MUH441 Bilişimde Güvenlik – 1

Prof. Dr. Hasan Hüseyin BALIK

(3. Hafta)

İçerik

- 2. Bilişim Güvenliği Teknolojisi ve İlkeleri
  - 2.1.Şifreleme Araçları
  - 2.2.Kullanıcı doğrulama
  - 2.3Giriş kontrolu
  - 2.4Veritabanı ve Veri Merkezi Güvenliği
  - 2.5Kötü amaçlı yazılım
  - 2.6.Hizmet Reddi Saldırıları
  - 2.7İzinsiz giriş tespiti
  - 2.8Güvenlik Duvarları ve Saldırı Önleme Sistemleri

2.2. Kullanıcı doğrulama

2.2.İçerik

- Elektronik Kullanıcı Doğrulama İlkeleri
- Parola Tabanlı Kimlik Doğrulama
- Belirteç (Jeton/Token) Tabanlı Kimlik Doğrulama
- Biyometrik Kimlik Doğrulama
- Uzaktan Kullanıcı Kimlik Doğrulaması
- Kullanıcı Kimlik Doğrulaması için Güvenlik Sorunları

Kimlik Doğrulama Süreci

- Temel yapı taşı ve birincil savunma hattı
- Erişim kontrolü ve kullanıcı sorumluluğu için temel

- Tanımlama adımı
  - Güvenlik sistemine bir tanımlayıcı sunulması
- Doğrulama adımı
  - Güvenlik sistemine bir tanımlayıcı sunulması

Tablo 3.1 Tanımlama ve Kimlik Doğrulama Güvenlik Gereksinimleri (SP 800-171)

	Temel Güvenlik Gereksinimleri:
1	Bilgi sistemi kullanıcılarını, kullanıcılar adına hareket eden süreçleri veya cihazları tanımlayın.
2	Kurumsal bilgi sistemlerine erişime izin vermek için bir ön koşul olarak bu kullanıcıların, süreçlerin veya cihazların kimliklerini doğrulayın.

	Türetilmiş Güvenlik Gereksinimleri:
3	Ayrıcalıklı hesaplara yerel ve ağ erişimi, ayrıcalığı olmayan hesaplara ağ erişimi için çok faktörlü kimlik doğrulamayı kullanın.
4	Ayrıcalıklı ve ayrıcalıklı olmayan hesaplara ağ erişimi için yeniden oynatmaya dayanıklı kimlik doğrulama mekanizmalarını kullanın.
5	Tanımlayıcıların belirli bir süre boyunca yeniden kullanılmasını önleyin.
6	Önceden belirlenmiş bir hareketsizlik süresinden sonra tanımlayıcıları devre dışı bırakın.
7	Yeni parolalar oluşturulduğunda minimum parola karmaşıklığı ve karakter farklılığı kuralını uygulayın.
8	Belirli sayıda eski paraloların parolanın yeniden kullanılmasını yasaklayın.
9	Kalıcı bir parolayla anında değişiklik yaparak sistem oturumları için geçici parola kullanımına izin verin.
10	Yalnızca kriptografik olarak korunan parolaları saklayın ve iletin.
11	Kimlik doğrulama bilgilerinin belirsiz geri bildirimini yapın.

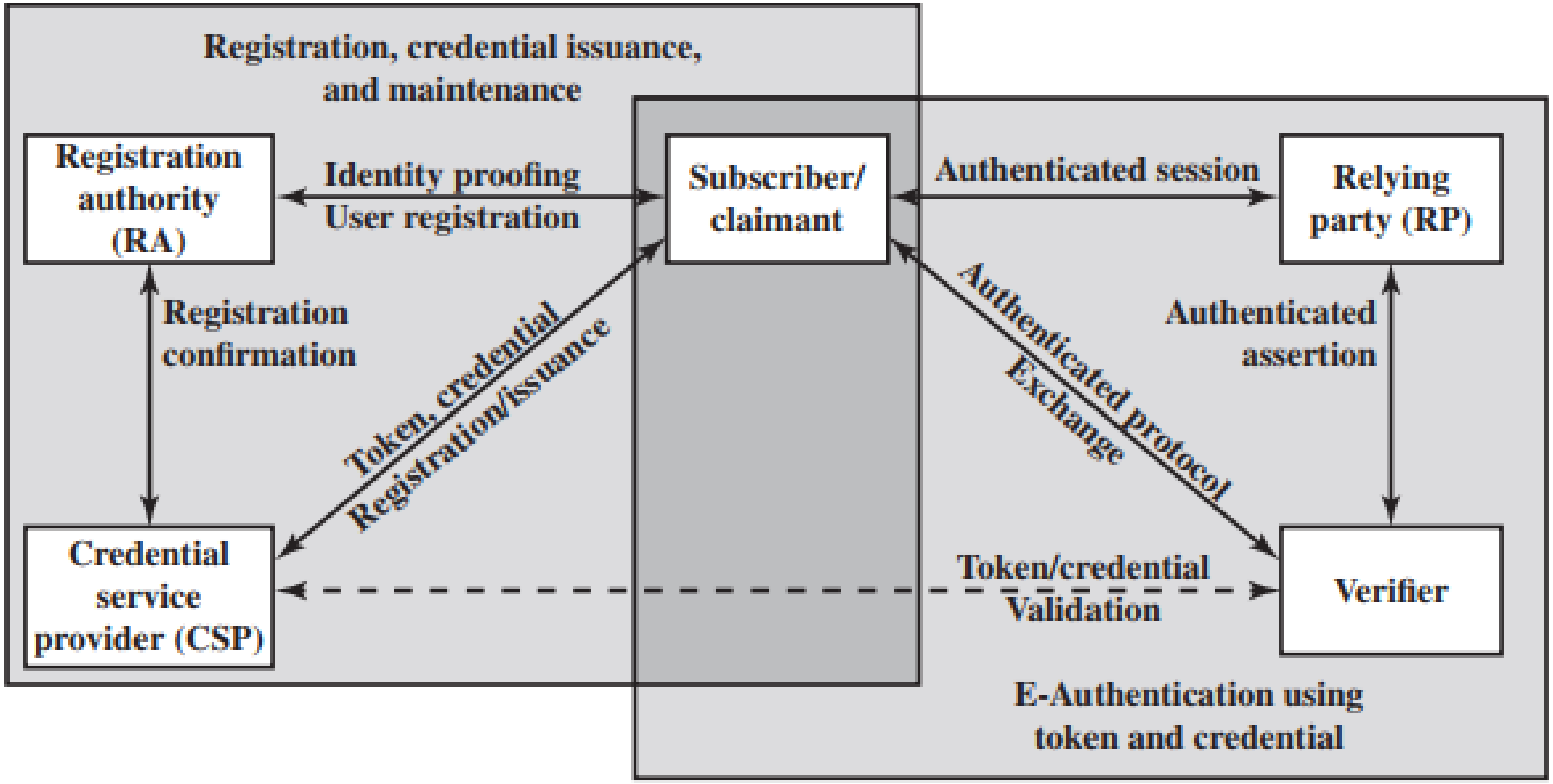


Figure 3.1 **The NIST SP 800-63-3 E-Authentication Architectural Model**

Kullanıcı kimliğini doğrulamanın dört yolu şunlara dayanır:

Kişinin bildiği bir şey	Bireyin sahip olduğu bir şey (belirteç)	Bireyin olduğu bir şey (statik biyometri)	Bireyin yaptığı bir şey (dinamik biyometri)
• Şifre, PIN, önceden ayarlanmış soruların yanıtları	• Akıllı kart, elektronik anahtar kart, fiziksel anahtar	• Parmak izi, retina, yüz	• Ses kalıbı, el yazısı, yazma ritmi

