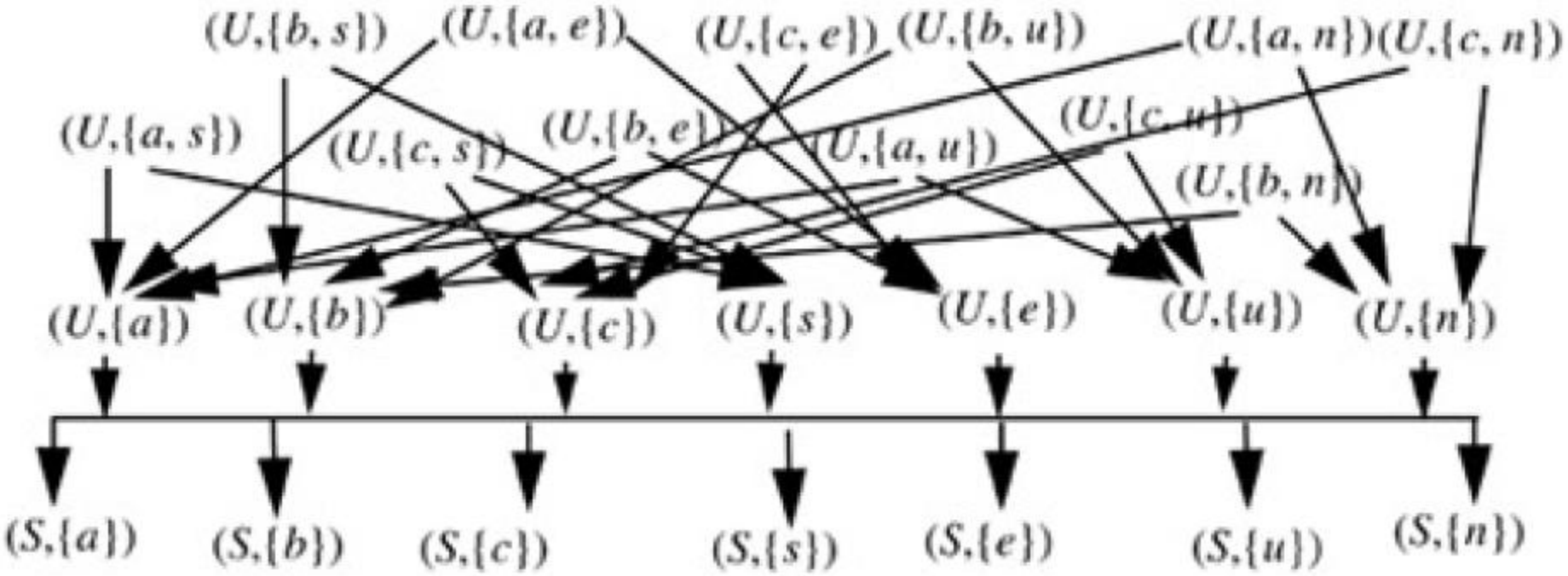
Bell LaPadula & Chinese Wall



- Her nesne iki nesneye dönüştürülmektedir:
  - **Sanitized**

  ve
  - **Unsanitized**

Bell LaPadula & Chinese Wall



- **(U, {a, s})** sınıfında bir güvenlik yetkilendirmesi olan özne → **(U, {a})** ve **(U, {s})** etiketlerine sahip nesneleri okuyabilir.

