CE407 GÃ¼venli Programlama Hafta-3

Veri GÃ¼venliÄŸi: KullanÄ±mda, AktarÄ±mda ve Depolamada

Yazar: Dr. Ã–Ğr. Üyesi UÄŸur CORUH

İçindekiler

Şekil Listesi

Tablo Listesi

1 CE407 GÃ¼venli Programlama

1.1 Hafta-3

1.1.0.1 Veri GÃ¼venliÄŸi: KullanÄ±mda, AktarÄ±mda ve Depolamada Ö°ndir PDF[1], DOCX[2], SLIDE[3], PPTX[4]

1.1.1 Outline

- Veri GÃ¼venliÄŸi: KullanÄ±mda, AktarÄ±mda ve Depolamada

[1] ce407-week-3.tr_doc.pdf
[2] ce407-week-3.tr_word.docx
[3] ce407-week-3.tr_slide.pdf
[4] ce407-week-3.tr_slide.pptx

- YazÄ±lÄ±m GeliÅŸtirme SÃ¼reÃ§leri
  - KullanÄ±mda Veri GÃ¼venliÄŸi
  - AktarÄ±mda Veri GÃ¼venliÄŸi
  - Depolamada Veri GÃ¼venliÄŸi
- Dinamik ve Statik VarlÄ±klarÄ±n KorunmasÄ±

1.2 Hafta-3: Veri GÃ¼venliÄŸi - KullanÄ±mda, AktarÄ±mda ve Depolama Halindeki Veri GÃ¼venliÄŸi

1.2.0.1 Teorik Konu BaÅŸlÄ±klarÄ± ve Uygulamalar

1.3 KullanÄ±mda Veri GÃ¼venliÄŸi (Data-In-Use Security)

1.3.1 1. Ã‡alÄ±ÅŸma ZamanÄ± Uygulama Verisi GÃ¼venliÄŸi (Runtime Application Data Security)

1.3.1.1 Teorik AÃ§Ä±klama: KullanÄ±mda veri gÃ¼venliÄŸi, uygulama Ã§alÄ±ÅŸÄ±rken bellekte tutulan hassas bilgilerin korunmasÄ± ile ilgilenir. Bu gÃ¼venlik, Ã¶zellikle bellekte geÃ§ici olarak bulunan verilerin kÃ¶tÃ¼ amaÃ§lÄ± yazÄ±lÄ±mlar tarafÄ±ndan ele geÃ§irilmesini engellemek iÃ§in kullanÄ±lÄ±r.

1.3.1.2 Uygulamalar:

1. **Bellek Åžifreleme:** Bellekteki hassas verilerin ÅŸifrelenmesi.
2. **KÃ¶tÃ¼ye KullanÄ±m Tespiti:** Bellekteki ÅŸÃ¼pheli hareketlerin izlenmesi ve mÃ¼dahale edilmesi.
3. **Veri ManipÃ¼lasyonu Testleri:** Ã‡alÄ±ÅŸma zamanÄ±ndaki verilerin yanlÄ±ÅŸlÄ±kla veya kasÄ±tlÄ± olarak deÄŸiÅŸtirilip deÄŸiÅŸtirilmediÄŸini test etme.
4. **Dinamik Bellek YÃ¶netimi:** Bellek sÄ±zÄ±ntÄ±larÄ±nÄ± engellemek ve veri sÄ±zÄ±ntÄ±larÄ±nÄ± minimize etmek.
5. **SÃ¼rekli Kimlik DoÄŸrulama:** KullanÄ±cÄ±larÄ±n oturumlarÄ± sÃ¼resince kimliklerinin tekrar tekrar doÄŸrulanmasÄ±.
6. **Veri Maskelenmesi:** Hassas verilerin yalnÄ±zca yetkili sÃ¼reÃ§ler tarafÄ±ndan gÃ¶rÃ¼lebilir olmasÄ±.
7. **Tamperproof MekanizmalarÄ±:** Bellekteki verilerin manipÃ¼le edilip edilmediÄŸini kontrol eden ve bu verilerin deÄŸiÅŸtirilmesi durumunda sistemin tepki vermesini saÄŸlayan mekanizmalar.
8. **GÃ¼venlik Protokollerinin Ä°zlenmesi:** Uygulama Ã§alÄ±ÅŸÄ±rken kullanÄ±lan gÃ¼venlik protokollerinin anormal davranÄ±ÅŸlarÄ±nÄ± izleme.
9. **Veri GÃ¼venlik DuvarlarÄ±:** Bellek iÃ§indeki hassas verilerin yalnÄ±zca yetkili sÃ¼reÃ§ler tarafÄ±ndan eriÅŸilebileceÄŸi gÃ¼venlik katmanlarÄ± ekleme.
10. **GeliÅŸmiÅŸ KayÄ±t Tutma:** Bellekteki veriler Ã¼zerinde gerÃ§ekleÅŸtirilen tÃ¼m iÅŸlemlerin kayÄ±t altÄ±na alÄ±nmasÄ±.