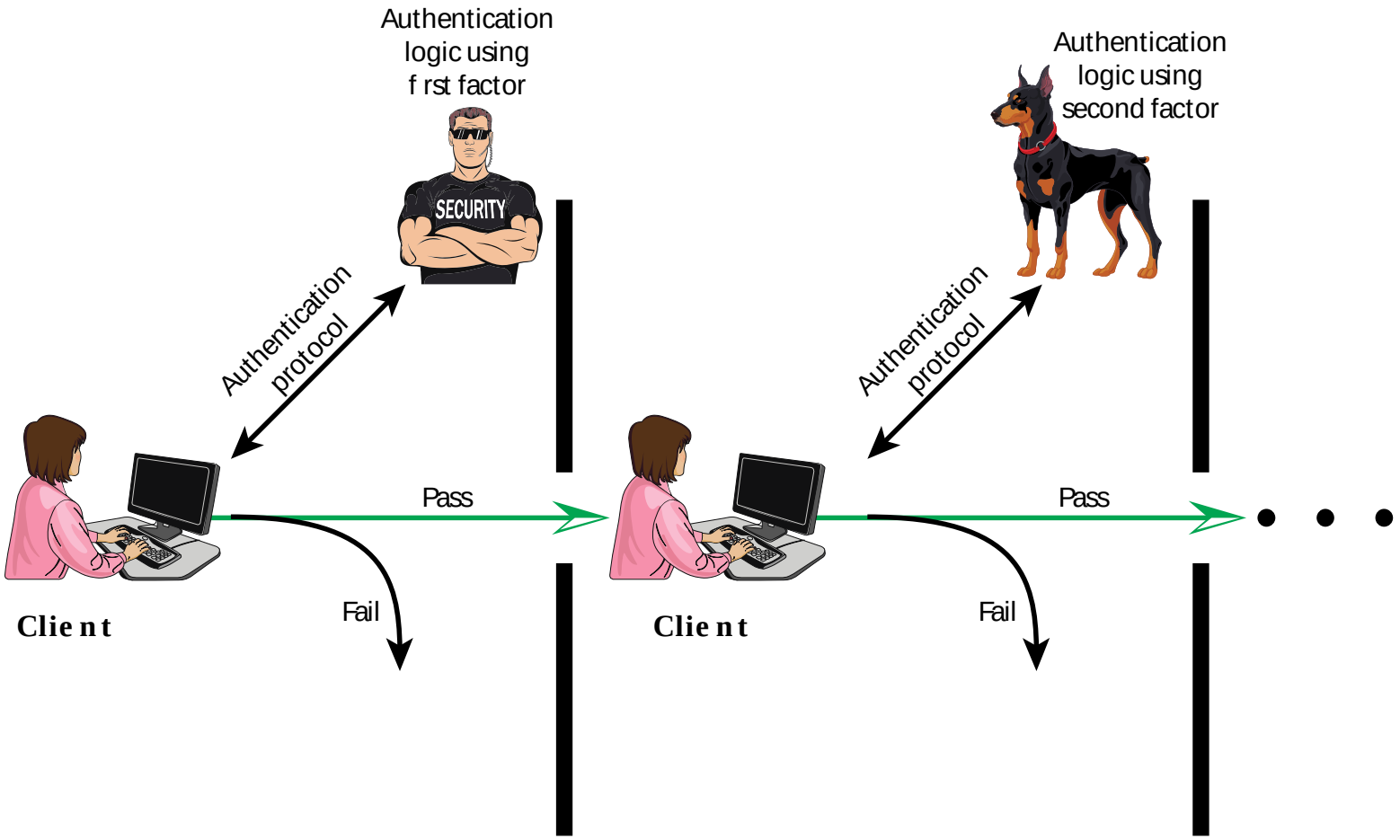
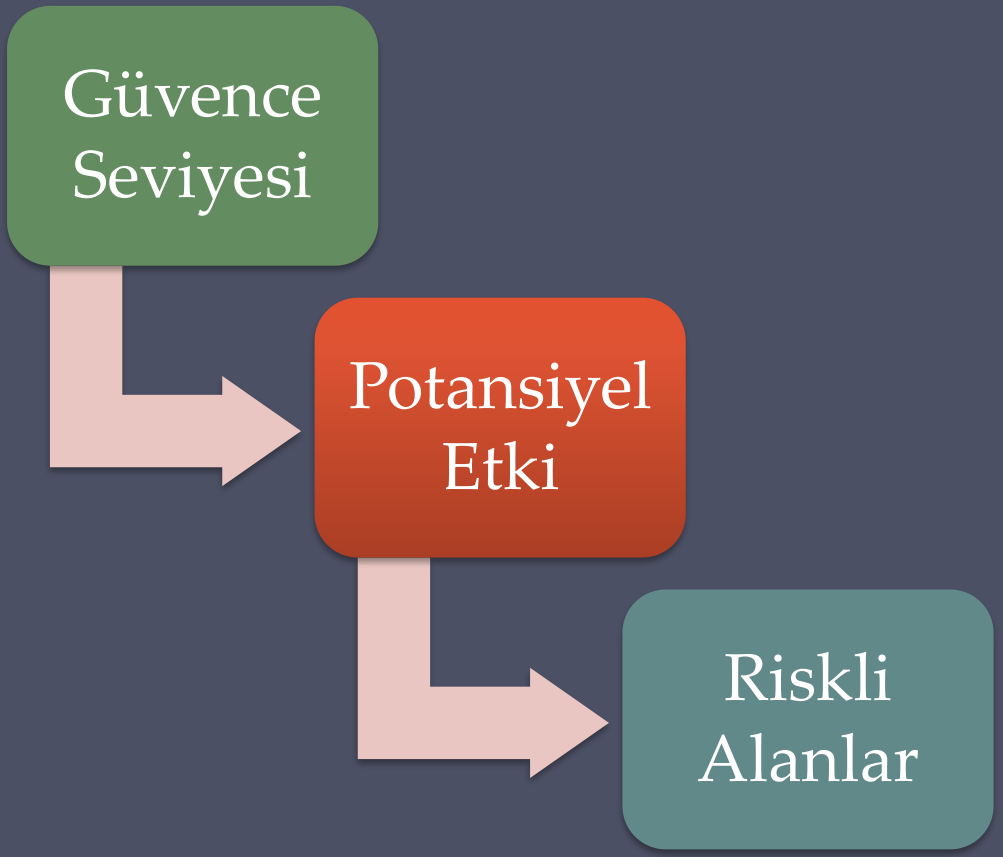


Figure 3.2 Multifactor Authentication

Kullanıcı Kimlik Doğrulaması için Risk Değerlendirmesi

- Üç ayrı kavram vardır:



Güvence Seviyesi

Bir kullanıcının kendi kimliğine atıfta bulunan bir kimlik bilgisi sunduğuna dair bir kuruluşun kesinlik derecesini açıklar

Daha spesifik olarak şu şekilde tanımlanır:

Kimlik belgesinin verildiği kişinin kimliğini belirlemek için kullanılan güvenlik inceleme sürecindeki güven derecesi

Kimlik bilgilerini kullanan kişinin, kimlik belgesinin verildiği kişi olduğuna dair güven derecesi

Güvencenin dört seviyesi

Seviye1
- İddia edilen kimliğin geçerliliğine çok az güven veya hiç güven yok

Seviye 2
- İddia edilen kimliğin geçerliliğine biraz güven var

Seviye 3
- İddia edilen kimliğin geçerliliğine yüksek güven var

Seviye 4
- İddia edilen kimliğin geçerliliğine çok yüksek güven var

Potansiyel etki

- FIPS 199, bir güvenlik ihlali olması durumunda kuruluşlar veya bireyler üzerinde üç düzeyde potansiyel etki tanımlar:
  - Düşük
    - Bir kimlik doğrulama hatasının organizasyonel operasyonlar, organizasyonel varlıklar veya bireyler üzerinde sınırlı bir olumsuz etkisi olması beklenebilir.
  - Orta
    - Bir kimlik doğrulama hatasının ciddi bir olumsuz etkisi olması beklenebilir
  - Yüksek
    - Bir kimlik doğrulama hatasının ciddi veya yıkıcı bir olumsuz etkisi olması beklenebilir

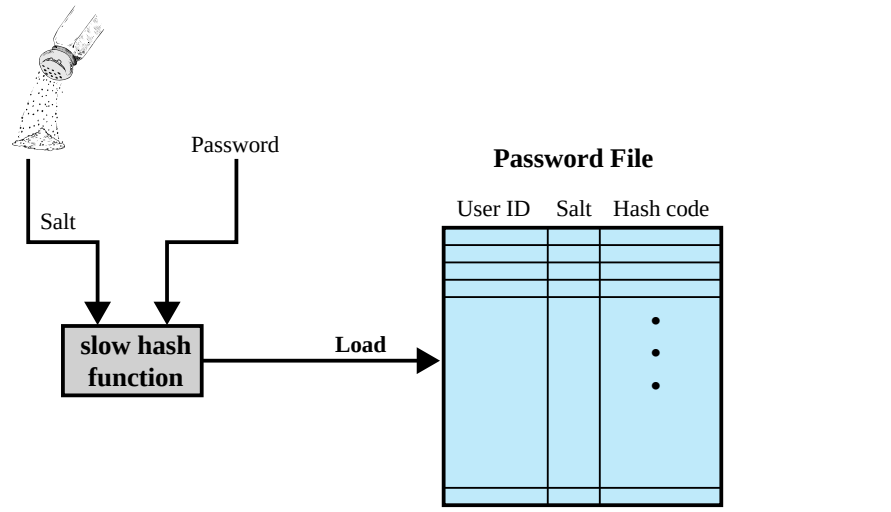
Her Güvence Seviyesi için Maksimum Potansiyel Etkiler

	Güvence Seviyesi Etki Profilleri			
Kimlik Doğrulama Hataları için Potansiyel Etki Kategorileri	1	2	3	4
Rahatsızlık, sıkıntı veya itibar kaybı veya itibarın zarar görmesi	Düşük	Orta	Orta	Yüksek
Mali veya organizasyon güvenilirliği kaybı	Düşük	Orta	Orta	Yüksek
Organizasyon programlarına veya ilgi alanlarına zarar	Hiçbiri	Düşük	Orta	Yüksek
Hassas bilgilerin yetkisiz olarak yayınlanması	Hiçbiri	Düşük	Orta	Yüksek
Kişisel güvenlik	Hiçbiri	Hiçbiri	Düşük	Orta / Yüksek
Sivil veya cezai ihlaller	Hiçbiri	Düşük	Orta	Yüksek

