EEE374 SİBER GÜVENLİK

Prof. Dr. Hasan Hüseyin BALIK

(1. Hafta)

İçerik

- Ders Bilgileri ve Politikaları
- Ders Müfredatı
- 1. Siber Güvenliğe Genel Bakış

Ders Bilgileri

- Dersin Hocası : Prof. Dr. Hasan H. BALIK, balik@aydin.edu.tr, www.hasanbalik.com
- Ders Ana Sayfası: http://www.hasanbalik.com/LectureNotes/SiberGuvenlik/

Kitap: Computer Security: Principles and Practice, 4th Edition, William Stallings and Lawrie Brown, 2018

Derecelendirme:

Vize sınavı	%30
Ödev/Proje	%30
Final	%40

Ders Müfredatı

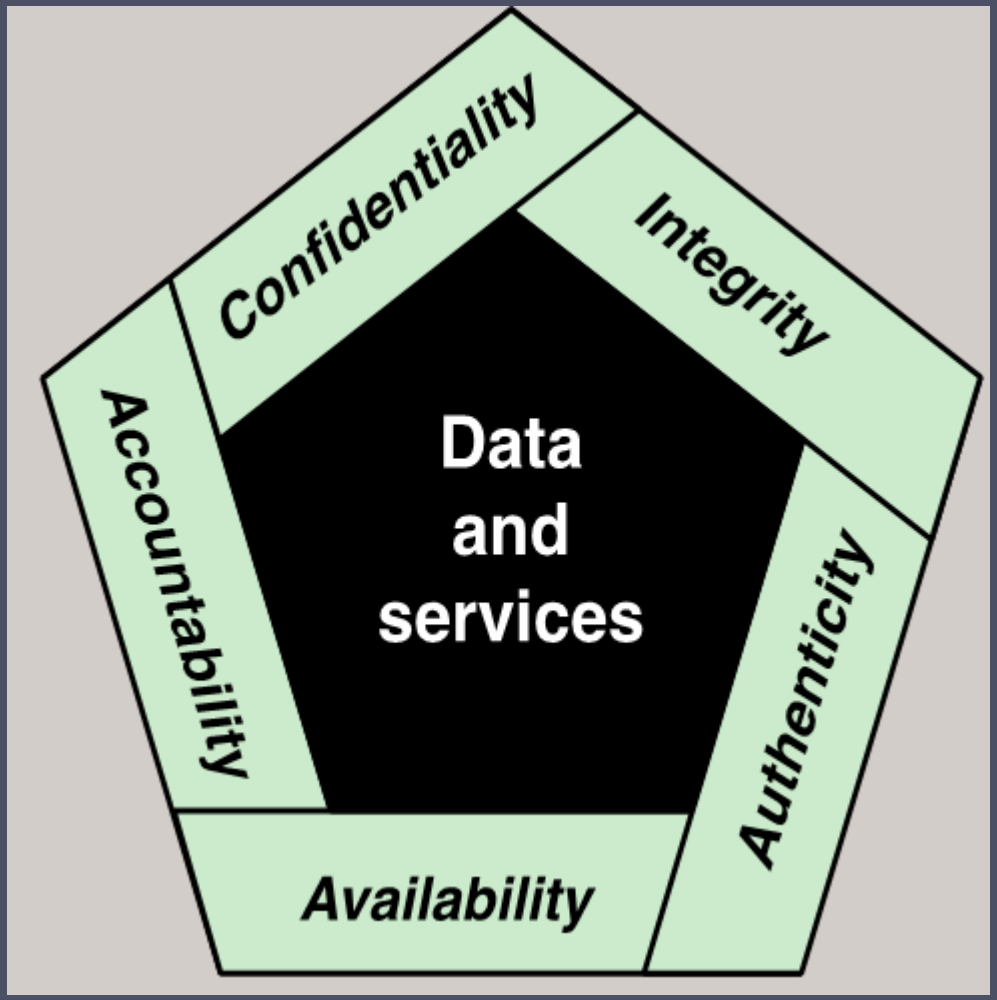
- Siber Güvenliğe Genel Bakış
- Bilişim Güvenliği Teknolojileri ve İlkeleri
  - Şifreleme Araçları
  - Kullanıcı Doğrulama
  - Giriş Kontrolu
  - Veritabanı ve Veri Merkezi Güvenliği
  - Kötü Amaçlı Yazılımlar
  - Hizmet Reddi Saldırıları
  - İzinsiz Giriş Tespiti
  - Güvenlik Duvarları ve Saldırı Önleme Sistemleri
- Yazılım Güvenliği ve Güvenilir Sistemler
  - Arabellek Taşması
  - Yazılım Güvenliği
  - İşletim Sistemi Güvenliği
  - Bulut ve IoT Güvenliliği

1. Siber Güvenliğe Genel Bakış

...

1.İçerik

- Bilgisayar Güvenliği Kavramları
- Tehditler, Saldırılar ve Varlıklar
- Güvenliğin İşlevsel Gereksinimleri
- Temel Güvenlik Tasarım İlkeleri
- Saldırı Yüzeyleri ve Saldırı Ağaçları
- Bilgisayar Güvenliği Stratejisi
- Standartlar



- **Gizlilik**
  - -veri gizliliği
  - -mahremiyet
- **Bütünlük**
  - veri bütünlüğü
  - sistem bütünlüğü
- **Kullanılabilirlik**

Bu üç kavram, genellikle CIA üçlüsü olarak adlandırılır ve temel güvenlik bileşenlerini oluşturur.

- **Özgünlük:** Hakiki olma ve doğrulanabilme özelliği ve güvenilir
- **Hesap verebilirlik**:Bir varlığın eylemlerinin o varlığa benzersiz olarak izlenmesi gereksinimini oluşturan güvenlik hedefi

Temel Güvenlik Kavramları

Gizlilik

- Kişisel gizliliğin ve özel bilgilerin korunmasına yönelik araçlar da dahil olmak üzere, bilgi erişimi ve ifşasına ilişkin yetkili kısıtlamaların korunması

Bütünlük

- Bilginin reddedilmemesini ve orijinalliğini sağlamak da dahil olmak üzere, uygunsuz bilgi değişikliği veya tahribatına karşı koruma

Kullanılabilirlik

- Bilgiye zamanında ve güvenilir erişim ve bilginin kullanılmasının sağlanması

*NIST Standardı FIPS 199 (Güvenlik Standartları Federal Bilgi ve Bilgi Sistemlerinin Sınıflandırılması, Şubat 2004)

Temel Güvenlik Kavramları

Özgünlük

- kullanıcıların söyledikleri kişi olduklarını ve sisteme gelen her girdinin güvenilir bir kaynaktan geldiğini doğrulamak

Hesap Verilebilirlik

- inkar etmeme, caydırıcılık, hata izolasyonu, izinsiz giriş tespiti ve önleme ve eylem sonrası kurtarma ve yasal işlemi destekleme

Etki Düzeyleri

Düşük

Kaybın, organizasyonel operasyonlar, organizasyonel varlıklar veya bireyler üzerinde sınırlı bir olumsuz etkisinin olması beklenebilir.

