IT522 – Yazılım Mühendisliği 2021

PhD Furkan Gözükara, Toros University

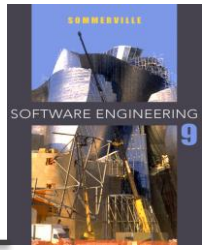
https://github.com/FurkanGozukara/Yazilim-Muhendisligi-IT522-2021

Ders 11

Güvenlik ve Güvenilebilirlik

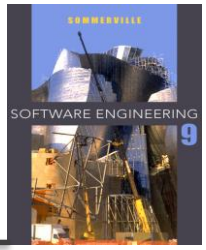
Kaynak : https://ifs.host.cs.st-andrews.ac.uk/Books/SE9/Presentations/index.html

Bölüm 1'de İşlenmiş Konular



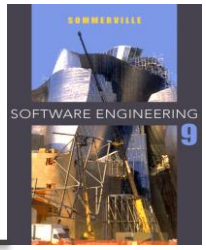
- Güvenilebilirlik özellikleri
  - Güvenilirliğe yol açan sistem özellikleri.
- Kullanılabilirlik ve güvenilebilirlik
  - Hizmet sunmak ve beklendiği gibi çalışmak için sistemler mevcut olmalıdır.
- Emniyet
  - Sistemler güvenli olmayan bir şekilde davranmamalıdır.
- Güvenlik
  - Sistemler kendilerini ve verilerini dış müdahalelerden korumalıdır.

Sistem Güvenilirliği



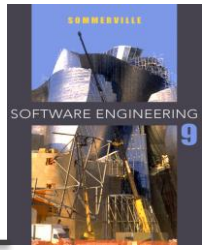
- Birçok bilgisayar tabanlı sistem için en önemli sistem özelliği sistemin güvenilirliğidir.
- Bir sistemin güvenilirliği, kullanıcının o sisteme olan güven derecesini yansıtır. Kullanıcının beklediği gibi çalışacağına ve normal kullanımda 'başarısız olmayacağına' dair kullanıcının güveninin derecesini yansıtır.
- Güvenilebilirlik, güvenilirlik, kullanılabilirlik ve güvenlik gibi ilgili sistem özelliklerini kapsar. Bunların hepsi birbirine bağlıdır.

Güvenilirliğin Önemi



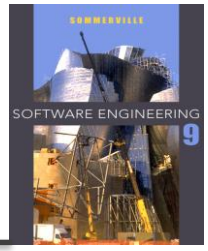
- Sistem arızalarının, başarısızlıktan etkilenen çok sayıda insanda yaygın etkileri olabilir.
- Güvenilir olmayan ve güvenilmez, güvenli olmayan veya emniyetsiz sistemler kullanıcıları tarafından reddedilebilir.
- Arıza ekonomik kayıplara veya fiziksel hasara yol açarsa, sistem arızasının maliyetleri çok yüksek olabilir.
- Güvenilir olmayan sistemler, yüksek bir kurtarma maliyeti ile bilgi kaybına neden olabilir.

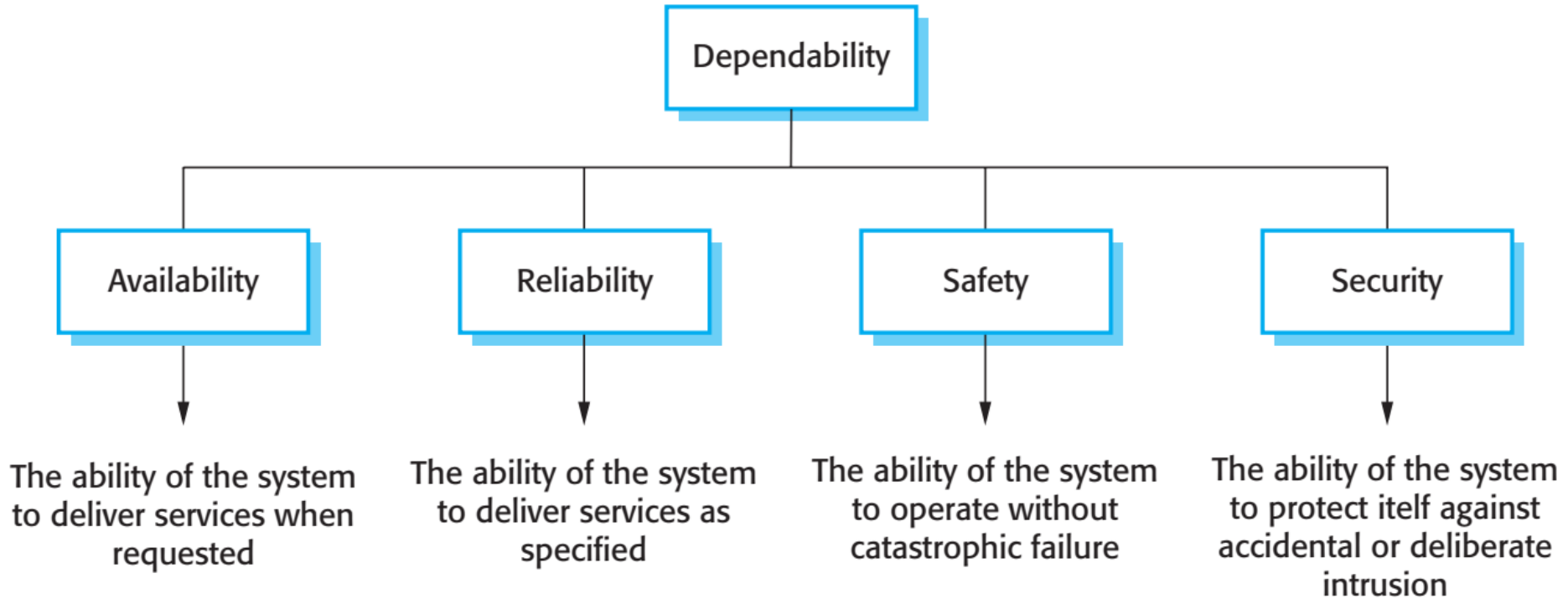
Başarısızlık Nedenleri



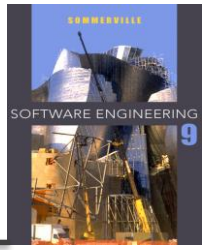
- Donanım arızası
  - Donanım, tasarım ve üretim hataları nedeniyle veya bileşenlerin doğal ömürlerinin sonuna ulaşması nedeniyle başarısız oluyor.
- Yazılım hatası
  - Yazılım, teknik özellikleri, tasarımı veya uygulamasındaki hatalar nedeniyle başarısız oluyor.
- Operasyonel arıza
  - İnsan operatörleri hata yapar. Şimdi belki de sosyo-teknik sistemlerdeki sistem arızalarının en büyük tek nedeni.

