

CEN429 Gvenli Programlama Hafta-3

Veri Gvenliyi: Kullanmada, Aktarmada ve Depolamada

Yazar: Dr. A.Yr. Aeyesi UYur CORUH

İçindekiler

| | |
|-----------------------------------------------------------------------------------------------------------|----------|
| 1 CEN429 Gvenli Programlama | 1 |
| 1.1 Hafta-3 | 1 |
| 1.1.1 Outline | 2 |
| 1.2 Hafta-3: Veri Gvenliyi - Kullanmada, Aktarmada ve Depolama Halindeki Veri Gvenliyi | 2 |
| 1.3 Kullanmada Veri Gvenliyi (Data-In-Use Security) | 2 |
| 1.3.1 1. AalÄma ZamanÄ Uygulama Verisi Gvenliyi (Runtime Application Data Security) | 2 |
| 1.4 Aktarmada Veri Gvenliyi (Data-In-Transit Security) | 2 |
| 1.4.1 1. Veri Aktarmada SÄrasÄnda Gvenlik YÄntemleri (Data Security Methods During Transportation) | 2 |
| 1.4.2 2. Sunucu AletiYimi (Server Communication) | 3 |
| 1.5 Depolamada Veri Gvenliyi (Data-At-Rest Security) | 3 |
| 1.5.1 1. Depolama Halindeki Veriler AÄŞin Gvenlik YÄntemleri (Data Security Methods During Stored State) | 3 |
| 1.6 Statik ve Dinamik VarlıklarÄn KorunmasÄ (Protection of Static and Dynamic Assets) | 4 |
| 1.6.1 1. Statik VarlıklarÄn KorunmasÄ (Protection of Static Assets) | 4 |
| 1.6.2 2. Dinamik VarlıklarÄn KorunmasÄ (Protection of Dynamic Assets) | 4 |
| 1.7 Varlık A-zellikleri (Property of Assets) | 5 |
| 1.8 HaftanÄn A-zeti ve Gelecek Hafta | 5 |
| 1.8.1 Bu Hafta: | 5 |
| 1.8.2 Gelecek Hafta: | 6 |

Şekil Listesi

Tablo Listesi

1 CEN429 Gvenli Programlama

1.1 Hafta-3

1.1.0.1 Veri Gvenliyi: Kullanmada, Aktarmada ve Depolamada A°ndir

- PDF¹
- DOC²
- SLIDE³
- PPTX⁴

¹pandoc_cen429-week-3.pdf

²pandoc_cen429-week-3.docx

³cen429-week-3.pdf

⁴cen429-week-3.pptx

1.1.1 Outline

- Veri G^{1/4}venli^ÄYi: Kullan^Ä±mda, Aktar^Ä±mda ve Depolamada
- Yaz^Ä±l^Ä±m Geli^ÄYtirme S^Ä¼re^ÄŞleri
 - Kullan^Ä±mda Veri G^{1/4}venli^ÄYi
 - Aktar^Ä±mda Veri G^{1/4}venli^ÄYi
 - Depolamada Veri G^{1/4}venli^ÄYi
- Dinamik ve Statik Varl^Ä±klar^Ä±n Korunmas^Ä±

1.2 Hafta-3: Veri G^{1/4}venli^ÄYi - Kullan^Ä±mda, Aktar^Ä±mda ve Depolama Halindeki Veri G^{1/4}venli^ÄYi

1.2.0.1 Teorik Konu Ba^ÄYl^Ä±klar^Ä± ve Uygulamalar

1.3 Kullan^Ä±mda Veri G^{1/4}venli^ÄYi (Data-In-Use Security)

1.3.1 1. Ä¼al^Ä±Ä^Yma Zaman^Ä± Uygulama Verisi G^{1/4}venli^ÄYi (Runtime Application Data Security)

1.3.1.1 Teorik AÄ^ŞÄ[±]klama: Kullan^Ä±mda veri g^{1/4}venli^ÄYi, uygulama Ä^Şal^Ä±Ä^YÄ[±]rken bel-
lekte tutulan hassas bilgilerin korunmas^Ä± ile ilgilenir. Bu g^{1/4}venlik, Ä[¶]zellikle bellekte ge^ÄŞici olarak
bulunan verilerin kÄ[¶]t^Ä¼ amaÄ^Şl^Ä± yaz^Ä±l^Ä±mlar taraf^Ä±ndan ele ge^ÄŞirilmesini engellemek iÄ^Şin
kullan^Ä±l^Ä±r.

