# Kimlik Denetleme (Authentication)

Yrd. Doç. Dr. Özgü Can

# Kimlik Denetleme

- Her özne bir başka dış varlık (external entity) adına hareket eder.
- Bu varlığın kimliği, öznenin gerçekleştirebileceği eylemleri kontrol eder.
- Bu nedenle, özneler bu dış varlığın kimliği ile bağlanmalıdır.

# Kimlik Denetleme

*Kimlik denetleme (authentication),*
*bir kimliğin bir özne ile bağlanmasıdır.*

# Kimlik Denetleme

- Dış varlık, sisteme kimliğini onaylatması için bilgi sağlamalıdır.
- Bu bilgi aşağıdakilerden biri olabilir:
  1. Varlığın **ne bildiği** (parola ya da gizli bir bilgi)
  2. Varlığın **neye sahip olduğu** (kimlik kartı vs..)
  3. Varlığın **ne olduğu** (parmak izi ya da retina özellikleri)
  4. Varlığın **nerede olduğu** (belirli bir terminalin başında vs..)

# Kimlik Denetleme

- Kimlik denetleme işlemi:
  - Varlıktan kimlik denetleme bilgisinin sağlanması
  - Verinin analiz edilmesi
  - Varlık ile ilişkili olup olmadığının belirlenmesinden

  oluşur.
- Bu nedenle;
  - Bilgisayar, varlık ile ilgili bazı bilgileri sağlamalıdır.
  - Verinin yönetimi ile ilgili düzeneklere ihtiyaç vardır.

# Kimlik Denetleme

- Kimlik denetleme sistemindeki ihtiyaçlar **beş bileşen** ile ifade edilmektedir:

1. ***Kimlik denetleme bilgisi kümesi***, ***A***, varlıkların kimliklerini kanıtladıkları belirli bir bilgi kümesidir.

# Kimlik Denetleme

2. ***Tümleyen (complementary) bilgisi kümesi***, ***C***, sistemin kimlik denetleme bilgisinin geçerliliğini denetlemek için sakladığı ve kullandığı bilgi kümesidir.

# Kimlik Denetleme

3. ***Tümleme fonksiyonları kümesi***, ***F***, kimlik denetleme bilgisinden tümleme bilgisini oluşturur.

$f \in F$, **f: A → C**

# Kimlik Denetleme

***4. Kimlik denetleme fonksiyonları kümesi***, ***L***, kimliği doğrular.

$l \in L$, **l: A x C → {true, false}**

# Kimlik Denetleme

5. ***Seçim (selection) fonksiyonları kümesi***, ***S***, bir varlığı kimlik denetimi ve tümleyen bilgisini yaratması ya da değiştirmesi için etkin (enable) kılar.

# Parola (Password)

- Parolalar, varlığın ne bildiğini temel alan kimlik denetleme düzeneğine bir örnektir.
- Kullanıcı bir parola sağlar ve bilgisayar bu parolanın geçerliliğini denetler.
- Parola kullanıcı ile ilişkili ise;
  - Kullanıcının kimliği yetkilendirilir.
  - Aksi takdirde, parola reddedilir ve kimlik yetkilendirme başarısız olur.

# Parola (Password)

*Parola,*
*varlığın kimliğini onaylayan,*
*varlık ile ilişkili bir bilgidir.*

# Parola (Password)

- Karakterler dizisinden oluşur.
- **Parola uzayı** → Parola olabilecek bütün karakter dizileri kümesidir.
  - ÖR:

    Sistem kullanıcının **10 haneli** bir parola seçmesini gerektiriyorsa

    

    Kimlik denetleme bilgisi kümesi ***A*** (0000000000'dan 9999999999'a kadar) $10^{10}$ dur.

# Parola (Password)

- Kimlik denetleme sisteminin amacı;
  - **Varlıkların kimliklerinin** doğru bir şekilde belirlendiğini garantilemektir.

- Eğer bir varlık diğer bir varlığın parolasını tahmin ederse → Onun yerine hareket ederek onu taklit edebilir.

# Parola (Password)

- Kimlik denetleme modeli bu problemi analiz etmek için sistematik bir yol izler.