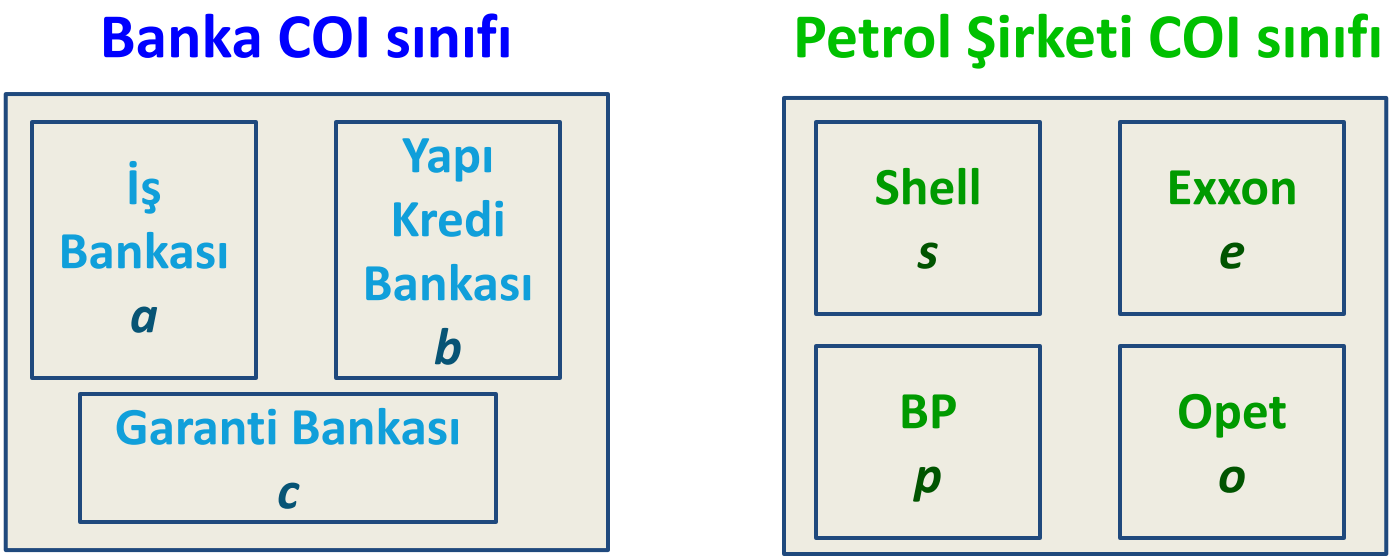
Bell LaPadula & Chinese Wall

- CW modelindeki her bir özneye kategoriler ile ilgili bir yetkilendirme atanmaktadır.
- Bu yetkilendirme, **birden fazla kategoriyi** içermemektedir.

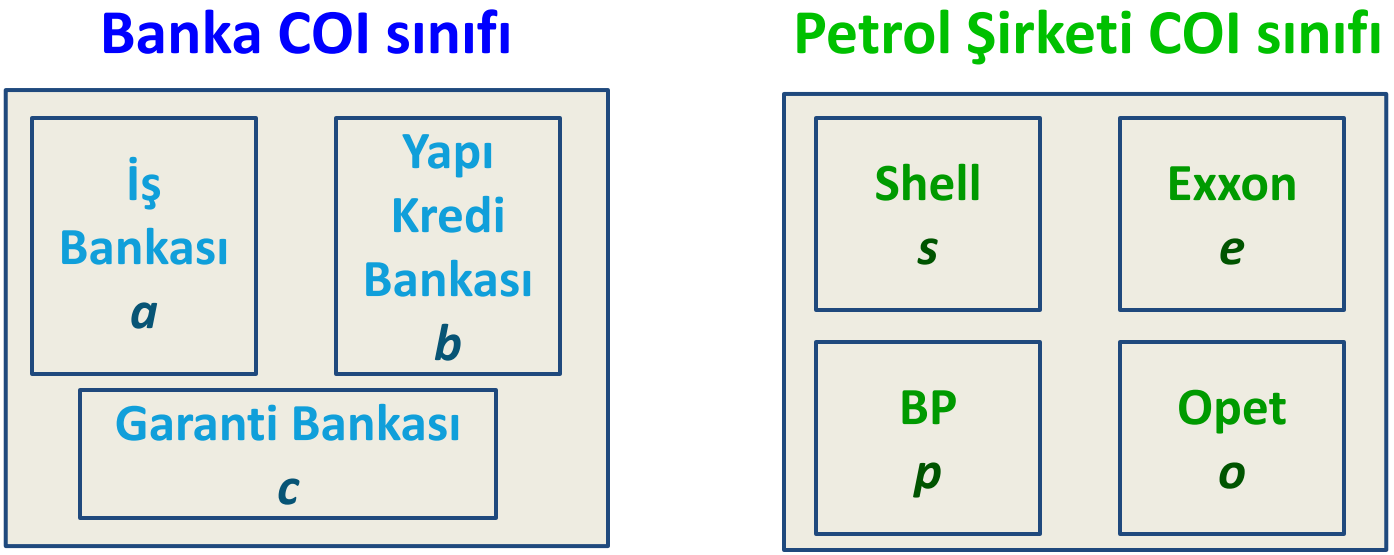
Bu durum, **aynı COI sınıfında yer alan CD'lere denk gelmektedir**.