Temel Güvenilebilirlik Özellikleri



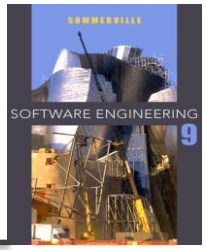


Temel Özellikler



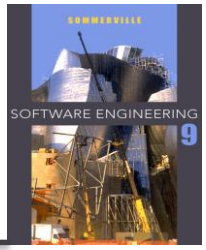
- Kullanılabilirlik
  - Sistemin çalışır durumda olma ve kullanıcılara yararlı hizmetler sunma olasılığı.
- Güvenilebilirlik
  - Sistemin, kullanıcıların beklediği gibi hizmetleri doğru bir şekilde sunma olasılığı.
- Emniyet
  - Sistemin insanlara veya çevresine zarar vermesinin ne kadar muhtemel olduğuna dair bir yargı.
- Güvenlik
  - Sistemin kazara veya kasıtlı müdahalelere ne kadar direnebileceğine dair bir yargı.

Diğer Güvenilebilirlik Özellikleri



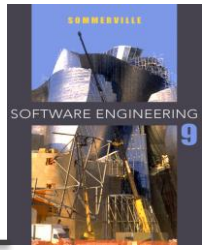
- Onarılabilirlik
  - Bir arıza durumunda sistemin ne ölçüde tamir edilebileceğini yansıtır
- Sürdürülebilirlik
  - Sistemin yeni gereksinimlere ne ölçüde uyarlanabileceğini yansıtır;
- Beka Kabiliyeti
  - Düşmanca saldırı altındayken sistemin ne ölçüde hizmet sunabileceğini yansıtır;
- Hata toleransı
  - Kullanıcı girişi hatalarının ne ölçüde önlenebileceğini ve tolere edilebileceğini yansıtır.

Onarılabilirlik



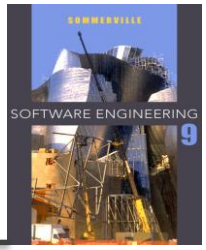
- Sistem hızlı bir şekilde onarılabilirse, sistem arızasından kaynaklanan kesinti en aza indirilebilir.
- Bu, sorun teşhisi, arızalı bileşenlere erişim ve sorunları gidermek için değişiklikler yapılmasını gerektirir.
- Onarılabilirlik, bir sistem arızasına yol açan arızaları düzeltmek için yazılımı tamir etmenin ne kadar kolay olduğuna dair bir hükümdür.
- Onarılabilirlik, işletim ortamından etkilenir, bu nedenle sistem dağıtımından önce değerlendirilmesi zordur.

Sürdürülebilirlik



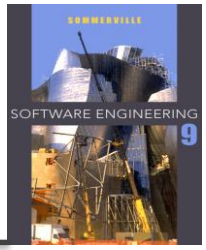
- Bir arıza tespit edildikten sonra sistemi tamir etmenin kolaylığıyla ilgilenen veya sistemi yeni özellikler içerecek şekilde değiştiren bir sistem özelliği.
- Onarılabilirlik - sistemi tekrar hizmete sokmak için kısa vadeli perspektif; Sürdürülebilirlik - uzun vadeli perspektif.
- Bakım sorunları nedeniyle arızalar genellikle bir sisteme girdiğinden kritik sistemler için çok önemlidir. Bir sistemin bakımı yapılabiliyorsa, bu arızaların ortaya çıkması veya tespit edilmemesi olasılığı daha düşüktür.

Beka Kabiliyeti



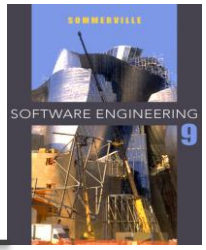
- Bir sistemin kasıtlı veya kazara saldırı karşısında kullanıcılara hizmetlerini sunmaya devam etme yeteneği
- Bu, güvenliği daha çok tehlikeye maruz kalan dağıtılmış sistemler için giderek daha önemli bir özelliktir
- Sürdürülebilirlik, esneklik kavramını kapsar - bir sistemin bileşen arızalarına rağmen çalışmaya devam etme yeteneği

Hata Toleransı



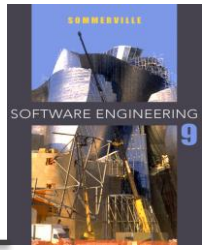
- Daha genel bir kullanılabilirlik özelliğinin parçasıdır ve kullanıcı hatalarının ne ölçüde önlendiğini, tespit edildiğini veya tolere edildiğini yansıtır.
- Kullanıcı hataları mümkün olduğunca otomatik olarak tespit edilip düzeltilmeli, sisteme aktarılmamalı ve arızalara neden olmamalıdır.

Güvenilebilirlik Özniteliği Bağımlılıkları



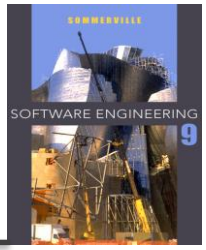
- Güvenli sistem işletimi, sistemin mevcut olmasına ve güvenilir şekilde çalışmasına bağlıdır.
- Bir sistem, verileri harici bir saldırı nedeniyle bozulmuş olduğu için güvenilmez olabilir.
- Bir sisteme yapılan hizmet reddi saldırıları, sistemi kullanılamaz hale getirmeyi amaçlar.
- Bir sisteme virüs bulaşmışsa, onun güvenilirliğinden veya güvenliğinden emin olamazsınız.