- Amaç;
  - Bir $a \in A$ bularak, $f \in F$ için **$f(a)=c \in C$**

  *c herhangi ya da belirli bir varlık ile ilişkilidir.*

# Parola (Password)

- **a**'nın herhangi bir varlık ile ilişkili olup olmadığı
  - Sadece **f(a)** hesaplanarak

  ya da

  - **l(a)** ile kimlik denetlemesi yapılarak

  belirlenebilir.

# Parola (Password)

- Parolaların korunması için aynı anda kullanılan iki yaklaşım:

  1. **Yeterli bilgiyi saklayarak; *a*, *c* ya da *f*'nin bulunmasını önlemek.**

  ÖR: UNIX sistemlerinde tümleme bilgisini içeren dosyalar sadece *root* tarafından okunabilir.

  *Shadow* parola dosyalarını kullanan bu yöntem *C* kümesini gizler → *f(a)* bilgisinin kullanıcı ile ilişkilendirilmesi için yeterli bilgi yoktur.

# Parola (Password)

- Parolaların korunması için aynı anda kullanılan iki yaklaşım:

  **2. *L* kimlik denetleme fonksiyonlarına erişim önlenmelidir.**

  ÖR: *Root*'un ağ üzerinden sisteme bağlanmasına izin vermeyen site.

# Parola Sistemine Saldırı

- En basit saldırı → **Parola tahmini**

***Sözlük saldırısı*** *(dictionary attack), tekrarlanan hata ve deneme ile parolanın tahmin edilmesi saldırısıdır.*

Tahmin için kullanılan kelimeler listesi

**“Sözlük” saldırısı**

# Parola Sistemine Saldırı

## Sözlük Saldırısı Tip-1

- Eğer **tümleme bilgisi** ve **fonksiyonu** biliniyorsa, sözlük saldırısı;
  - Her bir tahmin, *g*, ve $f \in F$ için **f(g)**'yi hesaplar.
  - Eğer *f(g)*, *E* varlığı için tümleme bilgisine karşılık geliyorsa, *g f* fonksiyonu için *E*'nin kimliğini doğrular.

# Parola Sistemine Saldırı

## Sözlük Saldırısı Tip-2

- Eğer tümleme bilgisi ya da fonksiyonu bilinmiyorsa, $l \in L$ kimlik denetleme fonksiyonları kullanılabilir.
  - Tahmin, $g$, $l$ içerisinde yer alıyorsa $g$ doğru paroladır.

# Parola Sistemine Saldırı

**ÖR:**

- **Tip 1** → UNIX sistem parola dosyasına sahip olan saldırgan bilinen tümleme fonksiyonunu kullanarak tahminlerini test eder.
- **Tip 2** → Saldırgan parola dosyasına erişmek için bilinen bir hesap ismi ile tahmini parolalar kullanarak sisteme girmeye çalışır.

# Parola Tahmini

- Parola tahmini;
  - tümleme fonksiyonuna

  ya da

  - tümleme bilgisine

  ya da

  - kimlik denetleme fonksiyonuna erişime

  ihtiyaç duyar.

# Parola Tahmini

- Amaç;
  - Parola tahmini için gerekli zamanı **max.**'a çıkarmaktır.

# Parola Tahmini

## Anderson's Formula

- **P:** Saldırganın belirli bir zaman içerisinde parolayı tahmin etmesi olasılığı
- **G:** Bir zaman biriminde test edilecek tahmin sayısı
- **T:** Tahminin meydana geleceği toplam zaman birimi
- **N:** Mümkün parola sayısı

$$P \geq \frac{TG}{N}$$

# Parola Seçimi

- İnsan faktörü önemlidir.

- Psikolojik çalışmalar, insanların **8 anlamlı karakteri** doğru bir şekilde hatırladıklarını göstermektedir.

  – Kişinin, iki 8 karakterli rastgele parolayı hatırlaması için not etmesi gereklidir.

# Parola Seçimi

- Yazılı parolaların savunmasızlığı → Nerede saklandığı ile ilgilidir.

- Kolay ulaşılabilecek bir yerde ise güvenliği tehdit eder.