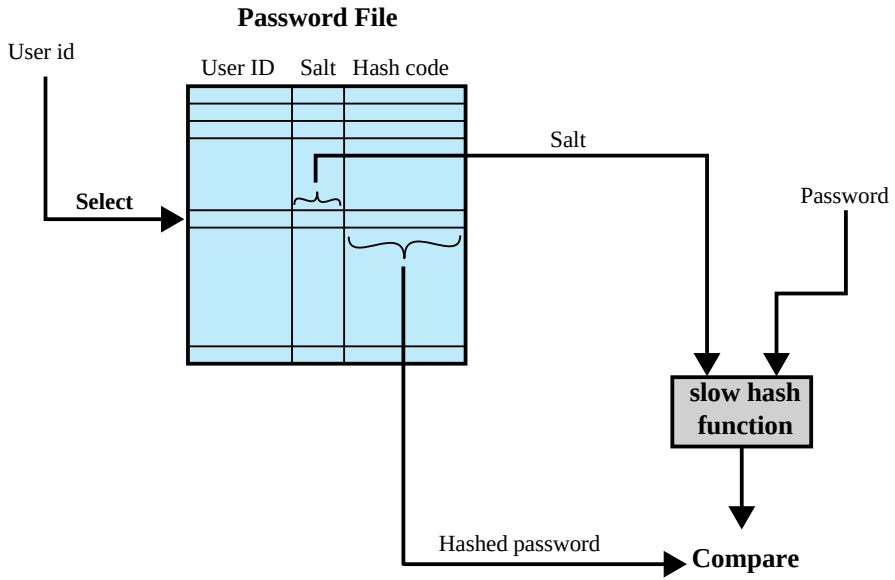
Şifre Tabanlı Kimlik Doğrulama

- Davetsiz misafirlere karşı yaygın olarak kullanılan savunma hattı
  - Kullanıcı adı/giriş ve şifre sağlar
  - Sistem, parolayı belirtilen oturum açma için saklanan parolayla karşılaştırır
- Kullanıcı kimliği:
  - Kullanıcının sisteme erişim yetkisi olduğunu belirler
  - Kullanıcının ayrıcalıklarını belirler
  - İsteğe bağlı erişim kontrolünde kullanılır

Parola Güvenlik Açıkları



(a) Loading a new password



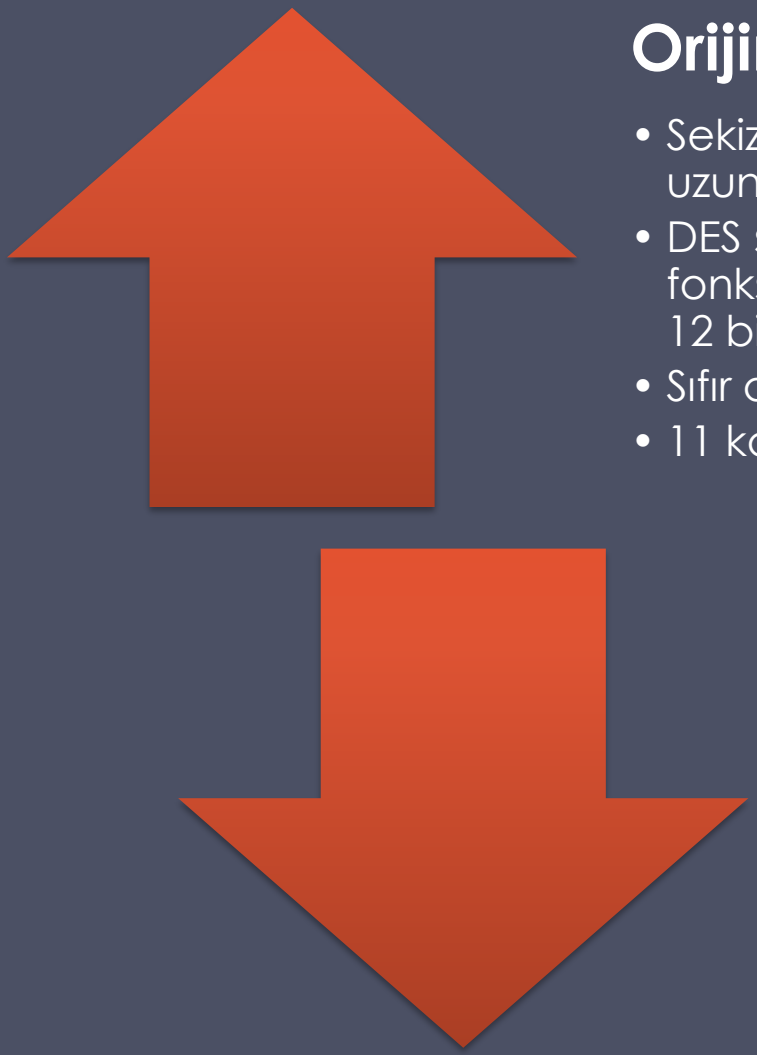
(b) Verifying a password

Figure 3.3 UNIX Password Scheme

Tuz Kullanım Amaçları

- Tuz üç amaca hizmet eder:
  - Parola dosyasında yinelenen parolaların görünmesini engeller. İki kullanıcı aynı şifreyi seçse bile, bu şifrelere farklı tuz değerleri atanır.
  - Çevrimdışı sözlük saldırılarının zorluğunu büyük ölçüde artırır. Bir tuz için uzunluk b bit ise, olası parola sayısı 2^b kat artırarak sözlük saldırısında parola tahmin etme zorluğunu artırır.
  - İki veya daha fazla sistemde şifresi olan bir kişinin hepsinde aynı şifreyi kullanıp kullanmadığını anlamak neredeyse imkansız hale geliyor.

UNIX Uygulaması



Orijinal şema

- Sekiz adede kadar yazdırılabilir karakter uzunluğunda.
- DES şifrelemesini tek yönlü özet fonksiyonuna dönüştürmek için kullanılan 12 bitlik tuz
- Sıfır değeri tekrar tekrar 25 kez şifrelenir
- 11 karakter dizisine çevrilmiş çıktı

Artık yetersiz görülüyor

- Saldırgan, yaklaşık 80 dakika içinde 50 milyondan fazla şifre tahminini işleyebiliyor
- Mevcut hesap yönetimi yazılımı veya çok satıcılı ortamlarla uyumluluk için hala sıklıkla gerekli olabiliyor

Geliştirilmiş Uygulamalar

Unix için çok daha güçlü özet/tuz şemaları mevcuttur

Önerilen karma işlevi MD5'i temel alır

- 48-bit'e kadar tuz
- Şifre uzunluğu sınırsızdır
- 128 bit özet üretir
- Yavaşlamayı sağlamak için 1000 yinelemeli bir iç döngü kullanır

OpenBSD, Bcrypt adlı Blowfish blok şifreleme tabanlı karma algoritmasını kullanır

- Unix özet/tuz şemasının en güvenli sürümü
- 192 bitlik özet değeri oluşturmak için 128 bitlik tuz kullanır
- Bcrypt, bir Bcyrpt gerçekleştirmek için gereken sürede artışa neden olan bir maliyet değişkeni içerir.
- Özet .

Şifre Kırma

Sözlük saldırıları

- Muhtemel parolalardan oluşan geniş bir sözlük geliştirin ve her birini parola dosyasına karşı deneyin
- Her şifre, her bir tuz değeri kullanılarak hash'lenmeli ve daha sonra saklanan hash değerleriyle karşılaştırılmalıdır.

Rainbow tablo Saldırıları

- Tüm tuzlar için özet değerlerin ön hesaplama tabloları
- Devasa bir hash değerleri tablosu
- Yeterince büyük bir tuz değeri ve yeterince büyük bir karma uzunluk kullanılarak karşı konulabilir

Parola kırıcılar, insanların kolayca tahmin edilebilir parolalar seçmesi gerçeğinden yararlanır

- Daha kısa şifre uzunluklarının kırılması da daha kolaydır

John the Ripper

- Açık kaynaklı şifre kırıcı ilk olarak 1996'da geliştirildi
- Kaba kuvvet ve sözlük tekniklerinin bir kombinasyonunu kullanır

Modern Yaklaşımlar

- Karmaşık şifre politikası
  - Kullanıcıları daha güçlü şifreler seçmeye zorlama
- Ancak şifre kırma teknikleri de gelişti
  - Şifre kırma için mevcut işleme kapasitesi önemli ölçüde arttı
  - Potansiyel şifreler oluşturmak için karmaşık algoritmaların kullanılması
  - Kullanımdaki gerçek şifre örnekleri ve yapıları inceleniyor