Güvenilebilirlik Başarısı



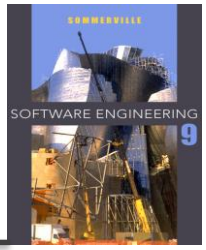
- Sistemi geliştirirken yanlışlıkla hataların ortaya çıkmasını önleyin.
- Sistemdeki kalıntı hataları keşfetmede etkili olan V & V süreçlerini tasarlayın.
- Dış saldırılara karşı koruma sağlayan koruma mekanizmaları tasarlayın.
- Sistemi işletim ortamı için doğru şekilde yapılandırın.
- Bir arızadan sonra normal sistem hizmetinin geri yüklenmesine yardımcı olmak için kurtarma mekanizmaları ekleyin.

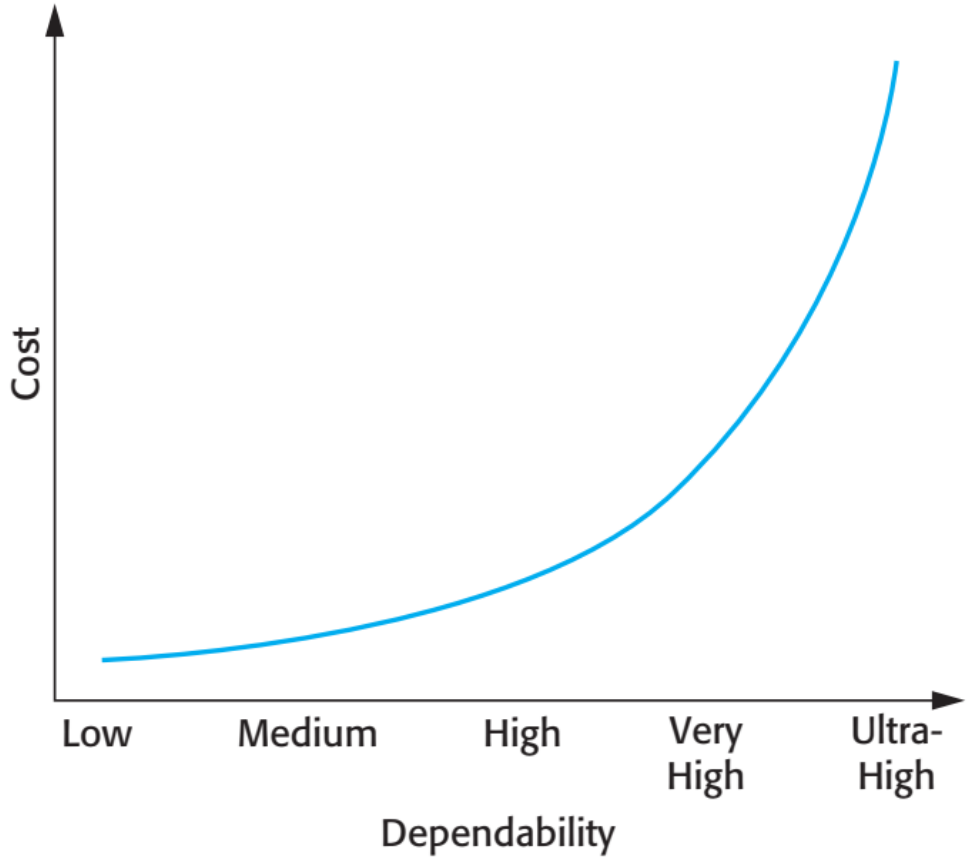
Güvenilebilirlik Maliyetleri



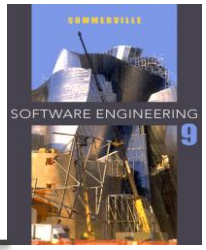
- Güvenilebilirlik maliyetleri, artan güvenilebilirlik seviyeleri gerekeceğinden katlanarak artma eğilimindedir.
- Bunun iki nedeni var
  - Daha yüksek düzeyde güvenilebilirlik elde etmek için gerekli olan daha pahalı geliştirme tekniklerinin ve donanımların kullanılması.
  - Sistem istemcisini ve düzenleyicileri gerekli güvenilebilirlik düzeylerine ulaşıldığına ikna etmek için gerekli olan artırılmış test ve sistem doğrulaması.

Maliyet / Güvenilebilirlik Eğrisi



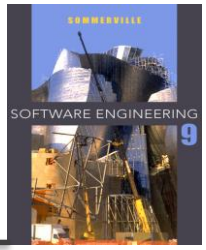


Güvenilebilirlik Ekonomisi



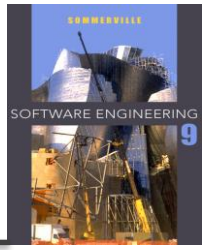
- Güvenilebilirlik başarısının çok yüksek maliyetleri nedeniyle, güvenilir olmayan sistemleri kabul etmek ve arıza maliyetlerini ödemek daha uygun maliyetli olabilir.
- Ancak bu, sosyal ve politik faktörlere bağlıdır. Güvenilemeyen ürünler için itibar, gelecekteki işlerini kaybedebilir
- Sistem türüne bağlıdır - bazı iş sistemleri için mütevazı düzeyde güvenilebilirlik yeterli olabilir

Kullanılabilirlik ve Güvenilebilirlik



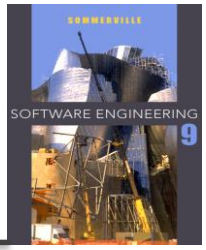
- Güvenilebilirlik
  - Belirli bir ortamda belirli bir amaç için belirli bir süre boyunca arızasız sistem çalışması olasılığı
- Kullanılabilirlik
  - Bir sistemin herhangi bir zamanda operasyonel olma ve talep edilen hizmetleri sunma olasılığı
- Bu özelliklerin her ikisi de nicel olarak ifade edilebilir, örneğin 0,999 kullanılabilirlik, sistemin %99,9 zaman çalışır durumda olduğu anlamına gelir.

Kullanılabilirlik ve Güvenilebilirlik



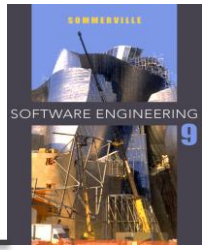
- Bazen sistem güvenilirliği kapsamında sistem kullanılabilirliğini hesaba katmak mümkündür
  - Açıkçası, bir sistem mevcut değilse, belirtilen sistem hizmetlerini sunmuyor demektir.
- Bununla birlikte, bulunması gereken düşük güvenilirliğe sahip sistemlere sahip olmak mümkündür.
  - Sistem arızaları hızlı bir şekilde onarılabildiği ve verilere zarar vermediği sürece, bazı sistem arızaları sorun olmayabilir.
- Bu nedenle kullanılabilirlik, sistemin hizmetlerini sunup sunamayacağını yansıtan ayrı bir özellik olarak en iyi şekilde değerlendirilir.
- Sistemin arızaları onarmak için hizmet dışı bırakılması gerekiyorsa, kullanılabilirlik onarım süresini hesaba katar.