Orta

Kaybın organizasyonel operasyonlar, organizasyonel varlıklar veya bireyler üzerinde ciddi bir olumsuz etkisi olması beklenebilir.

Yüksek

Kaybın, organizasyonel operasyonlar, organizasyonel varlıklar veya bireyler üzerinde çok ciddi veya katastrofik bir olumsuz etkiye sahip olması beklenebilir.

Bilgisayar Güvenliği Zorlukları

1. Bilgisayar güvenliği, acemilere ilk bakışta göründüğü kadar basit değildir.

2. Belirli bir güvenlik mekanizması veya algoritması geliştirirken, her zaman bu güvenlik özelliklerine yönelik olası saldırılar göz önünde bulundurulmalıdır.

3. Belirli hizmetleri sağlamak için kullanılan prosedürler genellikle mantık dışıdır.

4. Fiziksel ve mantıksal yerleşim belirlenmelidir.

5. Güvenlik mekanizmaları tipik olarak belirli bir algoritma veya protokolden fazlasını içerir ve ayrıca katılımcıların bu gizli bilgilerin oluşturulması, dağıtılması ve korunması hakkında sorular ortaya çıkaran bazı gizli bilgilere sahip olmalarını gerektirir.

6. Saldırganların yalnızca tek bir zayıf noktayı bulması gerekirken, tasarımcı mükemmel güvenlik elde etmek için tüm zayıflıkları bulup ortadan kaldırmalıdır.

7. Güvenlik, tasarım sürecinin ayrılmaz bir parçası olmaktan ziyade, tasarım tamamlandıktan sonra bir sisteme dahil edilmek için hala çok sık sonradan düşünülen bir şeydir.

8. Güvenlik, düzenli ve sürekli izleme gerektirir

9. Kullanıcıların ve sistem yöneticilerinin, bir güvenlik arızası meydana gelene kadar güvenlik yatırımından çok az fayda sağladığı algısına yönelik doğal bir eğilim vardır.

10. Birçok kullanıcı ve hatta güvenlik yöneticisi, güçlü güvenliği, bir bilgi sisteminin verimli ve kullanıcı dostu çalışmasına veya bilgi kullanımına bir engel olarak görür.

Bilgisayar Güvenliği Terminolojisi, RFC 2828'den,*İnternet Güvenliği Sözlüğü*, Mayıs 2000

Adversary-Düşman (tehdit ajanı)
Zararlı faaliyetler yürüten veya yürütme niyetinde olan kişi, grup, kuruluş veya hükümet.

Attack-Saldırı
Bilgi sistemi kaynaklarını veya bilginin kendisini toplamaya, bozmaya, reddetmeye, veya yok etmeye çalışan her türlü kötü niyetli faaliyet.

Countermeasure-karşı önlem
İstenmeyen veya düşmanca faaliyetlerin operasyonel etkinliğini bozmayı veya casusluk, sabotaj, hırsızlık veya hassas bilgi veya bilgi sistemlerine yetkisiz erişimi veya bu sistemlerin kullanımını önlemeyi amaçlayan bir cihaz veya teknikler.

Risk
Bir işletmenin olası bir durum veya olay tarafından ne ölçüde tehdit edildiğinin ölçüsü ve tipik olarak 1) durum veya olay meydana geldiğinde ortaya çıkacak olumsuz etkiler; ve 2) meydana gelme olasılığı.

Security Policy-Güvenlik Politikası
Güvenlik hizmetlerinin sağlanması için bir dizi kriter. Sistemler ve veriler için bir güvenlik koşulu sağlamak amacıyla bir veri işleme tesisinin faaliyetlerini tanımlar ve kısıtlar.

System Resource-Sistem Kaynağı (Asset-Varlık)
Ana uygulama, genel destek sistemi, yüksek etkili program, fiziksel tesis, kritik görev sistemi, personel, ekipman veya mantıksal olarak ilişkili bir sistem grubu.

Threat-Tehdit
Yetkisiz erişim, bilgilerin yok edilmesi, ifşa edilmesi, değiştirilmesi yoluyla bir bilgi sistemi aracılığıyla kurumsal operasyonları (misyon, işlevler, imaj veya itibar dahil), kurumsal varlıkları, bireyleri, diğer kuruluşları veya Ulusu olumsuz etkileme potansiyeli olan herhangi bir durum veya olay ve/veya hizmet reddi.

Vulnerability-güvenlik açığı
Bir tehdit kaynağı tarafından istismar edilebilecek veya tetiklenebilecek bir bilgi sistemi, sistem güvenlik prosedürleri, iç kontroller veya uygulamadaki zayıflık.

