

**ATATÜRK ÜNİVERSİTESİ MÜHENDİSLİK FAKÜLTESİ BİLGİSAYAR MÜHENDİSLİĞİ BÖLÜMÜ**

**BMS-302-50-50 BİLGİSAYAR – BİLGİ GÜVENLİĞİ VE YÖNETİMİ**

**Adı ve Soyadı : Muhammed Aziz KURT**

**Fakülte No : 130757009**

**Öğretim Görevlisi’nin Adı: Prof. Dr. Abdulsamet HAŞILOĞLU**

**Section 1.3.1: Biometric Identification**

**Section 1.3.2: Single Sign-On for the Enterprise**

**Araştırma Konusu: Kötü Amaçlı Yazılım Saldırısı**

İçindekiler

[1. Biyometrik Tanımlama 4](#_Toc9979158)

[1.1. Biyometrik Gelişime Giden Geçmiş ve Tarihçe 4](#_Toc9979159)

[1.2 . Biyometrik Gelişim 5](#_Toc9979160)

[1.3. Biyometrik Sistemlerin Özellikleri 7](#_Toc9979161)

[1.4. Doğruluk 7](#_Toc9979162)

[1.5. Yanlış Reddetme Oranı 7](#_Toc9979163)

[1.6. Yanlış Kabul Oranı 7](#_Toc9979164)

[1.7. Çapraz Hata Oranı (CER) 8](#_Toc9979165)

[1.7. Hız ve verim oranı 8](#_Toc9979166)

[1.7. Kullanıcılara Kabul Edilebilirlik 9](#_Toc9979167)

[1.8. Biyometrik Organ ve Eylemin Tekliği 9](#_Toc9979168)

[1.9. Sahteciliğe Karşı Direnç 9](#_Toc9979169)

[1.10. Güvenilirlik 10](#_Toc9979170)

[1.11. Data Storage Requirements 10](#_Toc9979171)

[1.11. Kayıt Süresi 10](#_Toc9979172)

[1.12. Veri Toplamanın Saldırganlığı 10](#_Toc9979173)

[1.12. Konu ve Sistem Temas Gereksinimleri 11](#_Toc9979174)

[1.13. Tarihsel Biyometrik Problemler 11](#_Toc9979175)

[1.14. Performans 11](#_Toc9979176)

[1.15. Donanım ve Yazılım Sağlamlığı 11](#_Toc9979177)

[1.16. Maintenance Requirements 12](#_Toc9979178)

[1.17. Sabotaj Duyarlılığı 12](#_Toc9979179)

[1.18. Kullanım Nedeniyle Algılanan Sağlık Maladies 12](#_Toc9979180)

[1.19. Yönetime Sunulan Özel Bilgiler 12](#_Toc9979181)

[1.20. Kart Sistemlerine Göre Biyometrik Tanımlamanın Özellikleri 13](#_Toc9979182)

[1.21. Kart Sistemi Hata Oranları 13](#_Toc9979183)

[1.22. Biyometrik Veri Güncellemeleri 13](#_Toc9979184)

[1.23. Farklı Biyometrik Sistem Çeşitleri ve Özellikleri 14](#_Toc9979185)

[1.24. Information Security Applications 18](#_Toc9979186)

[1.25.Özet 19](#_Toc9979187)

[2. Kuruluş için Tekli Oturum Açma 20](#_Toc9979188)

[2.1. Evrim 20](#_Toc9979189)

[2.2. Tekli Oturum Açma Nedir: Başlangıç 22](#_Toc9979190)

[2.3. Temel Sorun 23](#_Toc9979191)

[2.4. Mekanizmalar 24](#_Toc9979192)

[2.5. Tekli Oturum Açma Ne Sağlar? 25](#_Toc9979193)

[2.6. Dahili Yetenek Vakfı 25](#_Toc9979194)

[2.7. Genel Özellikleri 26](#_Toc9979195)

[2.8.Son Kullanıcı Yönetim Tesisleri 27](#_Toc9979196)

[2.9. Uygulama Yönetimi Olanakları 27](#_Toc9979197)

[2.10. Uç Nokta Yönetim Olanakları 28](#_Toc9979198)

[2.11. Mobil Kullanıcılar 29](#_Toc9979199)

