Güvenlik Politikaları

Yrd. Doç. Dr. Özgü Can

Güvenlik Politikaları

- Güvenlik politikası, sistem için “güvenli” olanı tanımlar.
- Informal ya da matematiksel olarak ifade edilebilir.

Güvenlik Politikaları - Tanım

Güvenlik politikası, sistem durumlarını **yetkilendirilmiş ya da güvenli** durumlar ve **yetkilendirilmemiş ya da güvensiz** durumlar kümelerine ayıran bir durumdur.

Güvenlik Politikaları

- Güvenli bir sistemi tanımlayabileceğimiz içeriği (context) ayarlar.

- Bir politika tanımında güvenli olan, bir başka politika tanımında güvenli olmayabilir.

Güvenlik Politikaları - Tanım

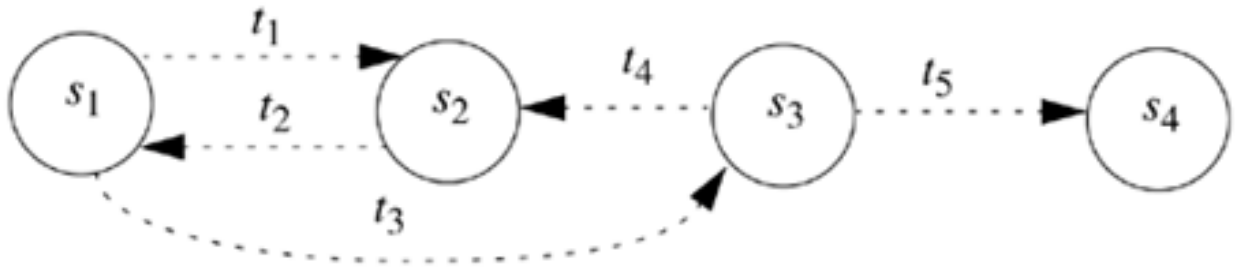
Güvenli bir sistem,

güvenli durumda çalışan

ve

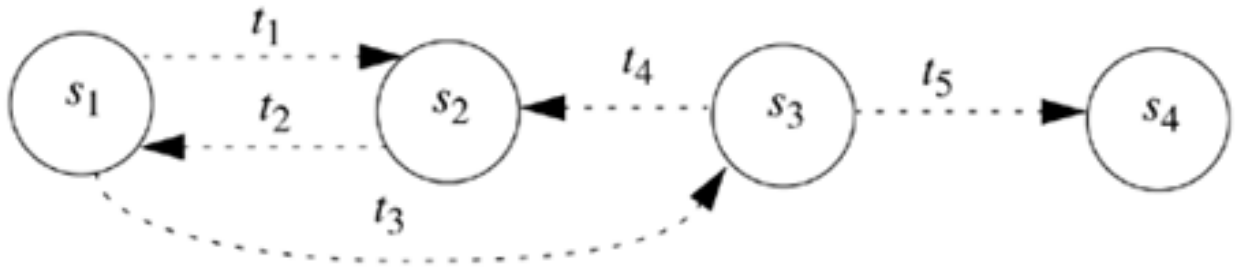
güvensiz duruma girmeyen sistemdir.

Güvenlik Politikaları



- Finite-state machine:
  - 4 durum & 4 geçiş (transition)
- Güvenlik politikası durumları yetkilendirilmiş ve yetkilendirilmemiş kümelere ayırır:
  - Yetkilendirilmiş durumlar A = $\{s_1, s_2\}$
  - Yetkilendirilmemiş durumlar UA = $\{s_3, s_4\}$

Güvenlik Politikaları



- Sistem güvenli değil:
  - Hangi yetkilendirilmiş durumda başlarsa başlasın yetkilendirilmemiş duruma girmektedir.
- s_1 ve s_3 arasındaki geçiş (t_3) olmazsa → Sistem güvenilir olacaktır.
  - Sistem, yetkilendirilmiş durumdan yetkilendirilmemiş duruma girmeyecektir.

