CEN429 GÃ¼venli Programlama Hafta-12

GÃ¼venlik Gereksinimleri ve Standartlar

Yazar: Dr. UÄŸur CORUH

İçindekiler

Şekil Listesi

Tablo Listesi

1 CEN429 GÃ¼venli Programlama

1.1 Hafta-12

1.1.0.1 GÃ¼venlik Gereksinimleri ve Standartlar Ä°ndir

- PDF[1]
- DOC[2]
- SLIDE[3]
- PPTX[4]

1.1.1 Outline

- GÃ¼venlik Gereksinimlerinin Ã–nemi
- UluslararasÄ± GÃ¼venlik StandartlarÄ±
- YaygÄ±n GÃ¼venlik SertifikalarÄ±

1.1.2 Hafta-12: GÃ¼venlik Gereksinimleri ve Standartlar

Bu hafta, gÃ¼venlik gereksinimlerinin nasÄ±l tanÄ±mlandÄ±ÄŸÄ±nÄ±, uluslararasÄ± gÃ¼venlik standartlarÄ±nÄ±n nasÄ±l oluÅŸturulduÄŸunu ve yaygÄ±n kullanÄ±lan gÃ¼venlik sertifikalarÄ± ile uyumlu olmanÄ±n neden Ã¶nemli olduÄŸunu Ã¶ÄŸreneceÄŸiz. GÃ¼venlik gereksinimleri, bir sistemin saldÄ±rÄ±lara karÅŸÄ± ne kadar dayanÄ±klÄ± olduÄŸunu belirlemek iÃ§in tasarlanmÄ±ÅŸtÄ±r. Bu standartlar, birÃ§ok sektÃ¶rde gÃ¼venliÄŸi saÄŸlamak iÃ§in kullanÄ±lÄ±r.

1.1.2.1 1. GÃ¼venlik Gereksinimlerinin Ã–nemi Teorik AÃ§Ä±klama: Bir sistemin gÃ¼venli olabilmesi iÃ§in, belirli gÃ¼venlik gereksinimlerini karÅŸÄ±lamasÄ± gereklidir. Bu gereksinimler, sistemin hangi tehditlere karÅŸÄ± korunmasÄ± gerektiÄŸini ve hangi gÃ¼venlik Ã¶nlemlerinin alÄ±nacaÄŸÄ±nÄ± belirler.

[1] pandoc_cen429-week-12.pdf
[2] pandoc_cen429-week-12.docx
[3] cen429-week-12.pdf
[4] cen429-week-12.pptx

- **GÃ¼venlik Gereksinimlerinin BaÅŸlÄ±ca Kategorileri:**
  - **Gizlilik (Confidentiality):** Yetkisiz kiÅŸilerin bilgilere eriÅŸiminin engellenmesi.
  - **BÃ¼tÃ¼nlÃ¼k (Integrity):** Verilerin yetkisiz kiÅŸiler tarafÄ±ndan deÄŸiÅŸtirilmesinin engellenmesi.
  - **Kimlik DoÄŸrulama (Authentication):** Sisteme eriÅŸen kiÅŸilerin kimliÄŸinin doÄŸrulanmasÄ±.
  - **Yetkilendirme (Authorization):** Sadece belirli kiÅŸilerin belirli kaynaklara eriÅŸebilmesi.
  - **KayÄ±t Tutma (Auditing):** OlaylarÄ±n kaydedilmesi ve izlenebilmesi.
  - **SÃ¼reklilik (Availability):** Sistemin kesintisiz Ã§alÄ±ÅŸmasÄ±nÄ± saÄŸlama.

Uygulama Ã–rnekleri:

1. Bir uygulama iÃ§in gÃ¼venlik gereksinimlerini belirleme.
2. VeritabanÄ± gÃ¼venliÄŸinin nasÄ±l saÄŸlanabileceÄŸini analiz etme.

1.1.2.2 2. ETSI (European Telecommunications Standards Institute) Teorik AÃ§Ä±klama: ETSI, Avrupa TelekomÃ¼nikasyon StandartlarÄ± EnstitÃ¼sÃ¼ tarafÄ±ndan belirlenen standartlar, Ã¶zellikle aÄŸ gÃ¼venliÄŸi, mobil iletiÅŸim ve IoT cihazlarÄ± gibi alanlarda kullanÄ±lÄ±r.

