Tasarım Esasları

Yrd. Doç. Dr. Özgü Can

Tasarım Esasları

- Güvenlik düzeneklerinin tasarımı ve gerçekleştirimi basitlik (simplicity) ve kısıtlamayı (restriction) temel alır.

- Basitlik (simplicity), tasarım ve düzeneklerin kolaylıkla anlaşılmasını sağlar.

- Politika içerisindeki olası tutarsızlıkları azaltır.

Örnek - Kural Çelişmesi

Politika → ***Ödevlerde yapılan herhangi bir aldatmadan haberdar olan bir asistan bu durumu yönetime haber vermelidir.***

1. Asistan, öğrencinin ödevi ile ilgili eksik dosyayı göndermesini ister.
2. Ögrenci, dosyanın dizininde olduğunu ve asistana dosyayı kopyalayabileceğini söyler.
3. Asistan, dizinde dosyayı ararken öğrencinin ödevinin yani sıra aynı ödevin başka bir öğrenciye kopyasını bulur.
4. Asistan, aldatma gerekçesi ile öğrenciyi yönetime rapor eder.
5. Ögrenci asistanı mahremiyetini ihlal etmekle suçlar.

Tasarım Esasları

- Kısıtlama, varlığın gücünü azaltır.
- Varlık, sadece ihtiyacı olan bilgiye erişir.
- ÖR: Need-to-know prensibi
  - Kişi, ihtiyacı olmadığı bilgiye erişemez.

Tasarım Esasları

- Varlıklar diğer varlıklar ile sadece ihtiyacı olduğunda iletişim kurabilir.
  - İletişim mümkün olduğunca az olmalıdır.

- ÖR: Mahkumların ziyaretçileri ile görüşmelerinin ve postalarının gözlemlenmesi
  - Tek ayrıcalıklı durum → Avukatları ile görüşmeleridir.

Tasarım Esasları

En Az Ayrıcalık (Least Privilege) Esası

Özneye,

<u>sadece</u> görevi tamamlaması için gerekli ayrıcalıklar verilmelidir.

En Az Ayrıcalık

- Eğer bir özne bir erişim hakkına ihtiyaç duymuyorsa, özneye bu hak verilmemelidir.
- Özneye atanan haklar kontrol edilmelidir.
- Belirli bir eylem öznenin haklarının arttırılmasını gerektiriyorsa, eylemin tamamlanmasından hemen sonra bu haklar özneden geri alınmalıdır.
  - Need-to-know prensibine benzerdir.
    - Bir öznenin bir görevi tamamlamak için bir nesneye erişmesi gerekmiyorsa, öznenin o nesneye erişim hakkı olmamalıdır.

En Az Ayrıcalık

- Öznenin bir nesneye *ekleme* (append) yapması gerekiyor, **fakat** nesnenin içermiş olduğu mevcut bilgide *değişiklik* (alter) yapması gerekmiyorsa;
  - Özneye **ekleme** izni verilmeli
  - **Yazma** izni verilmemelidir.

En Az Ayrıcalık

- Pratikte;
  - Bir çok sistemin ayrıcalık ölçümü bulunmamaktadır.
  - Güvenlik düzeneği tasarımcıları ***en az ayrıcalık*** esasını en iyi şekilde uygulamaya çalışmaktadırlar.
  - En az ayrıcalık esasını kullanmayan sistemlerin güvenlik problemlerinin sonuçları, en az ayrıcalık esasını kullanan sistemlere göre daha ciddi olmaktadır.

Bozulmaya Dayanıklı (Fail-Safe) Varsayılanlar Esası

- Özne ya da nesne yaratıldığında önceliklerin nasıl belirlendiğini kısıtlar.

- Öznenin nesneye erişimi, özneye nesneye erişim hakkı verilene kadar reddedilir.

- Nesneye varsayılan erişim "*nesneye erişimin olmadığı*" dır.

Bozulmaya Dayanıklı (Fail-Safe) Varsayılanlar Esası

- Erişim ve öncelikler açıkça belirtilmediği sürece erişim **reddedilecektir**.

- Eğer özne, eylemi ya da görevini tamamlayamayacaksa, sistemin güvenilir durumunda meydana gelen değişiklikler işlem sonlandırılmadan önce geri alınmalıdır.