Güvenlik Politikaları - Tanım

- **X** → Varlıklar kümesi

  ve

- **I** → Herhangi bir bilgi (Information) olsun.

Eğer **X**'in hiçbir üyesi **I** hakkında bir bilgi elde edemiyorsa,

X'e göre **I** gizlilik (confidentiality) özelliğine sahiptir.

Güvenlik Politikaları

- Gizlilik, bilginin belirli bir varlıklar kümesine açıklanmayacağını (disclose) belirtmektedir.
  - Bilgi, başka varlık kümelerine açıklanabilir.
- **X** kümesine üyelik çoğunlukla örtülüdür (implicit).
  - Gizli bir dokümandan bahsedildiğinde:
    - Bazı varlıkların dokümana erişimi vardır.
    - Yetkilendirilmemiş varlıkların kümesi **X** kümesini oluşturur.

Güvenlik Politikaları - Tanım

- **X**→ Varlıklar kümesi

  ve

- **I** → Bilgi ya da kaynak olsun.

Eğer **X**'in bütün üyeleri **I**'ya güveniyorsa,

X'e göre **I** bütünlük (integrity) özelliğine sahiptir.

Güvenlik Politikaları

- Bilginin kendisine güvenmeye ek olarak, **X**'in üyeleri:
  - Bilginin transferi ya da saklanması sırasında değiştirilmediğine güvenmektedirler. → Verinin Bütünlüğü (Data Integrity)

Güvenlik Politikaları

Köken bütünlüğü (Origin Integrity)

Aslıyla Aynılığını Kanıtlama (Authentication)

I, başka bir bilgi ya da varlıkla ilgili köken bir bilgi ise;

X'in üyeleri bilginin doğru ve değiştirilmemiş olduğuna güvenirler.

Güvenlik Politikaları

Güvence (Assurance)

I bir kaynak ise;

Bütünlük, kaynağın doğru bir şekilde işlediğini belirtir.

Gizlilikte olduğu gibi, bütünlükte de X' e üyelik örtülüdür (implicit).

Güvenlik Politikaları - Tanım

- **X** → Varlıklar kümesi

  ve

- **I** → Kaynak olsun

Eğer **X**'in bütün üyeleri **I**'ya erişebiliyorsa,

X'e göre **I** kullanılabilirlik (availability) özelliğine sahiptir.

Güvenlik Politikaları

- Kullanılabilirlik **X**'in üyelerinin
  - ihtiyaçlarına,
  - kaynağın yapısına ve
  - kullanımına göre

  değişebilir.

Güvenlik Politikaları

- Kitap satış sitesinde, kitap alımı işleminde servis süresi 1 saat → Kullanıcının kullanılabilirlik ihtiyacını karşılayabilir.

- Sağlık sistemi sunucusunun bir alerji hastası ile ilgili işlem isteğine cevap süresi 1 saat → Acil doktorunun kullanılabilirlik ihtiyacını karşılamaz.

Güvenlik Politikaları

- Güvenlik politikası;
  - gizlilik,
  - bütünlük ve
  - kullanılabilirlik

  ile ilgili bütün durumları değerlendirir.

Güvenlik Politikaları

Gizlilik ile ilgili:

- Yetkilendirilmemiş varlıklara bilginin sızması ile ilgili durumları tanımlar.
  - Bu tanımlama, sadece hakların sızdırılmasını değil, aynı zamanda bilgi akışını (information flow) da içerir.
- **Bilgi Akışı (Information Flow)**
  - Hakların sızdırılması olmadan, bilginin illegal bir şekilde iletilmesidir.