[2.12.Doğrulama 29](#_Toc9979200)

[2.13.Şifreleme 31](#_Toc9979201)

[2.14. Giriş Kontrolü 31](#_Toc9979202)

[2.15.Uygulama Kontrolü 33](#_Toc9979203)

[2.16 Yönetim 34](#_Toc9979204)

[2.17. Masaüstü Duyarlı Uygulamalar için Hizmetler 35](#_Toc9979205)

[2.18. Güvenilirlik ve Performans 36](#_Toc9979206)

[2.19. Gereksinimler 36](#_Toc9979207)

[2.20. Hedefler 36](#_Toc9979208)

[2.21. İşlevsel gereksinimler 37](#_Toc9979209)

[3.Ek Konu : Kötü amaçlı yazılım saldırısı 37](#_Toc9979210)

[3.1. Kötü Amaçlı Araçlar Sizi Nasıl Etkileyebilir? 37](#_Toc9979211)

[3.2.Kötü Amaçlı Araçlara Karşı Korunma 38](#_Toc9979212)

[4.Kaynakça 39](#_Toc9979213)

# 1. Biyometrik Tanımlama

**Donald R. Richards**

Güvenli bir binaya açılan kapının, bir kişinin fiziksel varlığına göre tanımlanması için otomatik bir sistem kullanılarak açılabildiği bir gün öngörülmekle birlikte, bu kişi kimliğini veya erişim kartını evde mutfak tezgahında bırakmış olsa da. Bir kişinin uçağa girişte biyometrik olarak doğrulanan pozitif bir tanımlamaya dayanarak uçağa girebileceğini, biletsiz havayolu seyahatini hayal edin. Arabaya binmek, motoru sürücünün vizörünü aşağı doğru iterek çalıştırmak, aynaya bakmak ve uzaklaşmak, sadece yetkili kişilerin aracın çalışmasını sağlayabilecekleri konusunda güvence altına alın.

Bu eylemler rutin olan günlük hızla yaklaşıyor. Aslında, hızlı, doğru, güvenilir ve kullanıcı kabul edilebilir biyometrik tanımladı fi katyon sistemlerinin uygulanması zaten devam ediyor. Toplumsal davranış kalıpları otomatik olumlu tanımladı fi katyon sistemleri için gereklilikleri sürekli artan sonuçlanır ve bu daha da hızla büyüyor. Bu sistemler için potansiyel uygulamalar yalnızca bir kişinin hayal gücü ile sınırlıdır. Performans iddiaları gerçekçi inanılmaz tam spektrum kapsamaktadır. Bu yeni teknolojiler ile Sistem uygulama sorunları tahmin edilebileceği yüksek olmuştur. Kullanıcı kabul engeller artıyor. Bu sistemlerin kullanımını öğrenen Güvenlik uygulayıcıları üreticileri ve satıcıları tarafından sağlanan genellikle çelişkili bilgiler ezici miktarlarda karşı karşıyayız.

Bu bölüm, güvenlik uzmanına, biyometrik bir tanımlama sisteminin seçilmesi, kurulması ve çalıştırılmasında olası tehlikelerin önlenmesi için gereken bilgileri sunar. Bu sistemlerin özellikleri, belirli uygulamalar için hangilerinin en önemli olduğu konusunda karar vermeyi mümkün kılmak için ayrıntılı olarak tanıtılmıştır. Biyometrik sistemlerin örgütsel kullanımında yaşanan tarihsel problemler de tartışılmaktadır. Son olarak, piyasada bulunan spesifik teknolojiler, veri toplama süreci, kayıt prosedürü, veri dosyaları, kullanıcı arayüzü işlemleri, hız, sahteciliği önleme bilgileri, doğruluk ve benzersiz sistem özellikleri dahil olmak üzere açıklanmıştır.<br>

# 1.1. Biyometrik Gelişime Giden Geçmiş ve Tarihçe

İnsanlığın ilk günlerinden beri, insanlar varlıklarını koruma sorunu ile mücadele etti. Yetkilendirilmemiş kişilerin, değerli olarak kabul edilen şeyleri, hatta bir yiyecek önbelleğini bile yapmaları etkili ve verimli bir şekilde nasıl önlenebilir? Tabii ki, en kısa sürede elde edilen çözüm, her zaman en yüksek değere sahip varlıklar için olduğu gibi bir bekçi oluşturmaktı. Ardından, şimdi olduğu gibi, insan korumanın, kaynakları korumak için yetersiz ve bazen etkisiz bir yöntem olduğu anlaşıldı.