1.3.1.2 Uygulamalar:

1. **Bellek Ä^Yifreleme:** Bellekteki hassas verilerin Ä^Yifrenlenmesi.
2. **KÄ[¶]t^Ä¼ye Kullan^Ä±m Tespiti:** Bellekteki Ä^YÄ^¼pheli hareketlerin izlenmesi ve mÄ^¼dahale edilmesi.
3. **Veri Manip^Ä¼lasyonu Testleri:** Ä¼al^Ä±Ä^Yma zaman^Ä±ndaki verilerin yanl^Ä±Ä^Yl^Ä±kla veya kasÄ[±]tl^Ä± olarak deÄ^YiÄ^Ytirilip deÄ^YiÄ^YtirilmediÄ^Yini test etme.
4. **Dinamik Bellek YÄ[¶]netimi:** Bellek sÄ[±]zÄ[±]ntÄ[±]larÄ[±]nÄ[±] engellemek ve veri sÄ[±]zÄ[±]ntÄ[±]larÄ[±]nÄ[±] minimize etmek.
5. **SÄ^¼rekli Kimlik DoÄ^Yrulama:** Kullan^Ä±cÄ[±]larÄ[±]n oturumlarÄ[±] sÄ^¼resince kimliklerinin tekrar tekrar doÄ^Yrulanmas^Ä±.
6. **Veri Maskelenmesi:** Hassas verilerin yaln^Ä±zca yetkili sÄ^¼reÄ^Şler taraf^Ä±ndan gÄ[¶]rÄ^¼lebilir olmas^Ä±.
7. **Tamperproof MekanizmalarÄ[±]:** Bellekteki verilerin manip^Ä¼le edilip edilmediÄ^Yini kontrol eden ve bu verilerin deÄ^YiÄ^Ytirilmesi durumunda sistemin tepki vermesini saÄ^Ylayan mekanizmalar.
8. **GÄ^{1/4}venlik Protokollerinin Ä[°]zlenmesi:** Uygulama Ä^Şal^Ä±Ä^YÄ[±]rken kullan^Ä±lan gÄ^{1/4}venlik protokollerinin anormal davran^Ä±Ä^YlarÄ[±]nÄ[±] izleme.
9. **Veri GÄ^{1/4}venlik DuvarlarÄ[±]:** Bellek iÄ^Şindeki hassas verilerin yaln^Ä±zca yetkili sÄ^¼reÄ^Şler taraf^Ä±ndan eriÄ^YilebileceÄ^Yi gÄ^{1/4}venlik katmanlarÄ[±] ekleme.
10. **GeliÄ^YmiÄ^Y KayÄ[±]t Tutma:** Bellekteki veriler Ä^¼zerinde gerÄ^ŞekleÄ^Ytirilen tÄ^¼m iÄ^Ylemlerin kayÄ[±]t altına alınmas^Ä±.

1.4 Aktar^Ä±mda Veri G^{1/4}venli^ÄYi (Data-In-Transit Security)

1.4.1 1. Veri Aktar^Ä±mÄ[±] SÄ[±]rasÄ[±]nda GÄ^{1/4}venlik YÄ[¶]ntemleri (Data Security Methods During Transportation)

1.4.1.1 Teorik AÄ^ŞÄ[±]klama: Verilerin aÄ^Y Ä^¼zerinden aktarÄ[±]lmasÄ[±] sÄ[±]rasÄ[±]nda, bu verilerin gizliliÄ^Yinin ve bÄ^¼tÄ^¼nlÄ^¼Ä^YÄ^¼nÄ^¼n korunmasÄ[±] gerekir. GÄ^{1/4}venli bir Ä^Yekilde veri aktarÄ[±]mÄ[±] saÄ^Ylamak iÄ^Şin Ä^Yifreleme, kimlik doÄ^Yrulama ve bÄ^¼tÄ^¼nlÄ^¼k kontrolleri uygulanÄ[±]r.

1.4.1.2 Uygulamalar:

1. **Oturum AnahtarÄ[±] (Session Key):** Ä[°]stemci ve sunucu arasÄ[±]nda dinamik olarak oturum anahtarÄ[±] oluÄ^Yturma ve bu anahtar ile Ä^Yifreleme yapma.

