IT522 – Yazılım Mühendisliği 2021

PhD Furkan Gözükara, Toros University

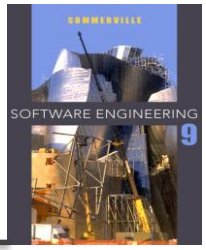
https://github.com/FurkanGozukara/Yazilim-Muhendisligi-IT522-2021

Ders 14

Güvenlik Mühendisliği

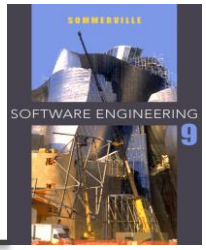
Kaynak : https://ifs.host.cs.st-andrews.ac.uk/Books/SE9/Presentations/index.html

Bölüm 1'de İşlenmiş Konular



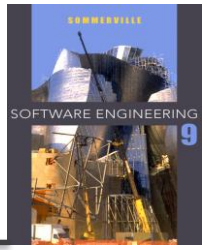
- Güvenlik mühendisliği ve güvenlik yönetimi
  - Uygulamalarla ilgili güvenlik mühendisliği; altyapı ile güvenlik yönetimi.
- Güvenlik riski değerlendirmesi
  - Güvenlik risklerinin değerlendirilmesine dayalı bir sistem tasarlamak.
- Güvenlik için tasarım
  - Güvenlik için sistem mimarilerinin nasıl tasarlanması gerektiği.

Güvenlik Mühendisliği



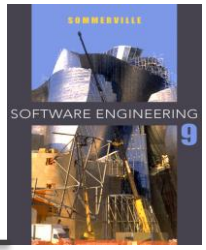
- Bilgisayar tabanlı bir sisteme veya onun verilerine zarar vermeyi amaçlayan kötü niyetli saldırılara direnebilecek sistemlerin geliştirilmesini ve bakımını destekleyecek araçlar, teknikler ve yöntemler.
- Daha geniş bilgisayar güvenliği alanının bir alt alanı.
- Güvenilirlik ve güvenlik kavramları (Ders 10) ve güvenlik gereksinimleri spesifikasyonu (Ders 12) hakkında arka plan bilgisini varsayar

Uygulama/Altyapı Güvenliği



- Uygulama güvenliği, sistemin saldırılara direnecek şekilde tasarlandığı bir yazılım mühendisliği sorunudur.
- Altyapı güvenliği, altyapının saldırılara direnecek şekilde yapılandırıldığı bir sistem yönetimi sorunudur.
- Bu Dersin odak noktası uygulama güvenliğidir.

Güvenliğin Tehlikeye Girebileceği Sistem Katmanları



Application

Reusable Components and Libraries

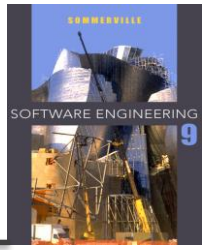
Middleware

Database Management

Generic, Shared Applications (Browsers, E-mail, Etc.)

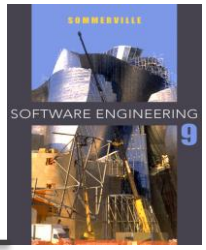
Operating system

Sistem Güvenliği Yönetimi



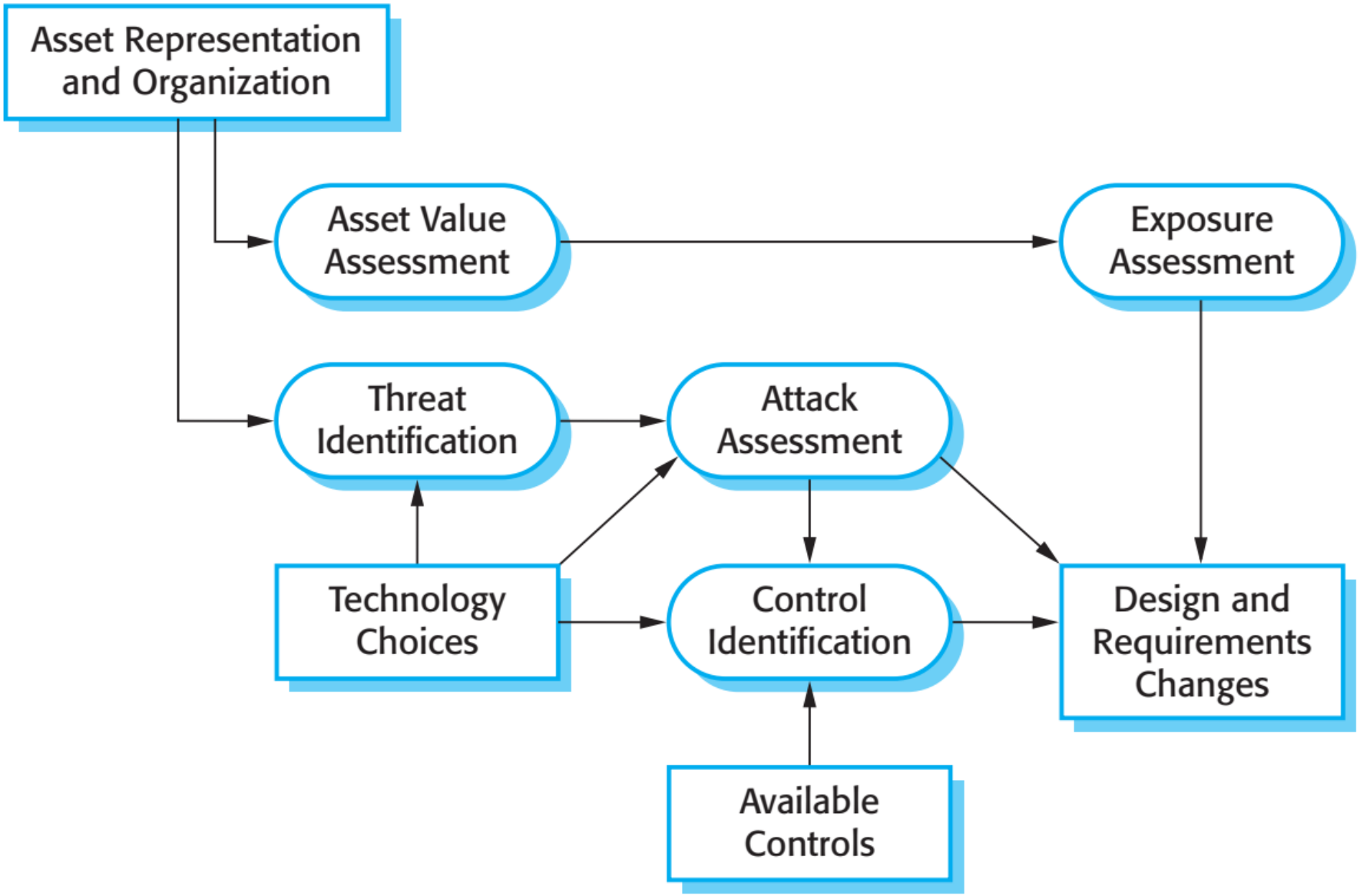
- Kullanıcı ve izin yönetimi
  - Sisteme kullanıcı ekleme, sistemden çıkarma ve kullanıcılar için uygun izinleri ayarlama
- Yazılım dağıtımı ve bakımı
  - Güvenlik açıklarından kaçınılması için uygulama yazılımı ve ara katman yazılımının yüklenmesi ve bu sistemlerin yapılandırılması.
- Saldırı izleme, algılama ve kurtarma
  - Sistemi yetkisiz erişime karşı izlemek, saldırılara direnmek için stratejiler tasarlamak ve yedekleme ve kurtarma stratejileri geliştirmek.

