

# **Güvenlik Mühendisliği (Security Engineering)**

Yrd. Doç. Dr. Özgü Can

# Güvenlik Mühendisliği

- Kötü niyetlere, hatalara ya da aksiliklere karşı güvenilir bir şekilde kalacak sistemler kurmaktır.
- Bir disiplin olarak;
  - Araçların, süreçlerin ve yöntemlerin tasarlanması, gerçekleştirimi ve sistemlerin test edilmesi
  - Mevcut sistemlerin uyarlanması

# Güvenlik Mühendisliği

- Çapraz disiplinli çalışma yaklaşımını gerektirir.
  - Kriptografi – Bilgisayar Güvenliği
  - Hardware tamper-resistance \*
  - Formal metodlar
  - Ekonomi
  - Uygulamalı Psikoloji
  - Hukuk

\* <http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/what-is-tamper-resistant-hardware.htm>

# Güvenlik Mühendisliği

- Sistem Mühendisliği
- İş Süreç Analizi
- Yazılım Mühendisliği

Değerlendirme ve  
teste odaklanır.



Kötü niyetli  
erişimler yerine  
hatalarla  
ilgilenmektedir.

# Güvenlik Mühendisliği

- Güvenlik sistemleri kritik güvence ihtiyaçları ile ilgilenmektedir.
- Başarısızlıkları;
  - İnsan hayatı ve çevreyi tehlikeye sokma
    - Nükleer kontrol sistemleri
  - Ekonomik altyapıya zarar verme
    - Bankacılık sistemleri
  - Kişisel gizliliği tehlikeye sokma
    - Sağlık sistemleri
  - İş sektörlerinin uygulanabilirliğini bozma
    - Öde-izle TV sistemleri
  - Suçu kolaylaştırma
    - Hırsızlık

# Güvenlik Mühendisliği

- Yazılım Mühendisliği → Olayların gerçekleşmesi
  - *John dosyayı okuyabilir.*
- Güvenlik → Olayların gerçekleşmeyeceğinin garanti edilmesi
  - *John dosyayı okuyamaz.*
- Güvenlik ihtiyaçları sistemden sisteme farklılık gösterebilir.

# Güvenlik Mühendisliği

- Sistemlerin başarısız olma nedenleri:
  - Tasarımcıların yanlış nesneleri koruması
  - Doğru nesneleri yanlış şekilde koruması
- Bu nedenle çözülmesi gerekenler:
  - **Neyin** korunmaya ihtiyacı var?
  - **Nasıl** korunması gerek?
  - Sistemi **kimler** koruyacak ve bakımını yapacak?

# Güvenlik Mühendisliği

- İyi bir güvenlik mühendisliği için:

Gerçekleştirilmesi  
gerektenler

Politika ↔ Teşvik

Sistemi koruyan ve bakımını  
yapanların işlerini düzgün  
bir biçimde  
gerçekleştirmeleri

Düzenek ↔ Güvence

Politikaların  
gerçekleştirimini  
sağlayacak araçlar  
ÖR: erişim denetim,  
hardware tamper-  
resistance cihazlar

Her bir güvenlik  
düzenegine  
atanacak güvenin  
miktarı



# Güvenlik Mühendisliği

Havaalanı güvenliğınden bıçak ile geçmek



Düzenek değil politika hatasıdır.



**Bir çok yer personelinin kontrolden geçmemesi  
Park halindeki uçakların güvenliğıinin sağlanmaması**

# Güvenlik Mühendisliği

Etkili kontroller yerine  
görünür kontrollerin tercih edilmesi



Güvenlik politikalarının zayıf olmasına neden olmaktadır.



[Bruce Schneier] Güvenlik Tiyatrosu - Security Theatre

Güvenlik hissi vermesi için geliştirilmiş ölçütler

# Güvenlik Mühendisliği

## Anlaşılması Gerekenler

- Riskleri ve tehditleri belirtmeli
- Neyin yanlış gidebileceği konusunda değerlendirmeler yapmalı
- Yararlı tavsiyeler vermeli

## Bağlantılı Konular

- Çeşitli sistemlerde nelerin yanlış gittiği
- Hangi saldırıların başarıya ulaştığı
- Saldırıların sonuçlarının ne olduğu
- Saldırıların nasıl durdurulduğu