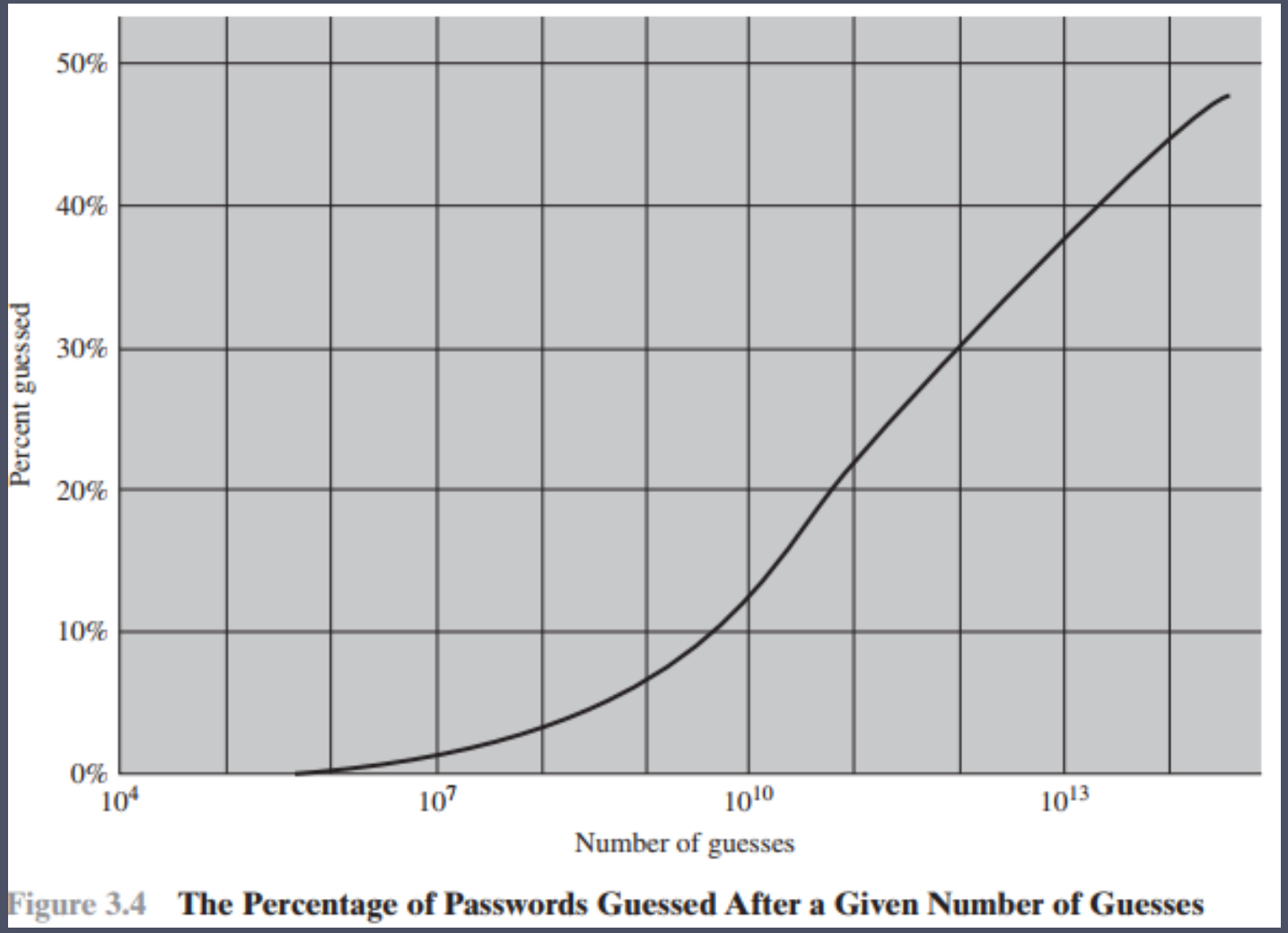


Figure 3.4 The Percentage of Passwords Guessed After a Given Number of Guesses

- Karmaşık bir şifre politikasına sahip bir araştırma üniversitesinde 25.000'den fazla öğrenci tarafından kullanılan şifrelerin analizi
- RockYou dosyası da dahil olmak üzere sızdırılmış şifre dosyaları koleksiyonundan oluşan bir veritabanı kullandılar.
- Grafik, tahmin sayısının bir fonksiyonu olarak kırılan şifrelerin yüzdesini gösterir. Parolaların %10'dan fazlası yalnızca 10^{10} tahminden sonra bulunabildi. 10^{13} tahminden sonra ise şifrelerin neredeyse %40'ı bulunabildi

Şifre Dosyasına Erişim Kontrolü

Şifrelenmiş parolalara erişimi engelleyerek çevrimdışı tahmin saldırılarını engelleyebilir

Yalnızca ayrıcalıklı kullanıcılar tarafından kullanılabilir yap

Gölge şifre dosyası kullan

Güvenlik açıkları

- **İşletim sisteminde dosyaya erişime izin veren zayıflık**
- **İzinleri kazara okunabilir hale getirme**
- **Diğer sistemlerde aynı şifreye sahip kullanıcılar**
- **Yedekleme ortamından erişim**
- **Ağ trafiğinde şifreleri snif etme**

Şifre Seçim Stratejileri

Kullanıcı eğitimi

Kullanıcılara tahmin edilmesi zor parolalar kullanmanın önemi anlatılabilir ve güçlü parolalar seçme yönergeleri verilebilir.

Bilgisayar tarafından oluşturulan şifreler

Kullanıcılar onları hatırlamakta zorlanıyor

Reaktif şifre kontrolü

Sistem, tahmin edilebilir şifreleri bulmak için periyodik olarak kendi şifre kırıcısını çalıştırır

Karmaşık şifre politikası

Kullanıcının kendi şifresini seçmesine izin verilir, ancak sistem şifrenin uygun olup olmadığını kontrol eder ve değilse reddeder.

Amaç, kullanıcının akılda kalıcı bir parola seçmesine izin verirken tahmin edilebilir parolaları ortadan kaldırmaktır.

Proaktif Şifre Kontrolü

- Kural uygulama
  - Parolaların uyması gereken belirli kurallar
- Şifre denetleyicisi
  - Kullanılmaması gereken büyük bir parola sözlüğü derleyin
- Bloom filtresi
  - Hash değerlerine dayalı bir tablo oluşturmak için kullanılır
  - Bu tabloya karşı istenen şifreyi kontrol edin

Belirteç Olarak Kullanılan Kart Türleri

Kart tipi	Tanımlayıcı Özellik	Örnek
Kabartmalı	Yalnızca ön tarafta yükseltilmiş karakterler	Eski kredi kartı
Manyetik şerit	Arkada manyetik şerit, önde karakterler	banka kartı
Hafıza	Elektronik hafıza içinde	Ön ödemeli telefon kartı
Akıllı İletişim Temassız	İçinde elektronik bellek ve işlemci Yüzeyde açıkta elektrik kontakları İçine gömülü radyo anteni	Biyometrik kimlik kartı

Hafıza kartları

- Verileri saklayabilir ancak işleyemez
- En yaygın olanı manyetik şeritli karttır.
- Dahili bir elektronik bellek içerir
- Fiziksel erişim için tek başına kullanılabilir
  - Otel odası
  - ATM
- Bir şifre veya PIN ile birleştirildiğinde önemli ölçüde daha fazla güvenlik sağlar
- Hafıza kartlarının dezavantajları şunları içerir:
  - Özel bir okuyucu gerektirir
  - Belirteç (token/jeton) kaybı
  - Kullanıcı memnuniyetsizliği

Akıllı Belirteçler

- Fiziksel özellikleri:
  - Gömülü bir mikroişlemci içerir
  - Banka kartına benzer
  - Hesap makineleri, anahtarlar, küçük taşınabilir nesneler gibi görünebilir
- Kullanıcı arayüzü:
  - Manuel arayüzler, insan/belirteç etkileşimi için bir tuş takımı ve ekran içerir
- Elektronik arayüz
  - Akıllı kart veya başka bir belirteç, uyumlu bir okuyucu/yazıcı ile iletişim kurmak için elektronik bir arabirim gerektirir
  - Temaslı ve temassız arayüzler
- Kimlik doğrulama protokolü:
  - Üç kategoride sınıflandırılır:
    - Statik
    - Dinamik şifre üreticisi
    - meydan okuma-tepki

Akıllı kartlar

- Akıllı belirtecin en önemli kategorisi
  - Kredi kartı görünümündedir
  - Elektronik bir arayüze sahiptir
  - Akıllı belirteç protokollerinden herhangi birini kullanabilir
- ….. içerir:
  - Bütün bir mikroişlemci
    - İşlemci
    - Hafıza
    - G/Ç bağlantı noktaları
- Tipik olarak üç tür bellek içerir:
  - Salt okunur bellek (ROM)
    - Kartın ömrü boyunca değişmeyen verileri depolar
  - Elektrikle silinebilir programlanabilir ROM (EEPROM)
    - Uygulama verilerini ve programları tutar
  - Rastgele erişim belleği (RAM)
    - Uygulamalar koşturulduğunda oluşturulan geçici verileri tutar

APDU = application protocol data unit
ATR = Answer to reset
PTS = Protocol type selection

Figure 3.6 Smart Card/Reader Exchange

Elektronik Kimlik Kartları (E-kimlik)

Vatandaşlar için ulusal kimlik kartı olarak akıllı kart kullanımı

Kamu ve ticari hizmetlere erişim için diğer ulusal kimlik kartları ve ehliyet gibi benzer kartlarla aynı amaça hizmet edebilir

Daha güçlü kimlik kanıtı sağlayabilir ve çok çeşitli uygulamalarda kullanılabilir

Gerçekte devlet tarafından geçerli ve orijinal olarak doğrulanmış bir akıllı karttır.