Sağlam bir kapının oluşturulması, örneğin, penceresiz bir oda veya sağlam bir kapı dışında başka açıklıklar olmayan bir oda, doğru yönde bir adımdı. Oradan kilit ve anahtarın eklenmesi, sürekli korumanın kaldırılmasını sağlayan küçük ama çok etkili bir hareketti. Korunan varlıklara yetkilendirilmiş erişime sahip olanlara, bu anahtarlara sahip oldukları gerçeğine dayanarak yetkili kişilerin tespit edilme döneminin başlangıcı olan anahtarlar verilmiştir. Yüzyıllar içinde, daha iyi güvenlik sağlamak için kilitler ve anahtarlar art arda geliştirildi. Kalıcı sorun kayboldu ve anahtarlar çalındı. Bu olaylar gerçekleştiğinde, tek çözüm kilidi (sonradan sadece silindir) ve zaman alan ve pahalı olan tüm anahtarların değiştirilmesiydi.

Bir sonraki büyük buluş, plastik kartlara sahip anahtar okuyucular tarafından kontrol edilen elektronik kilitlerin ortaya çıkmasıydı. Bu, yetkili kişilerin sahip oldukları şeylere (örneğin, kodlanmış plastik kartlara) dayanarak belirlenmesi dönemini sürdürmüştür. En büyük gelişme, kapının kilidini açmak için kaybolan veya çalınan (anahtar) kartların elektronik olarak kaldırılabilmesiydi. Bu nedenle, hiçbir zaman kilit ve anahtarların değiştirilmesi gerekmiyordu; zaman ve maliyette önemli tasarruflar vardı. Ancak, zaman geçtikçe deneyimler, bazı kişilerin yetkili kişilerin kartlarının kaybolduğunu veya çalındığını bile fark etmeden kaldırıldığını kanıtladı.

Kişisel Kimlik Numarası (PIN) tuş takımının kart okuyucusuna eklenmesi, bildirilmeyen kayıp veya çalınan kart sorununa çözüm oldu. Böylece, yetkili kişilerin sahip oldukları ve bildikleri şeylere (örneğin bir PIN) dayanarak belirlenmesi dönemi başladı. Bu, “kötü adamlar”, çoğu insanın doğum günleri, yıldönümleri veya hayatlarında önemli olan diğer sayılar gibi hatırlamaları kolay PIN'leri seçmesine karar verene kadar iyi çalıştı. Kayıp veya çalınan bir kart ve birkaç deneme ile “kötü adamlar” doğru PIN'i tahmin etmede ve korunan alana erişmede bazen başarılı olmuşlardır.

Açık olan çözüm, yalnızca rastgele sayıları PIN olarak kullanmaktı; bu da, PIN'lerin deneme veya yanılma yoluyla tahmin edilmesi veya bulunması sorununu çözdü. Bununla birlikte, rastgele sayıları hatırlama konusundaki zorluk başka öngörülebilir bir soruna neden olmuştur. PIN'ler (ve şifreler) bir kağıda, Post-It notlarına, ehliyetlerine, not defterlerine, bülten panolarına, bilgisayarlara veya gerektiğinde bulabilecekleri her yere yazılmıştır. Bazen giriş kartlarına kendileri yazılmışlardı. Ek olarak, girilen PIN'lerin gözlenmesi genellikle kolay olduğu için, hırsızlığı planlayan “kötü adamlar” bazen ilgili kartı çalmadan önce bu numarayı elde edebiliyorlardı. Bu senaryolar, kart okuyucuların, PIN'leri olanlar dahil olmak üzere, yetkili girişi olan kişilerin kimliğini olumlu olarak doğrulayamadıklarını göstermektedir.

Erişim kimliğini doğrulamakta gerçekten olumlu olmanın tek yolu, doğrulamayı kişilerin kendi fiziksel özelliklerine (yani biyometrik tanımlama) dayandırmaktır. Kimlik doğrulama gereksinimlerinin çoğu insanlar tam olarak giyindiğinde (boyundan ayağa ve bilekler) gerçekleştiğinden, vücudun bu amaç için uygun olan kısımları eller, yüz ve gözlerdir.