1.4 AktarÄ±mda Veri GÃ¼venliÄŸi (Data-In-Transit Security)

1.4.1 1. Veri AktarÄ±mÄ± SÄ±rasÄ±nda GÃ¼venlik YÃ¶ntemleri (Data Security Methods During Transportation)

1.4.1.1 Teorik AÃ§Ä±klama: Verilerin aÄŸ Ã¼zerinden aktarÄ±lmasÄ± sÄ±rasÄ±nda, bu verilerin gizliliÄŸinin ve bÃ¼tÃ¼nlÃ¼ÄŸÃ¼nÃ¼n korunmasÄ± gerekir. GÃ¼venli bir ÅŸekilde veri aktarÄ±mÄ± saÄŸlamak iÃ§in ÅŸifreleme, kimlik doÄŸrulama ve bÃ¼tÃ¼nlÃ¼k kontrolleri uygulanÄ±r.

1.4.1.2 Uygulamalar:

1. **Oturum AnahtarÄ± (Session Key):** Ã°stemci ve sunucu arasÄ±nda dinamik olarak oturum anahtarÄ± oluÅŸturma ve bu anahtar ile ÅŸifreleme yapma.
2. **Cihaz BaÄŸlama (Device Binding):** Verilerin belirli bir cihaza baÄŸlÄ± olarak iletilmesini saÄŸlayarak, verilerin farklÄ± bir cihazda Ã§Ã¶zÃ¼lmesini engelleme.

3. **SÃ¼rÃ¼m BaÄŸlama (Version Binding):** YalnÄ±zca belirli sÃ¼rÃ¼mlerin veri iletimine izin vererek, gÃ¼venlik aÃ§Ä±klarÄ± barÄ±ndÄ±ran eski sÃ¼rÃ¼mlerin veri almasÄ±nÄ± engelleme.
4. **Åžifrelenmiåž YÃ¼k (Confidential Payload):** TaåŸÄ±nan verinin åŸifrelenerek sadece yetkili taraflar tarafÄ±ndan okunabilir hale getirilmesi.
5. **BÃ¼tÃ¼nlÃ¼k KontrolÃ¼ (Integrity Control):** Veri aktarÄ±mÄ± sÄ±rasÄ±nda verilerin bozulmadan veya deÄŸiåŸtirilmeden iletildiÄŸini doÄŸrulama.
6. **Kimlik DoÄŸrulama (Authenticity Control):** Veri gÃ¶nderenin ve alÄ±cÄ±nÄ±n kimliklerinin doÄŸrulanmasÄ±.
7. **GÃ¼venli Ä°letiåžim Kanalları (Secure Communication Channels):** SSL/TLS protokollerini kullanarak gÃ¼venli veri aktarÄ±mÄ± gerÃ§ekleåŸtirme.
8. **SSL SertifikalarÄ±:** Sunucu doÄŸrulamasÄ±nda SSL sertifikalarÄ± kullanarak veri aktarÄ±mÄ± sÄ±rasÄ±nda gÃ¼venliÄŸi artÄ±rma.
9. **Veri Ä°zleme (Data Monitoring):** AktarÄ±m sÄ±rasÄ±nda verinin izlenmesi ve anormal durumlarÄ±n tespiti.
10. **Åžifreli Ä°letiåžim Protokolleri:** HTTPS, SSH gibi åŸifreli protokoller Ã¼zerinden veri iletiåŸimi yapma.