Güvenlik Riski Yönetimi

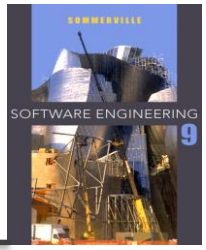


- Risk yönetimi, sisteme yapılan saldırılardan kaynaklanabilecek olası kayıpların değerlendirilmesi ve bu kayıpların, bu kayıpları azaltabilecek güvenlik prosedürlerinin maliyetlerine karşı dengelenmesi ile ilgilidir.
- Risk yönetimi, kurumsal bir güvenlik politikası tarafından yönlendirilmelidir.
- Risk yönetimi şunları içerir:
  - Ön risk değerlendirmesi
  - Yaşam döngüsü risk değerlendirmesi
  - Operasyonel risk değerlendirmesi

Ön Risk Değerlendirmesi

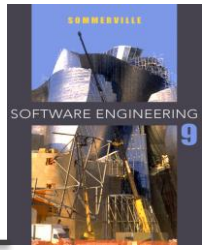


Kötüye Kullanım Durumları



- Kötüye kullanım durumları, bir sisteme yönelik tehdit örnekleridir
- Müdahale tehditleri
  - Saldırgan bir varlığa erişim kazanır
- Kesinti tehditleri
  - Saldırgan, bir sistemin bir bölümünü kullanılamaz hale getirir
- Değişiklik tehditleri
  - Kurcalanmışsa bir sistem varlığı
- Fabrikasyon tehditler
  - Bir sisteme yanlış bilgi eklenir

Varlık Analizi

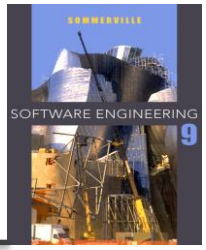


Varlık	Değer	Maruziyet
bilgi sistemi	Yüksek. Tüm klinik konsültasyonları desteklemek için gereklidir. Potansiyel olarak güvenlik açısından kritik.	Yüksek. Kliniklerin iptal edilmesi gerekebileceğinden mali kayıp. Sistemi geri yükleme maliyetleri. Tedavi reçete edilemezse olası hasta zararı.
hasta veritabanı	Yüksek. Tüm klinik konsültasyonları desteklemek için gereklidir. Potansiyel olarak güvenlik açısından kritik.	Yüksek. Kliniklerin iptal edilmesi gerekebileceğinden mali kayıp. Sistemi geri yükleme maliyetleri. Tedavi reçete edilemezse olası hasta zararı.
Bireysel hasta kaydı	Normalde düşüktür, ancak belirli yüksek profilli hastalar için yüksek olabilir.	Düşük doğrudan kayıplar ancak olası itibar kaybı.

Tehdit ve Kontrol Analizi

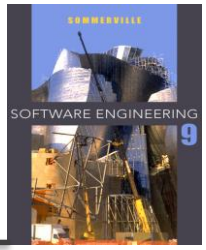
Tehdit	olasılık	Kontrol	Fizibilite
Yetkisiz kullanıcı sistem yöneticisi olarak erişim kazanır ve sistemi kullanılamaz hale getirir	Düşük	Yalnızca fiziksel olarak güvenli olan belirli konumlardan sistem yönetimine izin verin.	Düşük uygulama maliyeti, ancak anahtar dağıtımına ve acil bir durumda anahtarların hazır bulunmasına özen gösterilmelidir.
Yetkisiz kullanıcı sistem kullanıcısı olarak erişim kazanır ve gizli bilgilere erişir	Yüksek	Tüm kullanıcıların biyometrik bir mekanizma kullanarak kimliklerini doğrulamasını zorunlu kılın. Sistem kullanımını izlemek için hasta bilgilerindeki tüm değişiklikleri günlüğe kaydedin.	Teknik olarak uygulanabilir ancak yüksek maliyetli bir çözüm. Olası kullanıcı direnci. Uygulaması basit ve şeffaftır ve ayrıca kurtarmayı destekler.

Güvenlik Gereksinimleri



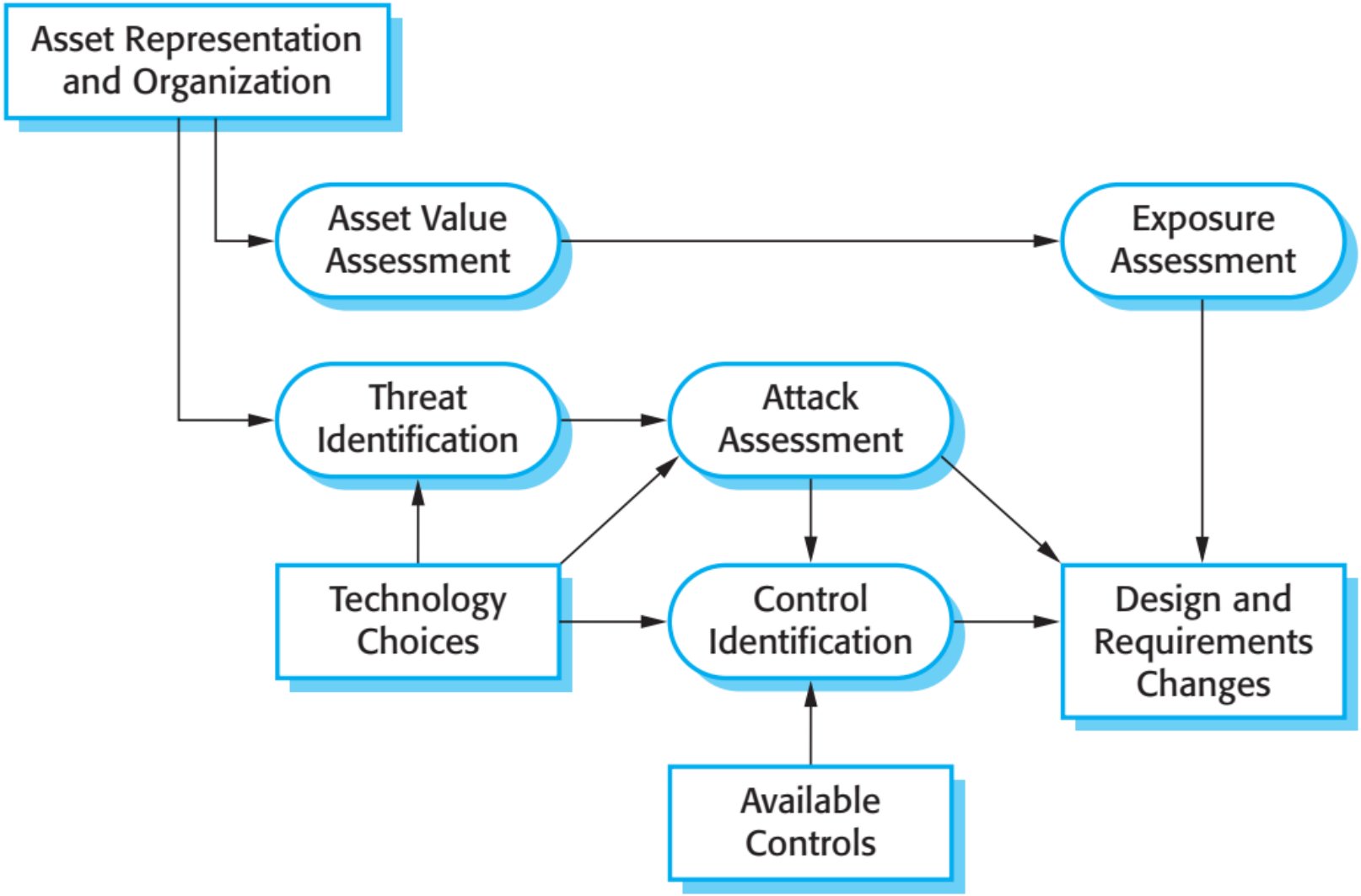
- Hasta bilgileri, bir klinik oturumunun başlangıcında, klinik personeli tarafından kullanılan sistem istemcisindeki güvenli bir alana indirilmelidir.
- Bir klinik oturumu bittikten sonra sistem istemcilerinde hasta bilgileri tutulmamalıdır.
- Sistem veritabanında yapılan tüm değişikliklerin veritabanı sunucusundan ayrı bir bilgisayarda bir günlük tutulması gerekir.

