



### 1.1.1 Outline

- Veri G $\bar{A}^{1/4}$ venli $\bar{A}^{\bar{Y}}$ i: Kullan $\bar{A}^{\pm}$ mda, Aktar $\bar{A}^{\pm}$ mda ve Depolamada
- Yaz $\bar{A}^{\pm}$ l $\bar{A}^{\pm}$ m Geli $\bar{A}^{\bar{Y}}$ tirme S $\bar{A}^{1/4}$ re $\bar{A}^{\bar{S}}$ leri
  - Kullan $\bar{A}^{\pm}$ mda Veri G $\bar{A}^{1/4}$ venli $\bar{A}^{\bar{Y}}$ i
  - Aktar $\bar{A}^{\pm}$ mda Veri G $\bar{A}^{1/4}$ venli $\bar{A}^{\bar{Y}}$ i
  - Depolamada Veri G $\bar{A}^{1/4}$ venli $\bar{A}^{\bar{Y}}$ i
- Dinamik ve Statik Varl $\bar{A}^{\pm}$ klar $\bar{A}^{\pm}$ n Korunmas $\bar{A}^{\pm}$

### 1.2 Hafta-3: Veri G $\tilde{A}$ $^{1/4}$ venliÄŸi - KullanÄ±mda, AktarÄ±mda ve Depolama Halindeki Veri G $\tilde{A}$ $^{1/4}$ venliÄŸi

### 1.2.0.1 Teorik Konu Başlıkları ve Uygulamalar

### 1.3 Kullanıcı Veri Güvenliği (Data-In-Use Security)

### 1.3.1 1. $\tilde{A} \nmid \tilde{a} \mid \tilde{A} \pm \tilde{A} \tilde{Y}$ ma Zaman $\tilde{A} \pm$ Uygulama Verisi $\tilde{G} \tilde{A}^{1/4} \text{venli} \tilde{A} \tilde{Y}$ i (Runtime Application Data Security)

**1.3.1.1 Teorik A** Kullandığımız veri g<sup>1/4</sup>venliyi, uygulama salıverken bel-  
 lekte tutulan hassas bilgilerin korunması ile ilgilenir. Bu g<sup>1/4</sup>venlik, zellikle bellekte geici olarak  
 bulunan verilerin k<sup>1/4</sup> amaşı yazılımlar tarafından ele geçirilmesini engellemek için  
 kullanılır.

### 1.3.1.2 Uygulamalar:

1. **Bellek  zifreleme:** Bellekteki hassas verilerin  yifrenlenmesi.
2. **K t ye Kullan m Tespiti:** Bellekteki   pheli hareketlerin izlenmesi ve m dahale edilmesi.
3. **Veri Manip lasyonu Testleri:**  tal ma zaman ndaki verilerin yanl yla kla veya kas tl  olarak de y tirilip de y tirilmedi ini test etme.
4. **Dinamik Bellek Y netimi:** Bellek s z nt lar n  engellemek ve veri s z nt lar n  minimize etmek.
5. **S rekli Kimlik Do rulama:** Kullan c lar n oturumlar  s resince kimliklerinin tekrar tekrar do rulanmas .
6. **Veri Maskelenmesi:** Hassas verilerin yaln zca yetkili s re ler taraf ndan g r lebilir olmas .
7. **Tamperproof Mekanizmalar :** Bellekteki verilerin manip le edilip edilmedi ini kontrol eden ve bu verilerin de y tirilmesi durumunda sistemin tepki vermesini sa layan mekanizmalar.
8. **G venlik Protokollerinin  zlenmesi:** Uygulama  sal  rken kullan lan g venlik protokollerinin anormal davran  lar n  izleme.
9. **Veri G venlik Duvarlar :** Bellek i isindeki hassas verilerin yaln zca yetkili s re ler taraf ndan eri ilebilece i g venlik katmanlar  ekleme.
10. **Geli mi  Kay t Tutma:** Bellekteki veriler   zerinde ger  kle tirilen t m i ylemlerin kay t altına alınmas .

#### 1.4 AktarÄ±mda Veri GÅ¼venliÄ±i (Data-In-Transit Security)

#### 1.4.1 1. Veri Aktarımlarında Güvenlik Yöntemleri (Data Security Methods During Transportation)

**1.4.1.1 Teorik AÄŞÄklama:** Verilerin aÄŸ Ä¼zerinden aktarÄ±lmasÄ± saÄ±rasÄ±nda, bu verilerin gizliliÄŸinin ve bÄ¼tÄ¼nlÄŸÄŸÄ¼nÄ¼n korunmasÄ± gerekir. GÄ¼venli bir ÄŸekilde veri aktarÄ±lmasÄ± saÄŸlamak iÄŸin ÄŸifreleme, kimlik doÄŸrulama ve bÄ¼tÄ¼nlÄŸÄ¼k kontrolleri uygulanÄ±r.