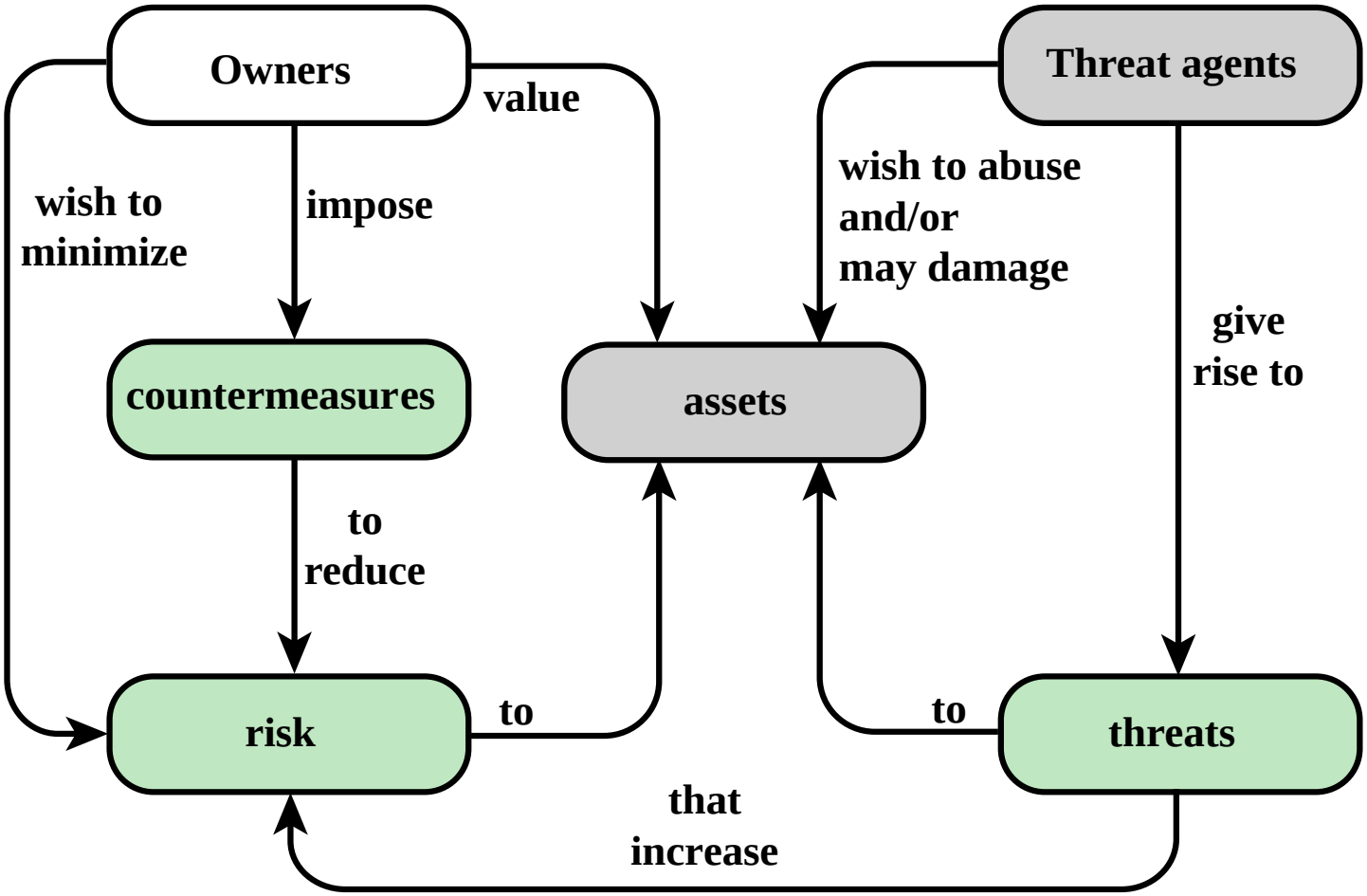
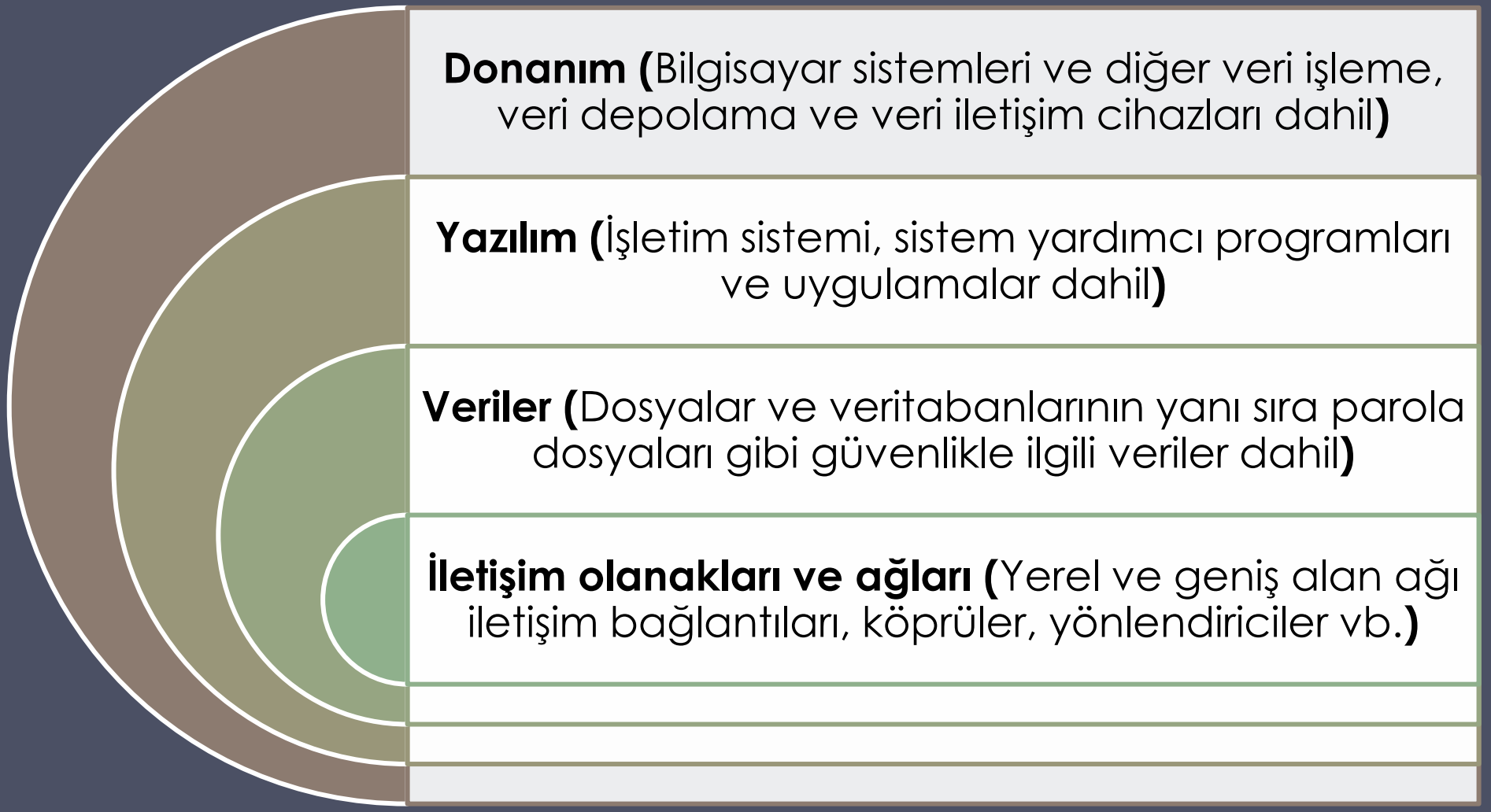