# Parola Seçimi

- Michele Crabb'in yazılı parolaların anlaşılabilirliğini güçleştirmek için geliştirdiği metot:
  - **X:** Karakterler kümesi
  - **t:** Dönüşüm algoritması, **t: X → A**
- X'in elemanları kağıt parçalarına yazılır.
- Parola olarak kullanılmadan önce *t* kullanılarak dönüşüm gerçekleştirilir.
  - *t* basit ve hatırlanabilir olmalıdır.
  - Periyodik olarak değiştirilmelidir.

# Parola Seçimi

ÖR:

- *t:* Kelimenin 3. harfini büyültülerek sonuna 2 eklenmesi
- *X:* bilmuh4
- *Parola:* biLmuh42

# Parola Seçimi

- Farklı sistemlere erişen sistem yöneticilerinin farklı parolaları hatırlamalarını kolaylaştırır.

- Kağıt kaybolsa bile sistem tehlikede olmayacaktır.

# Parola Seçimi

- **Telaffuz edilebilir kelimelerin kullanımı**
  - *tumircop*
  - *zonester*
- **Rastgele türetilmiş kelimeler:**
  - *yzbwscvk*
  - *obnfwsoa*
- Telaffuz edilebilir kelimelerin tahmin edilme zamanı, rastgele türetilmiş kelimelerin tahmin edilme zamanından **daha az**dır.

# Proaktif Parola Seçimi

- Kullanıcılara hatırlayabilecekleri parola seçme imkanı verir.
- Ancak, tahmin edilmesi kolay parolaların kullanımını reddeder.
- Tahmin edilmesi kolay parolalar, **tecrübelerden** ve **geçmiş çalışmalardan** elde edilmektedir.

# Tahmin Edilmesi Kolay Parolalar

- **Hesap adı ile aynı olan parolalar**
  - Hesap adının sonuna sayı eklenmesi
- **Kullanıcının adına dayanan parolalar**
  - İsmin tersten yazılması
  - Harflerin büyütülmesi
  - İsmin ilk harfinin soyadı ile birleştirilmesi
- **Bilgisayar isminin parola olarak kullanılması**

# Tahmin Edilmesi Kolay Parolalar

- Sözlük kelimeleri
  - Sözlük kelimelerinin tersten yazımı
  - Sözlük kelimelerinin birleştirimi
- Klavye örüntüleri (patterns)
- 6 karakterden kısa parolalar
- Araba plakaları
- Geçmişte kullanılan parolalar
- Kısaltmalar
  - USA, NASA, IEEE, vb..

# Güçlü Parola

- Güçlü bir parolada **en az**:
  - Bir rakam
  - Bir harf
  - Bir noktalama işareti
  - Bir kontrol karakteri

# Güçlü Parola

- **2. Yöntem:** *Bilinen bir şiirin bir mısrasından parola oluşturma*

ÖR: *Yahya Kemal Beyatlı*

**Âheste çek kürekleri, mehtâb uyanmasın,**

**Bir âlemi hayâle dalan âb uyanmasın.**

- *Beş harften fazla olan kelimelerin 3.harfini alıp, şairin ismi ile / kullanarak birleştirme*
  - **Erhaeyla/YKB.**

# Proaktif Parola Ölçütleri

Proaktif parola çeşitli ölçütleri sağlamalıdır:

1. Kullanıcıya **hatırlatma** yapılmalıdır, aksi takdirde kullanıcı proaktif düzeneği atlayabilir.
2. **Kolay tahmin edilen** parolalar reddedilmelidir.
3. **Kullanıcı tabanlı** bir ayrım yapılmalıdır.
   - "^AKemalD." geçerli bir parola olabilir ama kişinin "*Kemal Dinçer*" isminde bir oğlu varsa uygun değildir.

# Proaktif Parola Ölçütleri

4. **Site tabanlı** bir ayrım yapmalıdır.
   - Ege Üniversitesi Bilgisayar Mühendisliği sitesi için "EU^bil_muh." geçerli bir parola olmasına rağmen uygun değildir.
5. **Örüntü-uyumunu** sağlamalıdır.
   - "aaaaa" sözlükte olmamasına rağmen kolay tahmin edilebilir bir paroladır.
   - Basit örüntülerin tespit edilmesi gerekir.

