

**ERZURUM ATATÜRK ÜNİVERSİTESİ**

**MÜHENDİSLİK FAKÜLTESİ**

**BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

BMS 302 : Bilgisayar Bilgi Yönetimi ve Güvenliği

Information security management handbook  
(Bilgi güvenliği yönetimi el kitabı)

120757017 Hilâl Tansu YILDIRIM

**İçindekiler :**

**BİYOMETRİK TEKNOLOJİ İLE GÜVENLİĞİ ARTTIRMA** 1

Giriş1

Biyometri Temelleri1

Biyometri Nasıl Çalışır?2

Biyometrik Özellikler3

Biyometri için Ortak Kullanımlar3

Biyometrik Ölçüm Faktörleri4

Biyometrik Ölçüm6

Uygulama sorunları 9

Biyometrik teknolojiler 12

Biyometrik standartlar 20

Sonuç21

**BİYOMETRİK: YENİ OLAN NEDİR?** 21

Parmak izleri21

Göz tarama22

Yüz tanıma22

El ve Ses23

Yeni olan nedir?23

Yüz, Ses ve Dudak Hareketi Entegrasyonu23

Giyilebilir Biyometri Sistemi24

ATM Kartlarında Parmak İzi Çipi 24

Kişisel Kimlik Doğrulama25

Diğer Yeni Şeyler25

Microsoft Faktörü26

Standartlaştırma Sorunları 26

Seçim Kriterleri27

Sonuç27

**Siteler arası komut dosyası çalıştırma (xss)** 28

**BİYOMETRİK TEKNOLOJİ İLE GÜVENLİĞİ ARTTIRMA**

**Giriş**

ABD Göçmenlik ve Vatandaşlığa Kabul Hizmeti, ziyaretçinin elinin elektronik olarak okunması için ziyaretçinin eliyle elektronik okumalarını alarak, belli büyük havalimanlarında sık sık Amerika Birleşik Devletleri'ne seyahat edenlerin kişisel görüşme ve inceleme sürecini atlamasını sağlayacak bir program başlattı. Benzer bir sistem Sınırdan geçen insanları tanımlamak için parmak izi ve ses tanıma kullanan ABD / Kanada sınırında kullanılıyor.

1991 yılında Los Angeles County, ülkenin refah sistemindeki hileli ve çift hak taleplerini azaltmak için parmak izi tanıma kullanan bir sistem kurdu. İlçe, ilk altı ayda 5 milyon dolardan fazla tasarruf sağladı.

Las Vegas'tan Atlantic City'ye kadar olan casinolar, kayıpları azaltmak ve lisanslarını korumak amacıyla kumar hilelerini, kart sayaçlarını ve suçluları bulmak için yüz tanıma sistemlerini kullanıyor.

Bütün bu sistemler ortak bir noktaya sahiptir: hepsi insanların, yerlerin veya finansal çıkarların daha fazla güvenliğini sağlamak için biyometri kullanır. Biyometri, güvenlik alanındaki en hızlı büyüyen segmentlerden biri haline geliyor ve hem popüler basında hem de güvenlik mesleğinde büyük bir popülerlik kazandı. Biyometri kullanımı - nasıl çalıştığı, nasıl kullanıldığı ve ne kadar etkili olabileceği - bu bölümün konusudur.

**Biyometri Temelleri (Biometrics Basics)**

Yunan kökenli olan “biyometri” kelimesi kelimenin tam anlamıyla “yaşamın ölçülmesi” anlamına gelmektedir. Daha pratik kullanımda, biyometri biyolojik bilgiyi ölçme ve analiz etme bilimidir. Biyometri kullanımı, canlıların (tipik olarak insanın) çeşitli yönlerinin ölçümlerini almayı, bu ölçümler üzerinde analitik yargılarda bulunmayı ve bu yargılara dayanarak uygun önlemleri almayı içerir. En tipik olarak, bu kararlar ölçümün konusunu doğru bir şekilde tanımlamaya yardımcı olur. Örneğin, kolluk görevlileri suçluları tanımlamak için parmak izi biyometrikini kullanır. Bir şüphelinin parmak izleri olay yerinde toplananlara karşılık gelirse, şüpheli daha fazla sorgulama için tutulabilir. Parmak izleri eşleşmezse, şüpheli serbest bırakılabilir. Başka bir örnekte, güvenlik kameraları kalabalığın yüzlerini bir futbol stadyumunda tarayabilir, ardından taranan görüntüleri terörizmle ilişkili olduğu bilinen kişilerin veri tabanına karşı eşleştirebilir. Kalabalıktaki yüzlerden biri veri tabanında ki bir yüzle eşleşirse, polis bu kişiyi gözaltına almak için harekete geçebilir. Böyle bir sistem, Florida Tampa Bay'deki 2001 Super Bowl'da kullanıldı. Sistem, kalabalığın sabıka kaydı olan 19 kişisini tanımladı.

Güvenlik uzmanları, kimlik kartları, şifreler, PIN'ler ve akıllı kartlar dahil, kendilerine sunulan çok çeşitli kimlik ve kimlik doğrulama seçeneklerine sahiptir. Öyleyse neden biyometri farklı ve neden çoğu kişi tarafından doğru tanımlama ve doğrulama için “en iyi” yöntem olarak kabul ediliyor? Cevap, tanımlamanın ve doğrulamanın niteliğinden gelir. Her iki süreç de özgünlük (*uniqueness*) kavramına dayanıyor. İzole edilebilecek ve bu kişiyi pozitif olarak tanımlamak için kullanılabilecek bir kişinin kendine özgü bir yönü olduğunu varsayarlar. Bununla birlikte, mevcut tanımlama ve kimlik doğrulama biçimlerinin hepsi aynı yanlışlıktan muzdariptir: ölçtükleri “benzersiz” özellik bireye yapay olarak bağlanmaktadır. Kullanıcı kimlikleri ve parolalar kullanıcılara atanır ve kullanıcı tarafından hatırlanması gerekir. Kimlik rozetleri veya jetonları, daha sonra bulundurmaları gereken kullanıcılara verilir. Sürücü ehliyetleri, pasaportlar veya X.509 genel anahtar sertifikaları gibi sertifika kimlik doğrulama formları, bir kişiye sertifikadaki ad ile sertifikanın adı arasındaki resim veya genel anahtar arasındaki eşleşmeyi onaylayan bir yetkili tarafından atanır. Bunların hiçbiri, adlandırılan bireyi yanlış tanımlamaz veya doğrulamaz. Hepsi bir şekilde ya da başka şekilde kandırılabilir veya “taklit” edilebilir.

Biyometri, benzersizlik sorununa farklı bir şekilde yaklaşmaktadır. Özneye yapay olarak bir tür benzersizlik eklemek yerine, özgünlük, özne zaten sahip olduğu içsel bir kalite ile belirlenir. Parmak izleri, retina desenleri, el geometrisi ve DNA gibi özellikler hemen hemen tüm insanların zaten sahip olduğu ve hepsi doğal olarak benzersiz olan bir şeydir. Aynı zamanda, her zaman kişiyle birlikte olan ve böylece gerektiğinde uygun olan bir şeydir. Bir kullanıcı parmağını unutamaz veya sesini evde bırakamaz. Biyometrik özelliklerin benzersiz olmaları da kendine özgü bir güce sahiptir. Bir kişi zayıf bir biyometrik seçemez, zayıf bir şifre veya PIN seçebilir. Çok yüksek güvenlikli uygulamalar veya tanımlama veya doğrulama için son derece yüksek bir güvence seviyesinin gerekli olduğu durumlar için, bu yerleşik benzersizlik, biyometriye geleneksel tanımlama ve onaylama meslektaşları üzerinde ihtiyaç duyduğu üstünlüğü sağlar.

**Biyometri Nasıl Çalışır? (How Does Biometrics Work?)**

Biyometri arkasındaki fizyoloji oldukça karmaşık olsa da, bir uygulamada biyometrik ölçümlerin kullanılması süreci nispeten basittir. İlk adım, ölçülmesi gereken spesifik biyometrik özelliklerin belirlenmesidir. Bu, katı bir teknoloji sorusundan çok pratiklik, kişisel tercih ve kullanıcı tutumunun bir işlevidir. Uygun bir biyometrik ölçüm seçmeye giren farklı faktörler bu bölümde daha sonra ele alınmaktadır.

Ölçülecek olan spesifik özellik belirlendikten sonra, biyometrik bir okuma bazı mekanik veya teknik araçlarla alınır. Özel araçlar seçilen biyometrik özelliğe dayanacaktır, ancak biyometrik okumalar genellikle (1) bir karakteristiğin bir görüntüsünün fotoğraflanması veya taranması veya (2) konunun içindeki karakteristiğin yaşam işaretlerinin ölçülmesi yoluyla alınır. Okuma alındıktan sonra, daha fazla karşılaştırmayı kolaylaştıran bir forma dönüştürülmesi gerekir. Tüm taranan veya okunan görüntünün binlerce kişi için saklanması büyük miktarda depolama alanı kaplar ve tüm görüntünün karşılaştırma için kullanılması verimsizdir. Gerçekte, görüntünün sadece küçük bir kısmı, doğru karşılaştırma için gerekli olan önemli bilgileri içerir. Bu önemli bitlere eşleşme noktaları denir. Yalnızca eşleşme noktalarını belirleyerek ve toplayarak, biyometrik ölçümler doğru şekilde yapılabilir ve veri depolama gereksinimleri önemli ölçüde azaltılabilir.

Eşleşme noktaları, şablon adı verilen standart bir formatta toplanır. Şablon, sistemde depolanan veya kullanıcılardan toplanan diğer şablonlarla daha fazla karşılaştırma yapmak için kullanılır. Şablonlar, daha sonra alınması ve biyometrik uygulamanın kullandığı veri depolama sisteminde karşılaştırılması için saklanır. Daha sonra, bir kullanıcının tanımlanması veya doğrulanması gerektiğinde, konuyla ilgili başka bir biyometrik okuma alınır. Şablon bu yeni taramadan çıkarılır ve veritabanında depolanan bir veya daha fazla şablonla karşılaştırılır. Eşleşen bir şablonun varlığı veya yokluğu sistem tarafından uygun bir yanıtı tetikleyecektir.

**Biyometrik Özellikler (Biometric Traits)**

Tüm biyometrik sistemler, üç farklı insan özelliği türünden birine dayanmaktadır. Genotipik özellikler, bireyin genetik yapısına göre tanımlananlardır. Genotipik (Genotypic) özelliklerin örnekleri yüz geometrisi, el geometrisi ve DNA kalıplarıdır. Tek yumurta ikizleri veya klonları arasında bulunan genotipik özelliklerin çok benzer olduğunu ve ikisini birbirinden ayırmak için ayırt edici bir özellik olarak kullanmanın zor olduğunu not etmek ilginçtir.

Randotipik (Randotypic) özellikler, embriyonun gelişmesinde erken oluşan özelliklerdir. İnsanların sahip olduğu vücut özelliklerinin çoğu, bu gelişim aşamasında belirli kalıpları üstlenir ve bu kalıplar tüm popülasyon boyunca rastgele dağıtılır. Bu, çoğaltmayı oldukça olanaksız kılar ve bazı durumlarda imkânsız hale getirir. Randotipik özelliklerin örnekleri parmak izleri, iris düzenleri ve el damar düzenleridir.

Davranışsal (Behavioral) özellikler, bir kişinin eğitim veya tekrarlanan öğrenme yoluyla geliştirilen özellikleridir. İnsanlar geliştikçe yaşamları boyunca taşıdıkları belirli davranış biçimlerini öğrenirler. İlginçtir ki, davranışsal özellikler, bir kişi tarafından yeniden eğitim veya davranış değişikliği ile değiştirilebilen tek tip biyometrik özelliktir. Davranışsal özelliklere örnek olarak imza dinamikleri ve klavyeyle yazma kalıpları dâhildir.

**Biyometri için Ortak Kullanımlar (Common Uses for Biometrics)**

Biyometri bilimi ve uygulaması hem güvenlik hem de güvenlik dışı amaçlar için çeşitli kullanımlar bulmuştur. Bireylerin kimlik doğrulaması en popüler kullanımlardan biridir. Örneğin, el tarayıcıları yüksek güvenlikli bir binaya erişmeye çalışan kişilerin kimliğini doğrulamak için kullanılabilir. Öznenin alınan biyometrik okuması daha sonra veritabanındaki o kişiye ait tek kayıtla karşılaştırılır. Bu formda kullanıldığında, biyometrik kimlik doğrulama genellikle pozitif eşleştirme veya bire bir eşleme (positive matching or one-to-one matching) olarak adlandırılır.

Çok sık olarak, ihtiyaç duyulan tek şey, çok sayıda olası konudan belirli bir konunun temel tanımlanmasıdır. Londra'nın Newham ilçesindeki polis, ilçeden geçen insanların yüzlerini taramak için ilçeye monte edilmiş 140 kameradan oluşan bir sistem kullanıyor. Bu yüzler, herhangi birinin Newham’ın sokaklarında dolaşıp dolaşmadığını görmek için bilinen suçluların bir veritabanıyla karşılaştırıldı. Bu özel kullanımda, biyometrik sistem negatif eşleştirme veya birden çok eşleştirme gerçekleştiriyor. Pozitif eşleştirmede kullanılan tek kayıt aramasının aksine, Newham kameraları tarafından taranan her örnek yüz polis veri tabanındaki tüm kayıtlarla karşılaştırılarak olası bir eşleşme aranıyor. Aslında, sistem belirli bir yüzün veritabanında olmadığını (ve muhtemelen tanımlanmış bir suçlu olmadığını) göstermeye çalışıyor.

Sahtekârlık önleme biyometri için başka bir yaygın kullanımdır. Bir kullanıcı bir sisteme erişmek için biyometrik kimlik doğrulaması yaptığında, kullanıcının kimliği daha sonra kullanıcının gerçekleştirdiği her olay, etkinlik ve işlemle ilişkilendirilir. Sahte bir işlem tespit edilirse veya sistem bir soruşturmaya veya denetime tabi tutulursa, yasadışı faaliyete katılımlarını onaylayan veya reddeden bir kullanıcının eylemlerinin denetim izi oluşturulabilir. Sistemi kullanan personel kimlik etiketleme ve denetleme izlerinden haberdar edilirse, biyometri kullanımı sahtekârlığı ve kötüye kullanımı önlemek için caydırıcı olabilir.

