

# **Gizlilik Politikaları**

Yrd. Doç. Dr. Özgü Can

# Gizlilik Politikasının Amaçları

- Gizlilik politikası, aynı zamanda **bilgi akışı (information flow) politikası** olarak da adlandırılmaktadır.
- Bilgiyi yetkilendirilmemiş erişimlerden korumaktadır.
- Verinin yetkilendirilmemiş değişimi (integrity) ise ikincildir.

# Gizlilik Politikasının Amaçları

- ÖR: Askeriyede bir bölüğün yola çıkış tarihi gizli tutulmalıdır.
  - Tarih değişirse;
    - Sistemde ve kağıt üstündeki değişiklikler sonradan gerçekleştirilebilir.
    - Düşman tarihi öğrendiğinde → Saldırı gerçekleştirilebilir.

# Gizlilik Politikasının Amaçları

- Hükümetler;
  - Vatandaşların mahremiyetini korumalı
  - Kişisel bilgilerinin gizliliğini garantilemeli
- Gelir vergisi
- TC kimlik no

Belirli dokümanların ve bilginin dağıtımı  
sınırlandırılmalıdır.



Politikalar bu ihtiyaçları sağlamalıdır.

# Bell-LaPadula

- BLP
  - David Elliott Bell ve Leonard J. LaPadula tarafından geliştirilmiştir.
- Askeri ve hükümetSEL tarzda bir sınıflandırmadır.
- Diğer modellerin ve bilgisayar güvenliği teknolojilerinin geliştirilmesinde etkili olmuştur.
- Formel bir durum geçiş (state transition) modelidir.

# Bell-LaPadula

- Bilgi erişim yetkisi kümesinin *linear (total) ordering* ile sınıflandırılmasıdır.
- Bu yetki kümeleri, duyarlılık düzeyini (sensitivity level) temsil etmektedir.

# Linear Ordering

- Bir  $R$  (ör.  $\leq$ ) ilişkisi  $S$  kümesinde, aşağıdaki üç durumu sağlıyorsa bu ilişkinin *doğrusal sıralama (linear ordering)* olduğu söylenebilir:
  - Bütün  $a \in S$  için eğer  $aRa$  ise  
(*Yansıma-Reflexivity*)/(*Bütünlük/Tümlük-Totality*)
  - Eğer  $aRb$  ve  $bRa$  ise, bütün  $a, b \in S$  için  $a = b$  ise  
(*Antisimetri-Antisymmetry*)
  - Bütün  $a, b, c \in S$  için eğer  $aRb$  ve  $bRc$  den  $aRc$  ise  
(*Geçişlilik-Transitivity*)

# Linear Ordering

- $S = \{1, 2, 3\}$  kümesinde  $R (\leq)$  ilişkisi
- $R = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3)\}$ 
  - $1 \leq 1$  ,  $1 \leq 2$  ve  $2 \leq 3$ 
    - $(1, 1) \in R$  ve  $(1, 2) \in R$  ve  $(2, 3) \in R$
  - $3 \leq 2$  yazılamaz:
    - $(3, 2) \notin R$



# Bell-LaPadula

Bilgi erişim yetkisi yükseldikçe, bilginin duyarlılığı da artmaktadır.



Gizliliğin sağlanması ihtiyacı da artmaktadır.

# Bell-LaPadula

- BLP'de:
  - Öznenin *güvenlik erişim yetkisi (security clearance)*
  - Nesnenin *güvenlik sınıflandırması (security classification)*

vardır.

# Bell-LaPadula

## *Amaç:*

Güvenlik sınıflandırması  
özneden daha yüksek olan nesnelere  
okuma erişimi önlenmektedir.

# Bell-LaPadula

- Güvenlik etiketleri (security labels) **çok duyarlı** (most sensitive) ve **az duyarlı** (least sensitive) aralığında sınıflandırılmaktadır.
- Bell-LaPadula modelinde, güvenliğin (security) ve korunmanın (protection) açık bir ayrımı yoktur.
- Veri gizliliğine ve sınıflandırılmış bilgiye erişimin denetimine odaklanmaktadır.

# Bell-LaPadula

- Bell-LaPadula, erişim denetim modellerinden MAC ve DAC'i birleştirmektedir.
  - Model:
    - 2 MAC kuralı
      - Simple security property
      - \*-Property (star property)
    - 1 DAC kuralı
      - Discretionary security property
- tanımlar.