# Proaktif Parola Ölçütleri

6. **Alt programlar** çalıştırarak parolaları kabul ya da reddetmelidir. Program, sözlükte olmayan yazımlar ile ilgilenmelidir.

ÖR: "kalem" kelimesi sözlükte yer almakta, ancak çoğulu olan "kalemler" kelimesi çoğunlukla sözlüklerde bulunmamaktadır.

- Yazım denetleyici "kalemler" kelimesini farketmelidir.

# Proaktif Parola Ölçütleri

7. **Testlerin kurulumu** kolay olmalıdır.

   Böylece, sistem yöneticilerinin yanlışlıkla kolay tahmin edilen parolalara izin vermesi önlenmelidir.

# Kimlik Denetleme Fonksiyonları ile Tahminleme

- Tümleme ve tümleme fonksiyonları bilinmiyorsa, saldırganlar parola tahmini için **kimlik denetleme** fonksiyonlarını kullanmaktadır.

- Sistemin yasal kullanıcılar için erişilebilir olması gerekmektedir. → Bu saldırı **önlenemez**.
  - Parola bilgisi ile yetkilendirilmiş ve yetkilendirilmemiş kullanıcı ayrımı yapılamaz.

# Kimlik Denetleme Fonksiyonları ile Tahminleme

- Bu saldırıya karşı savunmada 4 teknik kullanılmaktadır:

1. Geri çekilme (Backoff)
2. Bağlantının kesilmesini gerektirme (Involve Disconnection)
3. Hizmet dışı bırakma (Disabling)
4. Hapsetme (Jailing)

# Geri Çekilme

- Kullanıcı kimlik denetlemede başarısız olursa;
  - Sistem yöneticisi tarafından bir ***x*** parametresi belirlenir.
  - Sistem isim ve kimlik denetlemeyi görüntülemeden önce $x^0=1$ ***sn.*** bekler. Kullanıcı tekrar başarısız olursa:
    - $x^1=x$ ***sn.*** bekler.
  - ***n*** başarısızlıktan sonra sistem $x^{1n}$ ***sn.*** bekler.

# Bağlantının Kesilmesini Gerektirme

- Birkaç başarısız kimlik denetleme girişimlerinden sonra bağlantı kesilir.

- Kullanıcı tekrar bağlantı kurmalıdır.

- Tekrar bağlantı için belirli bir sürenin geçmesi gerekmektedir.

# Hizmet Dışı Bırakma

- ***n*** başarısız girişimden sonra, güvenlik yöneticisi hesabı etkisiz kılar.

# Hapsetme

- Kimlik denetimi başarısız olan kullanıcıya, **sistemin kısıtlı bir kısmını** kullanma izni verilir.
- Kullanıcının tam erişim hakkı olduğuna inanması sağlanır.
- Kullanıcının eylemleri kaydedilir.
- Amaç;
  1. Saldırganın **ne istediği** anlaşılmaya çalışılır.
  2. Saldırgana **zaman** kaybettirilir.

# Hapsetme

- Hapsetme yöntemlerinden biri → **Honeypot**
- Çalışan sisteme sahte veri eklenir.
- Sisteme giren saldırgan bu sahte veriyi alacaktır.
- Saldırganın sahte veriyi ele geçirme süresi, **saldırganın izinin** telefon hatları üzerinden **bulunması** için yeterli bir süredir.

# Parolanın Eskimesi

- Parolanın tahmin edilmesi için:
  - **Tümleme**
  - **Tümleme Fonksiyonu**
  - **Kimlik Denetleme Fonksiyonu**

  elde edilmelidir.
- Bunların hiç biri elde edilemezse, zamanla parola tahmin edilir.
  - Saldırgan sisteme erişir.

# Parolanın Eskimesi

*Parola eskimesi,*

*belirli bir zaman geçtikten sonra*

*ya da*

*belirli bir olay meydana geldikten sonra parolanın değiştirilmesi ihtiyacıdır.*

# Parolanın Eskimesi

ÖR:

- Bir parolanın tahmin edilme süresi 180 gün ise:
  - 180 günde bir parola değişimi → Saldırgan tarafından **parolanın tahmin edilmesi olasılığını** düşürecektir.