Biyometri, temel erişim kontrolü olarak da kullanılabilir. Bireylerin tanımlarını geçmelerine izin verilmeden zorlayarak yüksek güvenlikli bölgelere erişimi kısıtlama mekanizması. Biyometri, genel olarak yalnızca fiziksel güvenlik erişim kontrolü rolündeki tanımlama için kullanılır. Diğer erişim kontrolü uygulamalarında, biyometri bir kimlik doğrulama mekanizması olarak kullanılır. Örneğin, kullanıcıların gizli veya özel bilgileri görüntülemelerine veya değiştirmelerine izin verilmeden önce kendilerini biyometrik olarak doğrulamaları gerekebilir. Normalde, fiziksel erişim kontrolünde bile, kişinin kendini tanımlayabildiği (ismini belirterek veya bir miktar fiziksel kimlik bilgisi sunarak) ve sistemin hızlı bir şekilde pozitif eşleştirme yapmasını sağladığı zaman bir eşleşme için veritabanında arama yapmak verimli değildir.

Daha az güvenlik odaklı bir biyometri kullanımı, bir kuruluşun müşteri hizmetlerini iyileştirmektir. Bir süpermarket, ödeme hattındaki müşterileri tanımlamak için yüz tanıma özelliğini kullanabilir. Müşteriler tanımlandıktan sonra, uygun “sık alışveriş yapan” indirimler verilebilir, kredi kartlarını otomatik olarak tahsil ettirebilir ve gelecekte müşterilere daha fazla kişisel hedefli satışlar ve özel ürünler sunmak için alışveriş kalıplarını analiz ettirebilir - hepsi de müşteriye ihtiyaç duymadan Shopper’ın Club kartını gösterin ya da kredi kartını kaydırın. Bu tür bir kullanımın mahremiyet yönünü bir kenara bırakarak (şimdilik), bu kişiselleştirilmiş müşteri hizmetleri uygulaması, oldukça rekabetçi pazarlardaki tüketici odaklı şirketler için çok arzu edilebilir.

**Biyometrik Ölçüm Faktörleri (Biometric Measurement Factors)**

Ölçüm, mekanik üreme ve analiz içeren herhangi bir işlemde olduğu gibi, burada sürecin başarısına veya başarısızlığına katkıda bulunan birçok faktör vardır. Bu faktörlerin tümü iki genel kategoriye ayrılır: ölçülen özelliklerin özellikleri ve ölçüm sürecinin özellikleri.

**Karakteristik özellikleri (Characteristic Properties)**

Biyometrik ölçüm için belirli bir özelliğin uygun olup olmadığını belirlemek için en önemli gereksinim benzersizliktir (uniqueness). Spesifik özellik, konu popülasyondaki her birey için ölçülebilir şekilde benzersiz olmalıdır. Bunun bir sonucu olarak, karakteristik ölçülen belirli bir kişiye özgü karşılaştırma noktaları üretebilmelidir. Bu benzersiz özellik esastır, çünkü aynı özelliklere sahip iki kişi, bir diğerinin olduğuna inanmak için ölçüm sistemini kandırabilir.

Karakteristik, ölçülen popülasyondaki tüm bireylerde bulunan evrensel olmalıdır. Bu ilk bakışta kolay olabilir, çünkü herkes parmak izi, herkesin DNA'sı ve herkesin sesi var. Yoksa onlar mı? Bir biyometrik ölçüm sistemi kurarken, güvenlik pratisyenlerinin, ölçülen popülasyonun belirli bir özelliği olmayan bir bölümünün olacağı gerçeğini göz önünde bulundurmaları gerekir. Örneğin, insanlar kazalara ve hastalıklara karşı parmaklarını kaybederler ve bazı insanlar konuşamaz. Bu insanlar için, parmak izi analizi veya ses tanıma, geçerli bir biyometrik mekanizma olarak çalışmaz. Belirli bir popülasyondaki bu niteliklere sahip olmayan insan sayısı çok azsa, bu vakalarla başa çıkmak için alternatif prosedürler ayarlanabilir. Sayı göreceli olarak büyükse, alternatif bir biyometrik yöntem veya hatta tamamen farklı bir güvenlik mekanizması dikkate alınmalıdır.

Evrensellik konusunda belirli bir biyometrik düşünülürken, güvenlik pratisyeni ayrıca kültürel düşünceleri de dikkate almalıdır. Belirli bir hedef popülasyona göre ayarlanmış bir ölçüm sistemi diğer ırk, etnik veya cinsiyet gruplarıyla iyi performans göstermeyebilir. Örneğin, bir şirketin doğru bir sesli yazı almak için kullanıcıların birkaç standart kelime konuşmasını gerektiren bir ses tanıma sistemi kullandığını varsayalım. Sistem, New York'lular (sistemin kullanıldığı yerlerde) tarafından konuşulan kelimeleri açıkça anlayacak şekilde ayarlanmışsa, bölgeye aktarılan derin bir Güney Amerika aksanı olan bir çalışan, standart kelimeleri söylerken tanınmakta zorluk çekebilir. Benzer şekilde, bazı kültürlerde nesnelerin dokunma ile ilgili gelenekleri ve aynı cihazın (el tarayıcı veya parmak izi okuyucusu gibi) paylaşılan kullanımına ilişkin sağlık endişeleri vardır. Kullanıcının okuma cihazıyla temas etmesini veya fiziksel olarak etkileşmesini gerektiren bir biyometrik sistem kurarken, bu tür hususların ele alınması gerekir.

Biyometrik bir özellik için bir diğer önemli özellik ise kalıcılıktır. Karakteristik, bireyin kalıcı bir parçası olmalı ve birey, ağır kişisel zarar veya tehlikeye neden olmadan, karakteristiği çıkaramaz veya değiştiremez. Bu kalıcılık özelliği zaman içinde de geçerlidir. Karakteristik zaman içinde önemli ölçüde değişmemelidir, aksi halde desen eşleşmesini yanlış hale getirir. Bu yönün birkaç ilginç sonuçları vardır. Örneğin, küçük çocukların fizyolojisi büyüme yıllarında oldukça hızlı bir şekilde değişmektedir, bu nedenle küçükken ölçülen ses veya yüz özellikleri sadece birkaç yıl sonra geçersiz olabilir. Aynı şekilde, fiziksel özellikleri ameliyat veya kaza sonucu yaralanma sonucu hasar görmüş olan yaşlı insanlar da iyileşmek için alışılmadık derecede uzun zaman alabilir, bu da herhangi bir fiziksel ölçümü en azından bir süre için yanlış yapar. Hamilelik, kadının gözünün arkasındaki kan damarlarının değişmesine neden olur, böylece retina taraması kullanılıyorsa yeniden kayıt yapılması gerekir. Son olarak, el yazısı imza kalıpları, insanlar yaşlandıkça veya düzenli olarak imzalamaları gereken belge sayısıyla ilişkili olarak zaman içinde değişir. Bu durumlar, biyometrik sistemin parçası üzerinde daha fazla sayıda yanlış reddedilmeye yol açacaktır. Bu tür sorunlardan kaçınmak için, sistemdeki her birey için periyodik olarak temel bir ölçüm yapmak yeniden avantajlı olabilir.

Kalıcılığa ek olarak, karakteristik değiştirilemez olmalıdır. Bir kişinin biyometrik sistemde bir hata durumuna neden olmadan veya konuyla ilgili zarar veya risk sunmadan karakteristiği değiştirmesi mümkün olmamalıdır. Örneğin, bir kişinin DNA'sını değiştirmek mümkün değildir. Ve birine yeni parmak izlerini vermek (teorik olarak mümkün olsa da (deri grefti veya rakam nakli yoluyla) mümkün olsa da, çoğu insan çoğu uygulama için güçlü bir tehdit olarak değerlendirilemeyecek kadar aşırı ve tehlikeli olduğunu düşünür.

Özelliğin bir tür kayıt cihazı tarafından yakalanması veya başka şekilde tanınması kabiliyetine sahip olması önemlidir. Bu özellik, bu özelliği (ve eşleşme noktalarını) insan veya teknik araçlarla okunabilir ve anlaşılabilir bir forma dönüştürebilen standart (belki de uzmanlaşmış) bir giriş cihazı ile ölçülebilir olmalıdır.

Herhangi bir biyometrik özelliğin nihai önemli özelliği, doğrulanabilmesidir. Bir bireyin özelliği, diğer konularda bulunan benzer özelliklerle eşleştirilebilmeli ve sunulan ölçüm ve eşleşme puanlarına dayanarak kesin bir pozitif veya negatif eşleşme sağlanabilmelidir.

**Ölçüm Özellikleri (Measurement Properties)**

Önceki bölüm, biyometride kullanılan çeşitli biyolojik özelliklerin özelliklerini ele alıyordu. Bununla birlikte, bir biyometrik sistemin başarısının veya başarısızlığının büyük bir kısmı ölçüm ve analiz sürecinde yatmaktadır. Sürecin en önemli yönlerinden biri doğruluktur. Herhangi bir izleme veya gözetim sisteminde olduğu gibi, biyometrik sistemin doğru ölçümler alması ve söz konusu özelliğin doğru bir gösterimini yaratması kritik önem taşır. Benzer şekilde, sistemin ölçümden ürettiği şablon, söz konusu karakteristiği doğru bir şekilde göstermeli ve sistemin diğer şablonlarla doğru karşılaştırmalar yapmasına izin vermelidir.

Sistemin şablon üretme ve bu şablonları daha sonra değerlendirmede kullanma yeteneği zaman içinde tutarlı olmalıdır. Ölçüm işlemi, karakteristiği belirsiz bir süre boyunca (zorunlu olarak zorunlu olmasa da) kesin bir şekilde ölçebilmeli ve değerlendirebilmelidir. Örneğin, bir çalışan işin ilk gününde yüz tarama sistemine kaydolduysa, bu tarama sistemi bu çalışanı tüm çalışma süresi boyunca doğru bir şekilde (yaşlanmanın, yüz kıllarının uzaması, büyümesi veya çıkarılması ve hatta zaman zaman kırılan burun oluşumu gibi) doğrulayabilmelidir.

Biyometrik sistemler, insan özelliklerinin incelemelerine dayandığından, sadece karakteristiğin özelliklerini veya eşleşme noktalarını kontrol etmenin aksine, sistemin karakteristiğin kaynağını doğrulaması önemlidir. Örneğin, sistem yüz geometrisini ölçüyorsa, konunun yüzünü fotoğraf makinesine doğru tutarak görüntünün gerçek bir kişiden olduğuna inanmak için onu kandırabilir mi? Bir parmak izi sistemi kullanılıyorsa, sistem parmağın canlı bir insana takılı olup olmadığını kontrol eder mi? (Bu, sanıldığı kadar zor değildir!) Vücut ısısı, kan akışı, hareket ve ses tonlaması gibi özelliklerin kontrol edilmesi, sistemin gerçek ürün ile mekanik bir üreme arasında ayrım yapmasına yardımcı olabilir.

Son olarak, ölçüm sistemi, biyometrik okumaların doğruluğuna etki edebilecek çevresel faktörlerin etkisini azaltmaya çalışmalıdır. Bunun bir örneği, yüz tarayıcılarının doğru yerleştirilmesi olabilir, böylece güneş ışığı veya parlama kameraları etkilemez. Parmak izi sistemleri, baskı okuyucunun lekelenmemesini veya kirlenmemesini sağlamak için mekanizmalar kullanmalı, böylece doğru ölçümler yapabilme yeteneğini etkilemelidir. Sesli eşleştirme sisteminin doğruluğu, kalabalık veya gürültülü bir kamu ortamında çalıştırılması durumunda tehlikeye girebilir. Tüm bu faktörler başarılı bir biyometrik operasyona karşı çalışır ve planlama aşamalarının başında herkes göz önünde bulundurulmalı ve ele alınmalıdır.

**Biyometrik Ölçüm (Biometric Measurement)**

Her ne kadar biyometri arkasındaki bilim ve teknoloji son yıllarda büyük ölçüde iyileşmiş olsa da, kusursuz değildir. Biyometrik cihazlar tarafından alınan ölçümlerin ve biyometrik özellikler arasında yapılan karşılaştırmaların kesin, yüzde 100 hatasız doğruluğu ne gerçekçidir ne de beklenemez. Bu nedenle, bir biyometrik sistemin uygulayıcılarının teknolojinin sınırlarını anlamaları ve olası hataya neden olabilecek durumları azaltmak için uygun adımları atmaları gerekir. Biyometrik sistemler, tüm güvenlik sistemleri gibi, kurulumun özel ihtiyaçlarına bağlı olarak “ayarlanmalıdır” ve kullanım ve çalışma ortamındaki gerçek dünyadaki farklılıkları hesaba katmalıdır.

**Ölçüm özellikleri (Measurement Characteristics)**

Benzer olup olmadıklarını (ve benzerliğin ne kadar uzadığını) belirlemek için biyometrik şablonları karşılaştırma işlemine eşleştirme denir. Eşleştirme işlemi, sunulan şablonun veri tabanında bulunan bir şablonla ne kadar iyi (veya ne kadar zayıf) karşılaştırıldığını gösteren bir skorla sonuçlanır. Her biyometrik sistem için, sistemin “başarılı” bir sonuç vermesi için karşılanması gereken özel bir eşik vardır. Bu eşleşme için üretilen puan eşiğin üstüne düşerse, şablon kabul edilir. Puan eşiğin altına düşerse, şablon reddedilir. Eşik değeri tipik olarak sistemin yöneticileri veya operatörleri tarafından ayarlanır ve operatörün istediği hassasiyet derecesine bağlı olarak ayarlanabilir.

İronik olarak, bir kullanıcı tarafından normal sistem kullanımı sırasında üretilen şablon ve bu kullanıcı için sistemde depolanan şablon nadiren tamamen aynı bir eşleşmeyle sonuçlanmalıdır. Biyometrik sistemlerde kullanıcı “oturumları” arasında her zaman bir miktar değişiklik (ancak küçük) vardır ve bu değişiklik dereceleri sistemin genel eşik ayarında dikkate alınmalıdır. Sunulan bir şablon ile depolanan arasında tamamen aynı bir eşleşmenin tespiti Şablon (örneğin, bir davetsiz misafir okuyucu çıktısının dijitalleştirilmiş bir kopyasını alırsa ve ardından kopyayı eşleştirme işlemine besleyerek okuyucuyu atlarsa) kurcalamanın veya mekanik olarak çoğaltılan biyometrik özelliklerin kullanılmasının bir göstergesi olabilir.