Güvenlik Politikaları

Gizlilik ile ilgili:

- Politika, yetkilendirmedeki dinamik değişikler ile başa çıkabilmek için bir *zaman (temporal)* elemanını da içermelidir.
  - ÖR: Bir şirket için çalışan sözleşmeli personelin sistemdeki dosyalara erişim hakkı sözleşmesi yenilenmediğinde sonlandırılmalı ve dosyalara erişim hakkı olmamalıdır.
- Gizlilik ile ilgili politikalar → Gizlilik politikası

Güvenlik Politikaları

Bütünlük ile ilgili:

- Güvenlik politikası,
  – bilginin değiştirilebileceği yetkilendirilmiş yolları
  ve
  – bilgiyi değiştirmeye yetkili varlıkları
  tanımlar.

Güvenlik Politikaları

Bütünlük ile ilgili:

- Yetkilendirme farklı ilişkilerden elde edilebilir ve dış etkiler yetkilendirmeyi sınırlayabilir.
  - **Görev Ayrılığı (Separation of Duties, SoD) ***
    - Bir işlemi tamamlamak için birden fazla varlığa ihtiyaç duyulur.
    - Varlığın işlemi tek başına tamamlamasını yasaklar.

* http://www.sans.edu/research/security-laboratory/article/it-separation-duties

Güvenlik Politikaları

Bütünlük politikası:

- Güvenlik politikasının verinin hangi koşullar altında değiştirilebileceğini belirten kısımlarıdır.

Güvenlik Politikaları

Kullanılabilirlik ile ilgili:

- Güvenlik politikası hangi servislerin sağlanması gerektiğini tanımlar.
- Aynı zamanda, servisler ile birlikte kullanılacak parametreleri de belirler.
  - ÖR: Browser, web sayfalarını indirebilir, ancak Java appletlerini indiremez.

Güvenlik Politikaları

Kullanılabilirlik ile ilgili:

- Güvenlik politikası, servis düzeyi isteyebilir.
  - **Servis kalitesi (quality of service)** ile direkt olarak ilgilidir.
    - ÖR: Yapılmış bir *authentication* isteğine 1 dk. içerisinde cevap verilmesi

Güvenlik Politikaları

- Güvenlik politikası, sistemin istenilen özelliklerinin durumunu formel olarak belirtir.
  - Eğer sistemin güvenirliği kanıtlanabiliyorsa;
    - Formel açıklama, tasarımcıların ve uygulayıcıların istenen özelliklerin sağlandığını kanıtlamasına izin verecektir.
  - Eğer formel kanıt mümkün değilse;
    - Analist istenen özellikleri bazı girdi kümeleri için test eder.

Güvenlik Politikaları

- Pratikte;
  - Daha az formel olan bir güvenlik politikası yetkilendirilmiş durumları tanımlar.
- Güvenlik politikası genellikle;
  - Kanunlar, organizasyon politikaları ve çevresel faktörleri içeren politikanın belirttiklerinin, politikayı okuyan tarafından anlaşıldığını kabul eder.
  - Güvenlik politikası; eylemleri, yetkilendirilmiş kullanıcıları ve yetkilendirilmiş kullanımı tanımlar.

Güvenlik Politikaları - Örnek

- Üniversite, öğrencilerin birbirlerinin ödevlerini (*izinli ya da izinsiz*) kopyalamalarını yasaklamaktadır.
  - Ödevini lab'da yapan bir öğrenci (A), başka bir öğrencinin (B) ödevini korumadığını görür ve kopyalar.

Güvenlik Politikaları - Örnek

Öğrenciler güvenlik politikasını ihlal etmiş midir?

- A ✗
  - Sadece ödevini korumamıştır.
  - Güvenlik politikası dosyaların korunması ile ilgili bir eylem belirtmemektedir.
- B ✓
  - Güvenlik politikası ödevlerin kopyalanmasını yasaklamaktadır.

Güvenlik Politikaları

Öğrencinin ödevi kopyalaması ve bu eyleme izin verilmesi **düzeneği politika ile karıştırmaya** yol açmaktadır.

Güvenlik Politikaları - Tanım

Güvenlik düzeneği,

güvenlik politikasının kısımlarını yerine getiren bir varlık ya da yordamdır.