# 1.2 . Biyometrik Gelişim

Gerçekten olumlu bir tanımlamanın sadece kişinin fiziksel özelliklerine dayanabileceği ortaya çıktığında, iki sorunun yanıtlanması gerekiyordu. İlk olarak, vücudun hangi kısmı kullanılabilir? İkincisi, performansta uygulanabilir olması için yeterli doğruluk, güvenilirlik ve hız ile tanımlama nasıl başarılabilir? Bununla birlikte, otomatik kişisel tanımlama gerektiren baskılar en yüksek seviyelerde hızlı bir şekilde artmıyorsa (gerekli kaynakları ve fonları mevcut kılıyordu), bu araştırma gerçekleşmeyecekti.

O zamanlar, evrensel olarak pozitif bir tanımlayıcı olarak kabul edilen insan vücudu ile ilişkili ölçülebilir tek karakter print ngerprint idi. Özel mürekkepler, toz alma tozları ve örneğin bant kullanılarak toplanan iletişim bilgileri, özel olarak eğitilmiş uzmanlar tarafından eşleştirilir. Eşsiz konumlandırılmış dilimler, sırtlar ve çatallanmalar yerleştirilmiş ve şablonlarla karşılaştırılmıştır. Bir cam parçasına bastırılmış bir parmakla yapılan baskıyı okuyabilen bir sensör gerekliydi. Toplanan baskıyı depolanmış bir şablonla eşleştirmek klasik bir bilgisayar görevidir. Neyse ki, bu tanımlama soruları sorulduğunda, bilgisayar işleme yetenekleri ve hızı hızla artarken, boyut ve maliyet düşüyordu. Durum böyle olmasaydı, ilk biyometrik sistem gelişimi bile gerçekleşmezdi.Biyometriklerin yaygın kabul edilebilirlik ve alan proliferasyonu elde etmeleri için 25 yıllık ek bir bilgisayar ve biyometrik ilerleme ve maliyet azaltma işlemi gerçekleştirdi.

Tahmin edilebileceği gibi, erken belirleme belirleyici doğrulama sistemleri piyasada başarılı değildi, ancak yapmak için tasarlandıklarını yapamadıkları için başarılı olamadılar. Onlar yaptı. Kilit problemler yavaş karar verme hızı ve sahte firmaların tespit edebilme yeteneğinin olmamasıydı. Dakikada iki ila üç kişinin iş çıkışı, bekleme çizgileri, kişisel hayal kırıklığı ve üretken zaman kaybına neden olur. Sahte girdilerin (örneğin lastik numaralar, fotoğraf görüntüleri) tespit edilmemesi, sahte uygulamaların yanlış kabul edilmesine neden olabilir.

Hızlı, doğru ve güvenilir biyometrik kimlik doğrulamasının değeri henüz tam olarak mevcut olmasa bile hızlı bir şekilde tanındı. Kısa bir süre sonra, organize biyometrik araştırma ve geliştirme çabalarının sayısı 20'yi aştı. Çoğu gergerger baskı şirketiydi: parmak izi; tam baskı; iplik kalıbı (yani, kısaltıcının alt tarafındaki kırışıklıklar); ve avuç içi baskı. El topografyası (yani, elin parçalarının bir yüzeye karşı yerleştirilmiş yandan görünüşlerinin yükselmesi), doğru doğrulama için yeterince benzersiz olmadığını kanıtlamış, ancak elin üstten bir görünümü (yani el geometrisi) ile birleştirildiğinde, Alandaki en başarılı sistemler. İki geometri, yakın zamanda pazarlanan bir varyasyondur.