**Hata Yapan Faktörler (Error-Producing Factors)**

Başlangıçta bir kişinin özelliklerini ölçme, bir şablon oluşturma ve bu şablonu bir sistemde saklama işlemine kayıt denir. Kayıt sürecinde, sistem konunun biyometrik özelliğini “öğrenir”. Bu öğrenme süreci, farklı koşullar altında karakteristiğin çeşitli okumalarını içerebilir. Sistem konuyla daha fazla tecrübe kazandıkça, karakteristiğin sunulabileceği çeşitli yolları öğrenir ve bu kullanıcı için depolanan şablonu iyileştirir. Ardından, gerçek işlem sırasında bu bilgiyi, karakteristiğin sunulma şeklindeki varyasyonları hesaba katmak için kullanır.

Kayıt sürecinin performansının sistemin genel doğruluğu üzerinde büyük etkisi olabilir. Kayıt işleminin yalnızca ideal koşullar altında (örneğin, iyi ışıklandırılmış sessiz bir odada) değil, aynı zamanda en uygun koşulların altında (örneğin, arka plan gürültüsü veya düşük ışıklandırma) altında yapılması hayati önem taşır. İyi yapılmış bir kayıt, normal kullanım sırasında sistem tarafından yapılan karşılaştırmaların doğruluğunu arttırır ve yanlış okuma olasılığını büyük ölçüde azaltır. Kayıt işleminde hatalar ortaya çıkarsa, kullanıcının daha sonraki sistem işlemleri sırasında kullanıcının doğrulanmasında hatalara neden olabilir veya aşırı koşullarda, bir sahtekârın sistem tarafından kabul edilmesine izin verebilir.

Biyometrik bir sisteme girilen hataların tümü mekanik arızalardan veya teknik hatalardan kaynaklanmamaktadır. Sistemlerin kullanıcıları, biyometrik sistemlerin karşılaştığı sorunların çoğuna neden olur. İnsanlar yeni ve farklı durumlara kolayca adapte olabiliyorlar ve yeni davranış modlarını makinelerden çok daha kolay öğrenebiliyorlar. Bir biyometrik sistemin bu değişimi nasıl ele aldığı genel etkinliğinde önemli bir rol oynayacaktır.

Örneğin, bir biyometrik sistem ilk kez devreye alındığında, kullanıcılar karakteristiklerini sisteme nasıl doğru bir şekilde sunacaklarından emin olmayabilirler. Doğru bir göz taraması yapabilmek için kafalarını nasıl tutmalılar? Parmaklarını okuyucuya nasıl yerleştiriyorlar, böylece doğru bir parmak izi okuması alınabiliyor mu? Sistemdeki bu ilk deneyimsizlik (ve olası rahatsızlık), kullanıcı popülâsyonu arasındaki sıkıntı ile birlikte çok sayıda yanlış okumaya yol açabilir. Kullanıcılar tarafındaki doğal tepki, sistemi daha da zorlaştıran kullanıcı olduğunda, yanlışlıklar için sistemi suçlamak olacaktır.

Zaman geçtikçe ve kullanıcılar sisteme daha aşina hale geldikçe, bilgilerini daha doğru ölçümlere yol açacak şekilde sunmaları şart koşulacak. Bu şartlandırma, ölçüm için kendilerini nasıl sunacaklarını öğrenirken doğal ve bilinçaltı olarak gerçekleşecektir. Aslında, kullanıcılar sistem tarafından nasıl okunacağını öğrenirler. Bu, sistemin verim oranını hızlandırma ve daha az yanlış okumaya neden olma etkisine sahiptir.

Kullanıcı davranışı ve fizyoloji de süreçte bir rol oynamaktadır. İnsanlar günleri, haftaları ve ayları boyunca ilerledikçe, fizyoloji ve psikolojilerinde düzenli döngüleri yaşarlar. Bazı insanlar günün erken saatlerinde daha uyanık ve dikkatlidir ve gün ilerledikçe görünür yorgunluk belirtileri gösterir. Diğerleri, öğle saatlerine ve hatta akşama kadar fiziksel doruklarına ulaşmıyor. Mevsimsel değişiklikler bazı insanlarda fizyolojik değişikliklere neden olmaktadır ve yapılan araştırmalar, kış aylarında kısa günlerden dolayı birçok insanın depresyonda olduğunu göstermiştir. Yorgunluk veya stres aynı zamanda bir kişinin fizyolojik yapısını da değiştirebilir. Bu döngüsel değişiklikler, gerçekleşebilecek herhangi bir biyometrik okumayı potansiyel olarak etkileyebilir.

Bir işlemin önemi ayrıca kullanıcı davranışını ve biyometrik okumaların yapılmasına yönelik tutumunu da etkiler. İnsanlar daha önemli, kritik, hassas veya değerli işlemler için biyometrik örneklemeye katılmaya çok isteklidir. Teknik olmayan örnekler bile bunun doğru olduğunu gösteriyor. Ortalama bir insan daha fazla zaman alacaktır ve 10 dolarlık çekten 100.000 dolarlık bir çek imzalamaya özen gösterecektir.

**Hata Oranları (Error Rates)**

Herhangi bir biyometrik sistemde, sistemin genel doğruluğunu etkileyen istatistiksel hata oranları vardır. Yanlış Reddetme Oranı (FRR- False Rejection Rate), meşru sistem kullanıcılarının reddedilme ve geçersiz kullanıcılar olarak kategorize edilme oranıdır. Yanlış reddetme, Tip I Hatası veya Yanlış Negatif olarak da bilinir(Type I Error , False Negative). Yanlış Reddetme Oranı hesaplaması için genel formül:

False Rejection Rate = NFR/NEIA (tanımlama sistemleri için)

Or

False Acceptance Rate = NFR/NEVA (kimlik doğrulama sistemleri için)

where:

NFR = Number of false rejections (Yanlış reddetme sayısı)

NEIA = Number of enrollee identification attempts (Kayıtlı kişi tespiti girişimi sayısı)

NEVA = Number of enrollee verification attempts (Kayıtlı doğrulama girişimlerinin sayısı)

Yanlış Kabul Oranı (FAR-False Acceptance Rate), gayri meşru olmayan kullanıcıların sistem tarafından yasal olarak kabul edildiği ve geçerli kullanıcılar olarak sınıflandırıldığı orandır. Yanlış kabul, aynı zamanda Tip II Hatası veya Yanlış Olumlu (*Type II Error* or a *False Positive*) olarak da bilinir. Yanlış Kabul Oranını hesaplamanın genel formülü şudur:

False Acceptance Rate = NFR/NEVA (kimlik doğrulama sistemleri için)!!!!!!!!

Or

False Rejection Rate = NFA/NIVA (kimlik doğrulama sistemleri için) !!!!!!!

where:

NFA = Number of false acceptances (Yanlış kabullerin sayısı)

NEIA = Number of imposter identification attempts (Sahtekâr tanıma girişimi sayısı)

NEVA = Number of imposter verification attempts (Sahtekâr doğrulama girişimleri sayısı)

Herhangi bir biyometrik sistem hakkında bilinmesi gereken son istatistik Eşit Hata Oranı (EER- Equal Error Rate) olarak da bilinen Çapraz Hata Oranıdır (CER- Crossover Error Rate). Bu, Yanlış Reddetme Oranının ve Yanlış Kabul Oranının, nüfusun büyüklüğüne eşit olduğu noktadır. Yani, sistem yanlış negatiflerin oranı ve sistem tarafından üretilen yanlış pozitiflerin oranı yaklaşık olarak eşit olacak şekilde ayarlanmıştır. İdeal olarak amaç, hem en az yanlış negatif hem de yanlış pozitif üretmek için sistemi Çapraz Hata Oranını mümkün olduğunca düşük tutacak şekilde ayarlamaktır. Ancak, bunun nasıl yapılacağına dair kesin bir kural yoktur ve sistemin hassasiyetinde yapılan değişiklikler her iki faktörü de etkiler. Sahte pozitifleri azaltmak amacıyla sistemi daha sıkı tanımlama için ayarlamak, hatalı ölçümlere neden olacaktır, çünkü sistem tarafından alınan şüpheli ölçümler kabulden ziyade reddedilme eğilimindedir. Aynı şekilde, sistemi sorgulanabilir okumaların daha fazla kabul edilmesi için ayarlarsanız (örneğin, müşteri hizmetlerini iyileştirme çabasıyla), daha fazla yanlış pozitif okuma olasılığını artırırsınız.

Son olarak, her biyometrik sistem için, Kayıt Oranı Arızası var veya FTE(Failure To Enroll rate). FTE, verilen bir kullanıcının sisteme kayıt olamaması olasılığıdır. Bu, sistemdeki hatalardan ya da kullanıcının biyometrik karakteristiğinin yeterince benzersiz olmadığı veya ölçülmesinin zor olmasından kaynaklanabilir. Biyometrik veri sağlayamayan kullanıcılar (örneğin, ampute ya da konuşamayanlar), genellikle sistemin FTE oranında sayılmaz.

**Uygulama sorunları (Implementation Issues)**

Son derece teknolojik yöntemler kullanan diğer tüm otomatik sistemler gibi, biyometrik sistemlerde kullanılan teknoloji de o sistemin genel etkinliğinde sadece bir rol oynamaktadır. Eşit derecede önemli olan bir diğer parça, bu teknolojinin sistemde nasıl uygulandığı ve kullanıcıların teknoloji ile nasıl etkileşime girdiğidir. Son teknoloji teknolojisi, eğer kötü uygulanırsa ya da sistemin kullanıcıları, kullanımına karşı dirençli (veya hatta düşmanca) ise, çok az kullanılır.

Önemli bir faktör, bir biyometrik sistem kullanıcılarının göreceli özerkliğidir. Bu, kullanıcıların biyometrik tanımlamayı kullanan bir sisteme katılmaya direnme veya reddetme yeteneklerini ifade eder. Genel olarak, şirket çalışanları (veya sözleşmeye bağlı zorunluluklarla bağlı olanlar) sistemi istihdam veya sözleşmelerinin bir şartı olarak kullanmaya ikna edilebilir veya zorlanabilir. Direnebilmelerine veya protesto etmelerine rağmen, çok az ricaları veya alternatifleri var. Öte yandan, genel halkın üyeleri, müdahaleci olduğunu veya kişisel mahremiyetlerini çok fazla ihlal ettiğini düşündükleri bir biyometrik sisteme katılımdan vazgeçme kabiliyetine sahipler. Bu kullanıcıların her biri “riske karşı kazanç” kararı verir ve sisteme katılıp katılmamaya karar verir.

Bazı kullanıcılar, fiziksel olarak rahatsız edici olduğunu düşündükleri bir biyometrik sistem kullanmaya direneceklerdir. Bazı biyometrik teknolojiler (örneğin, retina taramaları veya parmak izi okumaları) kullanıcılar üzerinde fiziksel olarak daha fazla etkilemektedir. Ses tanıma veya yüz tanıma gibi diğer teknolojiler sosyal olarak daha kabul edilebilir çünkü kişisel yakınlık riskini daha az etkiliyor ve kullanıcının fiziksel olarak herhangi bir şeye dokunmasını gerektirmiyor. Daha önce de belirtildiği gibi, kişisel dokunuşla ilgili veya kişisel görüntülerin yakalanması ile ilgili kültürel hususlar, müdahaleci olma konusunda da önemli bir rol oynamaktadır. Genel olarak, belirli bir biyometrik teknoloji ne kadar fiziksel olarak müdahaleci olursa, o kadar çok kullanıcı kullanımına direnecek ve aynı zamanda daha yüksek hata oranları üretebilecektir, çünkü rahatsız kullanıcılar ölçüm için kendilerini uygun şekilde sunmaya hazır olma şartına sahip olmayacaktır.

Kullanıcının sistemin nasıl kullanıldığına dair algısı, sistemin etkinliğinde de önemli bir rol oynar. Kullanıcılar, kullanımlarının arkasındaki motivasyonu anlamak isterler. Sistem sahibi “kötü adamları” yakalamak istiyor mu? Bu durumda, kullanıcılar, mal sahibinin gözünde potansiyel şüpheli olduklarını hissedebilir ve bunlardan birini “yakalama” denemelerine kibarca bakmayacaklardır. Öte yandan, sistemi kullanan insanları korumak ve izinsiz personelin binaya girmesini ve masum insanlara zarar vermesini önlemek için sistem kullanılıyorsa (ve tanıtılıyorsa), bu kullanım kullanıcı nüfusu için daha kolay kabul edilebilir ve kullanımlarına yönelik tutumlarını değiştirir.

Belirli teknolojilerin kendileri kullanıcılar ile ilgili olabilir. Parmak izi kullanımı en çok suçlu davranışlarıyla ilişkilendirilmiştir. Bir sistem sahibi tamamen iyi niyetli amaçlar için bir parmak izi tarama sistemi uygulasa bile, bu sistemin kullanıcıları suçlu gibi muamele görmüş gibi hissedebilir ve kullanımına direnebilir. Kullanım kolaylığı her zaman bir biyometrik sistemin doğru çalışmasında bir faktördür. Kayıt işlemi hızlı bir şekilde gerçekleştiriliyor mu ve minimum çaba gerektiriyor mu? Biyometrik ölçüm yapmak için özel prosedürler gerekli midir, yoksa kullanıcı başka bir aktivite yaparken ölçümler yapılabilir mi? Kullanıcılar, işlemi geçip geçmediklerini öğrenmek için ölçümleri yaptıktan sonra ne kadar süre beklemelidir? Uygun son kullanıcı operasyonel ve ergonomik planlama, düşük hata oranları ve daha yüksek kullanıcı memnuniyeti sağlama yönünde uzun bir yol kat edebilir.

Bu gizlilik ve kişisel bilgilerin güvenliği konusundaki farkındalığın arttığı günlerde, pek çok potansiyel sistem uygulayıcısının ve kullanıcının, biyometri kullanımının gizlilik yönleriyle ilgili endişeleri olması şaşırtıcı değildir. Diğer tanımlama yöntemlerinin çoğunda, adı, kimlik numarası, boyu, kilosu, yaşı vb. gibi söz konusu kişi hakkında bilgi toplar. Biyometrik uygulamalarda, sistem söz konusu kişinin parmak izi düzenleri veya ses düzenleri gibi bilgilerini tutar. Bu bilgi türü, kelimenin tam anlamıyla gerçek anlamda “kişisel” ve birçok kullanıcı bu kişisel detay seviyesini paylaşmaktan rahatsızlık duyuyor. Diğer tüm teknolojilerden daha fazla, biyometri, bir kişinin sahip olduğu en temel bilgilerin bir kısmını yakalama ve kaydetme yeteneğine sahiptir.