Güvenlik Politikaları - Örnek

- Politika → Hiçbir öğrenci, başka bir öğrencinin ödevini kopyalayamaz.

- Düzenek → Dosya erişim denetimi
  - Eğer öğrenci (A), ödev dosyasının diğer öğrenci tarafından (B) okunmasını önleyecek şekilde izin ayarlarını tanımlamış olsaydı, B dosyayı kopyalayamayacaktı.

Güvenlik Politikaları - Örnek

- Şirket, sistemde yer alan dosyaların yedeğini almaktadır.
  - Yedekleme teypleri (backup tapes) bankada saklanmaktadır.
  - Sadece yetkilendirilmiş personelin yedekleme teyplerine erişim hakkı bulunmaktadır.
- Yedekleme teyplerinin ofisten bankaya ya da bankadan ofise iletiminde güvenlik düzenekleri dikkate alınmalıdır. → Teknik bir kontrol değildir.
  - İşlemsel ya da yordamsal denetimler de güvenlik düzeneğidir.

Güvenlik Politikaları

- Güvenlik politikaları çoğu zaman açık (explicit) değil örtülüdür (implicit).
  - Özellikle, politika düzenek üzerinden tanımlanmış ise karışıklığa neden olabilir.
    - ÖR: Bir eylemi bir düzenek önlüyorken diğer düzenekler izin veriyor olabilir.

Güvenlik Politikaları - Örnek

- UNIX işletim sisteminde;
  - A kullanıcısı B kullanıcısının dosyalarını silemez.
- Buradan çıkarılan güvenlik politikası:

  Kullanıcı;
  - Başka bir kullanıcının dosyasını silemez ya da bozamaz
  - Korunmamış dosya okunabilir
- UNIX işletim sisteminin kullanıldığı:
  - Küçük bir kullanıcı grubu varsa politika yeterli
  - Enstitüler, devlet ya da ticari kurumlarda bu politika yeterli değildir.

Güvenlik Politikaları - Tanım

Bir *politika modeli*,

belirli bir politikayı ya da politikalar kümesini temsil eden bir modeldir.

Güvenlik Politikası Türleri

- Gizlilik, bütünlük ve kullanılabilirlik düzeylerine göre her bir kurumun kendi ihtiyaçları vardır.
- Her bir kurum politikası, o kurumun ihtiyaçlarını belirtmektedir.
  - Askeri güvenlik politikası
  - Ticari güvenlik politikası
  - Gizlilik politikası
  - Bütünlük politikası

Güvenlik Politikası Türleri

Askeri Güvenlik Politikası

Bir askeri güvenlik politikası

(aynı zamanda devlet politikası)

temel olarak **gizliliği** sağlamaya yönelik olarak geliştirilmiş bir güvenlik politikasıdır.

Güvenlik Politikası Türleri

Ticari Güvenlik Politikası

Bir ticari güvenlik politikası

temel olarak **bütünlüğü** sağlamaya yönelik olarak geliştirilmiş bir güvenlik politikasıdır.

Güvenlik Politikası Türleri - Örnek

- Bir banka bilgisayarının gizliliğinin ihlal edilmesi sonucu bir müşterinin hesap bilgileri açığa çıkarsa;
  - Müşteri hesabını başka bankaya alır.
  - Bankanın kaybı küçük çaplıdır.
- Bankadaki hesapların bütünlüğü ihlal edilirse;
  - Müşteri hesaplarının bakiyeleri değiştirilebilir.
  - Bankaya finansal olarak zarar verici etkileri olacaktır.

Güvenlik Politikası Türleri - Tanım

İşleme-dayalı Bütünlük Politikası

(Transaction-oriented Integrity Policy)

- ÖR: Veritabanı işlemleri
  - Eylemlerin veritabanına eklenmesi ve silinmesi arasında tutarlılık olmalıdır.