1.4.2 2. Sunucu Ä°letiåžimi (Server Communication)

1.4.2.1 Teorik AÃ§Ä±klama: Sunucu ile istemci arasÄ±ndaki gÃ¼venli iletiåžim, verilerin gÃ¼venli bir åŸekilde sunucuya aktarÄ±lmasÄ±nÄ± saåŸlar. Bu sÃ¼reÃ§te sunucunun kimliÄŸini doÄŸrulamak ve iletilen verilerin åŸifrelenmesi bÃ¼yÃ¼k Ã¶nem taåŸÄ±r.

1.4.2.2 Uygulamalar:

1. **Sunucu Kimlik DoÄŸrulama Kodu (Server Authentication Code):** Sunucunun kimliÄŸini doÄŸrulayan Ã¶zel bir kimlik doÄŸrulama mekanizmasÄ± geliåŸtirme.
2. **GÃ¼venli Sunucu Ä°letiåžimi (Secure Server Communication):** Sunucu ve istemci arasÄ±nda verilerin SSL/TLS ile åŸifrelenmesini saåŸlama.
3. **Oturum AnahtarÄ± Åžifreleme (Session Key Encryption):** Verilerin oturum anahtarlarÄ± kullanÄ±larak åŸifrelenmesini saåŸlama.
4. **Sunucu Ãœzerinde Veri Ä°zleme (Data Monitoring):** Sunucuya gelen ve giden veri trafiÄŸini izleyip anormallikleri tespit etme.
5. **Veri BÃ¼tÃ¼nlÃ¼ÄŸÃ¼ DoÄŸrulama:** Verilerin sunucuya bozulmadan iletildiÄŸini doÄŸrulayan bÃ¼tÃ¼nlÃ¼k kontrol mekanizmalarÄ±nÄ± kullanma.
6. **Verilerin Åžifrelenmesi (Data Encryption):** Verileri sunucuya gÃ¶ndermeden Ã¶nce istemci tarafÄ±nda åŸifreleme.
7. **Sunucu YanÄ±tlarÄ±nÄ± Ä°mzalama (Response Signing):** Sunucudan gelen yanÄ±tlarÄ± dijital imza ile doÄŸrulama.
8. **Sunucu Yedekleme:** Sunucuda tutulan kritik verilerin dÃ¼zenli olarak yedeklenmesi ve åŸifreli olarak saklanmasÄ±.
9. **GÃ¼venli Oturum Kapatma (Secure Session Termination):** Oturum sona erdiÄŸinde oturum anahtarlarÄ±nÄ±n gÃ¼venli bir åŸekilde temizlenmesi.
10. **Kimlik DoÄŸrulama Loglama:** Sunucu tarafÄ±nda tÃ¼m kimlik doÄŸrulama iåŸlemlerinin loglanmasÄ± ve gerektiÄŸinde izlenebilmesi.

1.5 Depolamada Veri GÃ¼venliÄŸi (Data-At-Rest Security)

1.5.1 1. Depolama Halindeki Veriler Ä°Ã§in GÃ¼venlik YÃ¶ntemleri (Data Security Methods During Stored State)

1.5.1.1 Teorik AÃ§Ä±klama: Veriler sabit disklerde, veri tabanlarÄ±nda veya bulut ortamlarÄ±nda depolandÄ±ÄŸÄ±nda, bu verilerin korunmasÄ± gerekir. Åžifreleme ve bÃ¼tÃ¼nlÃ¼k kontrolÃ¼ gibi yÃ¶ntemler, depolanan verilerin izinsiz eriåŸimlere ve saldÄ±rÄ±lara karåŸÄ± korunmasÄ±nÄ± saåŸlar.