# **Güvenlik Kritik Sistemler**

# Örnek 1 – Bankacılık Sistemleri

- Muhasebecilik → Temel bankacılık işlemi
- En önemli tehdit → Banka Çalışanları
  - Şüpheli işlemleri takip eden alarm sistemleri
  - Personelin banka sistemine erişemeyeceği düzenli izinler
- ATM (**A**utomatic **T**eller **M**achine)
  - Kriptografinin ilk ticari kullanımı (~1970)
  - *Hırsızlar ATM servislerinin ağ hatlarını gözleyip, banka işlemlerini temsil eden şifreli mesajları analiz ediyorlar mı?*

# Örnek 1 – Bankacılık Sistemleri

- Banka web sayfaları
  - Online işlemler
  - Phishing saldırıları
- Güvenlik tiyatrosu → Müşterilere birikimlerinin güvende olduğunu belirten psikolojik mesaj verilmesi.
  - Kriptografi

# Örnek 2 – Askeri Sistemler

- Düşman radar sinyalleri ele geçirilmek istenirken, kendi sinyallerinin güvenliğinin sağlanması.
  - Taklit etme (Spoofing)
  - Servis reddi (Denial of service)
- Hassas bilgi kısıtlandırılmış sınıfa doğru ilerlemez.
  - **Top Secret** bir dosyada **Secret** bir bilgi olabilir. **Tersi geçerli değildir.**
  - Bilgiler hedeften istihbarat analizcisine doğru giderken, hedefin hangi iletişimlerinin tutulduğundan (intercept) haberi olmaması gerekmektedir.

# Örnek 3 – Sağlık Bilgi Sistemi

- Temel problem → Hasta güvenliği ve gizliliği
- Değişen rollere göre güvenlik düzenineğin uyarlanması zordur.
  - Hemşirelerin klinikler arasında yer değiştirmesi.
- Verinin anonimleştirilmesi
  - Sadece hasta isimlerinin şifrlenmesi yeterli değildir.
- Web tabanlı teknolojilerden kaynaklı problemler
  - Doktorların hasta kayıtlarına her yerden erişebilmesi kimlik denetimi (authentication) ve şifreleme araçlarına ihtiyaç duyulmasını gerektirmektedir.



# Örnek 3 – Sağlık Bilgi Sistemi

- Yeni teknolojilerin getirdiği riskler

Radyoloji sonuçlarının doktorlara sadece ağ üzerinden iletilmesi



**Servisin  
Reddi (DoS)  
Saldırısı**



© MAZK ANDERSON

WWW.ANDERSTOONS.COM



"I'd like a second opinion."

# Örnek 4 – Ev & Aile

- Web tabanlı elektronik bankacılık sistemlerinin kullanılması
- Telefon kartlarının klonlanması
  - GSM firmalarının kimlik denetimi için kriptografik protokoller kullanması
- İzle-Öde TV sistemlerinde kimlik denetimi protokolleri

# Tanımlar

- **Sistem**

- Bir ürün ya da bileşen
  - Kriptografik protokol, akıllı kart ya da donanımsal bir parça
- İşletim sistemi
- Uygulamalar
  - Office, browser, vs..
- IT elemanları
- Kullanıcılar
- Müşteriler

# Tanımlar

- **Güven (Trust)**

- Başarısızlığı durumunda güvenlik politikasını bozan bir sistem ya da bileşen.

- **Güvenilir (Trustworthy)**

- Başarısızlığa uğramayacak bir sistem ya da bileşen.

**Önemli bir bilgiyi satarken gözlemlenen  
bir çalışan**

***Trusted but not trustworthy***

# Tanımlar

- **Secrecy**

- Bilgiye erişecek olanları kısıtlayan düzenek
  - Kriptografi, erişim denetim kontrolleri

- **Confidentiality**

- Kişinin ya da kurumun (sizin bildiğiniz) sırlarını koruma zorunluluğu

- **Privacy**

- Kişisel bilginizi koruma hakkı
- Kurum gibi tüzel kişileri kapsamaz.

# Privacy & Confidentiality

Hastanenin hastanın gizliliğini koruması

Privacy

Kişinin yararına

Hastane personelinin hastaya karşı hasta gizliliğini koruması görevi

Confidentiality

Kurumun yararına

# Tanımlar

- Verinin kendisini korumak yeterli olmayabilir, üst-verinin (metadata) de korunması gerekir.
  - Mesajın sadece içeriğini değil, kimlerle iletişim kurulduğunu belirten günlüklerin de (logs) güvenliği sağlanmalıdır.
  - Kişinin AIDS olduğunun gizli tutulması
    - Gerçekleştirilen iletişimlerden kişinin AIDS olduğu sonucunun çıkarılması

# Tanımlar

Mesaj içeriğinin gizliliği



**Secrecy**

Mesaj kaynağının/hedefinin gizliliği



**Anonimleştirme (Anonymity)**