Bell LaPadula & Chinese Wall

- Aslı → **İş Bankası** ve **BP** CD'lerini **oku**yorsa:
  - Aslı'nin süreçleri (process) **(U, {a, p})** kategorileri için yetkilendirilmiş olacaktır.



Bell LaPadula & Chinese Wall



- Özneler için 12 olası yetkilendirme vardır:
  - **Banka COI** sınıfı için → 3 olası yetkilendirme
  - **Petrol Şirketi COI** sınıfı için → 4 olası yetkilendirme
- Bütün özneler → Bütün "**sanitized**" verileri okuyabilir.

Bell LaPadula & Chinese Wall

- CW simple security kuralı & CW *-property sağlanmaktadır.
- BLP *-property → Girdi nesneleri kategorisi, cıktı nesneleri kategorisinin bir alt kümesidir.
  - Bu nedenle, girdi nesneleri "**sanitized**" dır ya da aynı kategori (aynı CD) içerisindedir.

Bell LaPadula & Chinese Wall

- BLP modeli, CW modelini kullanarak sistem durumunu yakalayabilmektedir (capture).
- Ancak, zaman içinde meydana gelen değişimleri yakalayamaz.
- Aslı hastalanır. → Leyla, Aslı'nın erişim yetkisi olan bir veri kümesine erişmek istemektedir.

Sistem, Leyla'nın bu veri kümesine erişmeye izni olup olmadığını nasıl bilecektir?

Bell LaPadula & Chinese Wall

- **CW Modeli** → **Erişim geçmişini** takip etmektedir.
- Böylelikle, Leyla'nın ilgili CD'ye erişim izni belirlenebilecektir.
- Eğer ilgili kategori Leyla'nın yetkilendirmesinde değil ise;
  - **BLP Modeli** → CW kısıtlarını ihlal edecek olan erişimin belirlenmesi için gerekli olan **geçmiş bilgisini** sağlamamaktadır.

Bell LaPadula & Chinese Wall

BLP Modeli → **CW** Modeline **benzeyemez**.

CW Modeli → **BLP** Modeline **benzeyebilir**.

Clark Wilson & Chinese Wall

- **Clark Wilson Modeli** → Erişim denetimine ek olarak **bütünlük** ile ilgili bütün yönlerle (*onaylama-validation, dogrulama-verification*) ilgilenmektedir.
- **CW Modeli** → Sadece erişim denetimi ile ilgilenmektedir.

CW Modeli → **Clark Wilson** Modeline tam olarak **benzeyemez**.

Clark Wilson & Chinese Wall

- Clark Wilson Modeli → **ER2 (Enforcement Rule)**

Kullanıcıları TP (transformation procedure) ve CDI'ler ile ilişkilendirmektedir.

- Eger "özne (subject)" ve "süreç (process)" birbirinin yerini alabilir olarak kabul edilirse;
  - Tek bir kişi, birden fazla süreç kullanarak aynı COI sınıfındaki CD'ler içersindeki nesnelere erişebilir.

Clark Wilson & Chinese Wall

- CW Modeli → Süreçleri onları yürütenden bağımsız olarak değerlendirecektir.

- Özne bir birey olması gerektiğinde ve süreçlerde öznenin yerine yürütüldüğünde,

CW modeli Clark Wilson modeli ile **tutarlı** olacaktır.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

- Sağlık kayıtları **bütünlük** ve **gizliliği** birleştiren politikalara gereksinim duymaktadır.
- Yatırım şirketlerinden farklı olarak → **Çıkar çatışması** kritik bir problem değildir.
- **Kritik problem** → Hasta gizliliği, kayıtların doğruluğu, personelin kimlik denetimi ve kayıtların güvencesi (assurance).

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

- Anderson* tarafından sunulan bir modelde, hasta gizliliğinin ve kayıt bütünlüğünün korunması için bütünlüğü ve gizliliği birleştiren politikalar sunulmaktadır.
- Anderson, politika içerisinde 3 varlık tanımlamaktadır.

* R. Anderson , "A Security Policy Model for Clinical Information Systems," Proceedings of the 1996 IEEE Symposium on Security and Privacy, pp. 3448 (May 1996).