Yaşam Döngüsü Risk Değerlendirmesi

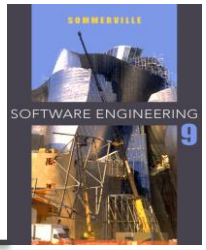


- Sistem geliştirilirken ve devreye alındıktan sonra risk değerlendirmesi
- Daha fazla bilgi mevcuttur - sistem platformu, ara katman yazılımı ve sistem mimarisi ve veri organizasyonu.
- Bu nedenle tasarım seçimlerinden kaynaklanan güvenlik açıkları belirlenebilir.

Yaşam Döngüsü Risk Analizi

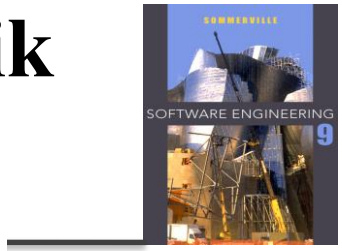


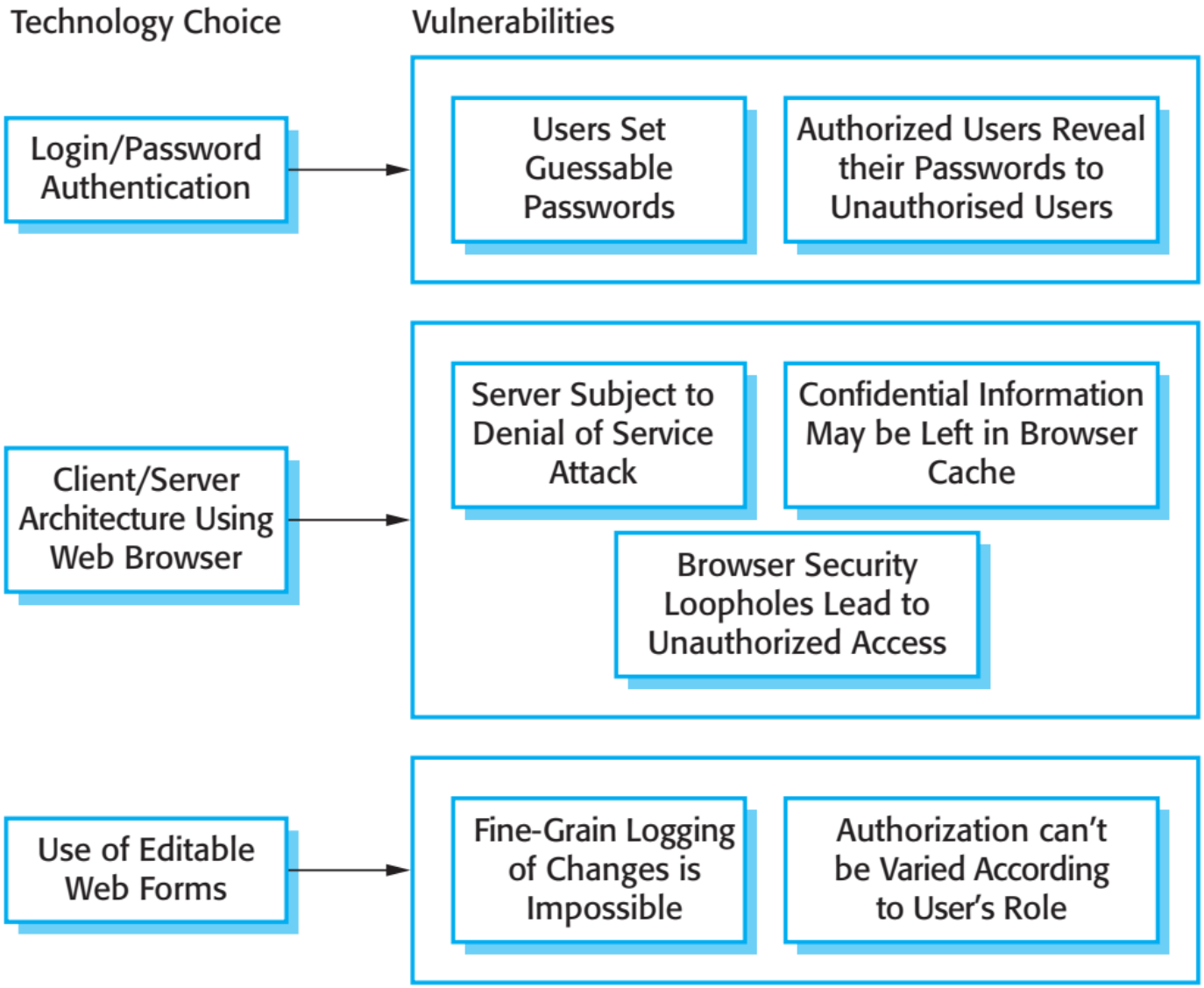
COTS (Hazır Yazılım) Kullanımından Kaynaklanan Tasarım Kararları



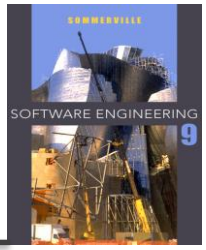
- Sistem kullanıcılarının kimlikleri bir ad/şifre kombinasyonu kullanılarak doğrulandı.
- Sistem mimarisi, istemcilerin sisteme standart bir web tarayıcısı aracılığıyla eriştiği istemci-sunucudur.
- Bilgi, düzenlenebilir bir web formu olarak sunulur.