Yeni Türkiye Kimlik Kartı

Yüzeyinde insan tarafından okunabilir veriler basılıdır

- Kişisel veri
- Belge Numarası
- Kart erişim numarası (CAN)
- Makine tarafından okunabilir bölge (MRZ)

E-kimlik kartları için Elektronik Fonksiyonlar ve Veri

İşlev	Amaç	PACE Şifresi	Veri	Kullanır
E-Geçiş (zorunlu)	Yetkili çevrimdışı denetim sistemleri verileri okur	CAN veya MRZ	Yüz görüntüsü; iki parmak izi görüntüsü (isteğe bağlı), MRZ verileri	Devlet erişimi için ayrılmış çevrimdışı biyometrik kimlik doğrulaması
e-Kimlik (etkinleştirme isteğe bağlı)	Çevrimiçi uygulamalar, verileri veya erişim işlevlerini yetkili olarak okur	e-Kimlik PIN'i	Aile ve verilen isimler; sanatsal isim ve doktora derecesi: doğum tarihi ve yeri; adres ve topluluk kimliği; Son kullanma tarihi	Kimlik; yaş doğrulaması; topluluk kimliği doğrulaması; kısıtlı tanımlama (takma ad); iptal sorgusu
	Çevrimdışı denetim sistemleri verileri okur ve adresi ve topluluk kimliğini günceller	CAN veya MRZ		
e-İmza (sertifika isteğe bağlı)	Bir sertifika yetkilisi imza sertifikasını çevrimiçi olarak yükler	e-Kimlik PIN'i	İmza anahtarı. X.509 sertifikası	Elektronik imza oluşturma
	Vatandaşlar eSign PIN ile elektronik imza atıyor	CAN		

CAN = kart erişim numarası
MRZ = makine tarafından okunabilir bölge
PACE = Parolayla doğrulanmış bağlantı kurulması
PIN = kişisel kimlik numarası

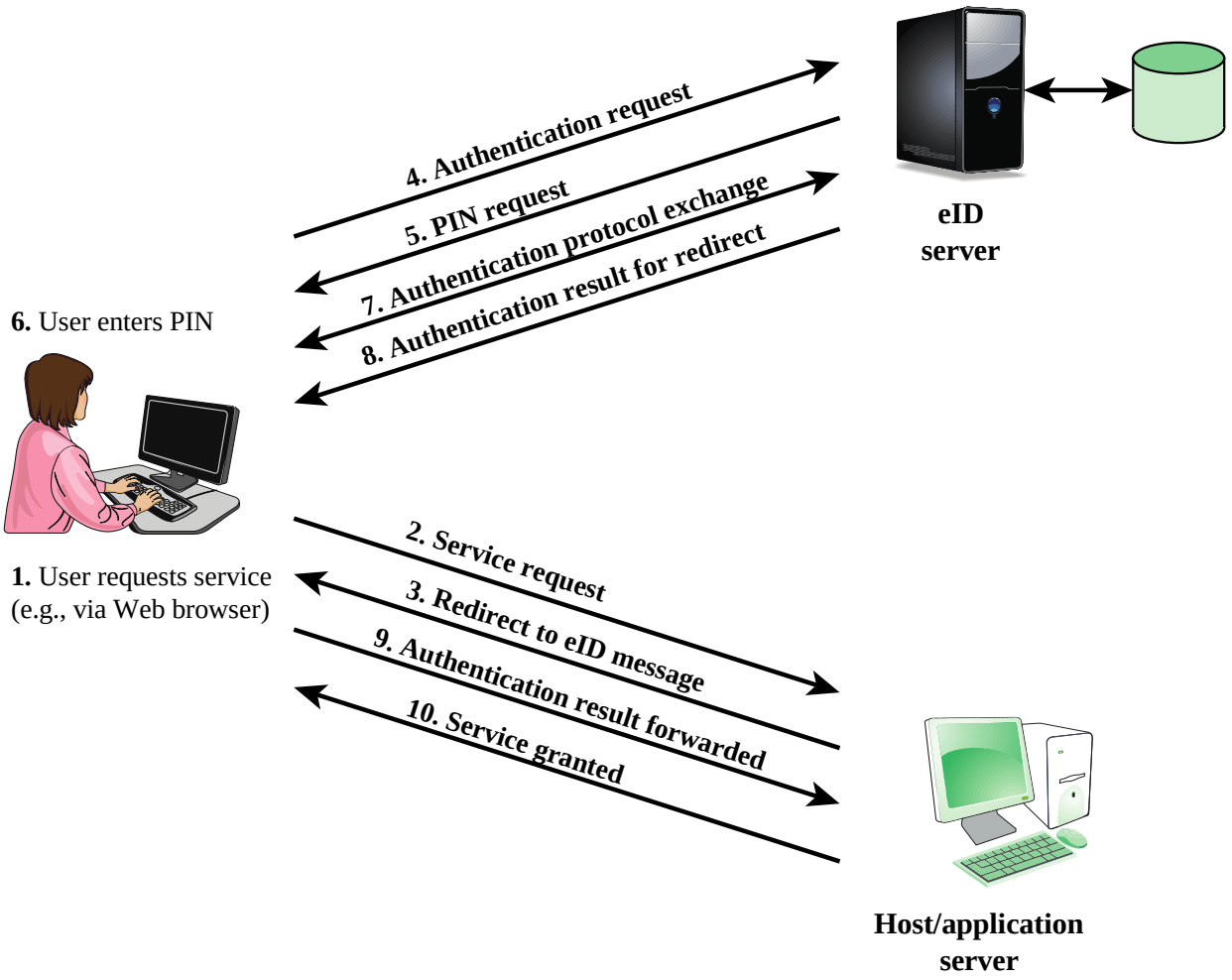


Figure 3.7 User Authentication with eID

Parolayla doğrulanmış bağlantı kurulması (PACE)

E-Kimlik kartındaki temassız RF çipinin açık erişim kontrolü olmadan okunamamasını sağlar

Çevrimiçi kullanımlar için, kullanıcının 6 haneli PIN'i (yalnızca kart sahibi tarafından bilinmesi gereken) girmesiyle erişim sağlanır.

Çevrimdışı uygulamalar için, kartın arka yüzünde yazılı MRZ veya ön yüzünde yazılı altı haneli kart erişim numarası (CAN) kullanılır.

Biyometrik Kimlik Doğrulama

- Eşsiz fiziksel özelliklere dayalı olarak bir bireyin kimliğini doğrulama girişimleri
- Örüntü tanımaya dayalı
- Şifreler ve belirteçlerle karşılaştırıldığında teknik olarak karmaşık ve pahalıdır
- Kullanılan fiziksel özellikler şunlardır;
  - yüz özellikleri
  - parmak izleri
  - el geometrisi
  - retina deseni
  - İris
  - İmza
  - Ses

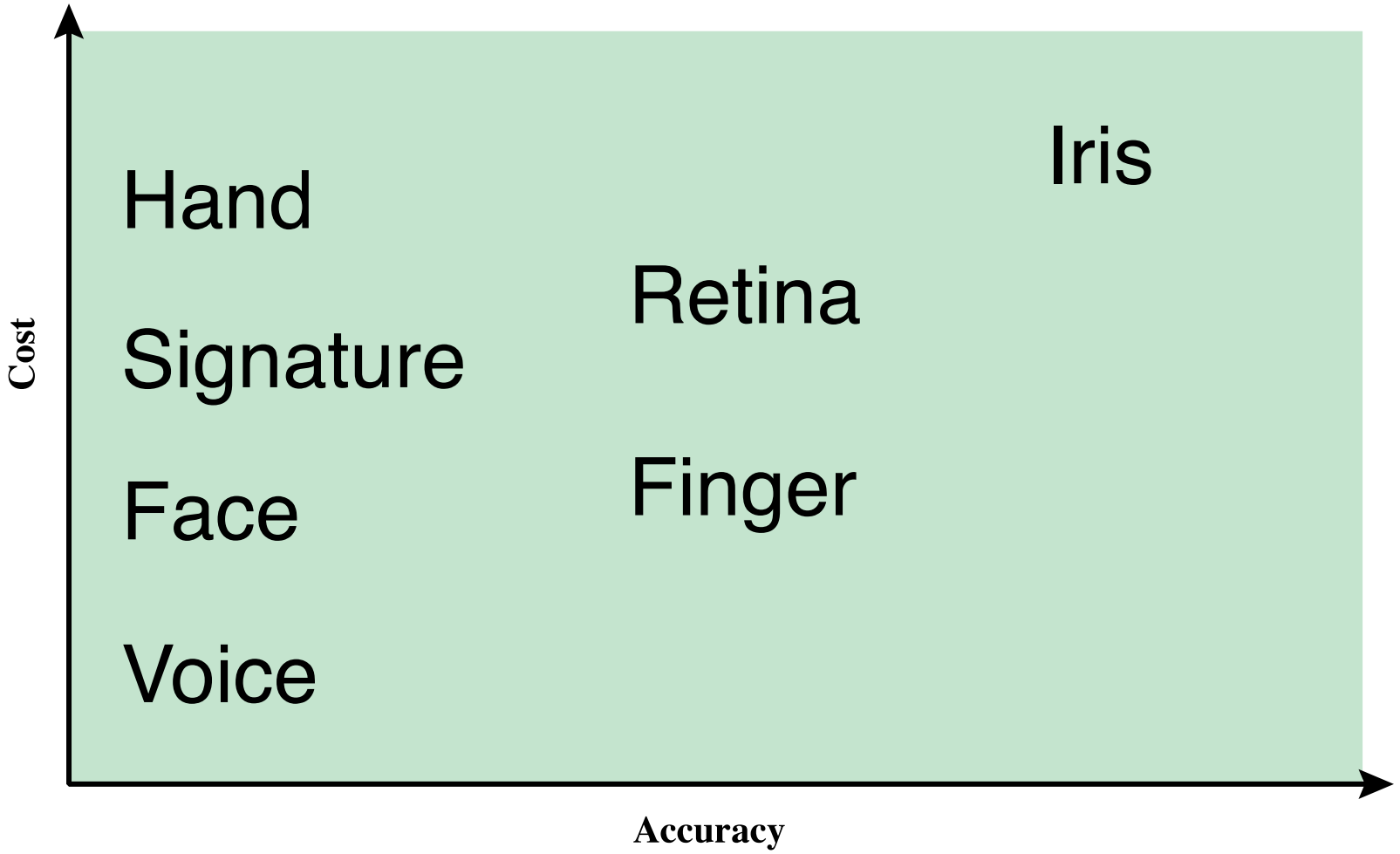
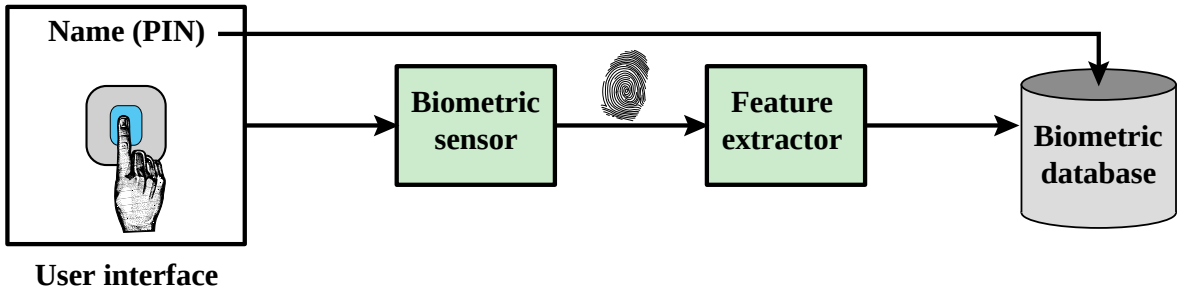
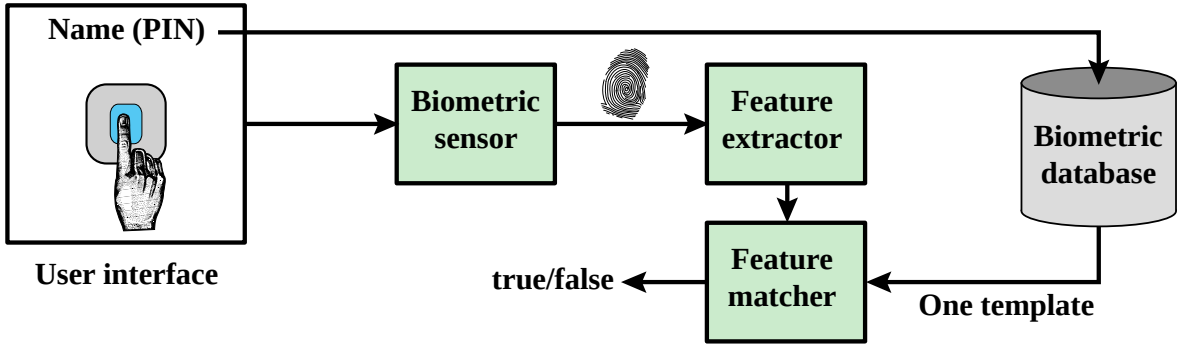