Bozulmaya Dayanıklı (Fail-Safe) Varsayılanlar Esası - Örnek

- Eğer mail sunucusu, kuyrukta (spool) dosya yaratamıyorsa:
  1. Ağ bağlantısını kapatmalı
  2. Hata mesajı vermeli ve
  3. Durmalıdır.
- Mesajı başka bir dizinde saklamaya çalışmamalıdır.
  - Saldırgan dosyayı diğer dizinde okuyabilir.

Düzeneğin Ekonomisi Esası

- Bu esas, güvenlik düzeneğinin mümkün olduğu kadar *basit* olması gerektiğini belirtmektedir.
- Tasarım ve gerçekleştirim basit ise → Hata olması ihtimali düşüktür.

Daha az bileşen ve durum test edilecektir.

Denetleme ve test **daha az karmaşık** olacaktır.

Eksiksiz Aracılık Esası

- Bu esas, nesneye olan bütün erişimlere izin verildiğinin garantilenmesidir.
- Özne, nesneyi okumak istediğinde, işletim sistemi bu eyleme aracılık eder.
  1. Öznenin, nesneyi okumak için **izni olup olmadığını** belirler.
  2. İzni varsa, okunacak **kaynakları** sağlar.

Eksiksiz Aracılık Esası

- Eğer, özne dosyayı yeniden okumak isterse, sistem öznenin hala nesneyi okumak için izni olup olmadığını kontrol eder.
- Birçok sistem, **ikinci kontrolü** yapmaz.
  - Birinci kontrolün sonuçlarını önbelleğe (cache) yazar ve ikinci erişimi önbellek sonuçlarından kontrol eder.

Açık Tasarım Esası

- Düzeneğin güvenliği, tasarım ve gerçekleştirimin gizliliğine bağlı olmamalıdır.
- **Bilinmezlik yoluyla gizlilik (Security through obscurity)**

Güvenlik kullanıcının bilgisizliğine dayanırsa

Bilgili bir kullanıcı güvenlik düzeneğini alt edebilir.

Önceliklerin Ayrımı Esası

- Bu esas, bir sistemin sadece tek bir koşula bağlı olarak izin onaylamaması gerektiğini belirtmektedir.
- Görev ayrılığı (separation of duty) prensibine benzer.
  - Bir işlemi tamamlamak için birden fazla varlığa ihtiyaç duyulur.
  - Varlığın işlemi tek başına tamamlamasını yasaklar.

Önceliklerin Ayrımı Esası

- Kaynaklara erişimi onaylayan sistemler ve programlar, **birden fazla koşul** sağlandığında erişimi onaylamalıdır.

ÖR: Berkeley-tabanlı UNIX işletim sisteminde;

Root'a geçecek kullanıcı:

1. Root şifresini bilmeli
2. Kullanıcı "wheel" grubunda (GID=0) olmalı

En Az Ortak Düzenek Esası

- Kaynaklara erişmek için kullanılan düzenekler paylaşılmamalıdır.

- Paylaşım *min.* olmalıdır.

ÖR: *Belirli bir servisi internet üzerinden sağlarken proxy kullanarak saldırganların sisteme erişimini kısıtlandıracaktır.*

Psikolojik Uygunluk Esası

- Güvenlik düzeneği, bir kaynağa erişimi, güvenlik düzeneği olmayan durumdan daha zor bir duruma getirmemelidir.

- Bir programın kurulumu ve konfigürasyonu mümkün olduğunca *basit* olmalıdır.

Psikolojik Uygunluk Esası

Güvenlik ile ilgili bir yazılımın konfigürasyonu karmaşık ise

Güvenlik yöneticileri yazılımı istemeden güvenli olmayan bir şekilde kurabilirler.

- Güvenlik ile ilgili kullanıcı programları da olabildiğince basit olmalıdır.
  - Kullanıcılar çıktı mesajlarını anlayabilmelidir.

Psikolojik Uygunluk Esası

ÖR:

- Bir parola değişimi işlemi sırasında parola kabul edilmiyorsa:
  - Şifreli hata mesajı verilmemelidir.
  - Parola değişim programı parolanın kabul edilmeme nedenini açıklamalıdır.

Psikolojik Uygunluk Esası

ÖR:

- Sisteme bağlanma işlemi sırasında, hatalı parola nedeni ile sisteme bağlanamayan kullanıcıya bağlantının başarısız olduğu belirtilmeli.
  - Parola hatası nedeni ile bağlantının başarısız olduğu belirtilirse;
    - Saldırgan kullanıcı adının doğru olduğunu anlayarak yeni parola denemeleri yapmaya devam edecektir.