Teknoloji Seçimleriyle İlişkili Güvenlik Açıkları



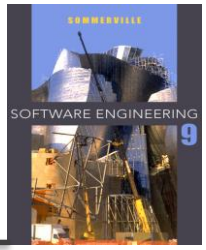


Güvenlik Gereksinimleri



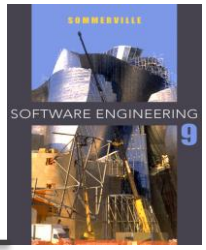
- Bir parola denetleyicisi hazır bulundurulacak ve günlük olarak çalıştırılacaktır. Zayıf şifreler sistem yöneticilerine bildirilecektir.
- Sisteme erişime yalnızca onaylı istemci bilgisayarlar tarafından izin verilecektir.
- Tüm istemci bilgisayarlarda sistem yöneticileri tarafından kurulmuş, onaylanmış tek bir web tarayıcısı olacaktır.

Operasyonel Risk Değerlendirmesi



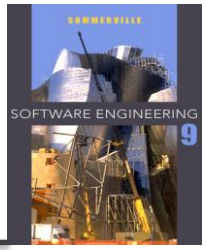
- Yaşam döngüsü risk değerlendirmesinin devamı, ancak sistemin kullanıldığı ortam hakkında ek bilgiler.
- Ortam özellikleri yeni sistem risklerine yol açabilir
  - Kesinti riski, oturum açmış bilgisayarların gözetimsiz bırakılması anlamına gelir.

Güvenlik İçin Tasarım



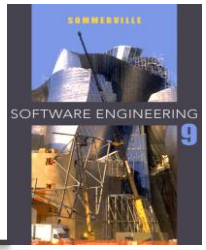
- Mimari tasarım
  - Mimari tasarım kararları bir sistemin güvenliğini nasıl etkiler?
- İyi pratik
  - Güvenli sistemler tasarlanırken kabul edilen iyi uygulama nedir?
- Dağıtım için tasarım
  - Bir sistem kullanım için dağıtıldığında güvenlik açıklarının ortaya çıkmasını önlemek için sisteme hangi destek tasarlanmalıdır?

Mimari Tasarım



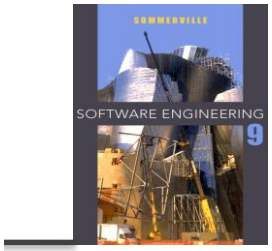
- Güvenlik için bir mimari tasarlarken iki temel konu dikkate alınmalıdır.
  - Koruma
    - Kritik varlıkların dış saldırılara karşı korunabilmesi için sistem nasıl organize edilmelidir?
  - Dağıtım
    - Başarılı bir saldırının etkilerinin en aza indirilmesi için sistem varlıkları nasıl dağıtılmalıdır?
- Bunlar potansiyel olarak çelişkili
  - Varlıklar dağıtılırsa, korunmaları daha pahalıdır. Varlıklar korunursa, kullanılabilirlik ve performans gereksinimleri tehlikeye girebilir.

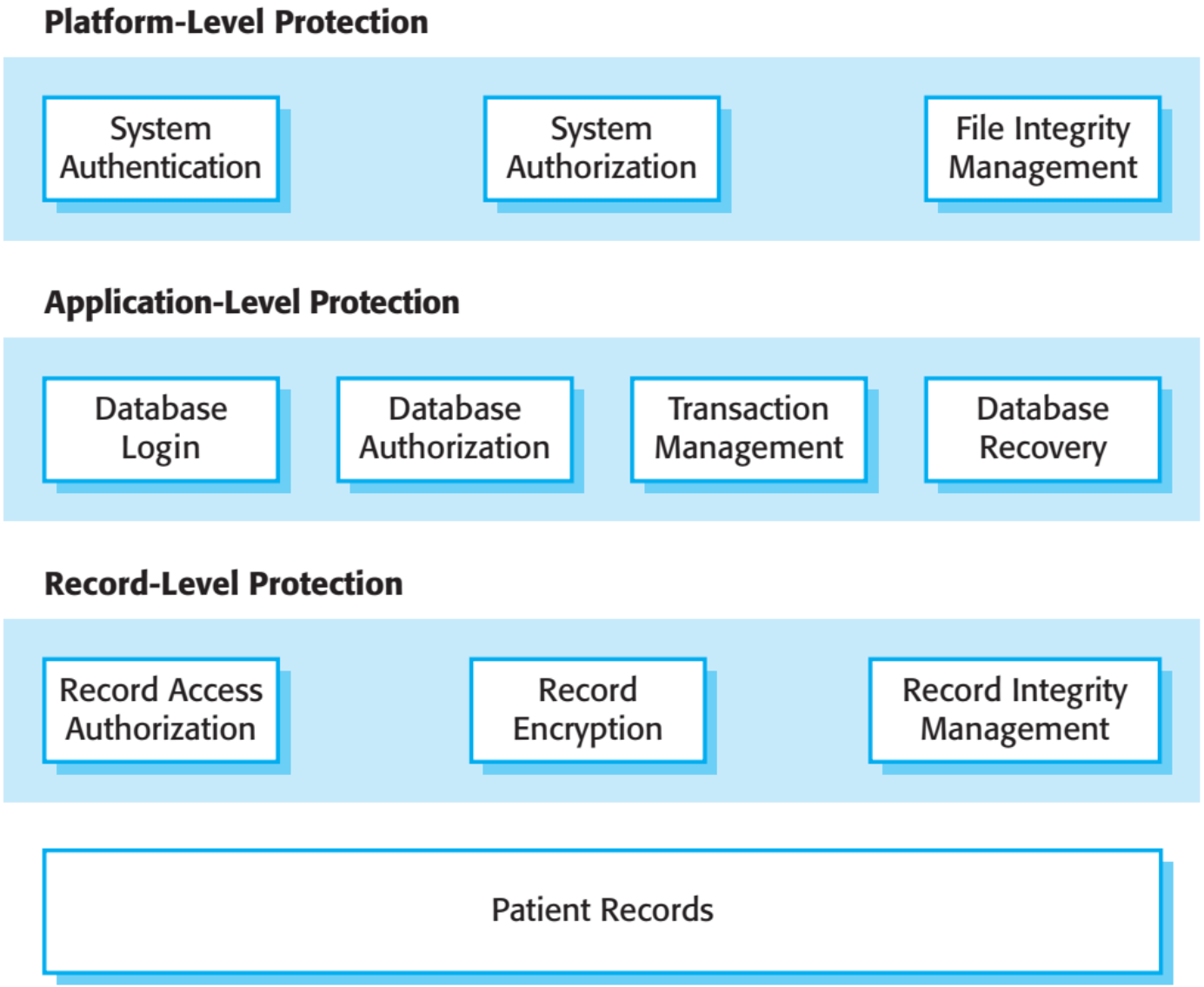
Koruma



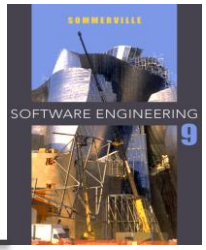
- Platform düzeyinde koruma
  - Bir sistemin üzerinde çalıştığı platformdaki üst düzey kontroller.
- Uygulama düzeyinde koruma
  - Uygulamanın kendisinde yerleşik özel koruma mekanizmaları, örneğin ek parola koruması.
- Kayıt düzeyinde koruma
  - Belirli bilgilere erişim istendiğinde çağrılan koruma
- Bunlar katmanlı bir koruma mimarisine yol açar