2. **Cihaz BaÄlama (Device Binding):** Verilerin belirli bir cihaza baÄlÄ± olarak iletilmesini saÄlayarak, verilerin farklı bir cihazda ÅzÄ±lmesini engelleme.
3. **SÄ±rÄ±m BaÄlama (Version Binding):** YalnÄ±zca belirli sÄ±rÄ±mlerin veri iletimine izin vererek, gÄ±venlik aÄklarÄ± barÄ±ndÄ±ran eski sÄ±rÄ±mlerin veri almasÄ±nÄ± engelleme.
4. **ÄziflenmiÅ YÄ±k (Confidential Payload):** TaÄÄ±nan verinin Äziflenerek sadece yetkili taraflar tarafÄ±ndan okunabilir hale getirilmesi.
5. **BÄ±tÄ±nlÄ±k KontrolÄ± (Integrity Control):** Veri aktarÄ±mÄ± sÄ±rasÄ±nda verilerin bozulmadan veya deÄiÅtirilmeden iletilmesini doÄrulama.
6. **Kimlik DoÄrulama (Authenticity Control):** Veri gÄ±nderenin ve alÄ±cÄ±nÄ±n kimliklerinin doÄrulanmasÄ±.
7. **GÄ±venli Ä°letiÅim KanallarÄ± (Secure Communication Channels):** SSL/TLS protokollerini kullanarak gÄ±venli veri aktarÄ±mÄ± gerÄekleÅtirme.
8. **SSL SertifikalarÄ±:** Sunucu doÄrulanmasÄ±nda SSL sertifikalarÄ± kullanarak veri aktarÄ±mÄ± sÄ±rasÄ±nda gÄ±venliÄi artÄ±rma.
9. **Veri Ä°zleme (Data Monitoring):** AktarÄ±m sÄ±rasÄ±nda verinin izlenmesi ve anormal durumlarÄ±n tespiti.
10. **Äzifli Ä°letiÅim Protokolleri:** HTTPS, SSH gibi Äzifli protokoller Ä±zerinden veri iletimini yapma.

1.4.2 2. Sunucu Ä°letiÅimi (Server Communication)

1.4.2.1 Teorik AAÄ±klama: Sunucu ile istemci arasÄ±ndaki gÄ±venli iletiÅim, verilerin gÄ±venli bir Äekilde sunucuya aktarÄ±lmasÄ±nÄ± saÄlar. Bu sÄ±reÅte sunucunun kimliÅini doÄrulamak ve iletilen verilerin Äziflenmesi bÄ±yÄ±k Änem taÄÄ±r.

1.4.2.2 Uygulamalar:

1. **Sunucu Kimlik DoÄrulama Kodu (Server Authentication Code):** Sunucunun kimliÅini doÄrulayan Äzel bir kimlik doÄrulama mekanizmasÄ± geliÅtirme.
2. **GÄ±venli Sunucu Ä°letiÅ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 trafiÅ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±nÄ± kullanma.
6. **Verilerin Äziflenmesi (Data Encryption):** Verileri sunucuya gÄ±ndermeden Änce istemci tarafÄ±nda Äzifleme.
7. **Sunucu YanÄ±tlarÄ±nÄ± Ä°mzalama (Response Signing):** Sunucudan gelen yanÄ±tlarÄ± dijital imza ile doÄrulama.
8. **Sunucu Yedekleme:** Sunucuda tutulan kritik verilerin dÄ±zenli olarak yedeklenmesi ve Äzifli olarak saklanmasÄ±.
9. **GÄ±venli Oturum Kapatma (Secure Session Termination):** Oturum sona erdiÅinde oturum anahtarlarÄ±nÄ± gÄ±venli bir Äekilde temizleme.
10. **Kimlik DoÄrulama Loglama:** Sunucu tarafÄ±nda tÄ±m kimlik doÄrulama iÅlemlerinin loglanması ve gerektiÅinde izlenebilmesi.