Birçoğu kişisel bilgilerinin depolanmasıyla da ilgilenmektedir. Nerede saklanacak, nasıl kullanılacak ve (en önemlisi) kime erişebilecek? Aslında, biyometrik sistem, bireyin özünü, o kişiyi benzersiz bir şekilde tanımlayabilen bir özelliği saklıyor. Yetkisiz kişiler bu bilgiyi elde ederse, bunu kendi çıkarlarına veya mağdurun zararına kullanabilirler. Depolanan biyometrik bilgilerin kaybı veya uzlaşması, en gerçek kimlik hırsızlığı biçimi için bir fırsat sunar.

Örneğin, “Joe Badguy” un bir kullanıcının parmak izi tanımlama için kullanılan şablonunu alabildiğini varsayalım. Bu şablonu sisteme bu kullanıcı olarak göstermek için kullanabilir veya belki de başka bir sisteme erişmek için bu şablonu başka bir sisteme besleyebilir. Şablonu meşru bir kullanıcı için değiştirebilir ve kendi şablon verilerini değiştirebilir. Bu noktada, Joe Badguy parmak izlerini sisteme sunabilir ve “Jane Masum, yetkili kullanıcı” olarak doğru bir şekilde tanımlanabilir.

Biyometri, kullanıcılarının kişisel yaşamlarında anonimlik olasılığını da azaltır. Kredi kartlarının küresel ekonomideki evrensel kullanımına rağmen, birçok kişi hala birçok işlem için nakit para kullanmayı tercih ediyor, çünkü bu kişilerin gizliliğini korumalarına izin veriyor. Nakit akışını takip etmek, kredi kartı kayıtlarını takip etmekten çok daha zordur. Müşterilerin ödeme hattını hızlandırmasına yardımcı olmak için yüz tanıma özelliğini kullanarak mağazanın önceki örneğini alarak, sistemin bir müşterinin satın aldığı ürünleri o müşterinin biyometrik verileriyle birlikte veri tabanında da sakladığını varsayalım. Bu sisteme davetsiz misafir (veya hatta güvenilir bir içerden gelen kişi), konunun kamuya açıklamayacağı (örneğin utanç verici bir sağlık durumunun göstergesi olabilecek bazı ilaçların satın alınması gibi) potansiyel olarak utanç verici veya tehlikeye atıcı bilgiler keşfedebilecektir. İnsanları satın alımlarla ilişkilendirmek için biyometri kullanarak, insanların özgür bir toplumun temel ilkelerinden biri olan kişilerin anonim davranmalarını azaltırsınız.

Genel olarak bilgi sistemleriyle ilgili büyük bir gizlilik sorunu ikincil kullanım konusudur. Bu, bir amaç için toplanan bilgilerin tamamen farklı bir amaç için kullanıldığı (veya üçüncü bir tarafa satıldığı) durumdur. İkincil kullanım, kendi başına biyometrik sistemlere özgü değildir, ancak biyometrik bir veri tabanında depolanan bilgilerin kişisel niteliği nedeniyle, kimlik sahtekarlığı potansiyeli daha da yüksektir. Bir kullanıcı, yüzünü ATM işlemlerini doğrulamak için bir sistemin bir parçası olarak kullanması için izin onay verebilirken (sonuçta, paraya rahat erişim için takas). Bu kullanıcı, aynı biyometrik karakteristik bilgiyi yerel bir satıcıyla paylaşmayı kabul etmeyebilir.

|  |  |
| --- | --- |
| **EK 1.1** Karakteristik Türüne Göre Biyometrik Teknolojiler | |
| **Çizgi türü ( Trait Type)** | **Biometric** |
| Phenotypic (Fenotipik) | Fingerprints ( Parmak izleri)  Eye scanning ( Göz tarama)  Vein patterns ( Damar desenleri)  Facial recognition ( Yüz tanıma)  DNA matching (DNA eşleştirme)  Hand geometry (El geometrisi)  Voice and speech recognition ( Ses ve konuşma tanıma)  Signature analysis ( İmza analizi)  Keystroke Dynamics ( Tuş vuruş dinamiği) |
| Genotypic (Geneotipik) |
| Behavioral (Davranışsal) |

Son olarak, karakteristik değiştirme sorunu var. Bir kişinin kredi kartı çalındığında, banka o kişiye yeni bir kart verir ve eskisini iptal eder. Bir bilgisayar kullanıcısı şifresini unuttuğunda, bir sistem yöneticisi eski şifreyi iptal edecek ve kullanıcıya yeni bir şifre atayacaktır. Bu iki işlemde, kimlik bilgilerinden ödün verildiğinde (kayıp veya hırsızlık nedeniyle), bazı otoriteler eski kimlik bilgilerini geçersiz kılar ve kullanıcıya yeni (ve farklı) bir tane verir. Ne yazık ki, biyometrik sistemler ile o kadar kolay değil. Bir insanın parmak izleri çalınmışsa, doktoru arayamaz ve yeni parmak alamaz! Ve estetik cerrahideki ilerlemelere rağmen, eski görüntünün riske atılmasından dolayı yeni bir yüz almak, normal (veya aklı başında) insanların çoğunun ulaşamayacağı bir yerdedir. Biyometrik sistemlerin kullanımı güvenlik açısından benzersiz zorluklar yaratır, çünkü sistemdeki verilerin uyuşması kurtarılamaz ve potansiyel olarak mağdur için felaket olabilir.

Biyometri tabanlı bir sistem için güvenliği tasarlarken, güvenlik uzmanı, uygulayıcının araç kutusundaki tüm araçları kullanmalıdır. Bu, derinlemesine savunma, güçlü erişim kontrolü, görevlerin ayrılması ve döndürülmesi ve sistemin hangi kısımlarına erişimi olanları kısıtlamak için en az ayrıcalık ilkesini uygulamak gibi zamana bağlı stratejileri içerir. Biyometrik sistemlerin kullanıcıları hakkında en kişisel bilgileri sakladığını ve bu nedenle güvenliklerine daha fazla dikkat edilmelerini gerektirdiğini unutmayın.

**Biyometrik teknolojiler (Biometric Technologies)**

Günümüzde mevcut olan farklı biyometrik teknolojiler, insanlarda bulunan üç tür biyometrik özellik arasında bölünebilir. Ek 1.1 en yaygın biyometrik teknolojileri ve bunların birbirleriyle ilişkilendirildiği özellik türlerini listeler.

**Parmak izleri (Fingerprints)**

Parmak izleri, tanımlama ve doğrulama için en popüler ve en yaygın kullanılan biyometrik özelliktir. Parmak izleri fetal aşamada (yaklaşık beş ayda) oluşur ve bir insanın ömrü boyunca sabit kalır. İnsan parmağı, parmak uçlarının yüzeyinde çok sayıda sırt ve oluklar içerir. Parmaklarda cilt yağı veya amino asit birikintileri, baskıları belirli bir yüzeyde bırakır. Bu baskılar yüzeyden çıkarılabilir ve analiz edilebilir.

* Nasıl çalışır. Parmak izi tarama sistemlerinde, kullanıcı iki veya üç saniye boyunca bir posta pulu boyutunda küçük bir optik veya silikon yüzeye bir parmak yerleştirir. İki farklı parmak tarama teknolojisi vardır. Birincisi, parmağın görsel bir görüntüsünü kullanan bir optik tarama. İkincisi, bir parmağın görüntüsünü elektronik olarak yakalamak için üretilen bir elektrik alanı kullanır.
* Kullanılan eşleşme noktaları. Her bir baskıdaki çıkıntılar ve oluklar analiz için çıkarılmıştır. Çıkıntı ve oluk desenleri dört gruba ayrılır: kemer (arch) (çok nadirdir), çadırlı kemer(*tented arch*), düğüm(whorl), ve ilmek(loop) (en yaygın olanı).
* Bir çizgi sonlandığında ya da bölündüğünde, “minutia” olarak adlandırılır. Parmak izi benzersizliğini veren çıkıntıların, olukların ve minutia 'in kesin şekli ve yeridir. Avrupa mahkemelerinin çoğu olumlu bir eşleşme için 16 minutia, birkaç ülke ise daha fazlasına ihtiyaç duyuyor. Amerika Birleşik Devletleri'nde, bir parmak izi uzmanının ifadesi, minitia'in eşleşme sayısından bağımsız olarak yasal olarak bir eşleşme oluşturmak için yeterlidir, ancak ondan az eşleme noktasına dayanan bir eşleşme savunmadan güçlü bir itirazla karşı karşıya kalacaktır.
* Depolama gereksinimleri. Parmak izi sistemleri, parmağın tüm görüntüsünü veya karşılaştırma için eşleşme noktalarının bir gösterimini saklar. ABD Federal Araştırma Bürosu dijitalleştirilmiş görüntüleri 256 gri seviyeli, inç başına 500 piksel çözünürlükte depolar. Bu standartla, 1,5 inç kare boyutunda tek bir parmak izi görüntüsü, parmak izi kartı başına yaklaşık 10 megabayt veri kullanır. Yerden tasarruf etmek için, birçok parmak izi depolama sistemi görüntünün tamamı yerine yalnızca sırtlar, oluklar ve minutialar hakkında bilgi depolar. Bu sistemler için depolama gereksinimi, görüntü başına tipik olarak 250 ila 1000 bayttır.
* Doğruluk. Parmak izi tarama sistemleri, yanlış pozitiflerden daha fazla yanlış negatif (yani meşru bir kullanıcıyı tanımakta başarısızlık) sergileme eğilimindedir. Piyasadaki çoğu parmak izi sistemi, yanlış görüntülerin sunumunu tespit etmeye çalışmak için çeşitli yöntemler kullanır. Örneğin, birisi meşru bir kullanıcı sisteme eriştikten hemen sonra sensörde gizli baskı kalıntısı kullanmaya çalışabilir veya hatta artık orijinal sahibine bağlı olmayan bir parmak kullanmaya çalışabilir. Bununla mücadele etmek için, birçok sensör bir parmağın canlı olup olmadığını ve insan yapımı malzemelerden (lateks veya plastik gibi) yapılmadığını belirlemek için özel ölçümler kullanır. Kan akışı, kan-oksijen seviyesi, nem, sıcaklık, nabız veya cilt iletkenliği için ölçümlerin tümü bu tehditle mücadelede kullanılan yöntemlerdir.

**Göz tarama (Eye Scanning)**

İnsan gözü, biyometrik ölçümlerde kullanım için en benzersiz ve ayırt edici özelliklerden bazılarını içerir. Göze dayalı biyometriklerin en yaygın iki şekli, iris tanıma ve retina tanımadır.

* Nasıl çalışır. Bir kişinin irisini tarama işlemi, gözbebeğini çevreleyen renkli dokuyu analiz etmekten oluşur. Taramalar standart bir video kamera kullanıyor ve denek gözlük taksa bile 2 ila 18 inç mesafede çalışacaktır. İris taraması tipik olarak üç ila beş saniye sürer. Buna karşılık, retinal tarama, gözün arkasında bulunan kan damarlarını analiz eder. Retina taraması, kullanıcının retinasını zıplayan düşük yoğunluklu bir yeşil ışık kaynağının kullanılmasını içerir ve ardından desenleri analiz etmek için tarayıcı tarafından okunur. Bununla birlikte, kullanıcının gözlükleri çıkarmasını, gözünü okuma cihazına yakın bir yere koymasını ve uzunca küçük yeşil bir ışığa odaklanmasını gerektirir. Kullanıcının başını sabit tutması ve gözünün birkaç saniye boyunca ışığa odaklanması gerekir; bu sırada cihaz kullanıcının kimliğini doğrular. Retina taramaları genellikle on ila on iki saniye sürer.
* Kullanılan eşleşme noktaları. İrisin içinde halkalar, oluklar ve çiller dahil olmak üzere 200'den fazla kullanılabilir kibrit noktası var. Retina taramaları, doğru şablonlar oluşturmak için 400 ila 700 farklı nokta arasında ölçüm yapar.
* Depolama gereksinimleri. Bir iris taraması için tipik şablon boyutu 256 ila 512 bayttır. Çoğu retina taraması daha küçük bir şablonda, genellikle 96 baytta saklanabilir.
* Doğruluk. Gözlerin insanlar arasındaki benzersizliği, göz taramasını biyometrik kullanım için çok güçlü bir aday yapar. Bu benzersizlik aynı kişinin sol ve sağ gözleri arasında bile var. Bir retinayı çoğaltmanın bilinen bir yolu yoktur ve ölü bir kişiden gelen retina aşırı derecede kötüleşir. Göz tarama teknolojisini kullanan yanlış pozitif olma olasılığı son derece düşüktür ve göreceli hızı ve kullanım kolaylığı güvenlik ve tanımlama uygulamaları için etkili bir seçimdir. Göz taramasının biyometrik olarak önündeki dezavantajları, taranması gereken kullanıcılar arasındaki sosyal ve sağlık sorunlarıdır. İnsanlar genellikle bir şeyin doğrudan gözlerine parlamasını sağlamaktan rahatsızdırlar ve ortaya çıkabilecek kalıcı sağlık etkileri konusunda endişelenirler. Bu sorun, tarama ışığına maruz kalma süresinin daha uzun olduğu retina tarama sistemleri kullanıcıları arasında daha belirgindir.

**Damar Desenleri (Vein Patterns )**

Damar desen tanıma, insan vücudunda, özellikle de insan elinin çevresinde, eşsiz yüzey ve deri altı damarlarını kullanır.

* Nasıl çalışır. Özel bir kamera ve kızılötesi sensör, avuç içi, el bileği veya elin arkasındaki damarların görüntüsünü alır. Görüntü daha sonra bir şablona sayısallaştırılır ve karşılaştırma için kullanılır.
* Kullanılan eşleşme noktaları. Görüntüler, her bireye özgü damarlardaki ağaç desenlerini gösterir ve damarlar ve diğer deri altı özellikleri, büyük, sağlam, kararlı ve büyük ölçüde gizli desenler sunar.
* Depolama gereksinimleri. Damar tarayıcıdan üretilen şablon yaklaşık 250 bayttır.
* Doğruluk. Benzersiz damar dağılımı deseni oldukça stabildir ve bir kişinin yaşamı boyunca aynı kalır. Bu bakımdan, damar desenleri tanımlanması için oldukça kararlı bir biyometrik sağlar. Sosyal olarak kabul edilebilirlik ile ilgili olarak, damar tanımada parmak izi uygulamasının sahip olduğu birçok cezai uygulama yoktur. Son olarak, damar örüntüleri, hafta sonu bahçeciliği veya duvarcılık gibi normal kullanım nedeniyle parmak izlerinin sık sık maruz kaldığı geçici hasarlara maruz değildir. Buna rağmen, damar taraması diğer biyometrik ölçümlerin bazılarının gördüğü yaygın yayılımı görmemiştir.