# Discretionary Security Property

*Erişim denetim matrisi (access control matrix)  
kullanılarak,  
kullanıcının kim olduğuna ve  
neye erişmek istediğine göre  
erişim izni verilmektedir.*

# Simple Security Property - Tanım

- $L(S) = I_s$ 
  - $S$  öznesinin güvenlik erişim yetkisi (security clearance)
- $L(O) = I_o$ 
  - $O$  nesnesinin güvenlik sınıflandırması
- Bütün güvenlik sınıflandırmaları  $I_i, i = 0, \dots, k$ 

***S** öznesi **O** nesnesini  
sadece ve sadece  
**O** üzerinde okuma hakkına sahip ve  $I_o \leq I_s$  ise  
okuyabilir.*

# Simple Security Property

Belirli bir güvenlik düzeyindeki özne,  
daha yukarıda ki güvenlik düzeyinde bulunan  
nesneyi okuyamaz. [No Read Up]



# Bell-LaPadula

Güvenlik Düzeyi	Özne	Nesne
TOP SECRET (TS)	Bob	Personel Dosyaları
SECRET (S)	Alice	Elektronik Mail Dosyaları
CONFIDENTIAL (C)	Bruce	Etkinlik Log Dosyaları
UNCLASSIFIED(UC)	Sally	Telefon Listeleri Dosyası

- Bob, bütün dosyaları okuyabilir.
- Bob ve Alice, Etkinlik Log Dosyalarını okuyabilir.
- Bruce, Personel ve Elektronik Mail Dosyalarını okuyamaz.
- Sally, sadece Telefon Listelerini okuyabilir.

# Bell-LaPadula

Güvenlik Düzeyi	Özne	Nesne
TOP SECRET (TS)	Bob	Personel Dosyaları
SECRET (S)	Alice	Elektronik Mail Dosyaları
CONFIDENTIAL (C)	Bruce	Etkinlik Log Dosyaları
UNCLASSIFIED(UC)	Sally	Telefon Listeleri Dosyası

- Bob, *personel* dosyalarının kopyasını *etkinlik log* dosyasına kopyalarsa → Bruce personel dosyalarını okuyabilir.
  - Bruce, daha yüksek güvenlik düzeyindeki dosyaları okuyabilecektir.

# **\*-Property**

*S öznesi O nesnesine,  
sadece ve sadece*

*O öznesine yazma hakkına sahip ve  $I_s \leq I_o$   
olduğunda yazabilir.*

Belirli bir güvenlik seviyesindeki özne,  
daha alt güvenlik seviyesindeki nesneye  
yazamaz. [No Write Down]

# Bell-LaPadula

Güvenlik Düzeyi	Özne	Nesne
TOP SECRET (TS)	Bob	Personel Dosyaları
SECRET (S)	Alice	Elektronik Mail Dosyaları
CONFIDENTIAL (C)	Bruce	Etkinlik Log Dosyaları
UNCLASSIFIED(UC)	Sally	Telefon Listeleri Dosyası

- Bob (TS), *personel* dosyalarının kopyasını *etkinlik log* dosyasına (C) kopyalayamaz.

# Bell-LaPadula



Kişinin güvenlik sınıflandırmasında daha alt seviyede bulunan dosyaya yazması neden istenmemektedir?

Güvenli bir sistem,  
“simple security condition” ve  
“\*-property” yi sağlar.

# Basic Security Theorem - Tanım

- $\Sigma$ : Başlangıç durumu  $\sigma_0$  olan güvenli bir sistem ve
- $T$ : Durum değişim kümesi olsun.

*Eğer,  $\forall t \in T$ ,*

*“simple security condition” ve “\*-property”*

*özelliklerini koruyorsa,*

*bütün  $\sigma_i$  durumları güvenlidir.*

# Basic Security Theorem

- Model, her bir güvenlik sınıfına kategoriler kümesi eklenerek genişletilebilir.
- Her bir kategori bir bilgiyi ifade eder.
- Birden fazla kategoriye\* yerleştirilen nesne, o kategorilerin bilgilerine sahiptir.
- Kategoriler “*need to know*” prensibinden meydana gelmektedir.

\* Bazı dokümanlarda kategori (category) ifadesi yerine compartment (bölüm) kullanılmaktadır.