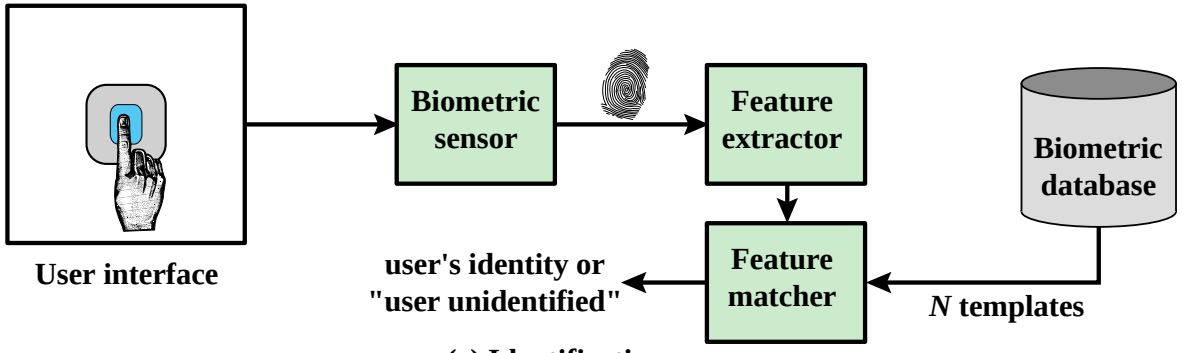
Figure 3.8 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.



(a) Enrollment



(b) Verification



(c) Identification

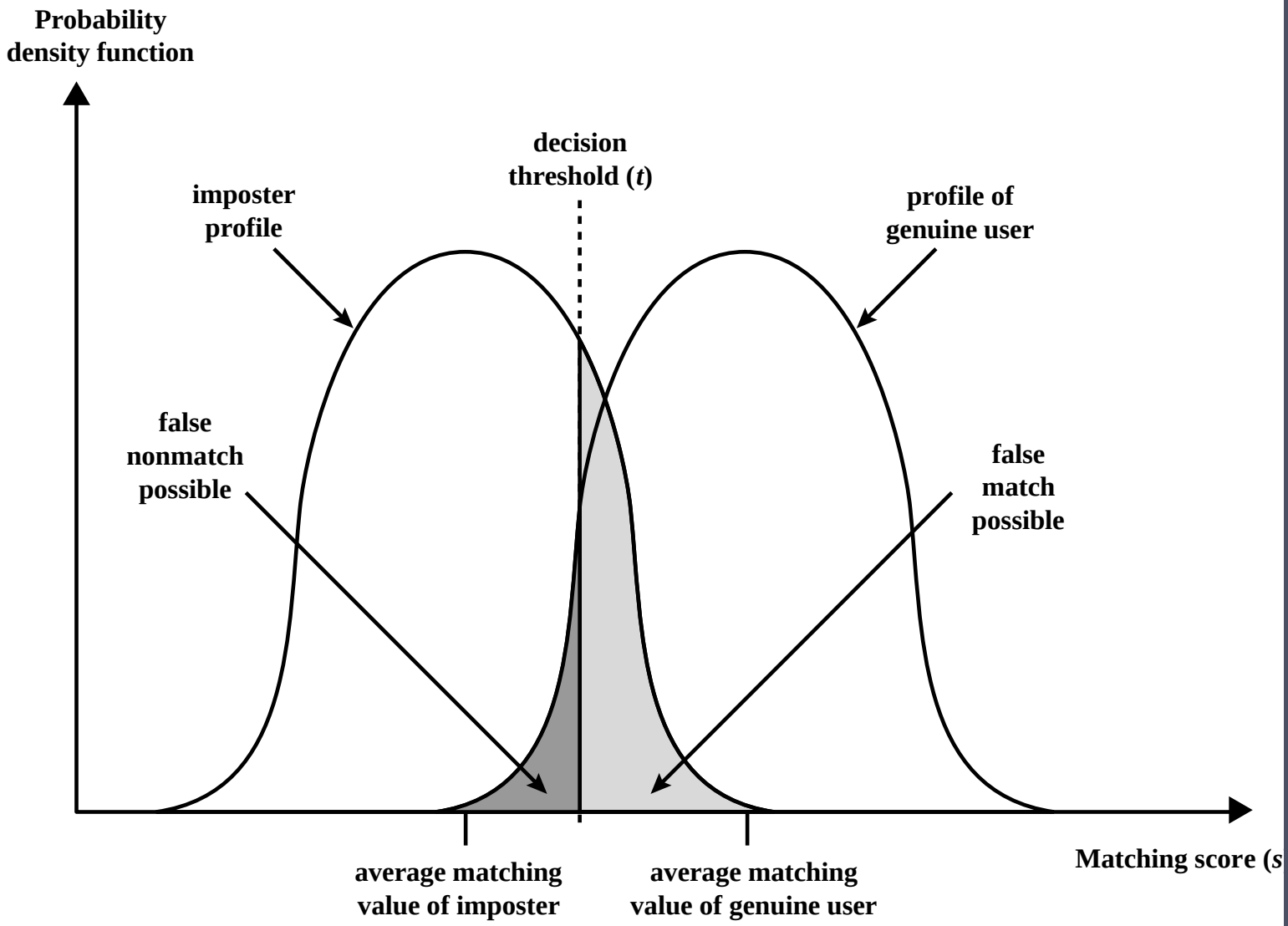


Figure 3.10 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (*s*) is greater than a preassigned threshold (*t*), a match is declared.