- **ETSIâ€™nin GÃ¶revleri:**
  - TelekomÃ¼nikasyon teknolojilerinde uluslararasÄ± standartlar geliÅŸtirmek.
  - Mobil aÄŸlar iÃ§in gÃ¼venlik Ã§Ã¶zÃ¼mleri saÄŸlamak.
  - 5G gÃ¼venlik standartlarÄ±nÄ± oluÅŸturmak.

Uygulama Ã–rnekleri:

1. ETSI standartlarÄ±na gÃ¶re bir IoT cihazÄ±nÄ±n gÃ¼venliÄŸini inceleme.
2. ETSI tarafÄ±ndan belirlenen gÃ¼venlik gereksinimlerine gÃ¶re bir aÄŸ yapÄ±landÄ±rmasÄ± oluÅŸturma.

1.1.2.3 3. GSMA (GSM Association) Teorik AÃ§Ä±klama: GSMA, mobil cihazlar ve aÄŸlar iÃ§in gÃ¼venlik standartlarÄ±nÄ± belirler. GSMA, Ã¶zellikle SIM kart gÃ¼venliÄŸi, aÄŸ gÃ¼venliÄŸi ve mobil operatÃ¶rler iÃ§in protokoller saÄŸlar.

- **GSMAâ€™nÄ±n RolÃ¼:**
  - Mobil aÄŸlarda kullanÄ±lan protokoller iÃ§in gÃ¼venlik standartlarÄ± oluÅŸturmak.
  - SIM kart ve eSIM gÃ¼venlik standartlarÄ±nÄ± yÃ¶netmek.
  - Mobil operatÃ¶rler arasÄ±nda gÃ¼venli veri alÄ±ÅŸveriÅŸini saÄŸlamak.

Uygulama Ã–rnekleri:

1. GSMA standartlarÄ±na gÃ¶re bir mobil cihazÄ±n gÃ¼venlik gereksinimlerini belirleme.
2. GSMA tarafÄ±ndan Ã¶nerilen gÃ¼venlik protokollerini mobil uygulama geliÅŸtirme sÃ¼reÃ§lerine entegre etme.

1.1.2.4 4. EMV (Europay, MasterCard, Visa) Teorik AÃ§Ä±klama: EMV, Ã¶deme kartÄ± gÃ¼venliÄŸini saÄŸlamak amacÄ±yla oluÅŸturulmuÅŸ bir standarttÄ±r. Ã–zellikle kredi kartlarÄ± ve POS cihazlarÄ±nÄ±n gÃ¼venliÄŸini artÄ±rmak iÃ§in kullanÄ±lÄ±r.

- **EMV StandartlarÄ±:**
  - **MasterCard:** Kart gÃ¼venliÄŸi ve Ã¶deme sistemlerinin korunmasÄ±.
  - **Visa:** Kart sahiplerinin ve POS cihazlarÄ±nÄ±n gÃ¼venliÄŸini saÄŸlayan protokoller.

Uygulama Ã–rnekleri:

1. EMV standartlarÄ±na uygun bir Ã¶deme sisteminin gÃ¼venlik gereksinimlerini oluÅŸturma.
2. MasterCard ve Visa tarafÄ±ndan saÄŸlanan gÃ¼venlik protokollerini bir POS cihazÄ±na entegre etme.

1.1.2.5 5. EAL (Evaluation Assurance Level) Teorik AÃ§Ä±klama: EAL (DeÄŸerlendirme GÃ¼vencesi Seviyesi), bir Ã¼rÃ¼nÃ¼n gÃ¼venlik gereksinimlerini karÅŸÄ±lama dÃ¼zeyini gÃ¶sterir. EAL seviyeleri, sistemin gÃ¼venliÄŸini ne Ã¶lÃ§Ã¼de test ettiÄŸimizi belirler.