**Yüz tanıma (Facial Recognition)**

Yüz tanıma teknolojisi, belirli yüz özelliklerinin analiz edilmesini, bir veri tabanında saklanmasını ve sistemlere erişen kullanıcıları belirlemek için bunları kullanmayı içerir. İnsanların tek bir yüzü tekinsiz bir hassasiyetle tanıma doğal bir yeteneği vardır, ancak nispeten yakın zamana kadar bu görevi otomatik olarak ele almak için bir sistem geliştirmenin son derece zor olduğu kanıtlanmıştır. Bilimsel araştırma ve hesaplama gücündeki son gelişmeler yüz tanıma teknolojisini biyometrik güvenlik için güçlü ve doğru bir seçim haline getirmiştir.

* Nasıl çalışır. Yüz tanıma, insan yüzünün bir kişinin kullanım ömrü boyunca çok az değişen, göz yuvalarının üst kısımları, yanak kemikleri etrafındaki alan ve ağzın yanları dahil olmak üzere özellikleri olduğu ilkesine dayanır. Tipik bir yüz tanıma sisteminde, kullanıcı üç ila dört saniye boyunca bir ila iki feet mesafedeki bir kameraya bakar. Birkaç farklı yüz tanıma türü vardır. MIT'de geliştirilen Eigenface (özyüz), farklı yüz özelliklerini temsil eden iki boyutlu gri ölçekli görüntüler kullanır. Yüzlerin çoğu, sayısal katsayılara dönüştürülen 100 ila 125 özyüz (eigenface) kullanılarak yeniden oluşturulabilir. Analiz sırasında, “canlı” yüz aynı işlem kullanılarak analiz edilir ve sonuçlar depolanan katsayılarla karşılaştırılır. Yüz hattı analizi yöntemi, yüzün farklı yerlerinden düzinelerce yüz özelliğini ölçer. Yüz hattı analizi, yüz hareketini veya değişken kamera açısını Eigenface yönteminden daha fazla affetmektir. Diğer bir alternatif olan Sinir Ağı Haritalama sistemleri hem canlı görüntüyü hem de depolanan görüntüyü birbiriyle karşılaştırır ve bir eşleşme olup olmadığına dair bir “oylama” yapar. Algoritma, zor aydınlatma koşullarını veya yüz özelliklerinin hareketini hesaba katarken işlem sırasında çeşitli özelliklere verdiği ağırlığı değiştirebilir. Son olarak, Otomatik Yüz İşleme, gözler, burnun ucu ve ağzın köşeleri gibi kolayca edinilen özellikler arasındaki mesafeleri kullanır.
* Kullanılan eşleşme noktaları. Kullanılan belirli eşleşme noktaları, kullanılan tarama metodolojisinin türüne bağlıdır. Neredeyse tüm yöntemler yüz özelliklerinin ölçümlerini, aralarındaki mesafenin bir fonksiyonu olarak veya “standartlaştırılmış” yüzlerle karşılaştırıldığında alır.
* Depolama gereksinimleri. Şablon boyutu kullanılan yönteme göre değişir. Bire bir eşleştirme uygulamaları genellikle 1 ila 2 Kb aralığında şablonlar kullanır. Birçok uygulamalar 100 bayt kadar küçük şablonları kullanabilir.
* Doğruluk. Yüz tarama teknolojisini pazarlayan birçok şirket, yüzde 98 ile 99 arasında yüksek doğruluk oranları talep ediyor. Bununla birlikte, yakın zamanda yapılan bir ABD Savunma Bakanlığı çalışması, çoğu sistemin sadece yüzde 50 ila 60'lık bir doğruluk oranına sahip olduğunu buldu. Buna rağmen, kullanım kolaylığı ve tarama cihazlarıyla doğrudan kullanıcı etkileşimi için ihtiyaç duyulmaması, yüz taramayı birçok uygulama için çekici bir yöntem haline getirmektedir.

**DNA Eşleştirme (DNA Matching)**

Belki de hiçbir zaman bir biyometrik tür son zamanlarda DNA eşleşmesinden daha fazla baskı alamadı. Suç soruşturması, afet mağduru kimliği ve çocuk güvenliği gibi çok çeşitli uygulamaların tümü yardım için DNA eşleşmesine baktı. Tüm canlı hücrelerde bulunan temel kalıtsal maddeye deoksiribonükleik asit veya DNA denir. Bu DNA, canlıların embriyonik gelişimi sırasında oluşur ve vücuttaki her hücreye kopyalanır.

* Nasıl çalışır. DNA moleküllerinin çoğunluğu tüm insanlar için aynıdır. Bununla birlikte, her bir insanın DNA molekülünün yaklaşık üç milyon çifti (baz çift olarak adlandırılır) kişiden kişiye değişir. DNA analizi yaparken, bilim adamları önce belirli bir örnekte bulunan DNA'yı izole ederler. Daha sonra, DNA, VNTR olarak bilinen DNA'nın aynı tekrar dizilerini içeren kısa parçalara bölünür. Ardından fragmanlar boyuta göre sıralanır ve bir DNA eşleşmesini belirlemek için karşılaştırılır.
* Kullanılan eşleşme noktaları. VNTR fragmanları izole edildikten sonra istatistiksel analizden geçirilir. Örneğin, belirli bir uzunluğa sahip herhangi bir VNTR “konumu” için, bir popülasyonda bu uzunlukta eşleşen bir VNTR'ye sahip birçok kişi olabilir. Bununla birlikte, VNTR lokuslarının diğer numuneleriyle birleştirildiğinde, bütün bu numunelerin kombinasyonu, sadece bu kişi tarafından sahip olunan istatistiksel olarak benzersiz bir desen haline gelir. Gittikçe daha fazla yer kullanarak, ilgisiz iki kişinin eşleşen bir DNA profiline sahip olma olasılığı oldukça düşüktür (istatistiksel olarak).
* Depolama gereksinimleri. DNA eşleştirme bilgisi, fiziksel biçimde (özel röntgen filmi kullanarak) veya özel bir veri tabanı kullanılarak elektronik biçimde saklanabilir. Dünyadaki birçok hükümet, yüzbinlerce eşsiz DNA profili ile büyük DNA veri tabanları geliştirmeye başlıyor. Her bir sistem DNA şablon bilgisini kendi formatında sakladığından, kesin boyutlandırma gerekliliklerini belirlemek zordur. Bununla birlikte, DNA şablonlarını kaydetmenin bir kişinin gerçek DNA'sını, popülerliğini artıran bir tıbbi uygulamayı depolamaktan farklı olduğunu unutmayın.
* Doğruluk. Dört VNTR lokusu bile kullanıldığında, DNA eşleşmesi olan iki kişi bulma olasılığı beş milyonda birdir. FBI analizi ortalama 13 lokus kullanır ve eşleşme ihtimalini 100 milyarda 1’e düşürür. Bu, DNA'yı biyometrik analizin en doğru formlarından biriyle eşleştirir. Bununla birlikte, karmaşıklığı nedeniyle, DNA analizi kesinlikle bir laboratuvar bilimidir. Henüz bir “tüketici pazarı” teknolojisi değil.

**El Geometrisi (Hand Geometry)**

El geometrisi analizi işlemi, tanımlama ve kimlik doğrulama yapmak için elin özelliklerinin geometrik şeklini ve yapılandırmasını kullanır. Parmak izleri dışında, bireysel el özellikleri, pozitif tanımlama sağlamak için yeterince benzersiz bilgiye sahip değildir. Bununla birlikte, kombinasyon halinde alındığında birçok özellik biyometrik kullanımı mümkün kılmak için yeterli eşleşme noktaları sağlar.

* Nasıl çalışır. Bir kullanıcı büyük bir metal yüzeye bir el, avuç içi aşağı yerleştirir. Bu yüzeyde, “kılavuz mandalları (guidance pegs)” adı verilen beş kısa metal temas noktası bulunur. Kılavuz mandalları, kullanıcının daha fazla hassasiyet için elini metal yüzey üzerinde hizalamasına yardımcı olur. Cihaz, elin özelliklerini “okur” ve çeşitli eşleşme noktalarını kaydeder. Sisteme bağlı olarak, tarama iki boyutlu veya üç boyutlu görüntü alabilir. İzler, kirler ve tırnaklar gibi özellikler göz ardı edilebilir, çünkü bu “özellikler” bir insanın yaşamı boyunca hızlı bir şekilde değişir. Tipik el taramaları iki ila dört saniye sürer.
* Kullanılan eşleşme noktaları. El tarama sistemleri tipik olarak, uzunluk, genişlik, kalınlık, cilt saydamlığı, parmaklar ve elin yüzey alanı da dahil olmak üzere 90 ila 100 bireysel el karakteristiği kaydeder. Bu özellikler, birbirleriyle olan ilişkinin yanı sıra (örneğin, uzaklık, bağıl boyut vb.) kaydedilir ve saklanır.
* Depolama gereksinimleri. El geometrisi şablonları, göreli olarak az bir miktarda, dokuz bayta kadar az bir depolama alanında saklanabilir. Bu, akıllı kartlar gibi bellek depolamasının üstün olduğu uygulamalar için idealdir.
* Doğruluk. El geometrisi sistemlerinin doğruluğu oldukça yüksektir ve bu onu tarihsel olarak popüler bir biyometrik yöntem haline getirir. Aynı zamanda kullanıcılar arasında oldukça kabul edilebilir bir değeri vardır ve mevcut uygulamaların kullanımı kolaydır. Bununla birlikte, el geometrisi sistemleri tipik olarak kimlik doğrulama amaçları için kullanılır, çünkü birçok tanımlama uyumu veri tabanının büyüklüğü arttıkça giderek daha zorlaşır. Ayrıca, ekipmanın mevcut ortamlara entegre edilmesi pahalı ve zor olabilir.

**Ses ve Konuşma Tanıma (Voice and Speech Recognition)**

Ses tabanlı biyometrilerin birkaç farklı çeşidi vardır. Bunlar, konuşmacının olumlu bir şekilde tanımlanması için kişinin konuşmasındaki kalıpların analiz edildiği konuşmacı doğrulamasını ve konuşmayı yapan kişiye bakılmaksızın konuşulan sözcükleri tanımlayan konuşmanın tanınmasını içerir. Konuşma tanıma sistemlerinde konuşmacı ile konuşma arasında doğrudan bir ilişki olmadığı için, tanımlama ya da doğrulama için yararlı değildir. Son olarak, sesli yazı sistemleri bir insan sesini kaydeder ve konuşmacının sesinde mevcut olan akustik bilginin bir analog veya dijital gösterimini oluşturur.

* Nasıl çalışır. Bir kullanıcı, bir mikrofonun veya telefon alıcısının yanına yerleştirilir, böylece sesi yakalanabilir ve analiz edilebilir. Kullanıcının birkaç senaryodan birine göre bir cümle okuması istenir:
* Metne bağlı sistemler (Text-dependent systems), kullanıcının belirli bir önceden tanımlanmış sözcük veya kelime öbeği dizisini okumasını gerektirir.
* Metinden bağımsız sistemler (Text-independent systems), kullanıcının istediği herhangi bir kelimeyi veya ifadeyi söylemesini ister. Bu sistemler, kullanıcının konuşmasını ölçmek için sesli planları kullanır.
* Metin istemli sistemler (Text-prompted systems), kullanıcının sistem tarafından sağlanan rasgele kelimeleri okumasını gerektirir.
* Kullanıcının sesi sistem tarafından dijitalleştirilir ve daha sonra karşılaştırmalar için bir model şablonu üretilir ve kullanılır. Ses tabanlı sistemlerde tipik tanıma süresi dört ila altı saniyedir.
* Kullanılan eşleşme noktaları. Sisteme konuşulan her kelime veya kelime öbeği, her biri birkaç baskın frekans içeren heceler veya fonemlerden (veya küçük fonetik birimlerden) oluşan küçük parçalara bölünür. Bu baskın frekanslar, segmentin tüm uzunluğu boyunca oldukça tutarlıdır. Sırasıyla, bu bölümlerin her biri yakalanan ve dijital bir formata dönüştürülen birkaç (üç ila beş) baskın ton içerir. Bu dijital bilgi daha sonra bir ana tabloya aktarılır. Tüm bölümler için birleşik ton tablosu, kullanıcının benzersiz sesli görüntüsünü oluşturur.
* Depolama gereksinimleri. Sesli yazı şablonları, uygulamaya ve sistem tarafından istenen ses bilgisinin kalitesine bağlı olarak büyük ölçüde değişir. Depolama boyutu, 300 - 500 bayt arasında, 5000 - 10.000 bayta kadar değişebilir. Bu, depolama veya analiz sisteminin düşük bellek veya depolama kapasitesine sahip olduğu uygulamalar için özellikle uygun değildir.
* Doğruluk. Çoğu ses tanıma sistemi yüksek bir doğruluk derecesine sahiptir. En iyileri yalnızca kullanıcının sesli raporunu analiz etmekle kalmaz, aynı zamanda sesin orijinal mi yoksa mekanik bir çoğaltma mı olduğunu doğrulamak için canlılığı kontrol eder. Sistem, kullanıcı için özel bir eğitim gerektirmediğinden, kullanıcılar arasında kabul ve uygunluk memnuniyeti yüksektir. Ancak, ortam gürültüsü ve kaydın aslına uygunluğu gibi dış faktörler işlemin doğruluğunu olumsuz yönde etkileyebilir.

**İmza Analizi (Signature Analysis)**

Muhtemelen tüm biyometrik işlemlerin en az tartışmalı olanı imza analizinin kullanılmasıdır. Bunun nedeni, bir imza üretme sürecinin yanı sıra bir tanesini kabul etmenin sosyal ve yasal etkilerinin neredeyse tüm modern toplumlarda iyi bir şekilde oluşturulmasıdır. Göz taramalarından veya parmak izlerinden farklı olarak, imza temelli biyometrik sistemlerin kullanımına bağlı neredeyse hiçbir sosyal damga yoktur. Güvenlik açısından, imzaların kullanımı kasıtlı bir eylemi oluşturur; asla tesadüf eseri verilmezler. Göz taramaları, parmak izleri ve DNA gibi diğer biyometrik bilgilerin tümü, kullanıcının bilgisi olmadan elde edilebilir. Buna karşılık, bir kişi kasıtlı olarak imzasını sağlamalıdır.