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Tanım-1

Hasta, *sağlık kayıtlarının öznesidir ya da bu kişinin yerine tedavi ile ilgili izinleri veren bir etmendir (agent).*

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Tanım-2

***Kişisel sağlık bilgisi**, hastanın sağlığı ya da tedavisi ile ilgili olarak hastanın kimliğinin saptanmasına olanak veren bilgidir.*

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Tanım-3

***Klinik tedavi uzmanı**, kişisel sağlık bilgisine erişerek sağlık hizmeti alanında çalışan bir uzmandır.*

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

- Kişisel sağlık bilgisi sağlık kayıtları içerisinde saklanmaktadır.
- Politikada:
  - Kişisel sağlık bilgisi → Aynı anda **bir birey** ile ilgili bir bilgidir.
  - Bazı durumlara, sağlık kayıtları içerisinde anne-baba ile ilgili bilgiler de bulunabilir.

Özel kuralların belirlenmesi gerekir.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

- Politika, Clark Wilson modelinde belirtilen *onaylama ve uygulama kurallarına* benzer prensipler ile yönlendirilmektedir.

- Bu prensipler; tıp etiği, klinik tedavi uzmanlarının deneyimleri ve önerileri doğrultusunda belirlenmektedir.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Erişim Prensipleri

- Sağlık kayıtlarına erişim ile ilgili prensiplerdir.
- Kayıtları kimlerin okuyabileceğini ve kimlerin kayıtlarda değişiklik yapabileceğini belirtir.
- Denetçiler (auditor), sağlık kayıtlarına erişebilirler, ancak değişiklik yapamazlar.
- Hastanın izin verdiği klinik tedavi uzmanları sağlık kayıtlarını okuyup değiştirebilirler.
  - Klinik tedavi uzmanları çoğunlukla bir gruba dahil olduğundan, bu izin gruba dahil olan diğer uzmanları da kapsar.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Erişim Prensibi 1

- Her bir sağlık kaydı bir erişim denetim listesine sahiptir.
- Erişim denetim listesi kaydı okuyabilecek ve kayıtta değişiklik yapabilecek kişileri ya da grupları belirtir.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Erişim Prensibi 2

- Erişim denetim listesindeki klinik tedavi uzmanı (*sorumlu uzman*), diğer klinik tedavi uzmanlarını erişim denetim listesine eklemek için yetkilendirilmelidir.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Hastanın tedavi için izin vermesi gerektiğinden

Hastanın sağlık kayıtlarına kimin erişeceğini ve kayıtlarında değişiklik yapabileceğini bilme hakkı vardır.

Hasta ile ilgili olmayan bir klinik tedavi uzmanı, hastanın kayıtlarına eriştiğinde, hasta bu **bilgi sızmasından** haberdar olmalıdır.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Erişim Prensibi 3

- Sorumlu uzman hastayı, hastanın sağlık kaydı her açıldığında erişim denetim listesindeki isimler konusunda bilgilendirmelidir.
  - Acil durumlar dışında, hastadan izin almalıdır.
- Kayıtların *audit* edilmesini kolaylaştırmak için hatalı bilgi silinmemeli düzeltilmelidir.
- *Audit* işlemi; bütün erişimlerin, kim tarafından gerçekleştirildiği, erişim günü ve saati bilgileri ile birlikte kaydedilmesini gerektirir.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Erişim Prensibi 4

- Klinik tedavi uzmanı, sağlık kayıdına erişim tarihi ve saati kaydedilmelidir.

- Benzer bilgi, silme işlemi içinde tutulmalıdır.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

- Bir diğer prensip kümesi kayıtların yaratılması ve bilginin silinmesi ile ilgilenmektedir.
- Yeni bir sağlık kaydı yaratıldığında, klinik tedavi uzmanı ve hasta kayıda erişebilmelidir.
- Kayıt bir sevk işlemi sonucu yaratılmış olabilir.
  - Sevk edilen klinik tedavi uzmanı, sevk işlemi gerçekleştirilen kişinin sonuçlarına erişebilmelidir.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Yaratma Prensibi

- Sevk işlemi sonucu açılan bir kaydın erişim denetim listesinde hasta, sevk eden ve sevk edilen klinik uzmanları bulunabilir.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

- Sağlık kayıtlarının ne kadar sure ile saklanacağı durumlara/koşullara göre değişebilir.
  - Normalde 8 yıl sonra silinmektedir. Ancak, bazı durumlarda (ÖR: kanser vakalarında) daha uzun saklanabilmektedir.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Silme Prensibi

- Klinik bilgisi, uygun bir zaman dilimi geçmeden sağlık kaydından silinemez.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