#### 1.4.1.2 Uygulamalar:

1. **Oturum AnahtarÄ± (Session Key):** Ä±stemci ve sunucu arasÄ±nda dinamik olarak oturum anahtarÄ± oluÅŸturma ve bu anahtar ile ÄŸifreleme yapma.

2. **Cihaz BaÄlama (Device Binding):** Verilerin belirli bir cihaza baÄlÄ± olarak iletilmesini saÄlayarak, verilerin farklı bir cihazda ÄzÄ±lmasını engelleme.
3. **SÄ±rÄ±m BaÄlama (Version Binding):** Yalnızca belirli sÄ±rÄ±mlerin veri iletimine izin vererek, gÄ±venlik aÄklarÄ± barındıran eski sÄ±rÄ±mlerin veri almasını engelleme.
4. **ÄziflenmiÄ YÄ±k (Confidential Payload):** TaÄnın verinin Äziflenerek sadece yetkili taraflar tarafından okunabilir hale getirilmesi.
5. **BÄ±tÄ±nlÄ±k KontrolÄ± (Integrity Control):** Veri aktarımÄ± sÄ±rasÄ±nda verilerin bozulmadan veya deÄtirilmeden iletilmesini doÄrulama.
6. **Kimlik DoÄrulama (Authenticity Control):** Veri gÄnderenin ve alÄ±cÄ±nın kimliklerinin doÄrulanmasını.
7. **GÄ±venli ÄletiÄim KanallarÄ± (Secure Communication Channels):** SSL/TLS protokollerini kullanarak gÄ±venli veri aktarımÄ± gerÄekleÄtirme.
8. **SSL SertifikalarÄ±:** Sunucu doÄrulanmasÄ±nda SSL sertifikalarÄ± kullanarak veri aktarımÄ± sÄ±rasÄ±nda gÄ±venliÄi artırma.
9. **Veri Äzleme (Data Monitoring):** Aktarım sÄ±rasÄ±nda verinin izlenmesi ve anormal durumlarÄ±n tespiti.
10. **Äzifli ÄletiÄim Protokolleri:** HTTPS, SSH gibi Äzifli protokoller Ä±zerinden veri iletilimi yapma.

#### 1.4.2 2. Sunucu ÄletiÄimi (Server Communication)

**1.4.2.1 Teorik AÄklama:** Sunucu ile istemci arasÄ±ndaki gÄ±venli iletiÄim, verilerin gÄ±venli bir Äekilde sunucuya aktarılmasını saÄlar. Bu sÄ±reÄte sunucunun kimliÄini doÄrulamak ve iletilen verilerin Äziflenmesi bÄ±yÄ±k Änem taÄr.

##### 1.4.2.2 Uygulamalar:

1. **Sunucu Kimlik DoÄrulama Kodu (Server Authentication Code):** Sunucunun kimliÄini doÄrulayan Äzel bir kimlik doÄrulama mekanizmasını geliÄtirme.
2. **GÄ±venli Sunucu ÄletiÄimi (Secure Server Communication):** Sunucu ve istemci arasÄ±nda verilerin SSL/TLS ile Äziflenmesini saÄlama.
3. **Oturum AnahtarÄ± Äzifleme (Session Key Encryption):** Verilerin oturum anahtarlarÄ± kullanarak Äziflenmesini saÄlama.
4. **Sunucu Äzerinde Veri Äzleme (Data Monitoring):** Sunucuya gelen ve giden veri trafiÄini izleyip anormallikleri tespit etme.
5. **Veri BÄ±tÄ±nlÄ±k ÄÄ± DoÄrulama:** Verilerin sunucuya bozulmadan iletilmesini doÄrulayan bÄ±tÄ±nlÄ±k kontrol mekanizmalarÄ±nı kullanma.
6. **Verilerin Äziflenmesi (Data Encryption):** Verileri sunucuya gÄndermeden Änce istemci tarafÄ±nda Äzifleme.
7. **Sunucu YanıtlarÄ±nÄ± Ämzalama (Response Signing):** Sunucudan gelen yanıtlarÄ± dijital imza ile doÄrulama.
8. **Sunucu Yedekleme:** Sunucuda tutulan kritik verilerin dÄ±zenli olarak yedeklenmesi ve Äzifli olarak saklanması.
9. **GÄ±venli Oturum Kapatma (Secure Session Termination):** Oturum sona erdiÄinde oturum anahtarlarÄ±nı gÄ±venli bir Äekilde temizlenmesi.
10. **Kimlik DoÄrulama Loglama:** Sunucu tarafÄ±nda tÄ±m kimlik doÄrulama iÄlemlerinin loglanması ve gerektiÄinde izlenebilmesi.