* Nasıl çalışır. Kullanıcı, adını özel bir tablete “imzalar”. Kalem vuruşlarını kaydetmek için mürekkep kullanmak yerine, tablet bir imza oluşturulmasını simüle etmek için kalem hareketini kaydetmek için özel bir sensör kullanır. İki farklı imza analizi türü vardır. İmza karşılaştırması, harf boyutu, aralık, açılar, konturlar ve eğik gibi özellikler de dahil olmak üzere imza içinde bulunan fiziksel özellikleri inceler. Ne yazık ki, imza karşılaştırma sistemlerinin kandırılması daha kolay olabilir çünkü mekanik reprodüksiyonların kullanımına ya da deneyimli ustaların el işlerine karşı hassastırlar. Buna karşılık, dinamik imza doğrulama bir adım daha ileri gider; İmza içindeki fiziksel özellikleri kontrol etmenin yanı sıra, imza oluşturma işlemini de hesaba katar. Dinamik imza doğrulama sistemleri, kişi adını imzalarken ortaya çıkan hız, zamanlama, baskı ve ivme değişikliklerini dikkate alır. Tecrübeli bir sahtekar, mağdurun imzasının görünümünü güvenilir bir şekilde yeniden yaratabiliyorsa, yalnızca bir imzanın yaratıcısı her seferinde tekrar tekrar benzer kalem vuruşları üretebilir. Bir imza biyometrik sistem için tipik doğrulama süresi dört ila altı saniyedir.
* Kullanılan eşleşme noktaları. Kullanılan belirli eşleşme noktaları satıcıdan satıcıya değişir. En yaygın sistemler, imzanın dijitalleştirilmiş bir grafik gösterimini, ayrıca imza işlemi sırasında kaydedilen değişken kalem hareketi ve basınç bilgisini saklar.
* Depolama gereksinimleri. İmza analiz sistemlerinin çoğu yaklaşık 1500 baytlık şablonları saklar. Bazı satıcılar (vendor), sıkıştırma ve optimizasyon teknikleriyle şablonun yaklaşık 200 bayta düşürülebileceğini iddia ediyor.
* Doğruluk. Genel olarak, imza analiz sistemleri, özellikle diğer biyometrik göstergelerle karşılaştırıldığında, yalnızca makul bir doğruluğa sahiptir. Bu belki de imza sistemlerinin üstesinden gelmesi gereken değişkenlikten kaynaklanmaktadır. Yorgunluk, hastalık, sabırsızlık ve hava durumu gibi faktörler, bir kişinin ismini herhangi bir durumda nasıl imzaladığını etkiler.

**Tuş Dinamiği (Keystroke Dynamics)**

Potansiyel bir biyometrik sistem için en çok arzu edilen yönlerden biri, kullanıcının iş sürecini değiştirmesini istemeden kullanıcı girişi toplamak veya (en iyi durumda) biyometrikin ölçülmekte olduğunun farkında olmaktır. Bu amaçla, tuşa basma dinamiği analizinin kullanılması, son kullanıcı için mümkün olduğunca göze çarpmayan olma konusunda en yakın olanıdır. Tuş vuruş dinamiklerini ölçmek, kullanıcıları bir klavyede yazarken izlemeyi ve ayrı tuş vuruşlarının hızını, süresini, gecikmelerini, hatalarını, kuvveti ve aralıklarını ölçmeyi içerir. Çoğu bilgisayar kullanıcısı, belirli bilinen kalıpları (kullanıcı kimlikleri veya standart bir cümle gibi) tekrar edilebilecek ve ölçülebilecek bir tutarlılıkla tekrar tekrar yazabilir, böylece onu biyometrik kullanım için doğal hale getirir.

* Nasıl çalışır. Bir kullanıcı klavyeye bir parola yazar. Bu ifade, daha önce kullanıcı tarafından bilinen ve tipik olarak her kullanıcı için standart hale getirilmiş olandır. Sistem klavyeyi saniyede 1000 kez tarar ve bir şablon oluşturmak için çeşitli ölçümler kaydeder. Giriş zamanı, parolanın uzunluğuna bağlı olarak değişir ve doğrulama süresi tipik olarak beş saniyeden azdır.
* Kullanılan eşleşme noktaları. Sistem, tuş vuruşlarını bir dizi digraph (iki bitişik tuş vuruşları) veya trigraph (üç bitişik tuş vuruşları) halinde ayırır. İmza / trigraftaki her bir anahtar arasındaki ilişki yakalanır ve o oturum için bir şablon oluşturmak üzere analiz edilir. Kilit zamanlamanın iki yönü özellikle önemlidir: bekleme süresi veya süre (belirli bir tuşun basılı tutulduğu süre) ve uçuş süresi veya gecikme süresi (tuşa basılanlar arasındaki süre miktarı).
* Depolama gereksinimleri. Tuş dinamiği sistemleri için depolama gereklilikleri, kullanılan parolanın boyutuna ve digraph başına alınan ölçüm sayısına bağlıdır.
* Doğruluk. Tuşa dayalı biyometrik sistemlerin genel doğruluğu, kullanılan ölçüm yöntemine ve kullanıcıdan istenen giriş türüne bağlı olarak oldukça değişken olabilir. Kullanıcının kendi parolasını girmesine izin vermek yerine, yapılandırılmış metni (yani, sistem tarafından sağlanan parolalar) kullanan bir sistemde, yüzde 90 veya daha fazla doğruluk oranları elde edilmiştir. Bununla birlikte, kullanıcının yazma yeterliliği ve hatta farklı bir klavyenin kullanılması da dahil olmak üzere birçok faktörün doğruluğunu etkileyebilir.

**Teknolojileri Birleştirmek (Combining Technologies)**

Hangi biyometrik sistemin kullanılacağı seçimi, özel güvenlik ihtiyacına, belirli bir yöntemin uygulanmasının maliyetine ve uygulanabilirliğine ve önlemin nasıl kurulabildiğine ve kullanılabileceğine dayanmaktadır. Bununla birlikte, her farklı biyometrik teknolojinin sınırlamaları vardır. Yüksek güvenlikli bir ortam yaratmaya çalışırken, zamanın güvendiği bir güvenlik stratejisi kullanmak avantajlı olabilir: derinlemesine savunma. Derinlemesine savunma kavramı, potansiyel bir saldırganla potansiyel bir hedef arasına birçok katman veya engel yerleştirmektir. Her katman, katmanı ondan önce tamamlar ve geliştirir, bir saldırganın hedefe ulaşmak için birden fazla (ve zor) engel atlamasını gerektirir.

Derinlemesine savunma biyometriye de uygulanabilir. Bunu başarmanın bir yöntemi katman kullanımıdır. Katmanlamanın ardındaki kavram, diğer geleneksel kimlik belirleme ve onaylama biçimleriyle birlikte biyometrik teknolojiyi kullanmaktır. Örneğin, bir binaya erişmek için bir ziyaretçinin hem fotoğraflı kimlik kartı göstermesi hem de parmak izi taramasından geçmesi gerekebilir. Çünkü fotoğraflı kimlikler kusursuz değildir (holografik mühürler ve filigranlar gibi modern sahteciliğe karşı tekniklerin kullanılmasına rağmen), İşlemin doğruluğuna olan güven, karttaki kişinin ve kapıdaki kişinin aynı olduğunu doğrulamak için parmak izlerinin kullanılmasıyla arttırılmıştır.

Derinlemesine savunma sağlamanın bir başka yolu da, multimodal biyometri kullanımıdır. Çok modlu bir kurulumda, iki (veya daha fazla) biyometrik teknoloji paralel olarak kullanılır ve kullanıcının başarılı bir şekilde tanımlanması için her birini geçmesi gerekir. Örneğin, bir kullanıcının sınıflandırılmış bir alana kabul edilebilmesi için hem iris taramasını hem de ses tanımlama testini geçmesi gerekebilir. Multimodal biyometri kullanımı, birkaç avantaja sahiptir. İlk olarak, daha yüksek hata oranlarına sahip olabilecek biyometrik teknolojilerin kullanılmasına izin verir, çünkü kullanımdaki ek biyometrik kullanım herhangi bir hatayı gevşekleştirir. Başka bir deyişle, bir biyometrik teknoloji yüzde 10'luk bir hata oranına ve diğeri yüzde 12'lik bir hata oranına sahip olabilir. Kendileri tarafından, bu oranların her biri pratik kullanım için çok yüksek olabilir. Ancak birleştirildiğinde, iki teknoloji birlikte yalnızca yüzde 1,5'lik bir hata oranına sahip olabilir. Bu potansiyel kullanıcı için çok daha kabul edilebilir olabilir. Ek olarak, çoklu biyometrelerin kullanımı herhangi bir ölçümde daha fazla çeşitliliğe izin verir. Örneğin, ses tanıma sistemleri cızırtılı seslerde (soğuk algınlığı nedeniyle) zorluk yaşayabilir ve diğer biyometriler değiştirilmiş vücut özelliklerinden (örneğin yara izleri, morluklar vb.) Dolayı zorluk yaşayabilir. Çok modlu kullanım, biyometrik süreçte hala yüksek bir genel güvence seviyesini korurken, vücut özelliklerinde daha fazla çeşitlilik sağlar.

**Biyometrik standartlar (Biometric Standards)**

Biyometrik ekipman ve sistemler geliştiren veya pazarlayan 200'den fazla satıcı var. Bu kadar çok farklı ürünün ve özelliklerin bulunduğu diğer tüm endüstrilerde olduğu gibi, bu, biyometrik ürünler ve ölçüm için sayısız “standart” olduğu ve biyometrik bilgilerin depolanması, alınması ve işlenmesi gibi birçok yöntem olduğu bir duruma yol açmıştır. Durumu düzeltmek ve ürün ve sistemleri birbiriyle daha uyumlu hale getirmek için, biyometrik arayüzleri ve işlemleri standart hale getirmek için çeşitli çabalar sarf edilmiştir.

En büyük çaba Biyometrik Uygulama Programı Arabirimi veya BioAPI'dir. Biyometrik sistemleri ve uygulamaları geliştiren 90'dan fazla kuruluştan oluşan bir grup olan BioAPI Konsorsiyumu, BioAPI'yi geliştirdi. BioAPI, çok çeşitli biyometrik teknolojilerle standart bir arayüz oluşturma uygulamaları sunar. Geliştiriciler BioAPI kullanarak, biyometrik sistemlerini teknolojiden bağımsız ve platformdan bağımsız bir şekilde bütünleştirebilirler. Örneğin, parmak tarama donanımı geliştiricileri, her ikisi de BioAPI spesifikasyonunu takip ettiği sürece sistemlerini herhangi bir bilgi işlem platformuyla bütünleştirebilecekler. BioAPI spesifikasyonu şu anda sürüm 1.1'dedir ve kamuya açıklanmıştır. Geliştiricilerin ürünlerini modellemek ve test etmek için kullanmaları için bir açık kaynak referans uygulaması da mevcuttur.

BioAPI, biyometrik teknoloji arayüzlerinin standardizasyonunu ele alırken, Ortak Biyometrik Değişim Dosya Formatı veya CBEFF, biyometrik şablonların depolanması ve değişimi için ortak bir format tanımlanması ile ilgilidir. Çok sık, biyometrik uygulamalar veri depolama için kendi tescilli veya platforma özel formatlarını kullanır. Ne yazık ki, bu biyometrik verilerin uygulamalar veya platformlar arasında aktarılmasını zorlaştırıyor. CBEFF, sistemler ve uygulamalar arasında biyometrik şablonların depolanması ve değişimi için platformdan bağımsız ve biyometrik bağımsız bir format tanımlayarak bu konuyu ele almaktadır. CBEFF, Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından desteklenmektedir ve kullanışlı bir standart olarak geniş destek almaktadır.

**Sonuç (Conclusion)**

Biyometrik teknolojinin kullanımının sınıflandırılmış askeri tesisler ve bilim kurgu filmleriyle sınırlı olduğu bir zaman vardı. Bir kişiyi tanımlamak, doğrulamak ve takip etmek için biyolojik özellikleri kullanma kavramı, “normal” kişilerin düşünmesi için çok ileri görünüyordu. Ancak, gün artık biyometriklerin günlük kullanımının mümkün olmadığı, her yerde yaşanıyor: ofis binalarında ve süpermarketlerde, bilgisayar ağlarında ve bankalarda, sokak köşelerinde ve futbol stadyumlarında. Maliyetin düşmesi ve fizibilite ve güvenilirlikteki büyük kazanımlar, sistem sahipleri ve güvenlik uzmanlarını, geleneksel kullanıcı tanımlama ve doğrulama sistemlerine ek olarak veya hatta bunun yerine, biyometri kullanımını düşünmeye zorladı. Son kullanıcılar bile günlük yaşamlarında biyometriyi kabullenmeye başlamıştır ve bu eğilim sadece geleceğe devam edecektir. Klavyelerin, parolaları değiştirmek için yerleşik parmak izi okuyucusuna sahip olacağı günler çok uzak değildir, ATM makineleri PIN'ler yerine iris taramaları kullanacak ve el tarayıcıları ofisteki kimlik kartlarının yerini alacaktır. Gelecek ne olursa olsun, kesin olan bir şey var: biyometri kalmak ve daha popüler olmak için burada. Başarılı (ve bilgili) güvenlik uzmanları, biyometrik teknolojiyi sürekli büyüyen güvenlik araçlarının bir parçası olarak planlamayı, uygulamayı ve kullanmayı öğrenmelidir.

**BİYOMETRİK: YENİ OLAN NEDİR?**

*Judith M. Myerson*

Yıllar boyunca, ağ dünyasında güvenlik, birinin bir şifresini, PIN'ini veya birinin annesinin kızlık soyadı gibi kişisel bir bilgisini bildiği şeylere dayanıyordu. Bu, birinin (bir kart anahtarı, akıllı kart veya belirteç) sahip olduğu şeyle kullanabileceği (biyometrik) bir şeyle desteklenmektedir. Biyometri, bir kişiyi parmak ucu, göz ve yüz özelliklerine göre ölçer. Biri ayrıca tuşları nasıl kullandığı ,konuşma şekli ve birinin nasıl yürüdüğü ile de ölçülür. Gelecekteki bir tarihte, bir kişinin kulağının oluşma şekline ve birinin nasıl işitdiğine bakılabilir. Geleneksel biyometrik sistemlere ve daha sonra yeni teknolojilere ve sistemlere bakın. Bunları standardizasyon sorunları ve seçim kriterleri üzerine kısa tartışmalar izlemektedir.