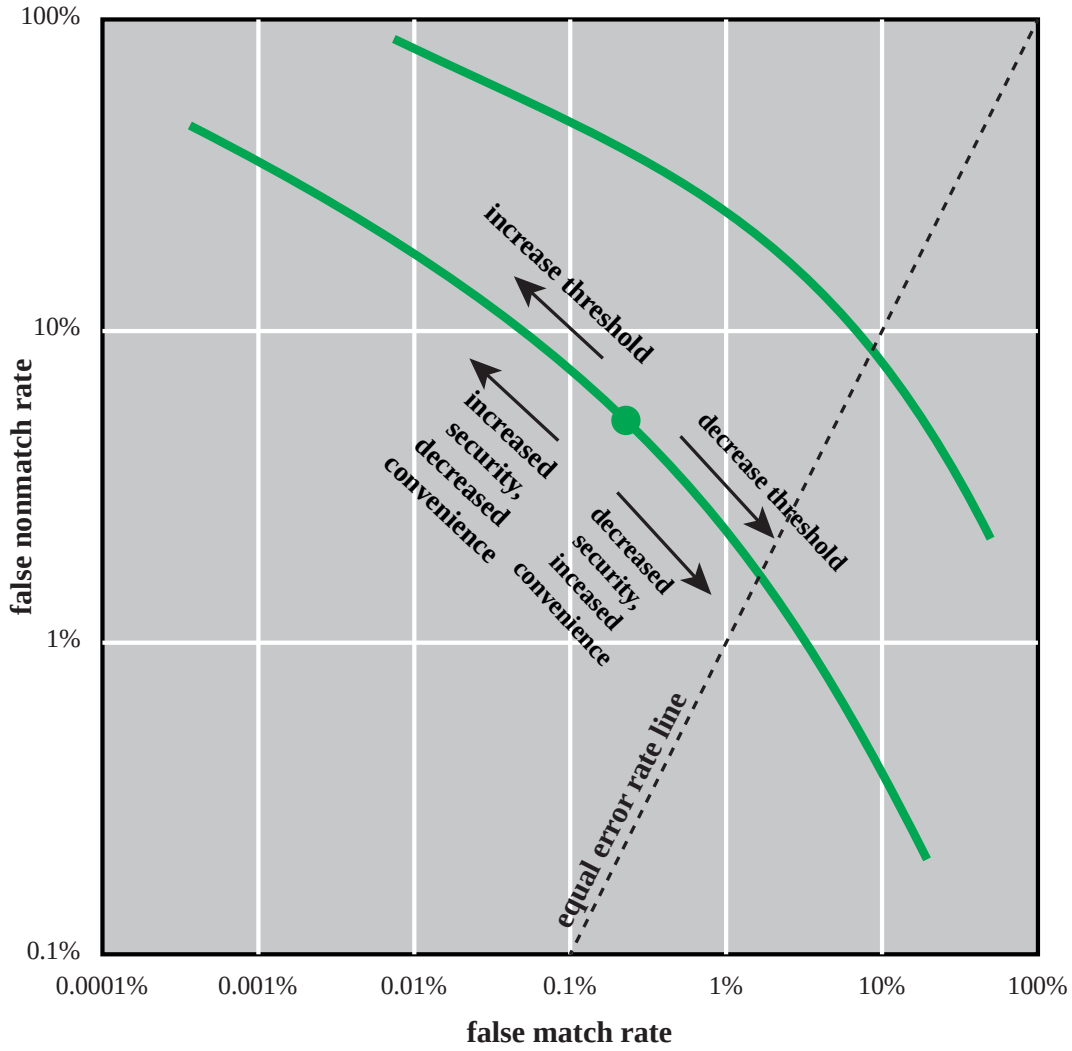


Figure 3.11 Idealized Biometric Measurement Operating Characteristic Curves (log-log scale)

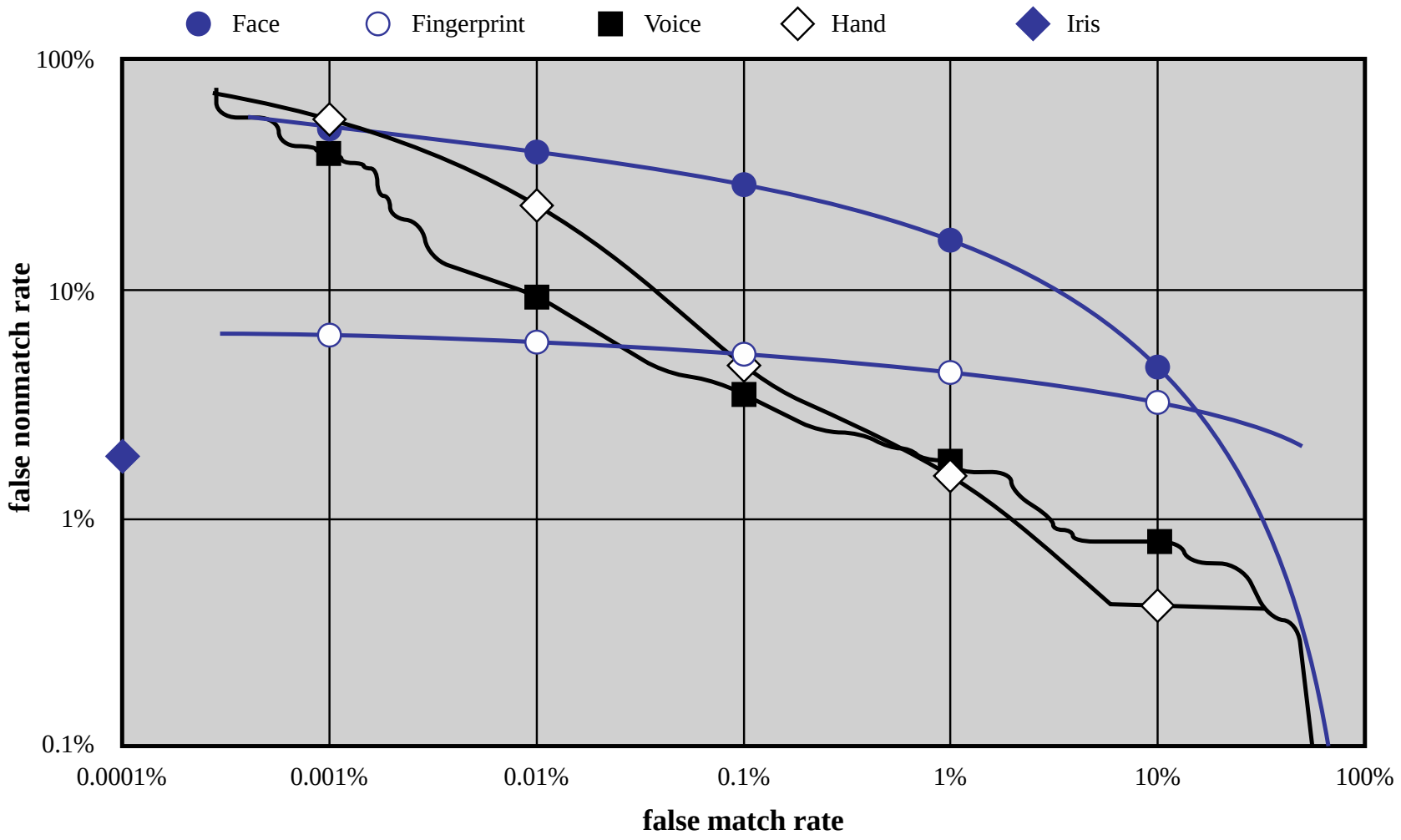
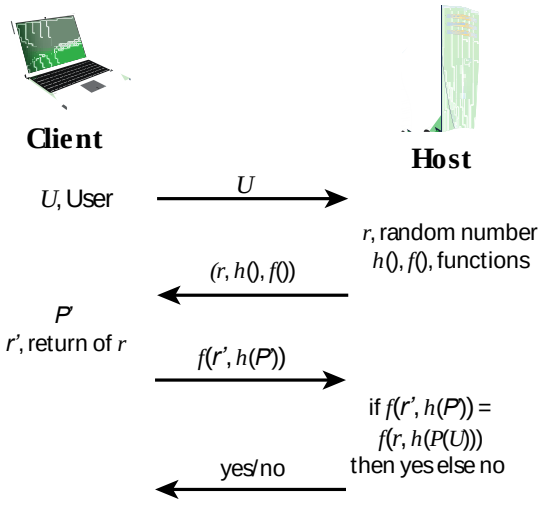


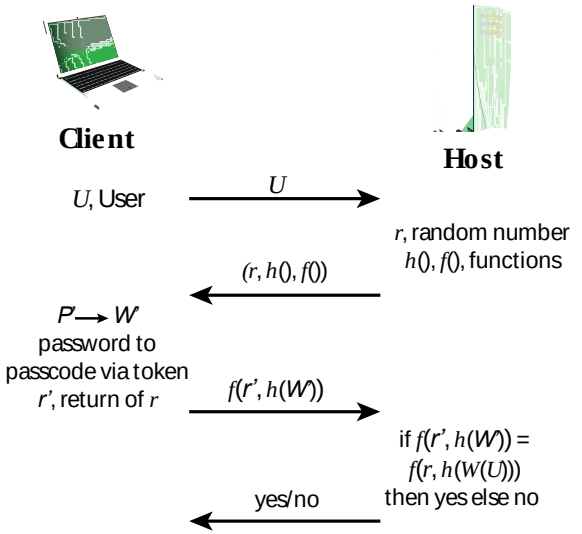
Figure 3.12 Actual Biometric Measurement Operating Characteristic Curves, reported in [MANS01]. To clarify differences among systems, a log-log scale is used.