1.5.1.2 Uygulamalar:

1. **Whitebox AES:** Depolama alanÄ±nda AES algoritmasÄ±nÄ± whitebox yÃ¶ntemiyle uygulayarak verilerin daha gÃ¼venli bir ÅŸekilde korunmasÄ±nÄ± saÄŸlama.
2. **Whitebox DES:** Whitebox DES algoritmasÄ±yla verilerin ÅŸifrelenmesi ve gÃ¼venlik testlerinin yapÄ±lmasÄ±.
3. **GÃ¼venlik Kabuk Matrisi (Security Shell Matrix):** Verilerin gÃ¼venli bir ÅŸekilde depolanmasÄ±nÄ± saÄŸlamak iÃ§in dosya sisteminde gÃ¼venlik kabuÄŸu oluÅŸturma.
4. **Anahtar YÃ¶netimi:** Åžifreleme anahtarlarÄ±nÄ±n gÃ¼venli bir ÅŸekilde saklanmasÄ± ve dÃ¼zenli olarak deÄŸiÅŸtirilmesi.
5. **Åžifreli VeritabanÄ±:** VeritabanÄ±ndaki hassas verilerin ÅŸifrelenmesi ve sadece yetkili kullanÄ±cÄ±larÄ±n eriÅŸebilmesi.
6. **Depolanan Verilerin Åžifrelenmesi:** TÃ¼m verilerin ÅŸifreli bir formatta saklanmasÄ± ve yetkisiz eriÅŸimlerin engellenmesi.
7. **Dosya BÃ¼tÃ¼nlÃ¼ÄŸÃ¼ Kontrolleri:** Depolanan dosyalarÄ±n izinsiz deÄŸiÅŸtirilip deÄŸiÅŸtirilmediÄŸini kontrol eden mekanizmalar.
8. **Veri Yedekleme:** Kritik verilerin dÃ¼zenli olarak yedeklenmesi ve yedeklerin ÅŸifreli olarak saklanmasÄ±.
9. **GÃ¼venli Silme:** Depolama alanÄ±ndaki verilerin silinmesi gerektiÄŸinde, verilerin geri alÄ±namaz ÅŸekilde silinmesi.
10. **BÃ¼tÃ¼nlÃ¼k Kontrolleri:** DosyalarÄ±n bÃ¼tÃ¼nlÃ¼ÄŸÃ¼nÃ¼ doÄŸrulayan ve yetkisiz deÄŸiÅŸiklikleri tespit eden mekanizmalar kullanma.

1.6 Statik ve Dinamik VarlÄ±klarÄ±n KorunmasÄ± (Protection of Static and Dynamic Assets)

1.6.1 1. Statik VarlÄ±klarÄ±n KorunmasÄ± (Protection of Static Assets)

1.6.1.1 Teorik AÃ§Ä±klama: Statik varlÄ±klar, veritabanÄ±nda veya sabit depolama ortamÄ±nda deÄŸiÅŸmeden duran verilerden oluÅŸur. Bu varlÄ±klarÄ±n korunmasÄ±, veri bÃ¼tÃ¼nlÃ¼ÄŸÃ¼nÃ¼ saÄŸlamak ve izinsiz eriÅŸimleri engellemek iÃ§in son derece Ã¶nemlidir.

1.6.1.2 Uygulamalar:

1. **AnahtarlarÄ±n Åžifrelenmesi:** Statik anahtarlarÄ±n gÃ¼venli bir ÅŸekilde depolanmasÄ± iÃ§in ÅŸifreleme yÃ¶ntemleri kullanma.
2. **Kaynak KodlarÄ± Koruma:** Kaynak kodlarÄ±nÄ±n izinsiz kopyalanmasÄ±nÄ± ve deÄŸiÅŸtirilmesini engelleyen mekanizmalar geliÅŸtirme.
3. **Statik DosyalarÄ±n BÃ¼tÃ¼nlÃ¼k KontrolÃ¼:** Sabit dosyalarÄ±n bÃ¼tÃ¼nlÃ¼ÄŸÃ¼nÃ¼ saÄŸlayarak izinsiz deÄŸiÅŸikliklerin Ã¶nlenmesi.
4. **Veri Ã°mzasÄ±:** Depolanan verilerin deÄŸiÅŸtirilemeyeceÄŸini doÄŸrulamak iÃ§in dijital imza kullanma.
5. **VeritabanÄ± BÃ¼tÃ¼nlÃ¼ÄŸÃ¼:** VeritabanÄ±nda bulunan kritik verilerin ÅŸifrelenmesi ve bÃ¼tÃ¼nlÃ¼ÄŸÃ¼nÃ¼n korunmasÄ±.
6. **Dosya EriÅŸim KontrolÃ¼:** Statik dosyalarÄ±n yetkisiz eriÅŸimlere karÅŸÄ± korunmasÄ± iÃ§in eriÅŸim kontrol mekanizmalarÄ±nÄ± devreye sokma.
7. **Gizli Anahtar YÃ¶netimi:** Statik anahtarlarÄ±n gÃ¼venli bir ÅŸekilde saklanmasÄ± ve yÃ¶netilmesi.
8. **VeritabanÄ± Åžifreleme:** Statik verilerin ÅŸifrelenerek veri tabanÄ±nda gÃ¼venli bir ÅŸekilde saklanmasÄ±nÄ± saÄŸlama.
9. **Ã°mza ve Åžifreleme Kombinasyonu:** Statik dosyalarÄ±n bÃ¼tÃ¼nlÃ¼ÄŸÃ¼nÃ¼ saÄŸlamak ve ÅŸifreleme ile birlikte dijital imza kullanarak gÃ¼venliÄŸi artÄ±rma.
10. **Dosya GÃ¼venlik DuvarÄ±:** Statik dosyalarÄ±n korunmasÄ± iÃ§in dosya gÃ¼venlik duvarÄ± oluÅŸturma.