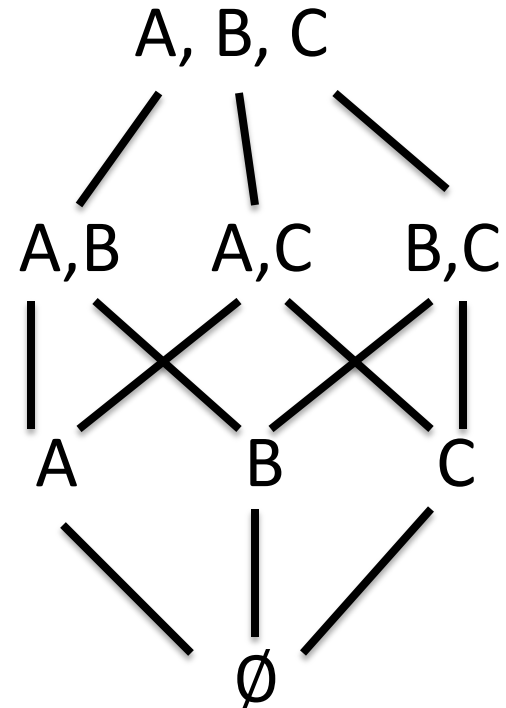
# **“Need-to-know” Prensipli**

*Öznenin işlevlerini gerçekleştirmesi için,  
nesneyi okuması gerekmiyorsa,  
özne nesneyi okumamalıdır.*



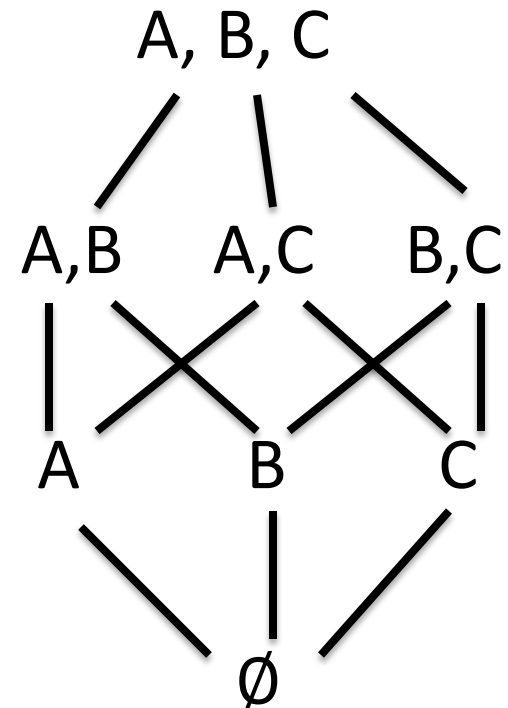
# Basic Security Theorem

- Kategoriler kümesi =  $\{A, B, C\}$
- Kişinin erişebileceği kategoriler kümesi:
  - $\emptyset, \{A\}, \{B\}, \{C\}, \{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}$
- Kategori kümesi  $\subseteq$  (alt küme) için *linear ordering*'i sağlamaktadır.



# Basic Security Theorem

- Bob; (SECRET, {B}) ve Alice; (TOP SECRET, {A, C}) seviyeleri için erişim yetkisine sahiptir.
- Bir doküman (CONFIDENTIAL, {B}) olarak sınıflandırılabilir.

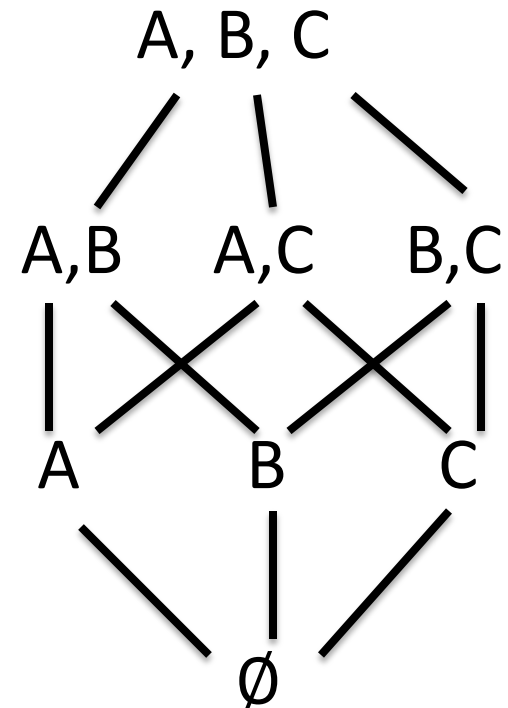


## NOT:

Öznelerin, güvenlik seviyesine ait erişim yetkisi vardır.  
Nesneler, bir güvenlik seviyesindedir.