Figure 1.2 Security Concepts and Relationships

Bilgisayar Sisteminin Varlıkları

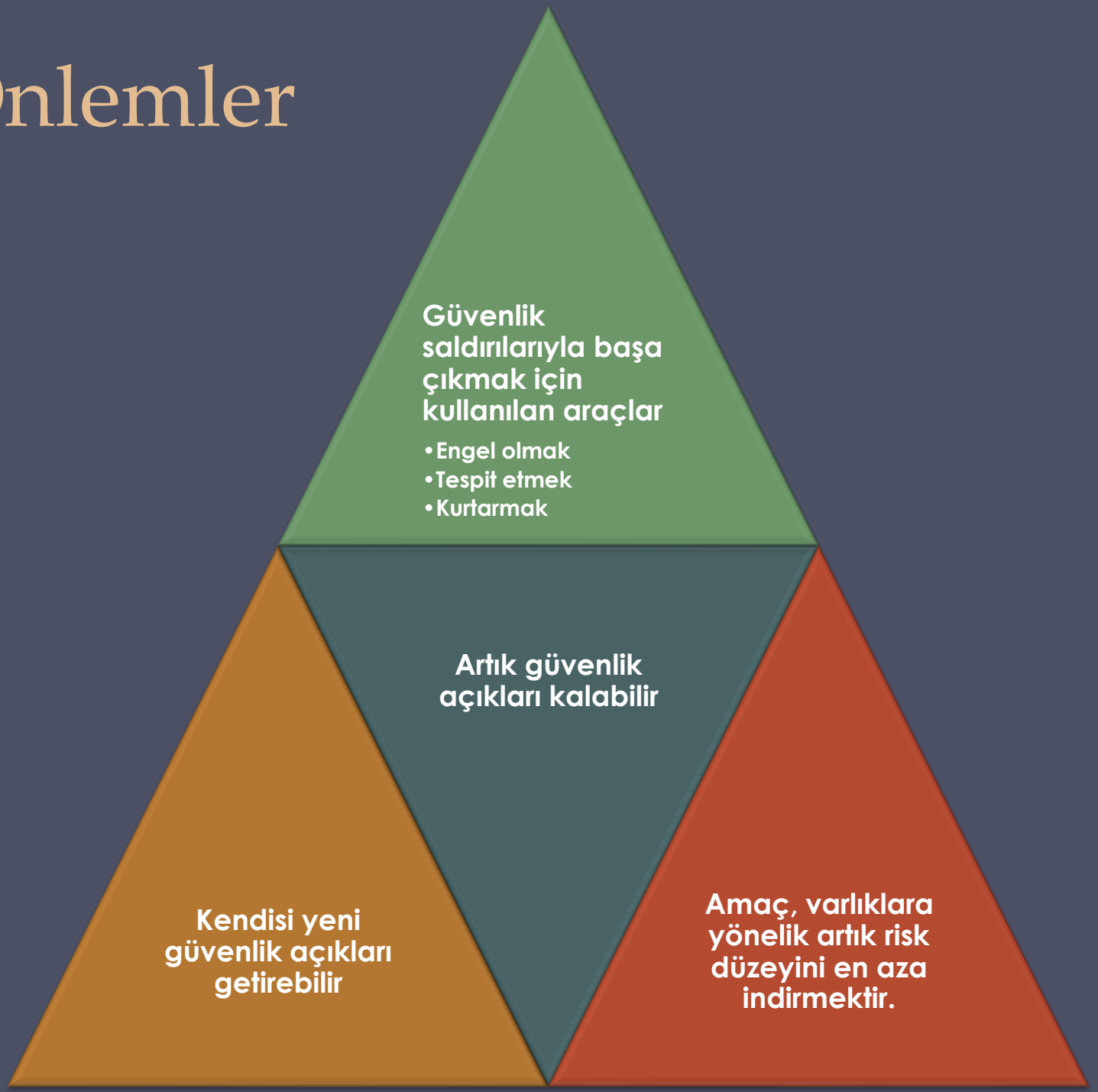


Güvenlik Açıkları, Tehditler ve Saldırılar

- Güvenlik açıkları kategorileri
  - Corrupted-Bozuk (bütünlük kaybı):
  - Leaky-Sızdıran (gizlilik kaybı)
  - Unavailable-Kullanılamaz veya çok yavaş (kullanılabilirlik kaybı)
- tehditler
  - Güvenlik açıklarından yararlanma yeteneği
  - Bir varlığa yönelik olası güvenlik zararını temsil eder
- Saldırılar (gerçekleştirilen tehditler)
  - Pasif - sistem kaynaklarını etkilemeyen sistemden bilgi öğrenmeye veya sistemden yararlanmaya çalışmak
  - Aktif - sistem kaynaklarını değiştirmeye veya operasyonlarını etkilemeye çalışın

  Kökenine göre sınıflandırmak
  - Insider – güvenlik parametresi içindeki bir varlık tarafından başlatılır
  - Outsider - çevrenin dışından başlatılan