Güvenlik Politikası Türleri - Tanım

İşleme-dayalı Bütünlük Politikası

(Transaction-oriented Integrity Policy)

- ÖR: Müşteri hesaplar arasında para transferi gerçekleştirirken, işlemin iki kısmı vardır:
  - Birinci hesap borçlandırılır.
  - İkinci hesap alacaklandırılır.
- İyi biçimlendirilmiş (well-formed) bir işlemde, işlem kesintiye uğrarsa veritabanı tutarlı olmalıdır.
  - Bankanın güvenlik politikasının ilgili kısmında da bütün işlemler iyi biçimlendirilmiş olmalıdır.

Güvenlik Politikası Türleri

Gizlilik Politikası

Gizlilik politikası
sadece **gizlilik** ile ilgilenen
bir güvenlik politikasıdır.

Güvenlik Politikası Türleri

Bütünlük Politikası

Bütünlük politikası
sadece **bütünlük** ile ilgilenen
bir güvenlik politikasıdır.

Güvenlik Politikası Türleri

- Gizlilik ve askeri politikaları *gizlilik* ile ilgilenmektedir.
  - Gizlilik politikası bütünlük ile ilgilenmez.
  - Askeri politika bütünlük ile ilgilenebilir.
- Bütünlük ve ticari politikalar *bütünlük* ile ilgilenmektedir.
  - Bütünlük politikası gizlilik ile ilgilenmez.
  - Ticari politika gizlilik ile ilgilenebilir.

Erişim Denetim Türleri

- Discretionary Access Control (DAC)
  İsteğe Bağlı Erişim Denetim

- Mandatory Access Control (MAC)
  Zorunlu Erişim Denetim

- Originator Controlled Access Control (ORCON/ORGCON)
  Yaratıcı Kontrollü Erişim Denetim

Erişim Denetim Türleri

Discretionary Access Control (DAC)

İsteğe Bağlı Erişim Denetim

Eğer kullanıcı;

nesneye erişim izni ya da reddi için bir erişim denetim düzeneği ayarlıyorsa bu düzenek *isteğe bağlı erişim denetimi*dir.

Aynı zamanda *identity-based access control (IBAC)* olarak da adlandırılmaktadır.

Erişim Denetim Türleri

Discretionary Access Control (DAC)

İsteğe Bağlı Erişim Denetim

- DAC'da erişim hakları öznenin ve nesnenin kimliğini temel almaktadır.
- Kimlik anahtardır.
- Nesnenin sahibi, sadece belirli öznelere erişim hakkı vererek kimlerin nesneye erişebileceğini kısıtlar.
- Nesnenin sahibi, kısıtları öznenin kimliğine ya da öznenin sahibine göre belirler.

Erişim Denetim Türleri

- Muhasebeci, maaş dosyasını okuma iznini sadece ofisin müdürüne vermektedir.
- Maaş dosyasına erişim:
  - Öznenin kimliğini → Müdür
  - Nesneyi okuma izni isteği → Maaş dosyası

  temel almaktadır.

Erişim Denetim Türleri

Mandatory Access Control (MAC)

Zorunlu Erişim Denetim

Bir sistem düzeneği nesneye erişimi denetlerken, bir kullanıcı bu erişimi değiştiremiyorsa, bu denetim *zorunlu erişim denetimi*dir.

Aynı zamanda,

rule-based access control olarak da adlandırılmaktadır.

Erişim Denetim Türleri

- İşletim sistemi MAC'i yürütmektedir.
- Özne ya da nesnenin sahibi erişime izin verilip verilmeyeceğini belirtemez.
- Genel olarak;
  - Sistem düzeneği özne ve nesne ile ilgili bilgiyi kontrol ederek, öznenin nesneye erişim izni olup olmayacağını belirler.
- ÖR: Emniyet müdürlüğüne pasaport için başvurulduğunda kişinin sicil kaydının incelenmesinde kişinin hiçbir denetimi yoktur.