### 1.5 Depolamada Veri GÄ±venliÄi (Data-At-Rest Security)

#### 1.5.1 1. Depolama Halindeki Veriler ÄÄsin GÄ±venlik YÄntemleri (Data Security Methods During Stored State)

**1.5.1.1 Teorik AÄklama:** Veriler sabit disklerde, veri tabanlarÄ±nda veya bulut ortamlarÄ±nda depolandÄ±Ända, bu verilerin korunmasını gerekir. Äzifleme ve bÄ±tÄ±nlÄ±k kontrolÄ± gibi yÄntemler, depolanan verilerin izinsiz eriÄimlere ve saldırılara karÄşı korunmasını saÄlar.

### 1.5.1.2 Uygulamalar:

1. **Whitebox AES:** Depolama alanında AES algoritmasıyla whitebox yöntemiyle uygulayarak verilerin daha güvenli bir şekilde korunması sağlama.
2. **Whitebox DES:** Whitebox DES algoritmasıyla verilerin şifrelenmesi ve güvenli testlerinin yapılması.
3. **Güvenlik Kabuk Matrisi (Security Shell Matrix):** Verilerin güvenli bir şekilde depolanması sağlama için dosya sisteminde güvenlik kabuğu oluşturulması.
4. **Anahtar Yönetimi:** Şifreleme anahtarları güvenli bir şekilde saklanması ve düzenli olarak değiştirilmesi.
5. **Şifreli Veritabanı:** Veritabanındaki hassas verilerin şifrelenmesi ve sadece yetkili kullanıcıların erişebilmesi.
6. **Depolanan Verilerin Şifrelenmesi:** Tüm verilerin şifreli bir formatta saklanması ve yetkisiz erişimlerin engellenmesi.
7. **Dosya Bütünlük Kontroleri:** Depolanan dosyaların izinsiz değiştirilip değiştirilmediğini kontrol eden mekanizmalar.
8. **Veri Yedekleme:** Kritik verilerin düzenli olarak yedeklenmesi ve yedeklerin şifreli olarak saklanması.
9. **Güvenli Silme:** Depolama alanındaki verilerin silinmesi gerektiğinde, verilerin geri alınamaz şekilde silinmesi.
10. **Bütünlük Kontroleri:** Dosyaların bütünlük kontrolünü sağlayan ve yetkisiz değişiklikleri tespit eden mekanizmalar kullanma.

## 1.6 Statik ve Dinamik Varlıkların Korunması (Protection of Static and Dynamic Assets)

### 1.6.1 1. Statik Varlıkların Korunması (Protection of Static Assets)

**1.6.1.1 Teorik Açıklama:** Statik varlıklar, veritabanında veya sabit depolama ortamında değiştirilmeden duran verilerden oluşur. Bu varlıkların korunması, veri bütünlüğü sağlama ve izinsiz erişimleri engellemek için son derece önemlidir.

### 1.6.1.2 Uygulamalar:

1. **Anahtarların Şifrelenmesi:** Statik anahtarları güvenli bir şekilde depolaması için şifreleme yöntemleri kullanma.
2. **Kaynak Kodların Koruma:** Kaynak kodlarının izinsiz kopyalanması ve değiştirilmesini engelleyen mekanizmalar geliştirme.
3. **Statik Dosyaların Bütünlük Kontrolü:** Sabit dosyaların bütünlük kontrolünü sağlayarak izinsiz değişikliklerin önlenmesi.
4. **Veri Ömürleri:** Depolanan verilerin değiştirilemeyeceğini doğrulamak için dijital imza kullanma.
5. **Veritabanı Bütünlük Kontrolü:** Veritabanında bulunan kritik verilerin şifrelenmesi ve bütünlük kontrolünü sağlama.
6. **Dosya Erişim Kontrolü:** Statik dosyaların yetkisiz erişimlere karşı korunması için erişim kontrol mekanizmaları devreye sokma.
7. **Gizli Anahtar Yönetimi:** Statik anahtarları güvenli bir şekilde saklanması ve yönetilmesi.
8. **Veritabanı Şifreleme:** Statik verilerin şifrelenerek veri tabanında güvenli bir şekilde saklanması sağlama.
9. **Ölüm ve Şifreleme Kombinasyonu:** Statik dosyaların bütünlük kontrolünü sağlamak ve şifreleme ile birlikte dijital imza kullanarak güvenli arttırma.
10. **Dosya Güvenlik Duvarı:** Statik dosyaların korunması için dosya güvenlik duvarı oluşturulması.