Katmanlı Bir Koruma Mimarisi



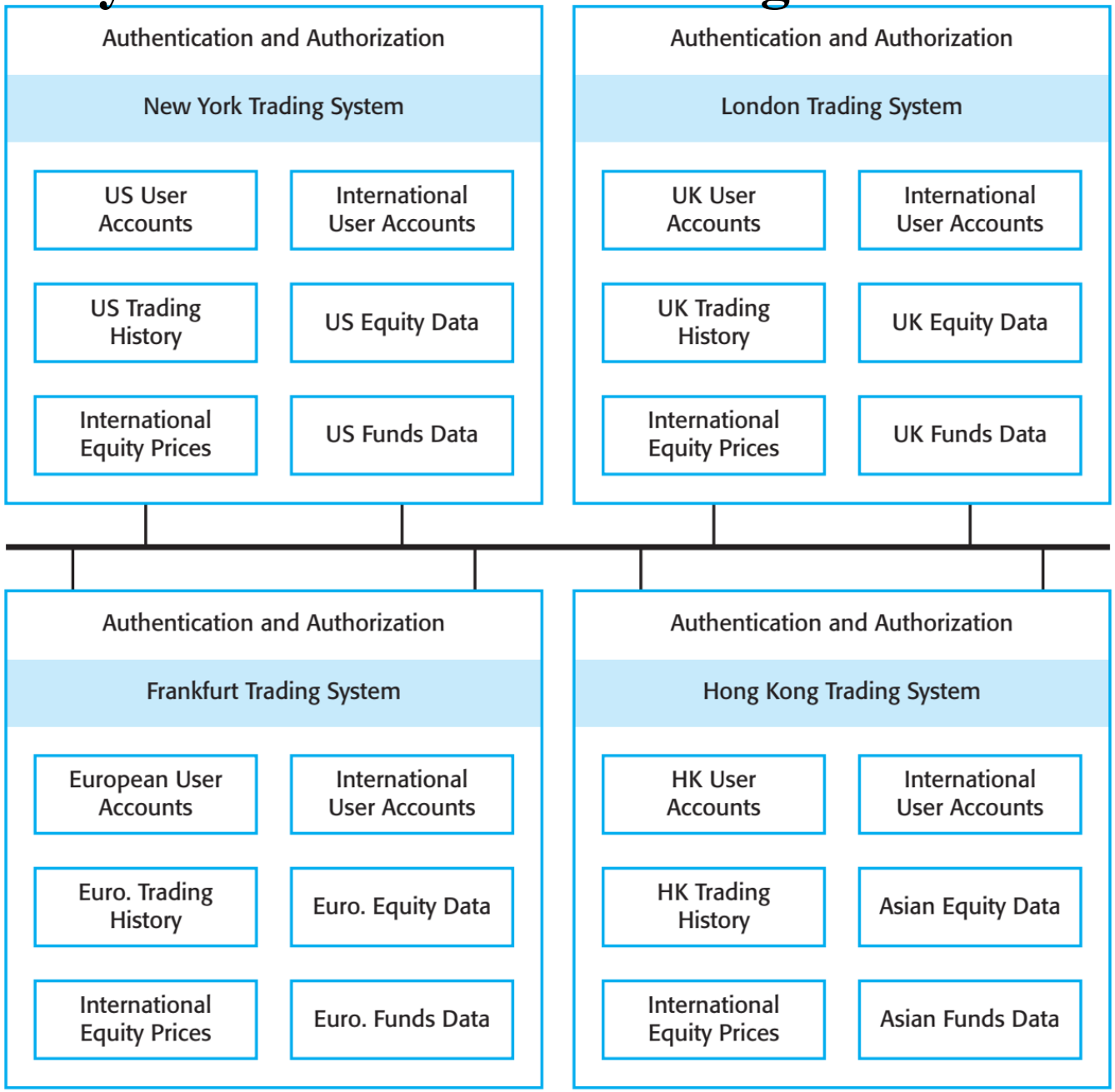


Dağıtım

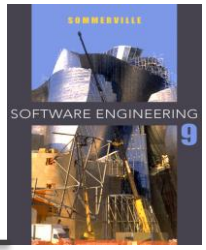


- Varlıkları dağıtmak, bir sisteme yapılan saldırıların mutlaka sistem hizmetinin tamamen kaybolmasına yol açmadığı anlamına gelir.
- Her platformun ayrı koruma özellikleri vardır ve ortak bir güvenlik açığını paylaşmamaları için diğer platformlardan farklı olabilir.
- Hizmet reddi saldırıları riski yüksekse dağıtım özellikle önemlidir

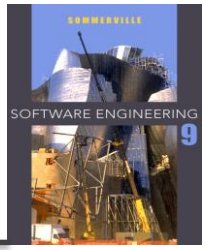
Bir Öz Sermaye Ticaret Sisteminde Dağıtılan Varlıklar



Bölüm 1'in Anahtar Noktaları



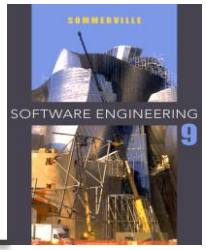
- Güvenlik mühendisliği, kötü niyetli saldırılara direnebilecek sistemlerin nasıl geliştirileceği ile ilgilenir.
- Güvenlik tehditleri, bir sistemin veya verilerinin gizliliğine, bütünlüğüne veya kullanılabilirliğine yönelik tehditler olabilir.
- Güvenlik riski yönetimi, saldırılardan kaynaklanan olası kayıpların değerlendirilmesi ve kayıpları en aza indirmek için güvenlik gereksinimlerinin türetilmesi ile ilgilidir.
- Güvenlik için tasarım, mimari tasarımı, iyi tasarım uygulamalarını takip etmeyi ve sistem açıklarının ortaya çıkmasını en aza indirmeyi içerir.