Erişim Denetim Türleri

Originator Controlled Access Control (ORCON/ORGCON)

Yaratıcı Kontrollü Erişim Denetim

Yaratıcı kontrollü erişim denetimi

nesnenin (ya da içerisindeki bilginin) yaratıcısını temel almaktadır.

Erişim Denetim Türleri

Originator Controlled Access Control (ORCON/ORGCON)

Yaratıcı Kontrollü Erişim Denetim

- Bu denetimin amacı, dosyanın ya da içerisindeki bilginin yaratıcısının bilginin yayılmasını denetlemesini sağlamaktır.
- Dosyanın yaratıcısı dosyaya kimin erişeceğini denetler.

Erişim Denetim Türleri

- **A** firması **B** firmasına ürettireceği **X** ürününün ayrıntılı bilgilerini vermektedir.
- **B** firması birlikte çalıştığı taşeron firmaya **X** ürünün ayrıntılarını verebilmesi için **A** firmasının iznine ihtiyacı vardır.

Güvenlik Politikaları

- Güvenlik politikaları az sayıda ya da çok fazla ayrıntıya sahip olabilir.
- Güvenlik politikasının belirginliği bulunduğu ortama bağlıdır.
  - Bir ofiste ya da araştırma lab ortamında yazılı olmayan politikalar olabilir.
  - Bir banka politikası ise açık olmalıdır.

Güvenlik Politikaları

- Pratikte;
  - Politikalar, organizasyon üyelerini kısıtlayan genel ifadelerdir.
  - Bu ifadeler *tehditlerin analiz edilmesinden* elde edilmektedir.

Politika Örnekleri

Acceptable Use Policy (AUP)

- Politika, belirli kaynakların kullanımı ile ilgili belirtimlerde bulunmamaktadır.
- Genel kısıtlamalardan bahsetmektedir.

Politika Örnekleri

- Örnek üniversite AUP:

  http://manuals.ucdavis.edu/PPM/310/310-23a.pdf

  - Kullanıcıların birbirlerinin haklarına ve sistem bütünlüğüne saygı duymaları gerektiği
  - Sistem yöneticilerinin ve kullanıcılarının kanunen uyması geren kurallar.
  - Sorumsuz kullanım olarak nitelendirilen eylemlerin listelenmesi: spam, gözleme (monitoring) vs..

Politika Örnekleri

Elektronik Mail Politikası

- Kurumların, genel politikalarını destekleyen ek politikaları olabilir.

- Elektronik mail erişim ve kullanımı ile ilgili kısıtları belirtir.
  - Genel politikaya uyar.
  - Sistem yöneticileri ve kullanıcılar için ek kısıtları belirtir.

Politika Örnekleri

Elektronik Mail Politikası

- ÖR: http://email.ucdavis.edu/
  - Email'ler özel (private) değildir.
    - Sistem bakımı sırasında okunabilir.
  - İletilen (forward) mailler taklit edilebilir ya da değiştirilebilir.
    - Genelde politikalar, bu şekilde kullanıcıları tehditlere karşı uyarmaz.
  - Kullanıcıların yapmasına izin verilen ve izin verilmeyen işlemler.
  - Kampüsteki ziyaretçiler bu politikalara uymak zorunda mı?
    - Evet

Politika Örnekleri

Tüm Politika (Full Policy)

- Politikanın içeriğini, amacını ve kapsamını belirtir.
- Genel koşulları içerir.
  - Kullanıcıların kanunen ve üniversite tarafından politikalarına uyması gerektiği.
  - Legal ve illegal kullanımlar

Kaynak

- Guide to write a policy

http://manuals.ucdavis.edu/resources/GuidetoWritingPolicy.pdf

- Policy writer resources

http://manuals.ucdavis.edu/Resources.htm

- Information technology policies

http://policy.ucop.edu/advanced-search.php?action=welcome&op=browse&subject=10

- Presidential Policies

http://policy.ucop.edu/manuals/index.html

Not

- Politikalar *neye* izin verildiğini belirtir.

- Düzenekler politikaların *nasıl* yürütüldüğünü denetler.