1.6.2 2. Dinamik VarlÄ±klarÄ±n KorunmasÄ± (Protection of Dynamic Assets)

1.6.2.1 Teorik AÃ§Ä±klama: Dinamik varlÄ±klar, uygulama Ã§alÄ±ÅŸÄ±rken oluÅŸturulan ve sÃ¼rekli deÄŸiÅŸen verilerdir. Bu verilerin korunmasÄ±, Ã¶zellikle oturum bilgileri ve dinamik anahtarlar gibi hassas bilgilerin gÃ¼venliÄŸini saÄŸlar.

1.6.2.2 Uygulamalar:

1. **Dinamik AnahtarlarÄ±n GÃ¼venliÄŸi:** Dinamik anahtarlarÄ±n yalnÄ±zca belirli oturumlar sÄ±rasÄ±nda kullanÄ±lmasÄ± ve gÃ¼venli bir ÅŸekilde deÄŸiÅŸtirilmesi.
2. **Oturum Bilgisi Åžifreleme:** KullanÄ±cÄ± oturumlarÄ±nÄ±n gizliliÄŸini saÄŸlamak iÃ§in oturum bilgilerini ÅŸifreleme.
3. **Cihaz Parmak Ä°zlerinin KorunmasÄ±:** Cihaz parmak izlerinin yalnÄ±zca yetkili taraflarca doÄŸrulanmasÄ±nÄ± saÄŸlama.
4. **Oturum Verisi KorumasÄ±:** Dinamik oturum verilerinin ÅŸifrelenerek gÃ¼vence altÄ±na alÄ±nmasÄ±.
5. **Dinamik Anahtar YÃ¶netimi:** Oturum sÄ±rasÄ±nda kullanÄ±lan dinamik anahtarlarÄ±n gÃ¼venli bir ÅŸekilde oluÅŸturulmasÄ± ve yÃ¶netilmesi.
6. **Oturum Zaman AÅŸÄ±mÄ±:** KullanÄ±cÄ± oturumlarÄ± iÃ§in otomatik zaman aÅŸÄ±mÄ± mekanizmasÄ± uygulayarak gÃ¼venliÄŸi artÄ±rma.
7. **Verilerin SÃ¼rekli Ä°zlenmesi:** Dinamik verilerin ÅŸifrelenerek izlenmesi ve gÃ¼venlik ihlallerinin anÄ±nda tespit edilmesi.
8. **Veri ManipÃ¼lasyonu Engelleme:** Dinamik verilerin manipÃ¼le edilmesini engelleyen gÃ¼venlik mekanizmalarÄ± kurma.
9. **Dinamik Veri Ä°mzasÄ±:** Oturum sÄ±rasÄ±nda deÄŸiÅŸtirilen verilerin bÃ¼tÃ¼nlÃ¼ÄŸÃ¼nÃ¼ doÄŸrulamak iÃ§in dijital imza kullanma.
10. **GerÃ§ek ZamanlÄ± Veri Analizi:** Oturum sÄ±rasÄ±nda oluÅŸan dinamik verileri analiz eden gÃ¼venlik protokollerini devreye sokma.