Ders 14 – Güvenlik Mühendisliği

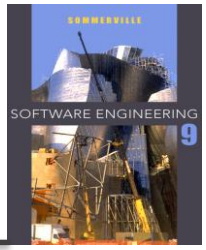
Bölüm 2

Bölüm 2'de İşlenmiş Konular



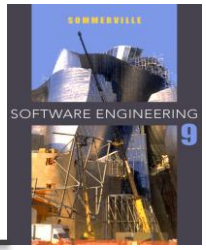
- Güvenlik için tasarım yönergeleri
  - Güvenli bir sistem tasarlamanıza yardımcı olacak yönergeler
- Dağıtım için tasarım
  - Güvenlik açıklarına neden olabilecek dağıtım sorunları en aza indirilecek şekilde tasarım yapın
- Sistem bekası
  - Sistemin saldırı altındayken temel hizmetleri sunmasına izin verin

Güvenlik Mühendisliği İçin Tasarım Yönergeleri



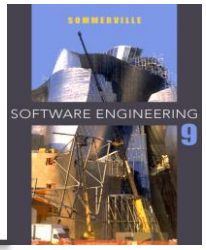
- Tasarım yönergeleri, güvenli sistem tasarımındaki iyi uygulamaları kapsar
- Tasarım yönergeleri iki amaca hizmet eder:
  - Bir yazılım mühendisliği ekibinde güvenlik sorunları konusunda farkındalık oluştururlar. Tasarım kararları alınırken güvenlik göz önünde bulundurulur.
  - Sistem doğrulama işlemi sırasında uygulanan bir gözden geçirme kontrol listesinin temeli olarak kullanılabilirler.
- Buradaki tasarım yönergeleri, yazılım spesifikasyonu ve tasarımı sırasında geçerlidir

Güvenli Sistem Mühendisliği İçin Tasarım Yönergeleri



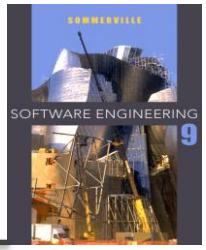
Güvenlik yönergeleri
Güvenlik kararlarını açık bir güvenlik politikasına dayandırın
Tek bir başarısızlık noktasından kaçının
Güvenli bir şekilde başarısız olun
Güvenlik ve kullanılabilirliği dengeleyin
Kullanıcı işlemlerini günlüğe kaydet
Riski azaltmak için artıklık ve çeşitlilik kullanın
Tüm girişleri doğrula
Varlıklarınızı bölümlere ayırın
Dağıtım için tasarım
Geri kazanılabilirlik için tasarım

Tasarım Yönergeleri 1-3



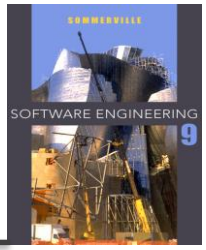
- Kararları açık bir güvenlik politikasına dayandırın
  - Tüm kurumsal sistemlere uygulanması gereken temel güvenlik gereksinimlerini belirleyen kuruluş için bir güvenlik politikası tanımlayın.
- Tek bir başarısızlık noktasından kaçının
  - Bir güvenlik hatasının yalnızca güvenlik prosedürlerinde birden fazla hata olduğunda ortaya çıkabileceğinden emin olun. Örneğin, parola ve soru tabanlı kimlik doğrulaması yapın.
- Güvenli bir şekilde başarısız olun
  - Herhangi bir nedenle sistemler arızalandığında, normal güvenlik prosedürleri mevcut olmasa bile hassas bilgilere yetkisiz kullanıcılar tarafından erişilemeyeceğinden emin olun.

Tasarım Yönergeleri 4-6



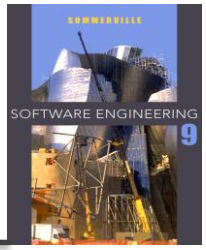
- Güvenlik ve kullanılabilirliği dengeleyin
  - Sistemin kullanımını zorlaştıran güvenlik prosedürlerinden kaçınmaya çalışın. Bazen sistemi daha kullanışlı hale getirmek için daha zayıf güvenliği kabul etmeniz gerekir.
- Kullanıcı işlemlerini günlüğe kaydet
  - Kimin ne yaptığını keşfetmek için analiz edilebilecek bir kullanıcı eylemleri günlüğü tutun. Kullanıcılar böyle bir günlükten haberdarlarsa, sorumsuzca davranma olasılıkları daha düşüktür.
- Riski azaltmak için artıklık ve çeşitlilik kullanın
  - Birden çok veri kopyasını saklayın ve çeşitli altyapıları kullanın, böylece bir altyapı güvenlik açığı tek hata noktası olamaz.

Tasarım Yönergeleri 7-10



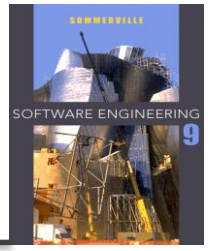
- Tüm girişleri doğrula
  - Beklenmeyen girişlerin sorunlara neden olmaması için tüm girişlerin aralık içinde olduğunu kontrol edin.
- Varlıklarınızı bölümlere ayırın
  - Sistemi, varlıklar ayrı alanlarda olacak ve kullanıcıların tüm sistem bilgileri yerine yalnızca ihtiyaç duydukları bilgilere erişebilecekleri şekilde düzenleyin.
- Dağıtım için tasarım
  - Dağıtım sorunlarını önlemek için sistemi tasarlayın
- Geri kazanılabilirlik için tasarım
  - Başarılı bir saldırıdan sonra kurtarılabilirliği basitleştirmek için sistemi tasarlayın.

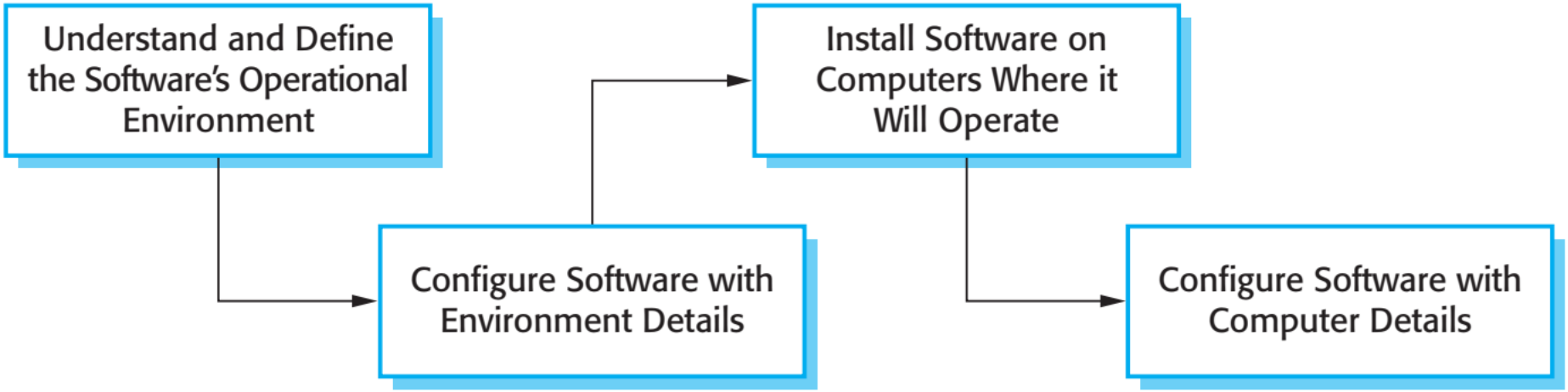
Dağıtım İçin Tasarım



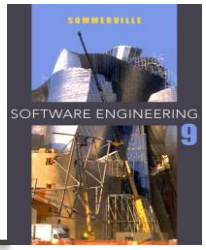
- Dağıtım, yazılımın çalışma ortamında çalışacak şekilde yapılandırılmasını, sistemin kurulmasını ve operasyonel platform için yapılandırılmasını içerir.
- Bu aşamada yapılandırma hataları sonucunda güvenlik açıkları ortaya çıkabilir.
- Sisteme dağıtım desteği tasarlamak, güvenlik açıklarının ortaya çıkma olasılığını azaltabilir.