**Parmak izleri (Fingerprints)**

Birkaç yıl içinde, parmak izi şablonlarının basılı kopyalarını almak için siyah mürekkep pedleri (black ink pads) kullanmak geçmişte kaldı. Kişinin en çılgın hayallerinin ötesinde şeyler yapmasına izin veren parmak izi sensörleri yaşını girin. Uzak bir ağ sistemine erişmek için sensör çipinde - hızlı ve temiz - bir parmak ucunu kaydırın. İki parmak izi aynı olmadığından, birinin parmak izlerinin kopyalanması zor olabilir.

Bir parmak izi parmak ucunda bulunan desenlerden oluşur. İyi bir desen, parmak izi endekslerinde minutiye olarak bilinen sonlanma ve bölünmelerden oluşur. Ortalama bir parmak izinde 40 ila 60 minutia vardır. Kalıplar kabul edilebilir bir minutia aralığında olsa bile, sensörler bir parmak ucunun tüm detaylarını yakalayamayabilir. Bazı kişiler için, klavyede günlük yazma veya piyanoda zor klasik müzik parçalarının çalınması nedeniyle desenler çok ince olabilir. Ek olarak, eğer bir birey genetik bir kusur ile doğarsa veya parmak ucunda büyük bir yara izi varsa, desenleri okumak zor olacaktır.

Bir parmak ucunun kalıplarını kayıtlı bir parmak izi şablonunun kalıplarıyla eşleştirmenin dört yolu vardır: Elektriksel, termal, optik ve karma sensörler. Bir elektrik sensörü, parmak izinin sırtları ve olukları arasındaki değişken elektriksel alan gücünü ölçer. Bir termal sensör, parmakla kaydırma işleminde sıcaklık farkını ölçer, sırtların sürtünmesi,merkez yüzeyi boyunca kayarken, temas etmeyen oluklardan daha fazla ısı üretir.

**Göz tarama (Eye Scanning)**

Bir parmak ucunun aksine, göz yapısı üzerinde binlerce minutia sağlayabilir. Parmak ucu minutileri, harici bir yapının şekli hakkında bilgi verirken, göz minutesi, gözün iç yapısının düzenine bakar. Bir kişi bu bilgiyi iki kaynaktan elde edebilir: retina ve iris tarama sistemleri. Birincisi retinadaki damarların şablonu ile ilgilidir, ikincisi ise irisde liflerin, dokuların ve halkaların şablonunu kullanır.

Retinanın benzersiz desenlerini taramak için retina tarayıcı, optik bir kuplör aracılığıyla düşük yoğunluklu bir ışık kaynağı kullanır. Böyle bir tarayıcı, birinin bir prize bakmasını ve belirli bir noktaya odaklanmasını gerektirir. Bu, düzeltici lens kullanan veya okuma cihazıyla yakın temasta rahat hissetmeyen kişiler hakkındaki endişeleri ortaya çıkarır.

İris taraması, diğer taraftan, oldukça geleneksel bir TV kamera elemanı kullanır ve yakın temas gerektirmez. İris biyometrisi, bir ışık kaynağı iyi iken düzeltici gözlük ve kontaklarla iyi çalışır. Bazı havayolları gezginleri uçaklara kabul etme sürecini hızlandırmak için iris tarayıcıları kurmuştur.

Göz kalıplarının hastalık veya yaralanma nedeniyle zaman içerisinde değişebileceğini unutmayın. Göz tarayıcıları insanları kör etmek için işe yaramaz. Bu görme engelli bireyler, özellikle retina hasarı olanlar için de geçerlidir

**Yüz tanıma (Facial Recognition)**

Yüz tanıma sistemleri, insanların yüzlerini televizyonda veya bir bina veya caddeyi izleyen kapalı devre kameralarda göründüğü gibi otomatik olarak tarayabilir. Yeni bir sistem, yüzün kızılötesi ısı düzenini biyometrik olarak görüyor ve sistemin karanlıkta çalıştığını gösteriyor. Kumarhane endüstrisi, güvenlik görevlileri tarafından hızlı bir şekilde tespit edilebilmesi için yüzlerce aldatmaca sanatçısı veri tabanı oluşturmak için ağ bağlantılı taramaya yatırım yaptı.

Bir birey görünüşünü belirgin bir şekilde değiştirdiğinde (örneğin, bir sakal yetiştirerek veya olağandışı bir yüz ifadesi yaparak) sistemin kafası karışabilir. Sistemi karıştırmanın bir başka yolu, bir insanın yüzünün kameralara yönelimini önemli ölçüde değiştirmektir. Sorgu görüntüsü ile veritabanı görüntüsü arasındaki konumdaki 15 derecelik bir fark performansı olumsuz yönde etkileyecektir. Açıkçası, 45 derecelik bir farkla, tanıma etkisiz hale gelir.

**El ve Ses (Hand and Voice)**

El geometrisi cezaevlerinde kullanılmıştır. Elin üç boyutlu özelliklerini kullanır,parmakların uzunluğu, genişliği, kalınlığı ve dağılımı; damarları; ve diğer özellikler. Bir el şişmiş parçaları veya genetik kusurları göstermemelidir.

Sesli baskılar Avrupa'da telefon görüşmesi erişimi için yaygın olarak kullanılmaktadır. Özellikle kışın, arayanların ellerini ısıtmak için eldiven giymesi gerektiğinde el izlerinden daha uygundurlar. Gürültülü bir ortamın yanı sıra yaralanma, yaş ve hastalık da ses doğrulamasını olumsuz yönde etkileyebilir.

**Yeni olan nedir? (What Is New?)**

Biyometrik uygulamalar bugüne kadar kimliğin değiştirilmemesini sağlamak için cezaevi ziyaretçi sistemlerinde ve sahte iddiaları ortadan kaldırmak için fayda ödeme sistemlerinde kullanılmıştır. Biyometrik sistemler, birden fazla lisansı kontrol etmek için kamyon şoförlerinin taşıyabileceği ve devlet sınırlarını veya ulusal sınırları geçtikleri zaman değiştirebilecekleri şekilde kurulmuştur. Yeni sınır kontrol sistemleri, seçilen biyometrik terminallerde ülkeye giren ve çıkan yolcuları izler. Biyometrik tabanlı oylama sistemleri, uygun seçmenlerin kimliğini doğrulamak için kullanılır, böylece bu tür sistemler henüz toplu olarak mevcut olmasa da, vekil oylamanın kötüye kullanılması önlenir.

Peki, yeni olan ne? Özellikle 1 Ocak 2001'de başlayan üçüncü binyıla geldikten sonra. Neler olduğuna bir göz atmak için, işte kısmi bir liste.

* Yüz, ses ve dudak hareketlerinin entegrasyonu
* Giyilebilir biyometrik sistemler
* ATM kartlarında parmak izi cips
* Kişisel kimlik doğrulama
* Diğer şey

Bu biyometrik çabaların bazıları çoktan pazara ulaştı, diğerleri ise hala araştırma aşamasında. Biyometrik entegrasyona ivme kazandıran, biyometrik girişimleriyle Microsoft'tur.

**Yüz, Ses ve Dudak Hareketi Entegrasyonu (Integration of Face, Voice, and Lip Movement)**

Elbette ilk madde, ilginçtir - özellikle dudak okuma hareketinin biyometrisi. Daha ilginç olan, bu modalitenin diğer iki yüz ve sesle bütünleşmesidir. Bu sistemin avantajı, eğer bir yöntem düzgün çalışmıyorsa, diğer iki yöntemin birincinin hatalarını telafi etmesidir. Bunun anlamı, eğer bir modülerlik bozulursa (örneğin, sesi boğan gürültülü bir ortam), diğer iki yöntem hala doğru bir tanımlamaya yol açar.

Böyle bir örnek, Dialog Communication Systems AG (Erlangen, Almanya) tarafından geliştirilen Multimodal Biyometrik Kimlik Sistemi BioID'dir. Bu sistem yüz, ses ve dudak hareketi tanıma özelliğini birleştirir. Sistem kayıtları almak ve her bir biyometrik özelliği ayrı ayrı işlemekle başlar. Sistemin eğitimi (kayıt sırasında), her özellik için biyometrik şablonlar oluşturulur. Sistem daha sonra bu şablonları yeni kaydedilenlerle karşılaştırır ve sonuçları tanımak için kullanılanları birleştirir.

BioID, dudak görüntülerini, her görüntü bölümünün video dizisindeki bir sonraki bölüme yerel hareketini temsil eden bir vektör alanını hesaplayan bir optik akış tekniği vasıtasıyla toplar. Bu işlem için ön işleme modülü, ağız bölgesini video dizisinin ilk 17 görüntüsünden keser. Dudak hareketlerini, dudakların çerçeveden çerçeveye hareketini temsil eden 16 vektör alanında toplar. Sesi duymadan dudakları okumanın bir dezavantajı, iki veya üç farklı kelime için dudakların aynı şekilde hareket ettiği görünmesidir.

Şirket, BioID'in, insanların bilgisayar ağları, İnternet ticareti ve bankacılık sistemleri ve ATM gibi teknik bir sisteme erişmesi gereken herhangi bir uygulama için uygun olduğunu iddia ediyor. Uygulamaya bağlı olarak, BioID, kişileri tanımlama veya doğrulama yoluyla yetkilendirir. Kimlik modunda, sistem bir kişiyi tanımlamak için tüm veritabanını aramalıdır. Doğrulama modunda, bir kişi ismini veya bir sayısını verir; sistem daha sonra biyometrik özellikleri kullanarak doğrulamak için doğrudan veritabanının küçük bir bölümüne gider.

**Giyilebilir Biyometri Sistemi (Wearable Biometrics System)**

Günümüzde kameralar ve mikrofonlar çok küçük ve hafiftir ve örneğin yüzleri tanımaya yardımcı olmak için kullanılan giyilebilir sistemlerle başarıyla entegre edilmiştir. Yüz tanıma yazılımından çok daha iyisi, birinin gözlüklerine yerleştirilmiş ses tabanlı bir kameraya sahip olmaktır. Bu cihaz, birinin kulağına fısıldayarak bakmakta olduğu kişinin adını hatırlamasına yardımcı olabilir. ABD Ordusu, bu tür cihazları Bosna'daki sınır muhafızları tarafından kullanılmak üzere test etti. Rochester Üniversitesi Gelecekteki Sağlık Merkezi'ndeki araştırmacılar, Alzheimer hastalığı olan hastalar için bu cihazlara bakıyorlar.

Yeni nesil tanıma sistemlerinin insanları gerçek zamanlı olarak ve çok daha az kısıtlı durumlarda tanıması bekleniyor. Gerçek zamanlı olarak çalışan sistemler, üç modalite ile sınırlı olan sistemlerden çok daha dinamiktir. Zaman geldiğinde, sistem bir kişiyi bir biyometrik varlık olarak tanıma yeteneğine sahip olacaktı - bu bireyin sadece bir ya da iki biyometrik parçası değil.

**ATM Kartlarında Parmak İzi Çipi (Fingerprint Chip on ATM Cards)**

Önde gelen bankaların çoğu, kartlar çalındığında ATM’de meydana gelen kimlik sahtekarlığı ile mücadele etmek için biyometrik deneyler yapıyor. Bir örnek, bir ATM üzerine bir parmak izi sensörü yongası yerleştirmektir. Bazı şirketler PKI'ya ATM kartındaki biyometri ile bakıyor. PKI, kullanıcı kimliği ve kimlik doğrulaması için açık anahtarlı şifreleme kullanır; Özel anahtar ATM kartında saklanır ve bir biyometrik ile korunur. PKI matematiksel olarak daha güvenli olsa da, en büyük dezavantajı kullanıcının özel anahtarının gizliliğini korumaktır. Güvende olmak için, özel anahtarın tehlikeye karşı korunması gerekir. Çözüm, özel anahtarı akıllı kartta saklamak ve biyometrik ile korumaktır.

18 Ocak 2001'de, Keyware (biyometrik ve merkezi kimlik doğrulama çözümleri sağlayıcısı) Context Systems ile ortaklığa girdi. Sonuncusu, ATM işletim sistemine bindirme olarak biyometrik bir arabirim için ağ güvenliği çözümleri ve PKI etkin uygulamalar sağlayıcısıdır. Bu arayüz, yetkilendirme veya doğrulama uygulaması olarak standart PIN'in yerine geçecektir. Bir banka kartı kartında bir parmak izi ve erişim kartı numarası, banka hesap numarası ve bankacılık kurumlarının kullanabileceği diğer anlamlı bilgiler gibi benzersiz bir kimlik numarası (UIN) bulunur.

**Kişisel Kimlik Doğrulama (Personal Authentication)**

Taşınabilir kimlik doğrulamadaki uygulamalar arasında kişisel bilgi işlem, şifreleme ve otomotiv bulunmaktadır. Birincisi yaygın kullanım kazanıyor, ikincisi ise uygulanabilir olan ilk yerle ilişkilendiriliyor. Üçüncüsü, üreticiler çip üzerindeki olumsuz çevresel etkileri kontrol etmenin daha iyi yollarını buldukları zaman mevcut olacaklar.

Taşınabilir bilgi işlem, kişisel kimlik doğrulamanın ilk yaygın uygulamalarından biridir. Bir şirket ağına erişim sağlayan bir dizüstü bilgisayardaki parmak izi sensörü yongasını içerir. Uygun yazılımla, çip, dizüstü bilgisayar içeriğine beş girişi doğrular: giriş, ekran koruyucu, açılış, dosya şifreleme ve ardından ağ erişimi.

Veridicom, dizüstü bilgisayar ve diğer taşınabilir bilgisayar kullanıcılarına, parmak izi sensörüyle birleştirilmiş akıllı kart okuyucusu sunar. Verilere, bilgisayar sistemlerine ve dijital sertifikalara erişim için şifreleri değiştirmeyi amaçlamaktadır. Klavyelerde, dizüstü bilgisayarlarda, kablosuz telefonlarda ve Internet cihazlarında yerleşik kimlik doğrulaması için şirketin sensör çipinin daha küçük ve daha verimli bir modeli mevcuttur.