Güvenilebilirlik Algıları



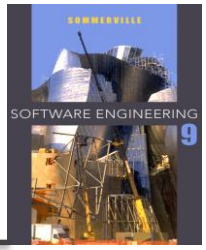
- Güvenilirliğin resmi tanımı, her zaman kullanıcının bir sistemin güvenilirliğine ilişkin algısını yansıtmaz.
  - Bir sistemin kullanılacağı ortam hakkında yapılan varsayımlar yanlış olabilir
    - Bir sistemin ofis ortamında kullanılması, aynı sistemin üniversite ortamında kullanımından oldukça farklı olabilir.
  - Sistem arızalarının sonuçları güvenilebilirlik algısını etkiler
    - Bir arabadaki güvenilmez ön cam silecekleri kuru bir iklimde önemsiz olabilir
    - Ciddi sonuçları olan arızalara (bir arabadaki motor arızası gibi) kullanıcılar tarafından rahatsız edici arızalardan daha fazla ağırlık verilir.

Güvenilebilirlik ve Özellikler



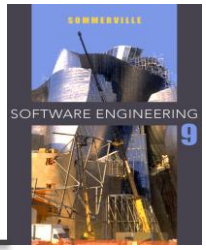
- Güvenilebilirlik, yalnızca bir sistem spesifikasyonuna göre resmi olarak tanımlanabilir, yani bir arıza, spesifikasyondan sapmadır.
- Bununla birlikte, birçok özellik eksik veya yanlıştır - bu nedenle, özelliğe uyan bir sistem, sistem kullanıcılarının bakış açısından 'başarısız olabilir'.
- Ayrıca, kullanıcılar spesifikasyonları okumazlar, bu nedenle sistemin nasıl davranması gerektiğini bilmiyorlar.
- Bu nedenle algılanan güvenilebilirlik uygulamada daha önemlidir.

Kullanılabilirlik Algısı

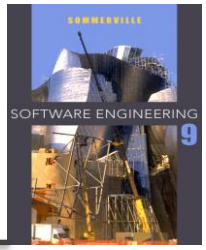


- Kullanılabilirlik genellikle sistemin hizmetleri sunmak için uygun olduğu sürenin yüzdesi olarak ifade edilir, örneğin %99,95.
- Ancak, bu iki faktörü hesaba katmaz:
  - Hizmet kesintisinden etkilenen kullanıcıların sayısı. Gecenin ortasında hizmet kaybı, çoğu sistem için en yoğun kullanım dönemlerinde hizmet kaybından daha az önemlidir.
  - Kesintinin uzunluğu. Kesinti ne kadar uzun olursa, aksama o kadar fazla olur. Birkaç kısa kesintinin, 1 uzun kesintiden daha az rahatsız edici olması olasıdır. Uzun onarım süreleri özel bir sorundur.

Bölüm 1'in Anahtar Noktaları



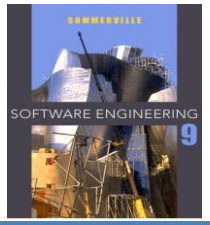
- Bir sistemdeki güvenilebilirlik, kullanıcının o sisteme olan güvenini yansıtır.
- Güvenilebilirlik, bir dizi ilgili "işlevsel olmayan" sistem özelliğini (kullanılabilirlik, güvenilebilirlik, emniyet ve güvenlik) tanımlamak için kullanılan bir terimdir.
- Bir sistemin kullanılabilirliği, talep edildiğinde hizmetlerin sunulması için mevcut olma olasılığıdır.
- Bir sistemin güvenilirliği, sistem hizmetlerinin belirtilen şekilde teslim edilme olasılığıdır.