Yazılım Dağıtımı



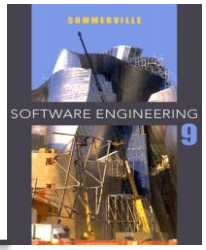


Yapılandırma Güvenlik Açıkları



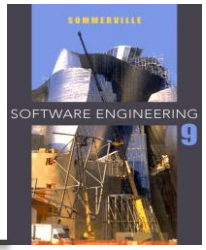
- Güvenlik açığı bulunan varsayılan ayarlar
  - Saldırganlar, yazılım için varsayılan ayarları bulabilir. Bunlar zayıfsa (genellikle kullanılabilirliği artırmak için), bir sisteme saldırırken kullanıcılar tarafından kullanılabilirler.
- Dağıtım yerine geliştirme
  - Sistemlerdeki bazı yapılandırma ayarları, geliştirme ve hata ayıklamayı desteklemek üzere tasarlanmıştır. Bunlar kapatılmazsa, saldırganlar tarafından istismar edilebilecek bir güvenlik açığı olabilir.

Dağıtım Desteği 1



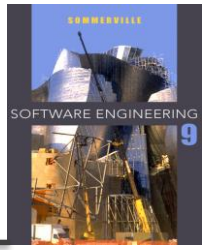
- Yapılandırmaları görüntüleme ve analiz etme desteğini dahil edin
  - Dağıtımdan sorumlu sistem yöneticisinin tüm yapılandırmayı kolayca görüntüleyebildiğinden emin olun. Bu, yapılan eksiklikleri ve hataları tespit etmeyi kolaylaştırır.
- Varsayılan ayrıcalıkları en aza indirin ve böylece neden olabilecek hasarı sınırlayın
  - Sistemi, bir yöneticinin varsayılan ayrıcalıkları en aza indirilecek şekilde tasarlayın. Bu, birisi yönetici erişimi kazanırsa, sistemin özelliklerine anında erişemeyeceği anlamına gelir.

Dağıtım Desteği 2



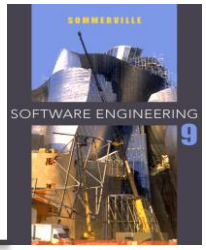
- Yapılandırma ayarlarını yerelleştirin
  - Bir sistem kurarken, bir sistemin aynı parçası veya bileşeni ile ilgili tüm bilgiler, hepsi bir kerede kurulacak şekilde yerelleştirilmelidir. Aksi takdirde, ilgili güvenlik özelliklerini kurmayı unutmak kolaydır.
- Güvenlik açıklarını düzeltmenin kolay yollarını sağlayın
  - Sorunlar algılandığında, dağıtılan sistemlerdeki güvenlik açıklarını onarmak için otomatik güncelleme gibi kolay yollar sağlayın.

Sistem Bekası (Hayatta Kalabilmesi)



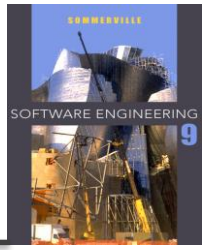
- Beka kabiliyeti, sistemin saldırı altındayken veya sistemin bir kısmı hasar gördükten sonra temel hizmetleri sunma yeteneğini yansıtan acil bir sistem özelliğidir.
- Hayatta kalma analizi ve tasarımı, güvenlik mühendisliği sürecinin bir parçası olmalıdır

Hayatta Kalmanın Önemi



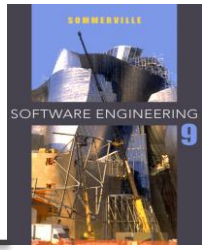
- Ekonomik ve sosyal hayatımız bilgisayar sistemlerine bağlıdır.
  - Kritik altyapı – elektrik, gaz, telekomünikasyon, ulaşım
  - Sağlık hizmeti
  - Hükümet
- Kısa bir süre için bile iş sistemlerinin kaybı çok ciddi ekonomik etkilere sahip olabilir
  - Havayolu rezervasyon sistemleri
  - E-ticaret sistemleri
  - Ödeme sistemleri

Servis Mevcudiyeti



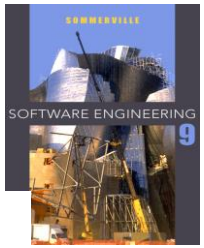
- Bir işletme için en kritik sistem hizmetleri hangileridir?
- Bu hizmetler nasıl tehlikeye girebilir?
- Sürdürülmesi gereken asgari hizmet kalitesi nedir?
- Bu hizmetler nasıl korunabilir?
- Bir hizmet kullanılamaz hale gelirse, ne kadar çabuk kurtarılabilir?