Karşı Önlemler



Tehdit Sonuç	Tehdit Eylemi (Saldırı)
Yetkisiz Açıklama Bir kuruluşun, yetkili olmadığı verilere erişim kazandığı bir durum veya olay.	**Maruziyet:** Hassas veriler doğrudan yetkisiz bir varlığa verilir. **Müdahale:** Yetkisiz bir varlık, yetkili kaynaklar ve hedefler arasında seyahat eden hassas verilere doğrudan erişir. **çıkarım:** Yetkisiz bir varlığın, iletişimin özelliklerinden veya yan ürünlerinden yola çıkarak hassas verilere (ancak iletişimde bulunan verilere zorunlu olarak değil) dolaylı olarak eriştiği bir tehdit eylemi. **izinsiz giriş:** Yetkisiz bir varlık, bir sistemin güvenlik korumalarını atlayarak hassas verilere erişim kazanır.
aldatma Yetkili bir kuruluşun yanlış veri almasına ve bunun doğru olduğuna inanmasına neden olabilecek bir durum veya olay.	**Maskeli:** Yetkisiz bir varlık, bir sisteme erişim kazanır veya yetkili bir varlık gibi davranarak kötü niyetli bir eylem gerçekleştirir. **tahrif:** Yanlış veriler yetkili bir varlığı aldatır. **reddetme:** Bir varlık, bir eylemin sorumluluğunu yanlış bir şekilde reddederek bir başkasını aldatır.
bozulma Sistem hizmetlerinin ve işlevlerinin doğru çalışmasını kesintiye uğratan veya engelleyen bir durum veya olay.	**Aciz bırakma:** Bir sistem bileşenini devre dışı bırakarak sistem çalışmasını engeller veya kesintiye uğratır. **Yolsuzluk:** Sistem işlevlerini veya verilerini olumsuz yönde değiştirerek sistem çalışmasını istenmeyen şekilde değiştirir. **Engel:** Sistemin çalışmasını engelleyerek sistem hizmetlerinin sunumunu kesintiye uğratan bir tehdit eylemi.
gasp Yetkisiz bir varlık tarafından sistem hizmetlerinin veya işlevlerinin kontrolüyle sonuçlanan bir durum veya olay.	**zimmete para geçirme:** Bir varlık, bir sistem kaynağının yetkisiz mantıksal veya fiziksel kontrolünü üstlenir. **Yanlış kullanım:** Bir sistem bileşeninin, sistem güvenliğine zarar veren bir işlevi veya hizmeti gerçekleştirmesine neden olur.

Tehdit Sonuçları,

ve

Çeşitleri

Tehdit Eylemleri

Bu Neden

Her biri

Sonuçlar

Dayalı

RFC 4949

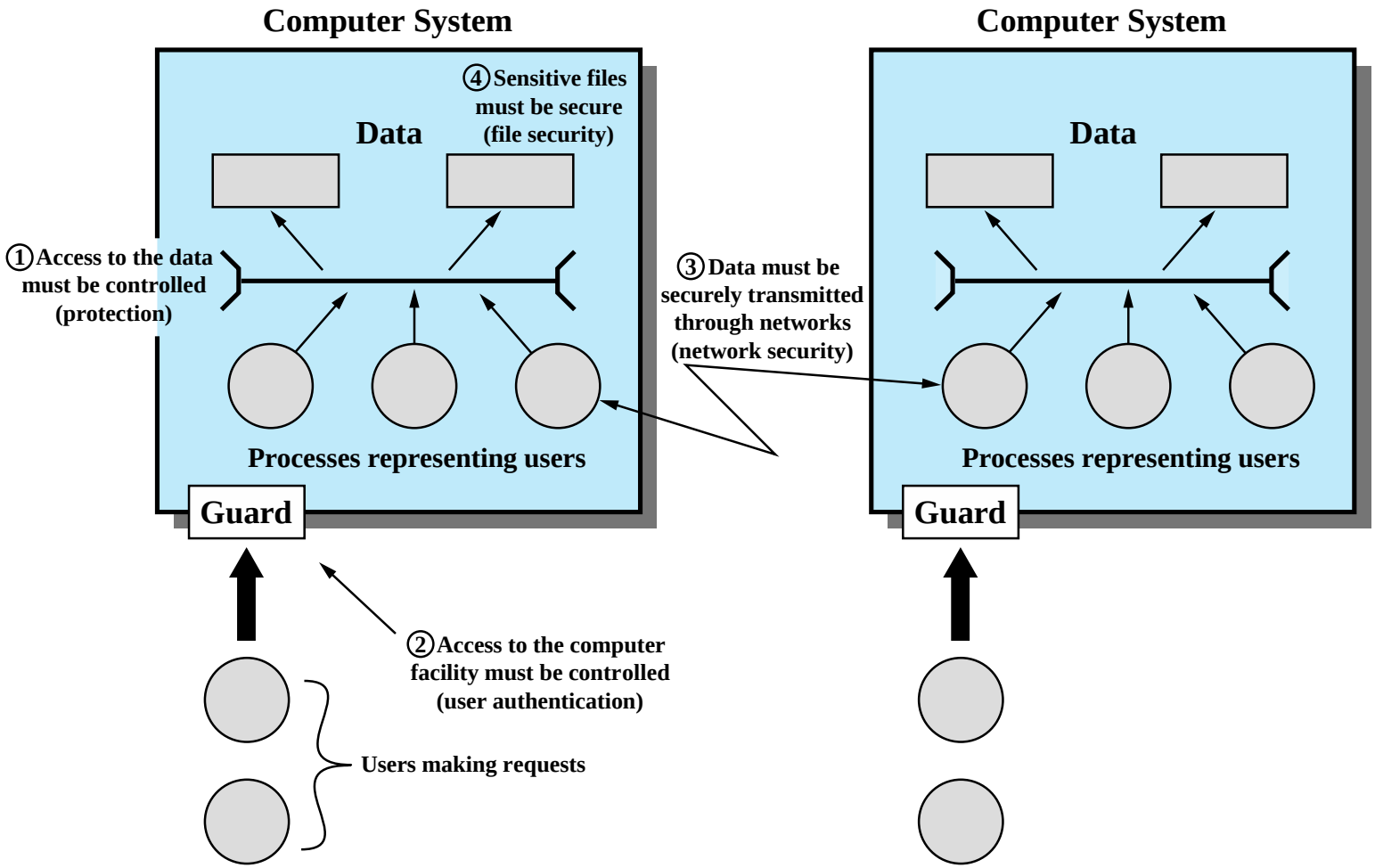


Figure 1.3 Scope of Computer Security. This figure depicts security concerns other than physical security, including control of access to computers systems, safeguarding of data transmitted over communications systems, and safeguarding of stored data.

Tehdit Örnekleriyle Bilgisayar ve Ağ Varlıkları

	Kullanılabilirlik	Gizlilik	Bütünlük
Donanım	Ekipman çalındı veya devre dışı bırakıldı, bu nedenle hizmet reddedildi.	Şifrelenmemiş bir CD-ROM veya DVD çalındı.	
Yazılım	Programlar silinir, kullanıcılara erişim reddedilir.	Yazılımın yetkisiz bir kopyası yapılır.	Çalışan bir program, yürütme sırasında başarısız olmasına veya istenmeyen bir görevi yapmasına neden olmak için değiştirilir.
Veri	Dosyalar silinir, kullanıcılara erişim reddedilir.	Yetkisiz bir veri okuması gerçekleştirilir. İstatistiksel verilerin analizi, temel verileri ortaya çıkarır.	Mevcut dosyalar değiştirilir veya yeni dosyalar üretilir.
İletişim Hatları ve Ağları	Mesajlar yok edilir veya silinir. İletişim hatları veya ağlar kullanılamaz hale getirildi.	Mesajlar okunur. Mesajların trafik düzeni gözlemlenir.	Mesajlar değiştirilir, ertelenir, yeniden sıralanır veya çoğaltılır. Sahte mesajlar uydurulmuştur.