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

1.5.1 1. Depolama Halindeki Veriler Ä°Åin GÄ±venlik YÄntemleri (Data Security Methods During Stored State)

1.5.1.1 Teorik AAÄ±klama: Veriler sabit disklerde, veri tabanlarÄ±nda veya bulut ortamlarÄ±nda depolandÄ±Åında, bu verilerin korunmasÄ± gerekir. Äzifleme ve bÄ±tÄ±nlÄ±k kontrolÄ± gibi yÄntemler, depolanan verilerin izinsiz eriÅimlere ve saldÄ±rlara karÅÄ± korunmasÄ±nÄ± saÄlar.

1.5.1.2 Uygulamalar:

1. **Whitebox AES:** Depolama alanında AES algoritması 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 için dosya sisteminde güvenli kabuk oluşturulması.
4. **Anahtar Yönetimi:** Şifreleme anahtarları güvenli bir şekilde saklanması ve düzenli olarak değiştirilmesi.
5. **Şifreli Veritabanı:** Veritabanındaki hassas verilerin şifrelenmesi ve sadece yetkili kullanıcılar erişebilmesi.
6. **Depolanan Verilerin Şifrelenmesi:** Tüm verilerin şifreli bir formatta saklanması ve yetkisiz erişimlerin engellenmesi.
7. **Dosya Güvenlik 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 alınmaz şekilde silinmesi.
10. **Dosya Güvenlik Kontroleri:** Dosyaların bütünlük kontrolü için oluşturulan 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 bütünlük kontrolü ve izinsiz erişimleri engellemek için son derece önemlidir.

1.6.1.2 Uygulamalar:

1. **Anahtarların Şifrelenmesi:** Statik anahtarları güvenli bir şekilde depolanması için şifreleme yöntemleri kullanma.
2. **Kaynak Kodların Koruma:** Kaynak kodlarının izinsiz kopyalanması ve değiştirilmesini engelleyen mekanizmalar geliştirme.
3. **Statik Dosyaların Güvenlik Kontrolü:** Sabit dosyaların bütünlük kontrolü için oluşturulan ve yetkisiz değişikliklerin önlenmesi.
4. **Veri Ömzeleri:** Depolanan verilerin değiştirilemeyeceğini doğrulamak için dijital imza kullanma.
5. **Veritabanı Güvenlik Kontrolü:** Veritabanında bulunan kritik verilerin şifrelenmesi ve bütünlük kontrolü için oluşturulan mekanizmalar.
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. **Özme ve Şifreleme Kombinasyonu:** Statik dosyaların bütünlük kontrolü için oluşturulan ve yetkisiz değişiklikleri engellemek için oluşturulan mekanizmalar.
10. **Dosya Güvenlik Duvarı:** Statik dosyaların korunması için dosya güvenli duvar 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 venli ini sa ylar.

1.6.2.2 Uygulamalar:

1. **Dinamik Anahtarlar n G venli i:** Dinamik anahtarlar n yaln zca belirli oturumlar s ras nda kullan lmas  ve g venli bir  yekilde de yitirilmesi.
2. **Oturum Bilgisi  zifreleme:** Kullan c  oturumlar 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 Korunmas :** Dinamik oturum verilerinin  zifrelenerek g vence alt na al nmas .
5. **Dinamik Anahtar Y netimi:** Oturum s ras nda kullan lan dinamik anahtarlar n g venli bir  yekilde olu turulmas  ve y netilmesi.
6. **Oturum Zaman A m :** Kullan c  oturumlar  i sin otomatik zaman a m  mekanizmas  uygulayarak g venli i art rma.
7. **Verilerin S rekli  zlenmesi:** Dinamik verilerin  zifrelenerek izlenmesi ve g venlik ihlallerinin an nda tespit edilmesi.
8. **Veri Manip lasyonu Engelleme:** Dinamik verilerin manip l edilmesini engelleyen g venlik mekanizmalar  kurma.
9. **Dinamik Veri  mzas :** Oturum s ras nda de yitirilen verilerin b t nl k do rulama i sin dijital imza kullanma.
10. **Ger sek Zamanl  Veri Analizi:** Oturum s ras nda olu an dinamik verileri analiz eden g venlik protokollerini devreye sokma.

1.7 Varl k  zellikleri (Property of Assets)

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

1.7.0.2 Uygulamalar:

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

- Statik ve Dinamik Varlıkların Korunması

1.8.2 Gelecek Hafta:

- Sertifikalar ve Şifreleme Yöntemleri
- Kimlik Doğrulama ve Veri Güvenliği

3.Hafta – Sonu