Dizüstü bilgisayar kullanıcıları için şifreleme, sahibinin parmak izini kullanarak özel bir anahtara erişim sağlamak için özel bir tuş kilidi kutusu olarak gelebilir. Sahip, bu kilit kutusunu özel ağlar ve Internet üzerinden bilgileri şifrelemek için kullanabilir. Bu kilit kutusu ayrıca dijital sertifikalar veya daha güvenli şifreler içermelidir.

Üreticiler şu anda arabanın kapı kolunda, arabanın kilidini açmak için bir anahtarlıkta veya kontağı açmak için gösterge panelinde bulabilecekleri otomotiv sensör çipleri üzerinde çalışıyor. Bir çipin aşırı hava koşulları altında çalışabilme kabiliyeti ve yolcu kabininde yüksek bir sıcaklık gibi güvenilirlik sorunlarının üstesinden gelmeye çalışıyorlar. Araştırılan diğer bir konu, daha yüksek seviyelerde elektrostatik boşalmaya dayanma yeteneğidir.

**Diğer Yeni Şeyler (Other New Stuff)**

Diğer yeni şeyler arasında çoklu seyahat parmak izi uygulamaları, kamu kimlik kartları ve gözetim sistemleri yer alıyor. Çok fonksiyonlu uygulamalar, yolcuların sık uçan yolcu ve sınır kontrol sistemlerine katılmalarını sağlar. Seyahat edenler uçak bileti ve otel odaları gibi seyahat masraflarını ödemek için uygun bir parmak izi şablonunu kullanabilirler. Çok amaçlı kullanım için kasık kimlik kartı biyometri içerebilir. Örneğin, bir kapalı devre gözetim video kamera sistemi, yüz yazılımı ile otomatik olarak izlenebilir.

Araştırmacılar, aydınlatma, yaşlanma, derinlemesine dönme ve genel ifadeler nedeniyle değişikliklere daha iyi uyum sağlamak için mevcut yüz tanıma algoritmalarının bazı kısıtlamalarını gevşetme üzerinde çalışıyor. Yüz kılı, gözlük ve makyaj gibi şeylerden dolayı görünümdeki değişikliklerle nasıl başa çıkılacağını da inceliyorlar - zaten kısmi çözümleri olan problemler.

**Microsoft Faktörü (The Microsoft Factor)**

Microsoft, 5 Mayıs 2000'de biyometrik kimlik doğrulama teknolojisini Windows işletim sistemlerine entegre etmek için I/O Yazılımı ile ortaklığa girdi. Microsoft, kullanıcılara kişisel yetkilendirme yöntemine dayanarak daha yüksek düzeyde ağ güvenliği sağlamak için I/O Yazılımları'nın Biyometrik API (BAPI) teknolojisi ve SecureSuite çekirdek kimlik doğrulama teknolojisi satın aldı.

Bu entegrasyon, kullanıcıların bilgisayarlarına giriş yapmalarını ve parola yerine kriptografik bir özel anahtarın parmak izi, iris deseni veya ses tanıma kombinasyonunu kullanarak güvenli E-ticaret işlemlerini yapmalarını sağlar. Biyometrik bir şablonun kopyalanması çok daha zordur, çünkü hiçbir iki birey aynı özelliklere sahip değildir. Biyometrik veriler şifreleri ve akıllı kart PIN'lerini değiştirmek için çok uygundur, çünkü biyometrik veriler unutulmaz, kaybedilmez, çalınamaz veya başkalarıyla paylaşılamaz.

**Standartlaştırma Sorunları (Standardization Issues)**

Biyometri endüstrisi, her biri kendi özel arayüzü, algoritması ve veri yapısına sahip 150'den fazla ayrı donanım ve yazılım satıcısı içerir. Ortak bir yazılım arayüzü sağlamak, biyometrik şablonların paylaşımına izin vermek ve farklı biyometrik teknolojilerin iyi karşılaştırılmasını ve değerlendirilmesini sağlamak için standartlar ortaya çıkmaktadır.

Böyle bir örnek, belirli bir biyometrik uygulama ile arayüz oluşturmak için ortak bir yöntem tanımlayan BioAPI standardıdır. BioAPI, 60'tan fazla satıcı ve devlet kurumundan oluşan bir konsorsiyum tarafından geliştirilen açık sistemler standardıdır. C ile yazılmış, kayıtlı kullanıcı, iddia edilen kimliği doğrulama (kimlik doğrulama) ve kimliği keşfetme gibi tüm biyometrik teknolojilerde ortak olan temel eylemleri gerçekleştirmek için bir dizi işlev çağrısından oluşur.

BioAPI Konsorsiyumu'nun kurucusu olan Microsoft, kendi BAPI biyometrik arayüz standardını bıraktı ve geliştirdi. Bu standart, Microsoft'un I / O Yazılımından edindiği BAPI teknolojilerine dayanmaktadır. Diğer bir taslak standart, çeşitli biyometrik cihazlardan toplanan şablonların değiş tokuş edilmesi ve saklanması için ortak bir araç tanımlayan Ortak Biyometrik Değişim Dosya Biçimidir. Biyometrik Konsorsiyum ayrıca, parmak izi teknolojisi tedarikçileri için birlikte çalışabilirlik düzeyi sağlamaya çalışan Ortak Parmak İzi Minutiae Değişim formatı için bir teklif sunmuştur.

Birlikte çalışabilirlik konularına ek olarak, biyometri standartları, biyometri güvencesi ve test metodolojileri için bir temel oluşturmanın bir yolu olarak görülmektedir. Biyometrik güvence, bir biyometrik cihazın amaçlanan güvenlik seviyesine ulaşabileceği güvencesini ifade eder. Biyometrik teknolojilerin karşılaştırılması için mevcut metrikler sınırlıdır.

Kısmi bir çözüm olarak, ABD Savunma Bakanlığı’nın Biyometri Yönetim Ofisi ve diğer gruplar standart test metodolojileri geliştirmektedir. Bu çalışmanın çoğu Ortak Ölçütlerin bağlamsal çerçevesi içinde gerçekleşiyor. Uluslararası güvenlik camiasının tüm güvenlik ürünlerinin değerlendirilmesini ve karşılaştırılmasını standartlaştırmak için geliştirdiği bir modeldir.

**Seçim kriterleri (Selection Criteria)**

Statik, entegre veya dinamik bir biyometrik sistemin seçimi, algılanan kullanıcı profillerine, diğer sistemler veya veri tabanları, çevre koşulları ve her özellik için diğer parametrelerle arayüz oluşturma ihtiyacına bağlıdır :

• Kullanım kolaylığı

• Hata insidansı

• Doğruluk

• Maliyet

• Kullanıcı kabülü

• Gerekli güvenlik seviyesi

• Uzun vadeli uygunluk

Hata oranı dışında her parametrenin derecesi orta ila çok yüksek arasında değişir. Hata insidansı parametresi, hataya neyin sebep olduğu hakkında kısa bir açıklama (örneğin kafa travması, yaş ve gözlük) anlamına gelir. Bu aynı zamanda bir sahtekarın doğru bir şekilde doğrulanabilme olasılığıdır (yetkili bir kişinin erişiminin reddedildiği durumlarda yanlış reddetmenin aksine yanlış kabul).

**Sonuç (Conclusion)**

Biyometri çağına giriyoruz. Bir zamanlar araştırma projesi olarak etiketlenen birçok teknoloji artık pazarlanabilir durumda. Onların popülaritesi, biyometrilerin şifreleri çalmak, unutmak veya kaybetmek konusunda daha zor olduğu gerçeğine bağlıdır. Bununla birlikte, her biyometrik türün kendi sınırlamaları vardır. Tüm bireyler için işe yaramayacaktır, çünkü bazılarının biyometrik bir sistemin şablon olarak kayıtsız kalması yetersizliği olabilir. Ayrıca görünüşlerini belirgin biçimde değiştiren bireylerle çalışmazlar.

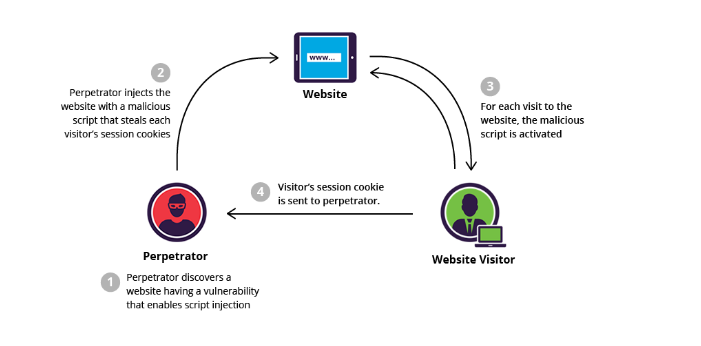
Yüz, ses ve dudak hareketlerini tanımanın entegrasyonu ilginç olsa da, dudak hareketlerinin daha yüksek tanecikliğine ihtiyaç duyulur. Birçok kişi, ses olmadan dudak okumanın biraz kafa karıştırıcı olabileceğinin farkında değildir. Bu, dudak hareketleri iki veya üç farklı kelime için aynı gibi göründüğü zaman geçerlidir. Giyilebilir biyometri - bir zamanlar bilim kurgu - şimdi bir gerçektir. Yıllar önce çizgi romanlarda görülen, şimdi askeri ve sağlık kullanımı ile ilgili onlar hakkında duyuyor.

Ayrıca, günümüzde dizüstü bilgisayarlar için kişisel bilgi işlem, özel bir anahtar, dijital sertifikalar ve güvenli şifreler içeren bir parmak izi güvenli lockbox ile birlikte. Yarın, birinin arabasına erişmek için birinin parmak ucunu arabanın kapı koluna kaydırması mümkün olabilir. Ancak bu, otomobil üreticileri, hafif havadan ağır havaya kadar çeşitli hava koşullarına uyum sağlayabilecek bir çip yapmayı başaramazsa bu olmayacak.

Bunların hepsi standardizasyon sorunları yarattı. Birlikte çalışabilirlik konusunda standartlar önerilmiş ve birkaçı uygulanmıştır. Bunları takip etmek, hala aşamada olan test metodolojileri için standartlardır. Standardizasyon çabaları daha olgunlaştığında, henüz görmediğimiz yeni biyometrik teknolojiler, pazara giriş yapmalarını sağlayacaktır. Bu teknolojilerin çoğu, gerçek zamanlı ve daha az kısıtlı ortamlarda daha dinamik olacaktır.

Biyometrik teknolojilerin yapacağı ilerlemeye rağmen, bir genetik kusur, hastalık, yaş veya yaralanma nedeniyle biyometrik bir şablonu kaydetme konusunda problem yaşayan bazı kişiler için şifreler burada kalacak. Tabii ki, bu bugün bir varsayımdır. Yarın olmayabilir - özellikle de henüz projelerin üzerinde değil, çığır açan teknolojilerle.

# [**WEB UYGULAMASI GÜVENLIĞI - CROSS SITE SCRIPTING**](http://www.berkgoksel.com/2016/09/web-uygulamas-guvenligi-cross-site_30.html)

[](https://2.bp.blogspot.com/-IFIzGkZPPCo/V9GgWRYgTGI/AAAAAAAAAQU/G2dEDSMDcwo4wdUZwUIBmiVOp04pwL4mgCLcB/s1600/Screen%2BShot%2B2016-09-08%2Bat%2B20.29.02.png)

Cross site scripting, saldırganın hedef web sitesini ziyaret eden tarayıcılar üzerinde komut çalıştırdığı saldırılara verilen isimdir. Saldırganlar cross-site-scripting saldırıları ile web sayfasını ziyaret eden müşterilerin hesap bilgilerini hatta bilgisayarlarını ele geçirebilir, sayfayı ziyaret eden tarayıcıları başka bir sayfaya yönlendirebilir veya sayfanın görünümünü değiştirebilir. Cross site scripting zafiyetleri başka zafiyetler ile birleştiğinde çok daha tehlikeli hale gelmektedir.

Cross Site Scripting üç kategoriye ayrılır :

1. Reflected XSS
2. Dom Based XSS
3. Stored XSS

XSS çoğunlukla web uygulamaların hatalı ya da eksik yapılandırılması ile oluşur. Web uygulaması kendisine gönderilen veriyi filtrelemeden kabul etmesiyle meydana gelir. En zararlı XSS türü Stored XSS’tir, çünkü uygulamaya gönderilen komut kaynak kodda kalıcı olarak yer eder.

**XSS Türleri:**

1. **Reflected XSS:**Kullanıcının girilmesi beklenen parametre yerine Javascript  kodu girerek bunu ekrana yansıtması ile tespit edilebilen XSS çeşitidir.
2. **Stored/Persistent XSS:**Adında anlaşılacağı üzere kalıcı XSS türüdür.Bu sefer girilen payloadlar anlık olarak yansımaz bir veritabanına yada başka bir yere kayıt edilir daha sonradan ziyaret edildiğinde çalışan XSS çeşitidir.
3. **Dom XSS:**Dom (Document Object Model) XSS Dom lardan kaynaklanan XSS dir.Gemelde # işaretinden sonra payload denenmesi ve sayfa yenilendiğinde alert alındığında DOM XSS var denilen XSS açıklığıdır.İşin teorik bilgisi DOM nesnesinden kaynaklandığı için en tehlikeli XSS türü olarak anılmaktadır.

**Xss ile Neler Yapılabilir ?**

**1-) JavaScript ile;**

* Şahısın kamerası ile oynanabilir, görüntü alınabilir.
* Ajax sayesinde kullanıcı kimliği uzak sunucularda ki dosyalara kaydedilebilir
* Botnet ağı kurulabilir.
* Oturum bilgileri alınabilir.

**2-) HTML ile**

* Sayfa yönlendirmesi yapılabilir
* Fake inputlar ile veri toplanabilir
* Sayfalara yönlendirilip veri alınabilir.

**Kaynakça**

<https://gurelahmet.com/xsscross-site-scripting-nedir-ve-xss-lab-uygulamas%C4%B1-web-for-pentester/>

<https://packetstormsecurity.com/files/112152/Cross-Site-Scripting-Payloads.html>

<https://kodedu.com/2014/07/xss-aciklarina-karsisanitize-islemi/>

<http://www.berkgoksel.com/2016/09/web-uygulamas-guvenligi-cross-site_30.html>

<https://www.turkhackteam.org/web-server-guvenligi/1669696-xss-nedir-cesitleri-nelerdir-teorina.html>