Pasif ve Aktif Saldırılar

Pasif Saldırı

- Sistemden bilgi öğrenmeye veya sistemden yararlanmaya çalışır ancak sistem kaynaklarını etkilemez.
- İletimlerin dinlenmesi veya izlenmesi
- Saldırganın amacı, iletilen bilgiyi elde etmektir.
- İki tip:
  - Mesaj içeriğinin serbest bırakılması
  - Trafik analizi

Aktif Saldırı

- Sistem kaynaklarını değiştirme veya operasyonlarını etkileme girişimleri
- Veri akışında bazı değişiklikler veya yanlış bir akış oluşturulmasını içerir
- Dört kategori:
  - tekrar oynat
  - maskeli
  - Mesajların değiştirilmesi
  - hizmet reddi

Giriş kontrolu: Bilgi sistemi erişimini yetkili kullanıcılar, yetkili kullanıcılar adına hareket eden süreçler veya cihazlar (diğer bilgi sistemleri dahil) ve yetkili kullanıcıların gerçekleştirmesine izin verilen işlem ve işlev türleri ile sınırlandırın.

Farkındalık ve eğitim:(i) Kurumsal bilgi sistemlerinin yöneticilerinin ve kullanıcılarının, faaliyetleriyle ilişkili güvenlik risklerinden ve kurumsal bilgi sistemlerinin güvenliğiyle ilgili geçerli yasa, yönetmelik ve politikalardan haberdar olmalarını sağlamak; ve (ii) personelin bilgi güvenliği ile ilgili görev ve sorumluluklarını yerine getirmesi için yeterince eğitim almasını sağlamak.

Denetim ve hesap verebilirlik:(i) Yasa dışı, yetkisiz veya uygunsuz bilgi sistemi etkinliğinin izlenmesi, analizi, araştırılması ve raporlanmasını sağlamak için gereken ölçüde bilgi sistemi denetim kayıtlarını oluşturmak, korumak ve saklamak; ve (ii) bireysel bilgi sistemi kullanıcılarının eylemlerinin, eylemlerinden sorumlu tutulabilmeleri için bu kullanıcılara benzersiz bir şekilde izlenebilmesini sağlamak.

Sertifikasyon, akreditasyon ve güvenlik değerlendirmeleri:(i) Kontrollerin uygulamalarında etkili olup olmadığını belirlemek için kurumsal bilgi sistemlerindeki güvenlik kontrollerini periyodik olarak değerlendirmek; (ii) kurumsal bilgi sistemlerindeki eksiklikleri gidermek ve güvenlik açıklarını azaltmak veya ortadan kaldırmak için tasarlanmış eylem planları geliştirmek ve uygulamak; (iii) kurumsal bilgi sistemlerinin ve ilgili her türlü bilgi sistemi bağlantılarının çalışmasına izin vermek; ve (iv) kontrollerin sürekli etkinliğini sağlamak için bilgi sistemi güvenlik kontrollerini sürekli olarak izlemek.

Konfigürasyon yönetimi:(i) İlgili sistem geliştirme yaşam döngüleri boyunca kurumsal bilgi sistemlerinin (donanım, yazılım, bellenim ve belgeler dahil) temel yapılandırmalarını ve envanterlerini oluşturmak ve sürdürmek; ve (ii) kurumsal bilgi sistemlerinde kullanılan bilgi teknolojisi ürünleri için güvenlik yapılandırma ayarlarını oluşturmak ve uygulamak.

Acil durum planlaması: Acil durumlarda kritik bilgi kaynaklarının mevcudiyetini ve operasyonların sürekliliğini sağlamak için acil müdahale, yedekleme operasyonları ve organizasyonel bilgi sistemleri için felaket sonrası kurtarma planları oluşturun, sürdürün ve uygulayın.

Tanımlama ve doğrulama: Bilgi sistemi kullanıcılarını, kullanıcılar adına hareket eden süreçleri veya cihazları tanımlayın ve kurumsal bilgi sistemlerine erişime izin vermek için bir ön koşul olarak bu kullanıcıların, işlemlerin veya cihazların kimliklerini doğrulayın (veya doğrulayın).

Olay yanıtı:(i) Yeterli hazırlık, tespit, analiz, sınırlama, kurtarma ve kullanıcı müdahale faaliyetlerini içeren kurumsal bilgi sistemleri için operasyonel bir olay işleme yeteneği oluşturmak; ve (ii) olayları takip etmek, belgelemek ve uygun organizasyon yetkililerine ve/veya yetkililerine bildirmek.

Bakım onarım:(i) Kurumsal bilgi sistemleri üzerinde periyodik ve zamanında bakım yapmak; ve (ii) bilgi sistemi bakımını yürütmek için kullanılan araçlar, teknikler, mekanizmalar ve personel üzerinde etkili kontroller sağlamak.

Güvenlik Gereksinimler

(FIPS 200)

(1 / 2)

Medya koruması:(i) Hem kağıt hem de dijital bilgi sistemi ortamını koruyun; (ii) bilgi sistemi medyasındaki bilgilere erişimi yetkili kullanıcılarla sınırlandırmak; ve (iii) elden çıkarmadan veya yeniden kullanım için serbest bırakmadan önce bilgi sistemi ortamını sterilize etmek veya imha etmek.

Fiziksel ve çevresel koruma:(i) Bilgi sistemlerine, ekipmana ve ilgili işletim ortamlarına fiziksel erişimi yetkili kişilerle sınırlandırmak; (ii) fiziksel tesisi korumak ve bilgi sistemleri için altyapıyı desteklemek; (iii) bilgi sistemleri için destekleyici hizmetler sağlamak; (iv) bilgi sistemlerini çevresel tehlikelere karşı korumak; ve (v) bilgi sistemleri içeren tesislerde uygun çevresel kontrolleri sağlamak.

Planlama: Bilgi sistemleri için mevcut veya planlanan güvenlik kontrollerini ve bilgi sistemlerine erişen bireylerin davranış kurallarını tanımlayan kurumsal bilgi sistemleri için güvenlik planları geliştirmek, belgelemek, periyodik olarak güncellemek ve uygulamak.