Ders 11 - Güvenlik ve Güvenilebilirlik

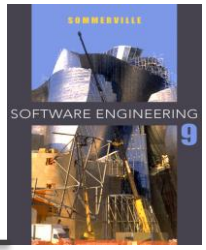
Bölüm 2

Güvenilebilirlik Terminolojisi



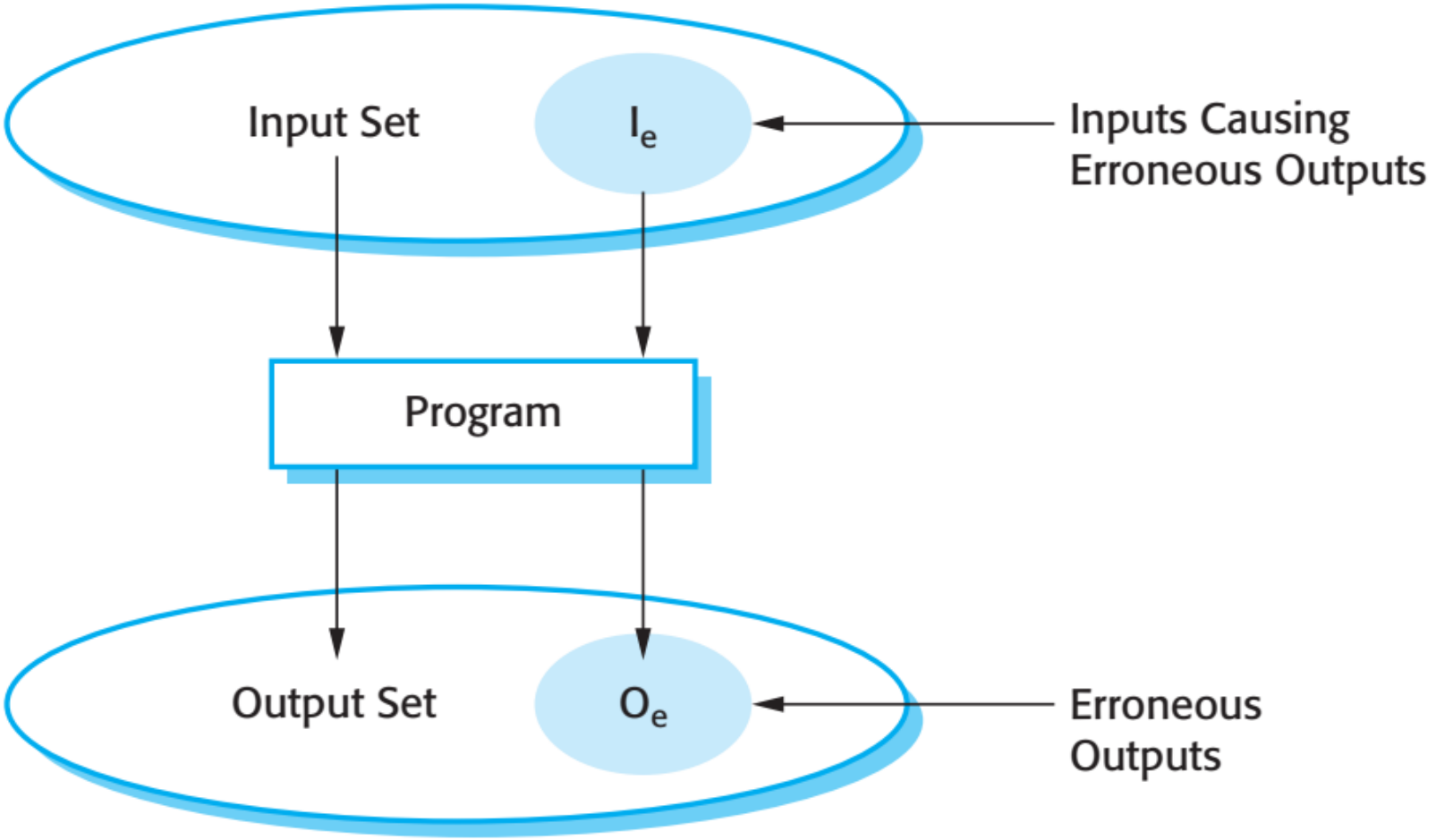
Terim	Açıklama
İnsan hatası veya hata	Hataların bir sisteme girmesiyle sonuçlanan insan davranışı. Örneğin, vahşi hava durumu sisteminde, bir programcı bir sonraki aktarım için zamanı hesaplamanın yolunun mevcut saate 1 saat eklemek olduğuna karar verebilir. Bu, iletim zamanının 23.00 ile gece yarısı arasında olduğu durumlar dışında çalışır (24 saatlik düzende gece yarısı 00.00'dır).
Sistem hatası	Sistem hatasına yol açabilen bir yazılım sisteminin özelliği. Arıza, kodun, saatin 23.00'den büyük veya buna eşit olup olmadığına bakılmaksızın, son iletim zamanına 1 saat eklenmesidir.
Sistem hatası	Sistem kullanıcıları tarafından beklenmeyen sistem davranışına yol açabilecek hatalı bir sistem durumu. Hatalı kod yürütüldüğünde iletim süresi değeri yanlış ayarlanmış (00.XX yerine 24.XX'e).
Sistem hatası	Sistemin, kullanıcılarının beklediği gibi bir hizmeti sunmadığı bir zamanda meydana gelen bir olay. Zaman geçersiz olduğu için hava durumu verisi gönderilmez.