# Parolanın Eskimesi

- Pratikte;
  - Parola tahmin süresi **ortalama** düzeydedir.
    - Kolay tahmin edilen ve zor tahmin edilen parolalar arasında ki tahmin süresini dengeler.
    - Kullanıcı kolay bir parola seçmiş ise **tahmin süresi azalacaktır**.

# Parolanın Eskimesi

- Parola eskimesi uygulamasında karşılaşılan problemler:

1. Kullanıcıyı **farklı** bir parola seçmeye zorlamak.

2. Parola **değişim ihtiyacını** belirtmek ve parola değişiminde **kullanıcı dostu** bir metot sağlamak.

# Parolanın Eskimesi

- Çözüm:
  - Kullanıcının aynı parolayı girmesini önlemek
    - Yeni parola önceki ***n*** parola ile karşılaştırılır.
    - Aynı ise değişim reddedilir.
  - Problem:
    - Kullanıcı hızlı bir şekilde parolasını ***n*** kez değiştirir ve tekrar aynı parolaya geri döner.

# Parolanın Eskimesi

- Parolanın hızlı bir şekilde döndürülmesini engellemek için:
  - Parola değişimine izin vermek için **min.** zaman kısıtlaması getirmek.

# Parolanın Eskimesi

- Gramp ve Morris tarafından yapılan çalışmada;
  - **En kolay tahmin edilen parolaların**, kullanıcılarına **parola süresinin bitmesine yaklaştığını** haber vermeyen sistemlerde olduğu belirtilmektedir.

# Kimlik Sorma/Yanıt Verme Yöntemi

## Challenge-Response

- Parolaların temel problemi → **Yeniden kullanılabilir olması**
  - Saldırgan parolayı ele geçirdiğinde;
    - Sisteme bağlanır.
    - Sistem yetkili ve yetkisiz kullanıcı arasındaki ayrımı yapamaz.

# Kimlik Sorma/Yanıt Verme Yöntemi

## Challenge-Response

- Saldırgan bir önceki işlemde kullanılan parolayı kullandığında;
  - Sistem erişimi reddedecektir.

# Kimlik Sorma/Yanıt Verme Yöntemi

- **U** : Kullanıcı & **S** : Sistem
- **U** ve **S** gizli bir ***f*** fonksiyonu üzerine anlaşmaktadır.
- **S**, **U**'ya rastgele bir ***m*** (**challenge**) mesajı gönderir.
- **U**, bu mesaja ***r = f(m)*** ile cevap verir. (***r*** = **response**)
- **S**, ***r***'yi hesaplar ve geçerliliğini denetler.

# Pass Algoritmaları

- Kimlik Sorma/Yanıt Verme sisteminde $f$ gizli fonksiyonu ***pass algoritması*** olarak adlandırılır.

- $f$ fonksiyonuna, herhangi bir kriptografik anahtar ya da gizli bir bilgi girdi olamaz.

# Pass Algoritmaları

ÖR:

- Girdi = abcdefg
  - Cevap= bdf
- Girdi = ageksido
  - Cevap = gkio

*Fonksiyon= Harfi takip eden harf*

# Tek-Seferli Parola

**One-Time Password**

- Kimlik Sorma/Yanıt Verme düzeneği **tek-seferli** parola metodunu kullanmaktadır.
  - Cevap (parola) *her seferinde* farklıdır.

# Tek-Seferli Parola

*Tek-seferli parola,*
*kullanılır kullanılmaz*
*geçersiz olan paroladır.*

# Biyometri (Biometrics)

- Kişinin **biyolojik** ya da **davranışsal özelliklerinin** otomatik olarak ölçülmesidir.
- Kullanıcıya bir hesap açıldığında, sistem yöneticisi kullanıcıyı belirten ölçümleri alır.
- Kullanıcı sisteme bağlandığında, biyometri kimlik denetleme düzeneği kullanıcının kimliğini doğrular.

# Biyometri (Biometrics)

- Lawton;
  - Herhangi bir **arama işlemi** gerçekleştirilmediği için, biyometri kimlik denetleme düzeneğinin **daha kolay** olduğunu

  belirtir.

# Biyometri (Biometrics)

- Parmak izi (Fingerprints)
- Ses (Voice)
- Göz (Eye)
  - İris ve retina taraması
- Yüz (Face)
- Kombinasyon