Personel güvenliği:(i) Kuruluşlar içinde (üçüncü şahıs hizmet sağlayıcılar dahil) sorumlu pozisyonlarda bulunan kişilerin güvenilir olduğundan ve bu pozisyonlar için belirlenmiş güvenlik kriterlerini karşıladığından emin olmak; (ii) işten çıkarmalar ve transferler gibi personel eylemleri sırasında ve sonrasında kurumsal bilgi ve bilgi sistemlerinin korunmasını sağlamak; ve (iii) kurumsal güvenlik politikalarına ve prosedürlerine uymayan personel için resmi yaptırımlar uygulamak.

Risk değerlendirmesi: Organizasyonel bilgi sistemlerinin işleyişinden ve organizasyonel bilgilerin işlenmesi, depolanması veya iletilmesinden kaynaklanan organizasyonel operasyonlara (misyon, işlevler, imaj veya itibar dahil), organizasyonel varlıklara ve bireylere yönelik riski periyodik olarak değerlendirin.

Sistem ve hizmet alımı:(i) Kurumsal bilgi sistemlerini yeterince korumak için yeterli kaynakları tahsis etmek; (ii) bilgi güvenliği hususlarını içeren sistem geliştirme yaşam döngüsü süreçlerini kullanmak; (iii) yazılım kullanımı ve kurulum kısıtlamaları uygulamak; ve (iv) üçüncü taraf sağlayıcıların, kuruluştan sağlanan bilgileri, uygulamaları ve/veya hizmetleri korumak için yeterli güvenlik önlemleri almasını sağlamak.

Sistem ve iletişim koruması:(i) Bilgi sistemlerinin dış sınırlarında ve temel iç sınırlarında kurumsal iletişimleri (yani kurumsal bilgi sistemleri tarafından iletilen veya alınan bilgiler) izlemek, kontrol etmek ve korumak; ve (ii) kurumsal bilgi sistemlerinde etkin bilgi güvenliğini destekleyen mimari tasarımları, yazılım geliştirme tekniklerini ve sistem mühendisliği ilkelerini kullanmak.

Sistem ve bilgi bütünlüğü:(i) Bilgi ve bilgi sistemi kusurlarını zamanında tespit etmek, raporlamak ve düzeltmek; (ii) kurumsal bilgi sistemleri içinde uygun yerlerde kötü amaçlı kodlara karşı koruma sağlamak; ve (iii) bilgi sistemi güvenlik uyarılarını ve tavsiyelerini izlemek ve yanıt olarak uygun önlemleri almak.

Güvenlik Gereksinimler

(FIPS 200)

(2/2)

Temel Güvenlik Tasarım İlkeleri

Mekanizma ekonomisi	Arızaya karşı güvenli varsayılanlar	Tam arabuluculuk	Açık tasarım
• Ayrıcalığın ayrılması	En az ayrıcalık	En az yaygın mekanizma	Psikolojik kabul edilebilirlik
İzolasyon	Kapsülleme	Modülerlik	Katmanlama

En az şaşkınlık

Saldırı Yüzeyleri

Bir sistemdeki erişilebilir ve yararlanılabilir güvenlik açıklarından oluşur

Örnekler:

- Dışa bakan web ve diğer sunuculardaki açık porlar ve bu açık portları dinleyen kodlar
- Güvenlik duvarının içinde bulunan hizmetler
- Gelen verileri, e-postayı, XML'i, ofis belgelerini ve sektöre özel veri alışverişi biçimlerini işleyen kod
- Arayüzler, SQL ve Web formları
- Bir sosyal mühendislik saldırısına karşı hassas bilgilere erişimi olan çalışan

Saldırı Yüzeyi Kategorileri

Ağ Saldırı Yüzeyi

Kurumsal ağ, geniş alan ağı veya İnternet üzerindeki güvenlik açıkları

Hizmet reddi saldırısı, iletişim bağlantılarının bozulması ve çeşitli davetsiz misafir saldırıları için kullanılanlar gibi ağ protokolü güvenlik açıkları bu kategoriye dahildir.

Yazılım Saldırı Yüzeyi

Uygulama, yardımcı program veya işletim sistemi kodundaki güvenlik açıkları

Özellikle odak noktası Web sunucusu yazılımıdır

İnsan Saldırı Yüzeyi

Sosyal mühendislik, insan hatası ve içeriden güvenilir kişiler gibi personel veya dışarıdan kişiler tarafından oluşturulan güvenlik açıkları