Hatalar ve Arızalar

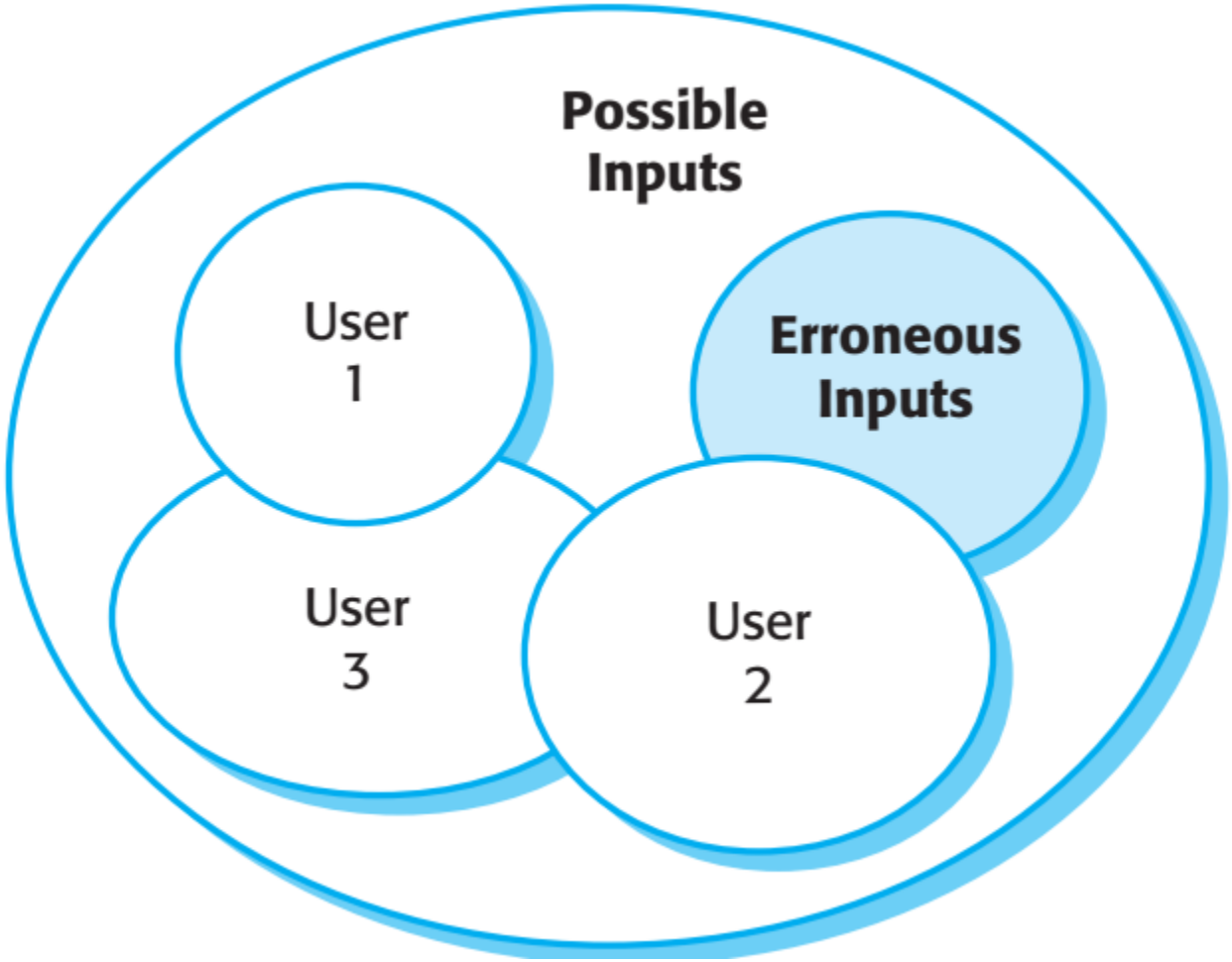


- Başarısızlıklar genellikle sistemdeki hatalardan kaynaklanan sistem hatalarının bir sonucudur.
- Bununla birlikte, hatalar mutlaka sistem hatalarına yol açmaz
  - Arızadan kaynaklanan hatalı sistem durumu geçici olabilir ve bir hata ortaya çıkmadan önce 'düzeltilebilir'.
  - Hatalı kod asla yürütülemez.
- Hatalar mutlaka sistem arızalarına yol açmaz
  - Hata, yerleşik hata algılama ve kurtarma ile düzeltilebilir
  - Arızaya karşı yerleşik koruma tesisleri ile korunabilir. Bunlar, örneğin, sistem kaynaklarını sistem hatalarından koruyabilir

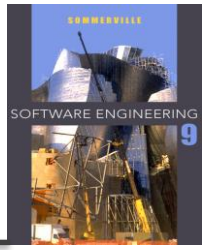
Giriş / Çıkış Eşlemesi Olarak Bir Sistem



Yazılım Kullanım Kalıpları

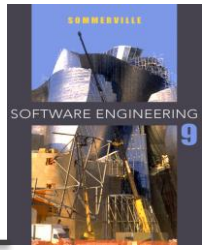


Kullanımda Güvenilebilirlik



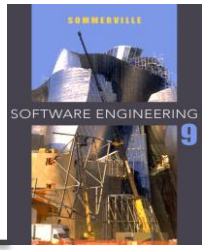
- Bir sistemdeki hataların %X'inin giderilmesi, güvenilirliği %X oranında artırmayacaktır. IBM'de yapılan bir araştırma, ürün kusurlarının %60'ının giderilmesinin güvenilebilirlikte %3'lük bir iyileşme sağladığını gösterdi.
- Program kusurları, kodun nadiren yürütülen bölümlerinde olabilir, bu nedenle kullanıcılar tarafından asla karşılaşılmayabilir. Bunların ortadan kaldırılması, algılanan güvenilirliği etkilemez.
- Kullanıcılar, kendileri için başarısız olabilecek sistem özelliklerinden kaçınmak için davranışlarını uyarlar.
- Bilinen hataları olan bir program, bu nedenle, kullanıcıları tarafından yine de güvenilir olarak algılanabilir.

Güvenilebilirlik Başarısı



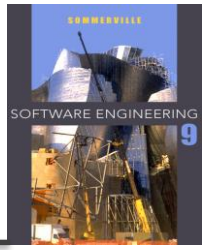
- Hata önleme
  - Sistem hatalarının ortaya çıkmasına neden olmadan önce hata olasılığını en aza indiren veya hataları tuzağa düşüren geliştirme teknikleri kullanılır.
- Arıza tespiti ve giderilmesi
  - Sistem hizmete girmeden önce hataları tespit etme ve düzeltme olasılığını artıran doğrulama ve doğrulama teknikleri kullanılmaktadır.
- Hata toleransı
  - Sistem kusurlarının sistem hatalarına neden olmamasını ve / veya sistem hatalarının sistem arızalarına yol açmamasını sağlamak için çalışma zamanı teknikleri kullanılır.

Emniyet



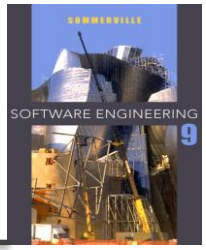
- Güvenlik, sistemin insan yaralanmasına veya ölümüne neden olma tehlikesi olmadan ve sistemin çevresine zarar vermeden normal veya anormal şekilde çalışma yeteneğini yansıtan bir sistem özelliğidir.
- Yazılım güvenliğini, arızası kritik öneme sahip çoğu cihaz artık yazılım tabanlı kontrol sistemlerini içerdiği için dikkate almak önemlidir.
- Güvenlik gereksinimleri genellikle özel gereksinimlerdir, yani gerekli sistem hizmetlerini belirtmek yerine istenmeyen durumları hariç tutarlar. Bunlar işlevsel güvenlik gereksinimleri oluşturur.

Güvenlik Kritikliği



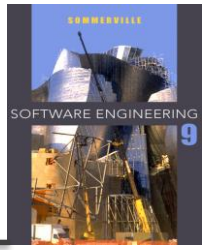
- Birincil güvenlik açısından kritik sistemler
  - Arızası, ilgili donanımın arızalanmasına neden olabilen ve insanları doğrudan tehdit edebilen gömülü yazılım sistemleri. Örnek, insülin pompası kontrol sistemidir.
- İkincil güvenlik açısından kritik sistemler
  - Arızası diğer (sosyo-teknik) sistemlerde arızalara neden olan ve daha sonra güvenlik sonuçları doğurabilecek sistemler. Örneğin, AK-HYS güvenlik açısından kritiktir çünkü başarısızlık, uygun olmayan tedavinin reçete edilmesine neden olabilir.

Güvenlik ve Güvenilebilirlik



- Güvenlik ve güvenilebilirlik birbiriyle ilişkilidir ancak farklıdır
  - Genel olarak, güvenilebilirlik ve kullanılabilirlik gereklidir ancak sistem güvenliği için yeterli koşullar değildir
- Güvenilebilirlik, belirli bir spesifikasyona uygunluk ve hizmet sunumu ile ilgilidir.
- Güvenlik, spesifikasyonuna uyup uymadığına bakılmaksızın sistemin hasara neden olmamasını sağlamakla ilgilidir.

