

CEN429 GÃ¼venli Programlama Hafta-12

GÃ¼venlik Gereksinimleri ve Standartlar

Yazar: Dr. U    ur CORUH

İçindekiler

| | | |
|----------|--|----------|
| 1 | CEN429 GÃ¼venli Programlama | 1 |
| 1.1 | Hafta-12 | 1 |
| 1.1.1 | Outline | 1 |
| 1.1.2 | Hafta-12: GÃ¼venlik Gereksinimleri ve Standartlar | 1 |

Şekil Listesi

Tablo Listesi

1 CEN429 GÃ¼venli Programlama

1.1 Hafta-12

1.1.0.1 G \tilde{A} $^{1/4}$ venlik Gereksinimleri ve Standartlar \tilde{A}° ndir

- PDF¹
- DOC²
- SLIDE³
- PPTX⁴

1.1.1 Outline

- G \tilde{A} $\frac{1}{4}$ venlik Gereksinimlerinin \tilde{A} -nemi
- Uluslararası \tilde{A} \pm G \tilde{A} $\frac{1}{4}$ venlik Standartlar \tilde{A} \pm
- Yayg \tilde{A} \pm n G \tilde{A} $\frac{1}{4}$ venlik Sertifikalar \tilde{A} \pm

1.1.2 Hafta-12: $G\tilde{A}^{1/4}$ venlik Gereksinimleri ve Standartlar

Bu hafta, g¹/₄venlik gereksinimlerinin nas¹/₂ tan¹/₂mland¹/₂Ä¹/₂Ä±nÄ±, uluslararası g¹/₄venlik standartlarÄ±nÄ±n nas¹/₂ olu¹/₂turulduÄ±yunu ve yaygÄ±n kullanÄ±lan g¹/₄venlik sertifikalarÄ± ile uyumlu olmanÄ±n neden Ä±nemli olduÄ±yunu Ä¶Ä±reneceÄ±iz. G¹/₄venlik gereksinimleri, bir sistemin saldÄ±rÄ±lara karÄ±Ä± ne kadar dayanÄ±klÄ± olduÄ±yunu belirlemek iÄ±sin tasarlanmÄ±Ä±tÄ±r. Bu standartlar, birÄ±çok sektÄ±rde g¹/₄venliÄ±yi saÄ±lamak iÄ±sin kullanÄ±lÄ±r.

1.1.2.1 1. GÃ¼venlik Gereksinimlerinin Ånemi Teorik AÃklama: Bir sistemin gÃ¼venli olabilmesi iÃin, belirli gÃ¼venlik gereksinimlerini karÅılamasÄ± gereklidir. Bu gereksinimler, sistemin hangi tehditlere karÅı korunmasÄ± gerektiÄini ve hangi gÃ¼venlik Åeplerinin alÄınacaÄını belirler.

¹[pandoc_cen429-week-12.pdf](#)

²pandoc_cen429-week-12.docx

³[cen429-week-12.pdf](#)

⁴cen429-week-12.pptx

- **Güvenlik Gereksinimlerinin Başlıca Kategorileri:**
 - **Gizlilik (Confidentiality):** Yetkisiz kişilerin bilgilere erişiminin engellenmesi.
 - **Bütünlük (Integrity):** Verilerin yetkisiz kişiler tarafından değiştirilmesinin engellenmesi.
 - **Kimlik Doğrulama (Authentication):** Sisteme erişen kişilerin kimliğinin doğrulanması.
 - **Yetkilendirme (Authorization):** Sadece belirli kişilerin belirli kaynaklara erişebilmesi.
 - **Kayıt Tutma (Auditing):** Olayların kaydedilmesi ve izlenebilmesi.
 - **Süreklilik (Availability):** Sistemin kesintisiz çalışması sağlama.

Uygulama Örnekleri:

1. Bir uygulama için güvenlik gereksinimlerini belirleme.
2. Veritabanı güvenliğinin nasıl sağlanabileceğini analiz etme.

1.1.2.2 2. ETSI (European Telecommunications Standards Institute) Teorik Açıklama:

ETSI, Avrupa Telekomünikasyon Standartları Enstitüsü tarafından belirlenen standartlar, özellikle radyo güvenliği, mobil iletişim ve IoT cihazları gibi alanlarda kullanılır.

- **ETSI'nin Güvenlik Gereksinimleri:**
 - Telekomünikasyon teknolojilerinde uluslararası standartlar geliştirmek.
 - Mobil ağlar için güvenlik gereksinimlerini belirlemek.
 - 5G güvenlik standartlarını oluşturmak.

Uygulama Örnekleri:

1. ETSI standartlarına göre bir IoT cihazının güvenliğini inceleme.
2. ETSI tarafından belirlenen güvenlik gereksinimlerine göre bir ağ yapılandırması oluşturulması.