- **EAL Seviyeleri:**
  - **EAL1:** Fonksiyonel olarak test edilmiÅŸ.
  - **EAL2:** YapÄ±sal olarak test edilmiÅŸ.
  - **EAL3:** Metodolojik olarak test edilmiÅŸ ve denetlenmiÅŸ.
  - **EAL4:** TasarÄ±m bazÄ±nda gÃ¶zden geÃ§irilmiÅŸ, metodolojik olarak test edilmiÅŸ.
  - **EAL5 ve Ã¼zeri:** YÃ¼ksek gÃ¼venlik gereksinimleri saÄŸlayan sistemler.

Uygulama Ã–rnekleri:

1. EAL seviyelerine gÃ¶re bir sistemin gÃ¼venlik derecesini belirleme.
2. EAL4 seviyesinde bir sistem iÃ§in test senaryolarÄ± geliÅŸtirme.

1.1.2.6 6. Common Criteria (Ortak Kriterler) Teorik AÃ§Ä±klama: Common Criteria (Ortak Kriterler), uluslararasÄ± bir gÃ¼venlik sertifikasyon standardÄ±dÄ±r. Bu standart, Ã¼rÃ¼nlerin gÃ¼venlik seviyesini deÄŸerlendirmek iÃ§in kullanÄ±lÄ±r ve dÃ¼nya Ã§apÄ±nda kabul gÃ¶rmÃ¼ÅŸtÃ¼r.

- **Common Criteriaâ€™nin AvantajlarÄ±:**
  - Ãœcretsiz gÃ¼venliÄŸinin kÃ¼resel Ã§apta onaylanmasÄ±nÄ± saÄŸlar.
  - GÃ¼venlik Ã¶zelliklerinin doÄŸrulanmasÄ± iÃ§in ortak bir dil sunar.
  - EAL sertifikasyon sÃ¼reÃ§lerine uyumludur.

Uygulama Ã–rnekleri:

1. Common Criteria kapsamÄ±nda bir gÃ¼venlik sertifikasyonu sÃ¼reci baÅŸlatma.
2. Common Criteria uyumlu bir yazÄ±lÄ±m geliÅŸtirme planÄ± hazÄ±rlama.

1.1.2.7 7. FIPS (Federal Information Processing Standards) Teorik AÃ§Ä±klama: FIPS, Amerika BirleÅŸik Devletleri hÃ¼kÃ¼meti tarafÄ±ndan kullanÄ±lan bilgi iÅŸlem standartlarÄ±nÄ± tanÄ±mlar. FIPS, Ã¶zellikle kriptografik modÃ¼llerin gÃ¼venliÄŸi iÃ§in kullanÄ±lan bir standarttÄ±r.

- **FIPSâ€™in Ã–nemi:**
  - ABD hÃ¼kÃ¼metine ait sistemlerde kullanÄ±lan gÃ¼venlik protokollerini tanÄ±mlar.
  - Kriptografik algoritmalar ve modÃ¼llerin sertifikalandÄ±rÄ±lmasÄ±nÄ± saÄŸlar.
  - Hassas bilgilerin gÃ¼venliÄŸini saÄŸlamak iÃ§in geliÅŸtirilmiÅŸ gÃ¼venlik standartlarÄ± sunar.

Uygulama Ã–rnekleri:

1. FIPS standardÄ±na uygun bir kriptografik modÃ¼l geliÅŸtirme.
2. FIPS sertifikalÄ± gÃ¼venlik algoritmalarÄ±nÄ± bir uygulamaya entegre etme.

1.1.2.8 SonuÃ§ Bu hafta, ETSI, GSMA, EMV, EAL, Common Criteria ve FIPS gibi gÃ¼venlik gereksinimleri ve standartlarÄ±nÄ± inceledik. Bu standartlar, uluslararasÄ± dÃ¼zeyde kabul gÃ¶rmÃ¼ÅŸ gÃ¼venlik protokollerini tanÄ±mlayarak sistemlerin ve Ã¼rÃ¼nlerin gÃ¼venliÄŸini saÄŸlamaya yardÄ±mcÄ± olur. GÃ¼venlik sertifikalarÄ±, Ã¼rÃ¼nlerin ve sistemlerin gÃ¼venlik aÃ§Ä±sÄ±ndan deÄŸerlendirildiÄŸini ve onaylandÄ±ÄŸÄ±nÄ± gÃ¶sterir.

$12. Hafta - Sonu$