Güvenli Olmayan Güvenilir Sistemler

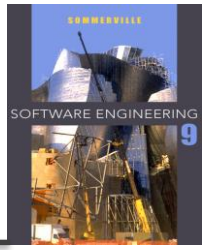


- Bir sistemde uzun yıllar tespit edilemeyen ve nadiren ortaya çıkan uykuda arızalar olabilir.
- Teknik özellik hataları
  - Sistem spesifikasyonu yanlışsa, sistem belirtildiği gibi davranabilir ancak yine de bir kazaya neden olabilir.
- Sahte girdiler oluşturan donanım arızaları
  - Spesifikasyonda tahmin etmek zor.
- Bağlama duyarlı komutlar, yani doğru komutu yanlış zamanda vermek
  - Genellikle operatör hatasının sonucudur.

Güvenlik Terminolojisi

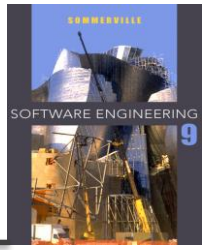
Terim	Tanım
Kaza (veya aksilik)	İnsan ölümü veya yaralanması, mülke veya çevreye zararla sonuçlanan planlanmamış bir olay veya olaylar dizisi. Aşırı dozda insülin, bir kaza örneğidir.
Tehlike	Bir kazaya neden olma veya katkıda bulunma potansiyeli olan bir durum. Kan şekerini ölçen sensör arızası, tehlikeye bir örnektir.
Hasar	Bir aksilikten kaynaklanan kaybın bir ölçüsü. Hasar, bir kaza sonucu birçok insanın ölmesinden küçük yaralanma veya mal hasarına kadar değişebilir. Aşırı dozda insülinden kaynaklanan hasar, ciddi yaralanma veya insülin pompası kullanıcısının ölümü olabilir.
Tehlike şiddeti	Belirli bir tehlikeden kaynaklanabilecek olası en kötü hasarın bir değerlendirmesi. Tehlike şiddeti, birçok insanın öldüğü felaketten, yalnızca küçük hasarların meydana geldiği hasarlara kadar değişebilir. Bireysel bir ölüm bir olasılık olduğunda, makul bir tehlike şiddeti değerlendirmesi 'çok yüksektir'.
Tehlike olasılığı	Bir tehlike oluşturan olayların gerçekleşme olasılığı. Olasılık değerleri keyfi olma eğilimindedir, ancak ' olası'dan (bir tehlikenin meydana gelme olasılığının 1 / 100'ü)' mantıksız'a (tehlikenin meydana gelebileceği akla gelebilecek hiçbir durum olası değildir) değişir . İnsülin pompasında aşırı dozla sonuçlanan bir sensör arızası olasılığı muhtemelen düşüktür.
Risk	Bu, sistemin bir kazaya neden olma olasılığının bir ölçüsüdür. Risk, tehlike olasılığı, tehlikenin ciddiyeti ve tehlikenin bir kazaya yol açma olasılığı dikkate alınarak değerlendirilir. İnsülin doz aşımı riski muhtemelen orta ila düşüktür.

Güvenlik Başarısı



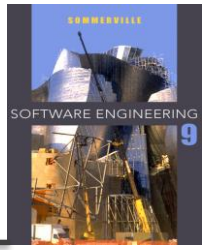
- Tehlikeden kaçınma
  - Sistem, bazı tehlike sınıflarının ortaya çıkamayacağı şekilde tasarlanmıştır.
- Tehlike tespiti ve giderilmesi
  - Sistem, bir kazayla sonuçlanmadan önce tehlikelerin tespit edilip ortadan kaldırılması için tasarlanmıştır.
- Hasar sınırlaması
  - Sistem, bir kazadan kaynaklanabilecek hasarı en aza indiren koruma özellikleri içerir.

Normal Kazalar



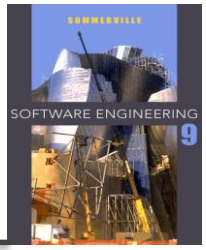
- Karmaşık sistemlerdeki kazaların nadiren tek bir nedeni vardır, çünkü bu sistemler tek bir arıza noktasına dayanıklı olacak şekilde tasarlanmıştır.
  - Tek bir arıza noktası kazaya neden olmayacak şekilde sistemleri tasarlamak, güvenli sistem tasarımının temel ilkesidir.
- Hemen hemen tüm kazalar, tek tek arızalardan ziyade arıza kombinasyonlarının bir sonucudur.
- Muhtemelen, özellikle yazılım kontrollü sistemlerde tüm problem kombinasyonlarını tahmin etmek imkansızdır, bu nedenle tam güvenliğe ulaşmak imkansızdır. Kazalar kaçınılmazdır.

Yazılım Güvenliği Avantajları



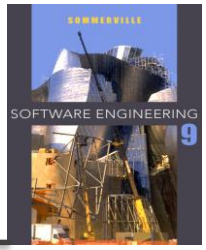
- Yazılım hataları güvenlik açısından kritik olabilse de, yazılım kontrol sistemlerinin kullanımı sistem güvenliğinin artmasına katkıda bulunur
  - Yazılım izleme ve kontrolü, elektromekanik güvenlik sistemleri kullanılarak mümkün olandan daha geniş bir koşul yelpazesinin izlenmesine ve kontrol edilmesine olanak tanır.
  - Yazılım kontrolü, insanların tehlikeli ortamlarda geçirdiği zamanı azaltan güvenlik stratejilerinin benimsenmesine olanak tanır.
  - Yazılım, güvenlik açısından kritik operatör hatalarını algılayabilir ve düzeltebilir.

Güvenlik



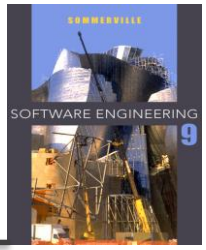
- Bir sistemin güvenliği, sistemin kendisini yanlışlıkla veya kasıtlı harici saldırılardan koruma yeteneğini yansıtan bir sistem özelliğidir.
- Çoğu sistem ağa bağlı olduğundan, sisteme İnternet üzerinden dışarıdan erişimin mümkün olması için güvenlik önemlidir.
- Güvenlik, kullanılabilirlik, güvenilebilirlik ve güvenlik için temel bir ön koşuldur.