1.1.2.3 3. GSMA (GSM Association) Teorik Açıklama:

GSMA, mobil cihazlar ve ağlar için güvenlik standartlarını belirler. GSMA, özellikle SIM kart güvenliği, radyo güvenliği ve mobil operatörler için protokoller sağlar.

- **GSMA'nın Rolü:**
 - Mobil ağlarda kullanılan protokoller için güvenlik standartlarını oluşturmak.
 - SIM kart ve eSIM güvenlik standartlarını yayınlamak.
 - Mobil operatörler arasında güvenli veri alışverişini sağlamak.

Uygulama Örnekleri:

1. GSMA standartlarına göre bir mobil cihazın güvenlik gereksinimlerini belirleme.
2. GSMA tarafından önerilen güvenlik protokollerini mobil uygulama geliştirme süreçlerine entegre etme.

1.1.2.4 4. EMV (Europay, MasterCard, Visa) Teorik Açıklama:

EMV, ödeme kartı güvenliğini sağlamak amacıyla oluşturulmuş bir standarttır. Özellikle kredi kartları ve POS cihazları için güvenliğini artırmak için kullanılır.

- **EMV Standartları:**
 - **MasterCard:** Kart güvenliği ve ödeme sistemlerinin korunması.
 - **Visa:** Kart sahiplerinin ve POS cihazlarının güvenliğini sağlayan protokoller.

Uygulama Örnekleri:

1. EMV standartlarına uygun bir ödeme sisteminin güvenliğini oluşturulması.
2. MasterCard ve Visa tarafından sağlanan güvenlik protokollerini bir POS cihazına entegre etme.

1.1.2.5 5. EAL (Evaluation Assurance Level) Teorik Açıklama:

EAL (Değerlendirme Güvenliği Seviyesi), bir ürünün güvenlik gereksinimlerini karşılamada düzeyini gösterir. EAL seviyeleri, sistemin güvenliğini ne ölçüde test ettiğimizi belirler.

- **EAL Seviyeleri:**

- **EAL1:** Fonksiyonel olarak test edilmiÅŸ.
- **EAL2:** Yapısal olarak test edilmiÅŸ.
- **EAL3:** Metodolojik olarak test edilmiÅŸ ve denetlenmiÅŸ.
- **EAL4:** Tasarım bazında g zden ge şirilm  , metodolojik olarak test edilmiÅŸ.
- **EAL5 ve   zeri:** Y ksek g venlik gereksinimleri sa layan sistemler.

Uygulama   nekleri:

1. EAL seviyelerine g re bir sistemin g venlik derecesini belirleme.
2. EAL4 seviyesinde bir sistem i şin test senaryoları geli tirme.

1.1.2.6 6. Common Criteria (Ortak Kriterler) Teorik A ş klama: Common Criteria (Ortak Kriterler), uluslararası bir g venlik sertifikasyon standardıdır. Bu standart,   r nlerin g venlik seviyesini de erlendirmek i şin kullanılab r ve d nya   apında kabul g rm  t r.

- **Common Criteria  nin Avantajları:**

-   r n g venli inin k resel   apta onaylanması sa lar.
- G venlik   zelliklerinin do rulanması i şin ortak bir dil sunar.
- EAL sertifikasyon s re lerine uyumludur.

Uygulama   nekleri:

1. Common Criteria kapsamında bir g venlik sertifikasyonu s reci ba latma.
2. Common Criteria uyumlu bir yazılım geli tirme planı hazırlama.

1.1.2.7 7. FIPS (Federal Information Processing Standards) Teorik A ş klama: FIPS, Amerika Birle ik Devletleri h k meti tarafından kullanılan bilgi i lem standartlarıdır. FIPS,   zellikle kriptografik mod llerin g venli i i şin kullanılan bir standarttır.

- **FIPS  n   nemi:**

- ABD h k metine ait sistemlerde kullanılan g venlik protokollerini tanımlar.
- Kriptografik algoritmalar ve mod llerin sertifikalandırılması sa lar.
- Hassas bilgilerin g venli ini sa lamak i şin geli tirilmi  g venlik standartları sunar.

Uygulama   nekleri:

1. FIPS standardına uygun bir kriptografik mod l geli tirme.
2. FIPS sertifikalı g venlik algoritmaları bir uygulamaya entegre etme.

1.1.2.8 Sonu  Bu hafta, ETSI, GSMA, EMV, EAL, Common Criteria ve FIPS gibi g venlik gereksinimleri ve standartları inceledik. Bu standartlar, uluslararası düzeyde kabul g rm   g venlik protokollerini tanımlayarak sistemlerin ve   r nlerin g venli ini sa lamaya yardımcı olmaktadır. G venlik sertifikaları,   r nlerin ve sistemlerin g venlik a  s ndan de erlendirildi ini ve onayland  nı g sterir.