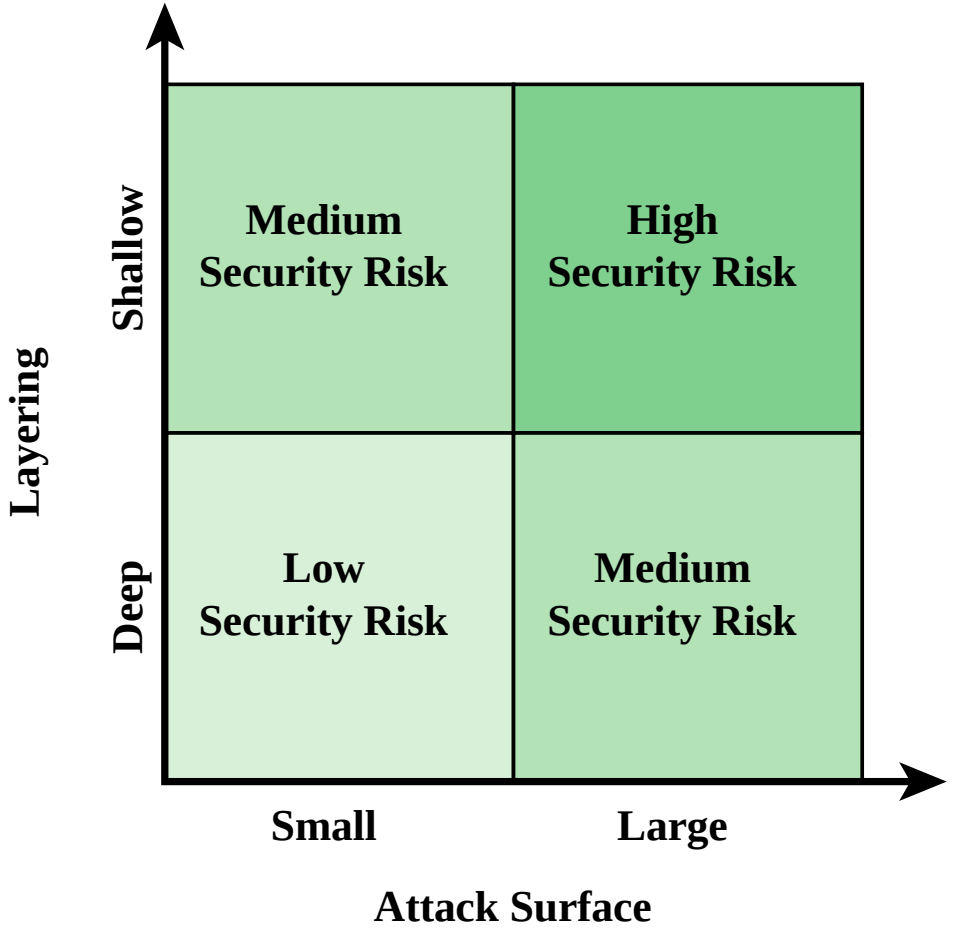
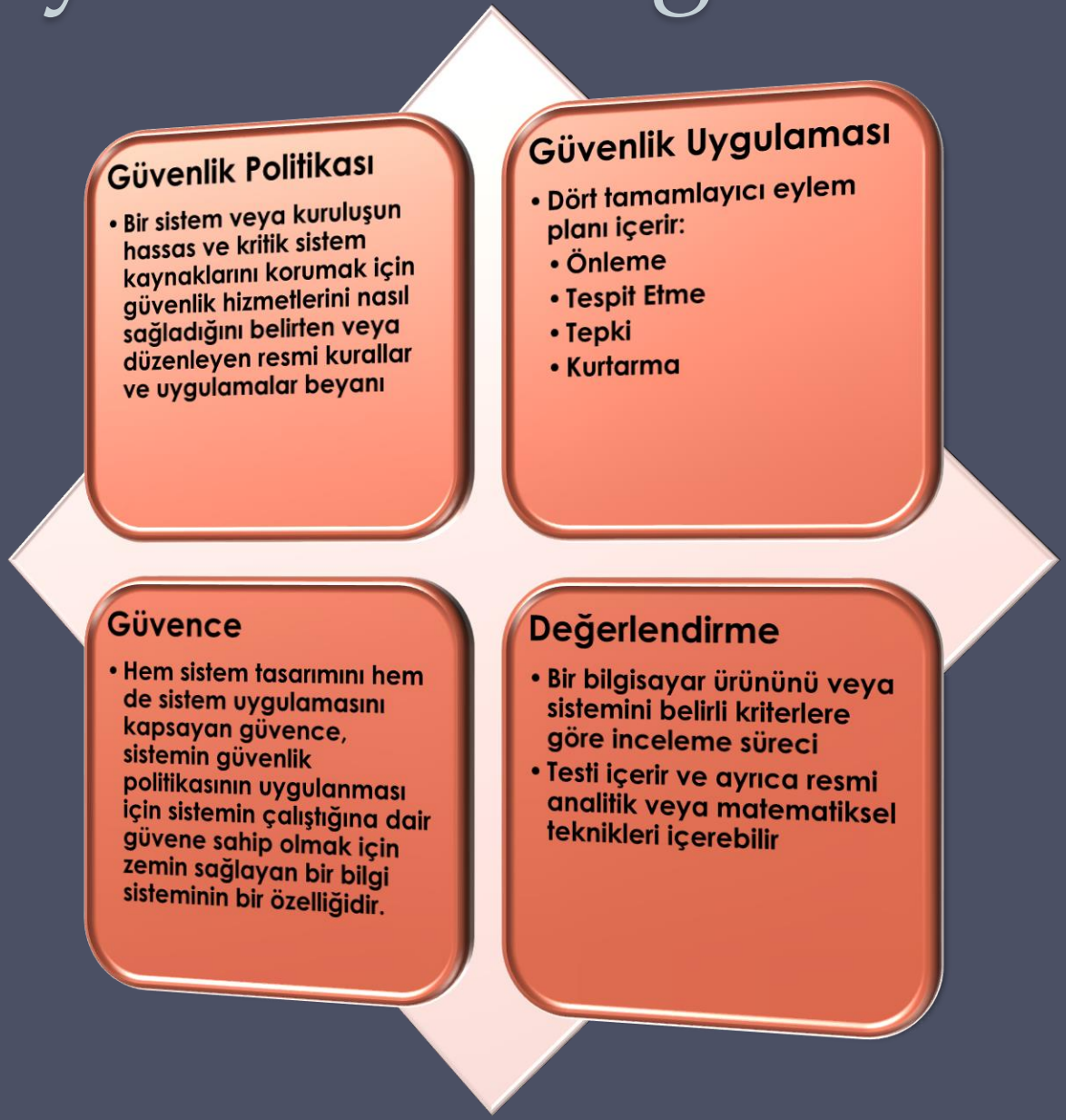


Figure 1.4 Defense in Depth and Attack Surface

Bilgisayar Güvenliği Stratejisi



Standartlar

- Yönetim uygulamalarını ve güvenlik mekanizmalarının ve hizmetlerinin genel mimarisini kapsayacak şekilde standartlar geliştirilmiştir.
- Bu kuruluşların en önemlileri şunlardır:
  - **Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)**
    - **NIST, ABD hükümetinin kullanımı ve ABD özel sektör inovasyonunun teşviki ile ilgili ölçüm bilimi, standartları ve teknolojisi ile ilgilenen bir ABD federal kurumudur.**
  - **İnternet Topluluğu (ISOC)**
    - **ISOC, İnternet'in geleceğiyle ilgili sorunların ele alınmasında liderlik sağlayan ve İnternet altyapı standartlarından sorumlu grupların evi olan profesyonel bir üyelik topluluğudur.**
  - **Uluslararası Telekomünikasyon Birliği (ITU-T)**
    - **ITU, hükümetlerin ve özel sektörün küresel telekom ağlarını ve hizmetlerini koordine ettiği bir Birleşmiş Milletler kuruluşudur.**
  - **Uluslararası Standardizasyon Örgütü (ISO)**
    - **ISO, çalışmaları Uluslararası Standartlar olarak yayınlanan uluslararası anlaşmalarla sonuçlanan bir sivil toplum kuruluşudur.**