Temel Güvenlik



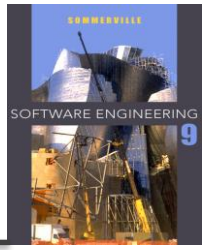
- Bir sistem ağ bağlantılı bir sistemse ve güvensizse, güvenilirliği ve güvenliği hakkındaki ifadeler güvenilmezdir.
- Bu ifadeler, yürütme sistemine ve geliştirilen sistemin aynı olmasına bağlıdır. Ancak, izinsiz giriş, yürütme sistemini ve / veya verilerini değiştirebilir.
- Bu nedenle, güvenilebilirlik ve güvenlik güvencesi artık geçerli değildir.

Güvenlik Terminolojisi



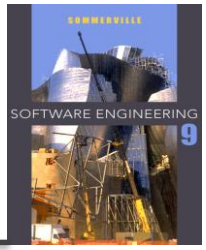
Terim	Tanım
Varlık	Korunması gereken değerli bir şey. Varlık, yazılım sisteminin kendisi veya bu sistem tarafından kullanılan veriler olabilir.
Maruziyet	Bir bilgi işlem sisteminde olası kayıp veya zarar. Bu, veri kaybı veya hasarı olabilir veya bir güvenlik ihlalinden sonra kurtarma gerekiyorsa zaman ve çaba kaybı olabilir.
Güvenlik Açığı	Kayba veya zarara neden olmak için suistimal edilebilen bilgisayar tabanlı bir sistemdeki zayıflık.
Saldırı	Bir sistemin güvenlik açığından yararlanma. Genellikle bu, sistemin dışındandır ve kasıtlı bir hasara neden olma girişimidir.
Tehditler	Kayba veya zarara neden olma potansiyeli olan durumlar. Bunları bir saldırıya maruz kalan bir sistem güvenlik açığı olarak düşünebilirsiniz.
Kontrol	Bir sistemin güvenlik açığını azaltan koruyucu bir önlem. Şifreleme, zayıf bir erişim kontrol sisteminin güvenlik açığını azaltan bir kontrol örneğidir.

Güvenlik Terminolojisi Örnekleri (AS-HYS)



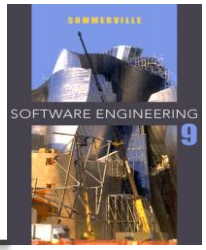
Terim	Misal
Varlık	Tedavi gören veya almış her hastanın kayıtları.
Maruziyet	Verilerini korumak için kliniğe güvenmedikleri için tedavi istemeyen gelecekteki hastaların potansiyel mali kaybı. Spor yıldızının yasal işleminden kaynaklanan mali kayıp. İtibar kaybı.
Güvenlik Açığı	Kullanıcıların tahmin edilebilir şifreler belirlemesini kolaylaştıran zayıf bir şifre sistemi. Adlarla aynı olan kullanıcı kimlikleri.
Saldırı	Yetkili bir kullanıcının kimliğine bürünme.
Tehdit	Yetkisiz bir kullanıcı, yetkili bir kullanıcının kimlik bilgilerini (oturum açma adı ve şifresi) tahmin ederek sisteme erişecektir.
Kontrol	Normalde bir sözlüğe dahil edilen doğru adlar veya sözcükler olan kullanıcı parolalarına izin vermeyen bir parola kontrol sistemi.

Tehdit Sınıfları



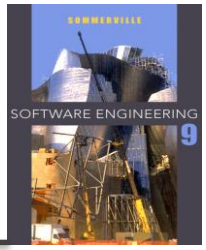
- Sistemin ve verilerinin gizliliğine yönelik tehditler
  - Bu bilgilere erişim yetkisi olmayan kişilere veya programlara bilgileri ifşa edebilir.
- Sistemin ve verilerinin bütünlüğüne yönelik tehditler
  - Yazılıma veya verilere zarar verebilir veya bozabilir.
- Sistemin ve verilerinin kullanılabilirliğine yönelik tehditler
  - Yetkili kullanıcılar için sisteme ve verilere erişimi kısıtlayabilir.

Güvensizlikten Kaynaklanan Hasar



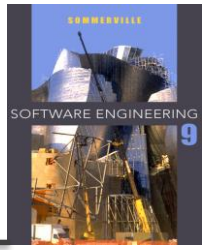
- Hizmet reddi
  - Sistem, normal hizmetlerin kullanılamadığı veya hizmet sunumunun önemli ölçüde azaldığı bir duruma zorlanır.
- Programların veya verilerin bozulması
  - Sistemdeki programlar veya veriler yetkisiz bir şekilde değiştirilebilir.
- Gizli bilgilerin ifşa edilmesi
  - Sistem tarafından yönetilen bilgiler, bu bilgileri okuma veya kullanma yetkisi olmayan kişilere maruz kalabilir.

Güvenlik Güvencesi



- Güvenlik açığından kaçınma
  - Sistem, güvenlik açıkları oluşmayacak şekilde tasarlanmıştır. Örneğin, harici ağ bağlantısı yoksa harici saldırı imkansızdır.
- Saldırı tespiti ve yok etme
  - Sistem, güvenlik açıklarına yönelik saldırılar açığa çıkmadan önce tespit edilecek ve etkisiz hale getirilecek şekilde tasarlanmıştır. Örneğin, virüs denetleyicileri, bir sisteme bulaşmadan önce virüsleri bulur ve temizler.
- Maruz kalma sınırlaması ve kurtarma
  - Sistem, başarılı bir saldırının olumsuz sonuçlarını en aza indirecek şekilde tasarlanmıştır. Örneğin, bir yedekleme politikası, hasarlı bilgilerin geri yüklenmesine izin verir

Bölüm 2'nin Anahtar Noktaları



- Güvenilebilirlik, operasyonel kullanımda meydana gelen bir hata olasılığı ile ilgilidir. Hatalı olduğu bilinen bir sistem güvenilir olabilir.
- Güvenlik, sistemin insanları veya çevreyi tehdit etmeden çalışma yeteneğini yansıtan bir sistem özelliğidir.
- Güvenlik, sistemin kendisini dış saldırılardan koruma yeteneğini yansıtan bir sistem özelliğidir.
- Bir sistem güvenli değilse, kod veya veriler bozulabileceği için güvenilebilirlik tehlikeye girer.