# Basic Security Theorem

- Güvenlik seviyeleri erişimi değiştirmektedir.
- Kategoriler, “*need to know*” prensibinde çalıştıkları için ;
  - {A,C} kategorisine erişim hakkı olan kişinin, {B} kategorisine erişim hakkına ihtiyacı olmayabilir.
  - Bu nedenle → Öznenin güvenlik erişim yetkisi, nesnenin güvenlik sınıflandırmasından yüksek olsa bile okuma izni yoktur.



# Dom (Dominates) - Tanım

*Eğer  $L' \preceq L$  ve  $C' \preceq C$  ise,  
 $(L, C)$  güvenlik seviyesi  
 $(L', C')$  güvenlik seviyesini  
baskılar (dominates).*

*$(L, C)$  dom  $(L', C')$  yanlış ise  
 $(L, C) \neg\text{dom } (L', C')$ 'dur.*

# Örnek

- Bob; (SECRET, {A, B}) güvenlik seviyesinde erişim yetkisine sahiptir.
- DokA; (CONFIDENTIAL, {A})
- DokB; (SECRET, {B, C})
- DokC; (SECRET, {B}) sınıflandırmalarına sahiptir.
- **Bob dom DokA**  
 $\text{CONFIDENTIAL} \leq \text{SECRET}$   
 $\{A\} \subseteq \{A, B\}$
- **Bob  $\neg$ dom DokB**  
 $\{A, B\} \not\subseteq \{B, C\}$
- **Bob dom DokC**  
 $\text{SECRET} \leq \text{SECRET}$   
 $\{B\} \subseteq \{A, B\}$

# Simple Security Condition - Tanım

***S** öznesi **O** nesnesini  
sadece ve sadece*

***O** nesnesini okuma hakkına sahip ve **S dom O** ise  
okuyabilir.*

# Örnek

- Bob; (SECRET, {A, B})
- Alice; (SECRET, {A, B, C})  
güvenlik seviyesinde erişim yetkilerine sahiptir.
- DokA; (CONFIDENTIAL, {A})
- DokB; (SECRET, {B, C})  
sınıflandırmalarına sahiptir.

- **Bob dom DokA**  
 $\text{CONFIDENTIAL} \leq \text{SECRET}$   
 $\{A\} \subseteq \{A, B\}$
- **Bob  $\neg$ dom DokB**  
 $\{A, B\} \not\subseteq \{B, C\}$
- Alice DokB'yi okuyup, içeriğini DokA'ya yazabilir.  $\rightarrow$  Bob DokA'yı okuyarak DokB'ye erişmiş olur.

# **\*-Property - Tanım**

***S** öznesi **O** nesnesine,  
sadece ve sadece*

***O** nesnesine yazma hakkına sahip ve **O dom S** ise  
yazabilir.*



# Örnek

- Bob; (SECRET, {A, B})
- Alice; (SECRET, {A, B, C})  
güvenlik seviyesinde erişim yetkilerine sahiptir.
- DokA; (CONFIDENTIAL, {A})
- DokB; (SECRET, {B, C})  
sınıflandırmalarına sahiptir.

- **Bob dom DokA**

**CONFIDENTIAL  $\leq$  SECRET**

**$\{A\} \subseteq \{A, B\}$**

- **DokA  $\neg$ dom Alice**

**SECRET  $\not\leq$  CONFIDENTIAL**

**$\{A, B, C\} \not\subseteq \{A\}$**

# Örnek

- Albay; (SECRET, {A, B})
- Binbaşı; (SECRET, {B})
- Albay, binbaşıya mesaj göndermek isterse, bu mesaj;
  - En fazla (SECRET, {B}) seviyesinde olmalıdır.



(SECRET, {B})  $\neg$ dom (SECRET, {A, B})

**\*-Property özelliğini ihlal etmektedir.**

# Bell-LaPadula

- Özne, max. güvenlik seviyesine ve mevcut güvenlik seviyesine sahip olabilir.
- Max. güvenlik seviyesi, mevcut güvenlik seviyesini baskılamalıdır (dominates).
- Özne, diğer varlıklar ile mesajlaşabilmek için, güvenlik seviyesini max.'dan daha aşağı güvenlik seviyesine düşürebilir.

# Örnek

- Albay; (SECRET, {A, B})
- Binbaşı; (SECRET, {B})
- Albay, binbaşıya mesaj göndermek isterse;
  - Güvenlik seviyesini (SECRET, {B})'ye düşürebilir.



(SECRET, {A, B}) dom (SECRET, {B})