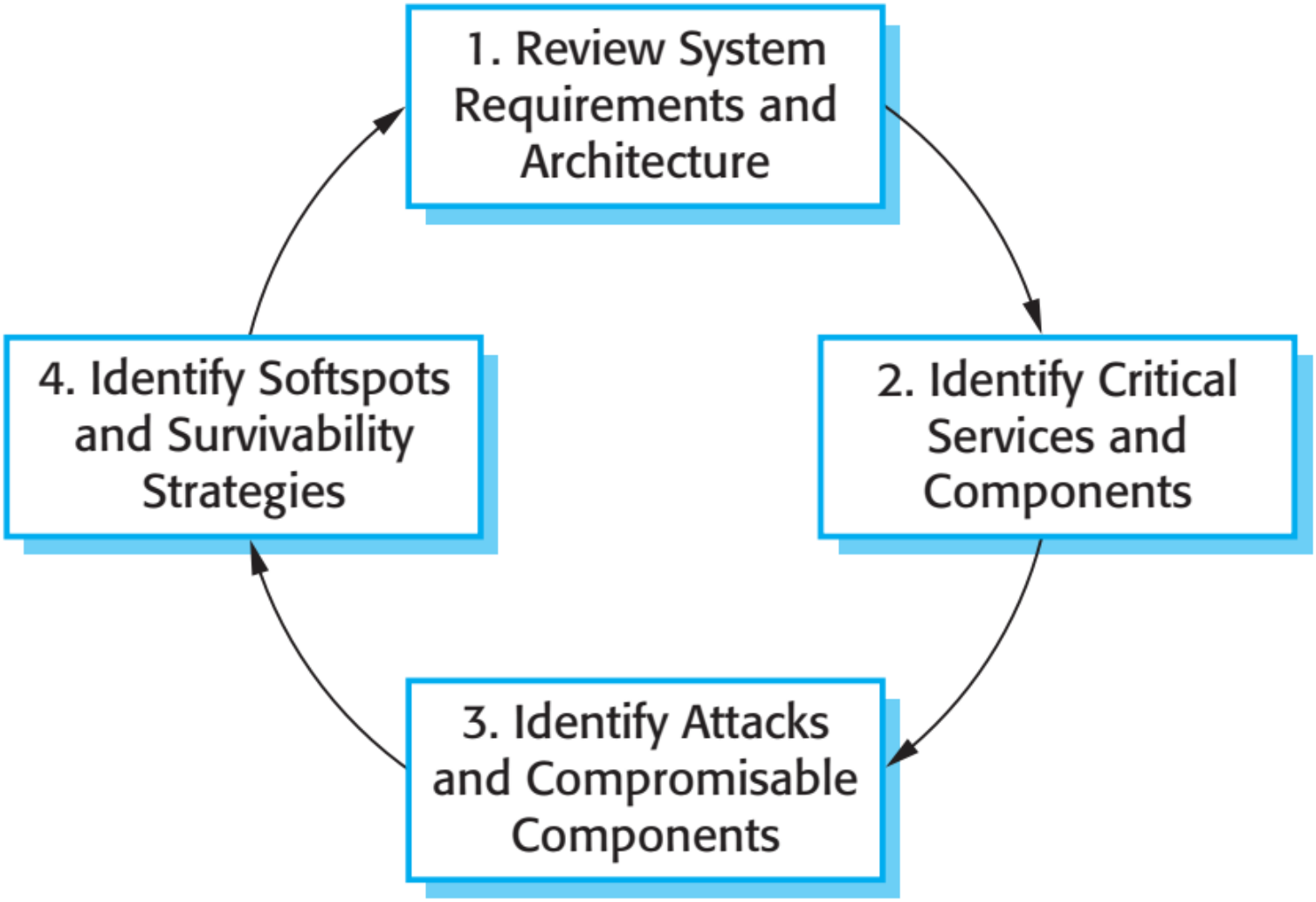
Hayatta Kalma Stratejileri



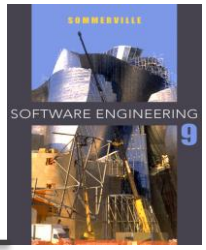
- Direnç
  - Saldırılara direnmek için sisteme yetenekler ekleyerek sorunlardan kaçınmak
- Tanıma
  - Saldırıları ve arızaları tespit etmek ve ortaya çıkan hasarı değerlendirmek için sisteme yetenekler ekleyerek sorunları tespit etmek
- Kurtarma
  - Saldırı altındayken hizmet sunmak için sisteme yetenekler ekleyerek sorunları tolere etmek

Hayatta Kalma Analizindeki Aşamalar



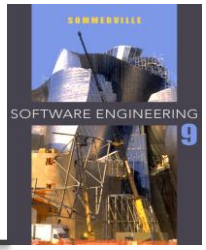


Anahtar Faaliyetler



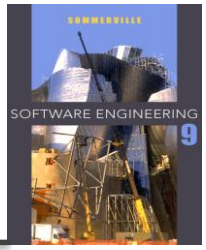
- Sistem anlayışı
  - Hedefleri, gereksinimleri ve mimariyi gözden geçirin
- Kritik hizmet tanımlama
  - Bakımı yapılması gereken hizmetleri belirleyin
- Saldırı simülasyonu
  - Saldırı senaryoları tasarlayın ve etkilenen bileşenleri belirleyin
- Beka analizi
  - Uygulanacak hayatta kalma stratejilerini belirleyin

Borsa Sistemi Beka



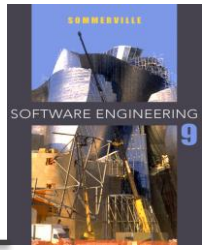
- Birden fazla sunucuya çoğaltılan kullanıcı hesapları ve hisse senedi fiyatları, böylece bir sunucu çalışmaz hale gelse bile hizmet devamı sağlanabilir
- Korunması gereken temel yetenek, stok için sipariş verme yeteneğidir.
- Siparişler doğru olmalı ve bir tüccar tarafından yapılan gerçek satışları/satın almaları yansıtmalıdır.

Hayatta Kalabilen Sipariş Hizmeti



- Hayatta kalması gereken kritik hizmet, yetkili kullanıcıların stok için sipariş verme yeteneğidir.
- Bu, sistemin 3 bileşeninin kullanılabilir olmasını ve çalışma güvenilirliğini gerektirir:
  - Yetkili kullanıcıların sistemde oturum açmasına izin veren kullanıcı kimlik doğrulaması
  - Fiyat teklifi, alış ve satış fiyatlarının kote edilmesini sağlar
  - Alış ve satış emirlerinin yapılmasına imkan veren emir yerleştirme

Olası Saldırılar

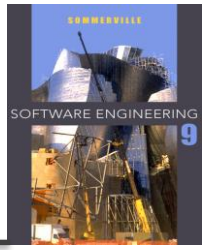


- Kötü niyetli kullanıcı meşru bir kullanıcı gibi davranır ve meşru kullanıcı için sorun oluşturmak amacıyla kötü niyetli hisse senedi siparişleri verir.
- Yetkisiz bir kullanıcı, işlem veritabanını bozarak satış ve satın almaların mutabakatını imkansız hale getirir.

Bir Hisse Senedi Alım Satım Sisteminde Beka Analizi

saldırı	Direnç	Tanıma	Kurtarma
Yetkisiz kullanıcı kötü niyetli siparişler verir	Sipariş vermek için giriş şifresinden farklı bir işlem şifresi isteyin.	İrtibat telefon numarası ile yetkili kullanıcıya siparişin kopyasını e-posta ile gönderin (kötü niyetli siparişleri tespit edebilmeleri için). Kullanıcının sipariş geçmişini koruyun ve olağandışı ticaret modellerini kontrol edin.	İşlemleri otomatik olarak 'geri almak' ve kullanıcı hesaplarını geri yüklemek için mekanizma sağlayın. Kötü niyetli ticaretten kaynaklanan kayıplar için kullanıcılara geri ödeme yapın. Dolaylı kayıplara karşı sigortalayın.
İşlem veritabanının bozulması	Ayrıcalıklı kullanıcıların, dijital sertifikalar gibi daha güçlü bir kimlik doğrulama mekanizması kullanarak yetkilendirilmesini zorunlu kılın.	Uluslararası bir sunucudaki bir ofis için işlemlerin salt okunur kopyalarını koruyun. Yolsuzluğu kontrol etmek için işlemleri periyodik olarak karşılaştırın. Yolsuzluğu tespit etmek için tüm işlem kayıtlarıyla kriptografik sağlama toplamını koruyun.	Veritabanını yedek kopyalardan kurtarın. İşlem veritabanını yeniden oluşturmak için işlemleri belirli bir zamandan itibaren yeniden oynatmak için bir mekanizma sağlayın.

Bölüm 2'nin Anahtar Noktaları



- Genel güvenlik yönergeleri, tasarımcıları güvenlik sorunlarına karşı duyarlı hale getirir ve gözden geçirme kontrol listeleri olarak hizmet eder
- Yapılandırma görselleştirme, yerelleştirme ayarı ve varsayılan ayrıcalıkların en aza indirilmesi, dağıtım hatalarının azaltılmasına yardımcı olur
- Sistemin beka kabiliyeti, bir sistemin saldırı altındayken veya sistemin bir kısmı hasar gördükten sonra hizmet sunma yeteneğini yansıtır.