### 1.6.2 2. Dinamik Varlıkların Korunması (Protection of Dynamic Assets)

**1.6.2.1 Teorik Açıklama:** Dinamik varlıklar, uygulama çalışırken oluşturulan ve sürekli değişen verilerdir. Bu verilerin korunması, özellikle oturum bilgileri ve dinamik anahtarlar

gibi hassas bilgilerin g ¼venli  ini sa  lar.

### 1.6.2.2 Uygulamalar:

1. **Dinamik Anahtarlar  n G ¼venli  i:** Dinamik anahtarlar  n yaln  zca belirli oturumlar s  ras  nda kullan  lmas   ve g ¼venli bir    ekilde de  i  tirilmesi.
2. **Oturum Bilgisi   zifreleme:** Kullan  c   oturumlar  n  n gizlili  ini sa  lamak i  sin oturum bilgilerini   zifreleme.
3. **Cihaz Parmak   zlerinin Korunmas  :** Cihaz parmak izlerinin yaln  zca yetkili taraflarca do  rulanmas  n   sa  lama.
4. **Oturum Verisi Korumas  :** Dinamik oturum verilerinin   zifrelenerek g ¼vence alt  na al  nmas  .
5. **Dinamik Anahtar Y  netimi:** Oturum s  ras  nda kullan  lan dinamik anahtarlar  n g ¼venli bir    ekilde olu  turulmas   ve y  netilmesi.
6. **Oturum Zaman A    m  :** Kullan  c   oturumlar   i  sin otomatik zaman a    m   mekanizmas   uygulayarak g ¼venli  i art  rma.
7. **Verilerin S  rekli   zlenmesi:** Dinamik verilerin   zifrelenerek izlenmesi ve g ¼venlik ihlallerinin an  nda tespit edilmesi.
8. **Veri Manip  lasyonu Engelleme:** Dinamik verilerin manip  le edilmesini engelleyen g ¼venlik mekanizmalar   kurma.
9. **Dinamik Veri   mzas  :** Oturum s  ras  nda de  i  tirilen verilerin b  t  nl      n   do  rulamak i  sin dijital imza kullanma.
10. **Ger   ek Zamanl   Veri Analizi:** Oturum s  ras  nda olu  an dinamik verileri analiz eden g ¼venlik protokollerini devreye sokma.

## 1.7 Varl  k   zellikleri (Property of Assets)

**1.7.0.1 Teorik A    klama:** Bir varl     n         , onun ad  n  , tan  m  n  , konumunu, kayna  n  , boyutunu, olu  turulma ve silinme zaman  n   i    r. Ayr  ca, bir varl     n gizlilik (Confidentiality), b  t  nl       (Integrity) ve do  rulama (Authentication) gibi g ¼venlik gereksinimlerine kar     nas  l korunaca  n   belirlemek   nemlidir.

### 1.7.0.2 Uygulamalar:

1. **Varl  k   smi (Asset Name):** Varl     n ad  n   belirleyerek bu varl     n ne oldu  unu tan  mlama.
2. **Tan  m (Description):** Varl     n ne i  lev g        n   ve hangi bilgileri i      ni a    klama.
3. **Konum (Location):** Varl     n bulundu  u veri taban  , tablo veya kolon gibi fiziksel konumunu belirleme.
4. **Kaynak (Source):** Varl     n kayna  n   belirleyerek hangi s  re   veya veri kayna    ndan geldi  ini tan  mlama.
5. **Boyut (Size):** Varl     n boyutunu belirleyerek depolama ihtiya  lar  n   optimize etme.
6. **Olu  turulma Zaman   (Creation Time):** Varl     n olu  turuldu  u tarihi ve zaman   belirleyerek log kay  tlar  n   tutma.
7. **Silinme Zaman   (Destroy Time):** Varl     n ne zaman imha edilece  ini ve bu s  recin nas  l y  netilece  ini belirleme.
8. **Varsay  lan De  er (Default Value):** Varl     n varsay  lan de  erini tan  mlayarak, ilk durumda nas  l olaca  n   belirtme.
9. **Gizlilik, B  t  nl       ve Do  rulama:** Varl     n g ¼venlik gereksinimlerine g  re koruma seviyelerini tan  mlama (C - Confidentiality, I - Integrity, A - Authentication).
10. **Varl  k Koruma   zemas  :** Her varl     n g ¼venlik ihtiya  lar  na g  re     el bir koruma plan   olu  turarak, hangi        n al  nmas   gerekti  ini belirleme.

## 1.8 Haftan  n   zeti ve Gelecek Hafta

### 1.8.1 Bu Hafta:

- Kullan  mda, Aktar  mda ve Depolamada Veri G ¼venli  i

- Statik ve Dinamik Varlıkların Korunması

#### 1.8.2 Gelecek Hafta:

- Sertifikalar ve Şifreleme Yöntemleri
- Kimlik Doğrulama ve Veri Güvenliği

*3.Hafta – Sonu*