- Kapsama (containment) bilgiyi korumayı amaçlamaktadır.
- Bir kayıttan diğer bir kayıda kopyalanan verinin yeni bir kullanıcı grubuna açıklanmasını engellemeyi garantilemektedir.
- Böylelikle, bir kayıttan kopyalan veriye sadece o kayıdın erişim denetim listesinde yer alan kişiler tarafından erişilecektir.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Kapsama Prensibi

- Bir sağlık kaydındaki veri, farklı bir sağlık kaydına sadece ve sadece ikinci kaydın erişim denetim listesi ilk kaydın erişim denetim listesinin bir **alt kümesi** ise **kopyalanabilir**.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

- Bir klinik tedavi uzmanı bir çok kayda erişim hakkına sahip olabilir.
- Eğer bu uzman rüşvet almış ya da şantaja maruz kalmış ise birçok sağlık kaydının gizliğinin ihlali söz konusu olabilir.
- Hastanın bilgilendirilmesi, bu tehdidi kısıtlamaktadır.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Kümeleme Prensibi

- Hasta verisinin kümelenmesi ile ilgili önlemler etkin olmalıdır.
- Hasta, sağlık kayıtlarının erişim denetim listesine yeni bir kişi eklenmesi durumunda bilgilendirilmelidir.

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

- Sistem, bu prensipleri uygulayacak düzenekleri gerçekleştirmelidir (*implementation*).

Klinik Bilgi Sistemleri İçin Güvenlik Politikası

Uygulama Prensibi

- Sağlık kayıtlarını isleyen herhangi bir bilgisayar sistemi belirtilen bu prensipleri uygulayacak alt sistemlere sahip olmalıdır.
- Bu uygulamanın etkinliği, bağımsız denetçilerin tarafından değerlendirmeye tabi olmalıdır.

Bell LaPadula & Clark Wilson

- Klinik Bilgi Sistemleri İçin Güvenlik Politikası modelinde yer alan **Kapsama Prensibi**, Bell LaPadula modelini uygulamaktadır.

*Bir sağlık kaydındaki veri, farklı bir sağlık kaydına sadece ve sadece ikinci kaydın erişim denetim listesi ilk kaydın erişim denetim listesinin bir **alt kümesi** ise **kopyalanabilir**.*

Bell LaPadula & Clark Wilson

- **Bell LaPadula Modeli**
  - Öznelerin güvenlik etiketlerinden daha çok olması nedeni ile → Nesnelere erisen **öznelere** odaklanmaktadır.
- **Klinik Bilgi Sistemi Modeli**
  - Hastaların ve sağlık kayıtlarının klinik tedavi uzmanı sayısından daha fazla olması nedeni ile → Özneler tarafından erişilen **nesnelere** odaklanmaktadır.

Bell LaPadula & Clark Wilson

- Clark Wilson modeli, Klinik Bilgi Sistemi modeli için bir çatı sağlamaktadır.
- Sağlık kayıtları ve kayıtlarla ilgili erişim denetim listeleri → **CDI**
- Sağlık kayıtlarını güncelleyen fonksiyonlar ve onların erişim denetim listeleri → **TP**

Bell LaPadula & Clark Wilson

- IVP'ler (Bütünlük Doğrulama Yordamı) birçok öğeyi onaylamaktadır:
  - Klinik tedavi uzmanı olarak tanımlanan kişi, klinik tedavi uzmanıdır.
  - Bir klinik tedavi uzmanı, sağlık kaydında yer alan bilgiyi onaylar/doğrular ya da onaylamıştır/doğrulamıştır.
  - Hastanın ya da klinik tedavi uzmanının, bir olay ile ilgili olarak bilgilendirilmesi gerekiyorsa, ilgili bilgilendirme gerçekleştirilir.
  - Hastanın ya da klinik tedavi uzmanının, bir izin (consent) vermesi gerekiyorsa, izin verilmeden işlem gerçekleştirilemez.

Bell LaPadula & Clark Wilson

- **Clark Wilson** modelinde yer alan *auditing* ile ilgili onaylama kuralı **CR4**:
  - Bütün kayıtlar *append-only* yapılarak

  ve

  - Hastalar erişim denetim listesi her değiştiğinde bilgilendirilerek

  sağlanmaktadır.

Bütün TP'ler, işlemle ilgili yeterli bilgiyi günlüğe (log) eklemelidir.