1.7 VarlÄ±k Ã–zellikleri (Property of Assets)

1.7.0.1 Teorik AÃ§Ä±klama: Bir varlÄ±ÄŸÄ±n Ã¶zellikleri, onun adÄ±nÄ±, tanÄ±mÄ±nÄ±, konumunu, kaynaÄŸÄ±nÄ±, boyutunu, oluÅŸturulma ve silinme zamanÄ±nÄ± iÃ§erir. AyrÄ±ca, bir varlÄ±ÄŸÄ±n gizlilik (Confidentiality), bÃ¼tÃ¼nlÃ¼k (Integrity) ve doÄŸrulama (Authentication) gibi gÃ¼venlik gereksinimlerine karÅŸÄ± nasÄ±l korunacaÄŸÄ±nÄ± belirlemek Ã¶nemlidir.

1.7.0.2 Uygulamalar:

1. **VarlÄ±k Ä°smi (Asset Name):** VarlÄ±ÄŸÄ±n adÄ±nÄ± belirleyerek bu varlÄ±ÄŸÄ±n ne olduÄŸunu tanÄ±mlama.
2. **TanÄ±m (Description):** VarlÄ±ÄŸÄ±n ne iÅŸlev gÃ¶rdÃ¼ÄŸÃ¼nÃ¼ ve hangi bilgileri iÃ§erdiÄŸini aÃ§Ä±klama.
3. **Konum (Location):** VarlÄ±ÄŸÄ±n bulunduÄŸu veri tabanÄ±, tablo veya kolon gibi fiziksel konumunu belirleme.
4. **Kaynak (Source):** VarlÄ±ÄŸÄ±n kaynaÄŸÄ±nÄ± belirleyerek hangi sÃ¼reÃ§ veya veri kaynaÄŸÄ±ndan geldiÄŸini tanÄ±mlama.
5. **Boyut (Size):** VarlÄ±ÄŸÄ±n boyutunu belirleyerek depolama ihtiyaÃ§larÄ±nÄ± optimize etme.
6. **OluÅŸturulma ZamanÄ± (Creation Time):** VarlÄ±ÄŸÄ±n oluÅŸturulduÄŸu tarihi ve zamanÄ± belirleyerek log kayÄ±tlarÄ±nÄ± tutma.
7. **Silinme ZamanÄ± (Destroy Time):** VarlÄ±ÄŸÄ±n ne zaman imha edileceÄŸini ve bu sÃ¼recin nasÄ±l yÃ¶netileceÄŸini belirleme.
8. **VarsayÄ±lan DeÄŸer (Default Value):** VarlÄ±ÄŸÄ±n varsayÄ±lan deÄŸerini tanÄ±mlayarak, ilk durumda nasÄ±l olacaÄŸÄ±nÄ± belirtme.
9. **Gizlilik, BÃ¼tÃ¼nlÃ¼k ve DoÄŸrulama:** VarlÄ±klarÄ±n gÃ¼venlik gereksinimlerine gÃ¶re koruma seviyelerini tanÄ±mlama (C - Confidentiality, I - Integrity, A - Authentication).
10. **VarlÄ±k Koruma Åžemasi:** Her varlÄ±ÄŸÄ±n gÃ¼venlik ihtiyaÃ§larÄ±na gÃ¶re Ã¶zel bir koruma planÄ± oluÅŸturarak, hangi Ã¶nlemlerin alÄ±nmasÄ± gerektiÄŸini belirleme.

1.8 HaftanÄ±n Ã–zeti ve Gelecek Hafta

1.8.1 Bu Hafta:

- **KullanÄ±mda, AktarÄ±mda ve Depolamada Veri GÃ¼venliÄŸi**
- **Statik ve Dinamik VarlÄ±klarÄ±n KorunmasÄ±**

1.8.2 Gelecek Hafta:

- **Sertifikalar ve Åžifreleme YÃ¶ntemleri**
- **Kimlik DoÄŸrulama ve Veri BÃ¼tÃ¼nlÃ¼ÄŸÃ¼**

$3. Hafta - Sonu$