Uzaktan Kullanıcı Kimlik Doğrulaması

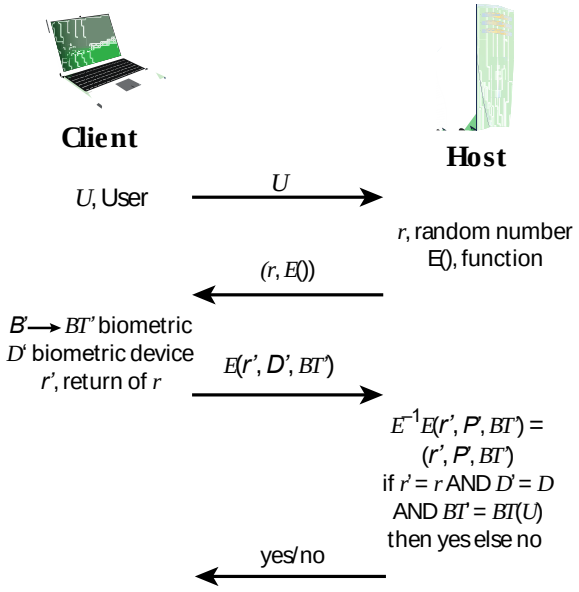
- Bir ağ, İnternet veya bir iletişim bağlantısı üzerinden kimlik doğrulaması daha karmaşıktır
- Ek güvenlik tehditleri içerir:
  - Gizlice dinleme, bir parola yakalama, gözlemlenen bir kimlik doğrulama sırasını yeniden oynatma
- Tehditlere karşı genellikle bir tür meydan okuma-yanıt protokolüne güvenilir



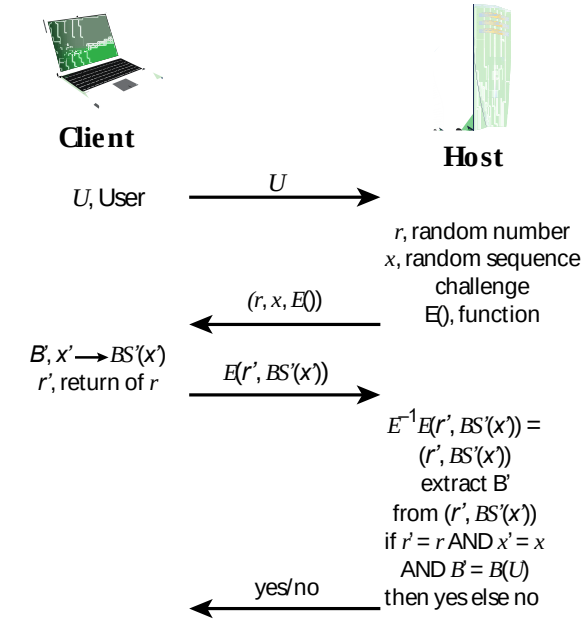
(b) Protocol for a password



(b) Protocol for a token



(c) Protocol for static biometric



(d) Protocol for dynamic biometric

saldırılar	doğrulayıcılar	Örnekler	Tipik savunmalar
İstemci saldırısı	Şifre	Tahmin, kapsamlı arama	Büyük entropi; sınırlı denemeler
	Belirteç (Token/Jeton)	Ayrıntılı arama	Büyük entropi; sınırlı girişimler, nesne hırsızlığı varlığı gerektirir
	Biyometrik	yanlış eşleşme	Büyük entropi; sınırlı denemeler
Ana bilgisayar saldırısı	Şifre	Düz metin hırsızlığı, sözlük/kapsamlı arama	Karma; büyük entropi; şifre veri tabanının korunması
	Belirteç (Token/Jeton)	şifre hırsızlığı	Şifre ile aynı; 1 kerelik şifre
	biyometrik	Şablon hırsızlığı	Cihaz kimlik doğrulamasını yakalayın; meydan okuma yanıtı
Dinleme, hırsızlık ve kopyalama	Şifre	"Omuz sörfü"	Gizli tutmak için kullanıcı titizliği; güvenliği ihlal edilmiş parolaları hızla iptal etmek için yönetici özeni; çok faktörlü kimlik doğrulama
	Belirteç (Token/Jeton)	Hırsızlık, sahtecilik donanımı	Çok faktörlü kimlik doğrulama; kurcalamaya dayanıklı/belirgin belirteç
	biyometrik	Biyometrik kopyalama (sahtecilik)	Yakalama cihazında kopyalama algılama ve yakalama cihazı kimlik doğrulaması
Tekrar oynat	Şifre	Çalınan parola yanıtını tekrar oynat	Meydan okuma-cevap protokolü
	Belirteç (Token/Jeton)	Çalınan parola yanıtını tekrar oynat	Meydan okuma-tepki protokolü; 1 kerelik şifre
	biyometrik	Çalınan biyometrik şablon yanıtını tekrar oynat	Yakalama cihazında algılamayı kopyalayın ve sorgulama-yanıt protokolü aracılığıyla cihaz kimlik doğrulamasını yakalayın
Truva atı	Şifre, Belirteç (Token/Jeton), biyometrik	Hileli istemci veya yakalama aygıtının yüklenmesi	Güvenilen güvenlik çevresi içinde istemci veya yakalama cihazının kimlik doğrulaması
Hizmet reddi	Şifre, Belirteç (Token/Jeton), biyometrik	Birden çok başarısız kimlik doğrulaması ile kilitleme	Belirteçli çok faktörlü

Bazı Potansiyel saldırılar,
Duyarlı Doğrulayıcılar,
ve
Tipik Savunmalar

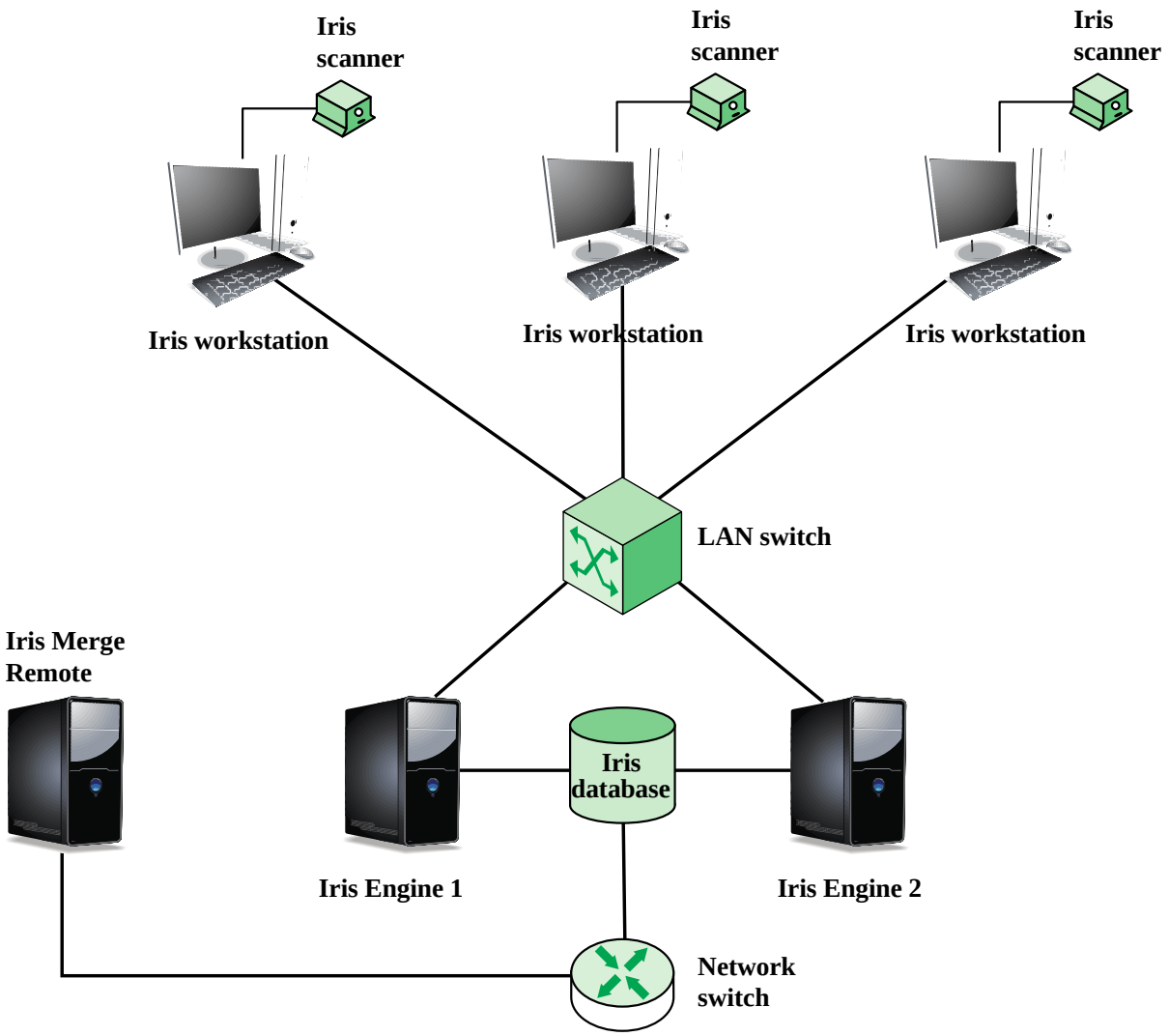


Figure 3.14 General Iris Scan Site Architecture for UAE System

KIMLIK DOĞRULAMA GÜVENLIK SORUNLARI

Dinleme

Saldırgan, kullanıcının ve saldırganın fiziksel yakınlığını içeren bir tür saldırı ile parolayı öğrenmeye çalışır.

Ana Bilgisayar Saldırıları

Parolaların, belirteç parolalarının veya biyometrik şablonların depolandığı ana bilgisayardaki kullanıcı dosyasına yönlendirilir

Hizmet Reddi Saldırısı

Hizmeti çok sayıda kimlik doğrulama girişimiyle doldurarak bir kullanıcı kimlik doğrulama hizmetini devre dışı bırakma girişimleri

Tekrar Oynatma

Saldırgan, önceden yakalanmış bir kullanıcı yanıtını tekrarlar

Truva atı

Bir uygulama veya fiziksel cihaz, bir kullanıcı şifresi, şifre veya biyometrik yakalama amacıyla gerçek bir uygulama veya cihaz gibi görünüyor.

İstemci Saldırıları

Saldırgan, uzak ana bilgisayara veya araya giren iletişim yoluna erişim olmadan kullanıcı kimlik doğrulaması elde etmeye çalışır.