En azından bir dereceye kadar pazar kabulü elde eden diğer teknolojiler arasında ses kalıpları, retina taraması (yani göz küresinin içindeki kan damarı şablonu), imza dinamikleri (yani, kalem vuruşlarının hızı, yönü ve baskısı) ve iris yer alır. Tanınma (yani, gözün gözbebeği etrafındaki renkli kısımdaki özelliklerin paterni). Pazara ulaşmış ancak henüz kalmamış diğerleri, tuş dinamiklerini (yani, kelimeleri yazarken ölçülen hız ve zamanın deseni) ve imza tanıma (eşleştirme) içerir. Potansiyel biyometrik tanımlayıcılar olarak araştırılan ve halen araştırılmakta olan diğer fiziksel özellikler arasında, uzunluk uzunluğu (tamamen benzersiz olmasa da), bilek damarları (altta), el damarları (elin arkası), mafsal kırışıklıkları (bir bar tutulduğunda),ert parmak ucu yapısı (derinin altındaki kan damarı modeli), sections bölümleri (birinci ve ikinci eklem arasında), kulak şekli ve dudak şekli. Bir kuruluş, vücut kokusuna dayanan biyometrik tanımlamayı araştıran önemli miktarda para ve zaman harcamaktadır.

Dikkat çekici (ve fonlama) alan doğrulama alanını tanımlayan bir başka biyometrik yüz tanımadır. Bu kısmen, standart görüntü teknolojisi ile yüz görüntüleri elde etmenin kolaylığından ve başarılı bir yüz tanıma sisteminin yararlanabileceği algılanan yüksek kazanımın sonucudur. Yüz termografisi (yani yüz dokusunun ısı düzenleri), yüksek kamera maliyeti nedeniyle pahalı bir varyasyondur. Biyometrik belirleyici doğrulama sistemlerinin gelişiminin tarihi tam olmaktan uzaktır. Girişimciler daha hızlı, daha doğru ve güvenilir teknoloji için zengin ödüller görmeye devam ediyorlar ve gelişmiş gelişim devam edecek. Ancak, gelişmelerin mevcut teknolojilerin iyileştirilmesi veya değişmesi olması bekleniyor. Bunlar, “ne olduğumuz” sistemleri için eller, gözler ve yüz ile ilişkilendirilecektir.ve “yaptığımız” sistemlerin sesi ve imzası.

# 1.3. Biyometrik Sistemlerin Özellikleri

Bunlar, etkili bir biyometrik sistem için gerekli olan önemli faktörlerdir: doğruluk, hız ve verim oranı, kullanıcılara kabul edilebilirlik, biyometrik organın ve eylemin benzersizliği, sahteciliğe karşı direnç, güvenilirlik, veri saklama gereksinimleri, kayıt süresi, veri toplama yetkisizliği ve konu ve sistem iletişim gereklilikleri.

# 1.4. Doğruluk

Doğruluk, bir biyometrik tanımlayıcı doğrulama sisteminin en kritik özelliğidir. Sistem gerçek kişileri sahtekârlardan doğru bir şekilde ayıramazsa, biyometrik bir tanımlama sistemi olarak bile adlandırılmamalıdır.

# 1.5. Yanlış Reddetme Oranı

Genel olarak otantik, kayıtlı kişilerin tanımlanamayan veya doğrulanmamış kişilerin biyometrik bir sistem tarafından reddedilme yüzdesi olarak belirtilen oran, sahte reddetme oranı olarak adlandırılır. Yanlış ret bazen Tip I hata olarak adlandırılır. Erişim kontrolünde, eğer “kötü adamları” dışarıda tutmak şartsa, yanlış reddetme en az önemli hata olarak kabul edilir. Bununla birlikte, diğer biyometrik uygulamalarda, en önemli hata olabilir. Müşteri kimliğini ve hesap bakiyesini doğrulamak için bir banka veya perakende mağazası tarafından kullanıldığında, yanlış reddetme, işlemin veya satışın (ve ilişkili ürün) kaybolduğu ve müşterinin üzüldüğü anlamına gelir. Çoğu bankacı ve perakendeci, yanlış reddetmediği sürece birkaç yanlış kabul etmeye isteklidir.

Yanlış reddetmeler ayrıca, verim, hayal kırıklığı ve engelsiz işlemler üzerinde olumsuz etkiye sahiptir, çünkü personel hareketlerinde gereksiz gecikmelere neden olurlar. Bazen yanlış bir şekilde reddedilme ile ilişkilendirilen ilgili bir problem, edinilememesidir. Elde edilememesi, biyometrik sensöre, gerçek veya sahtekar bir karar vermek için yeterli miktarda kullanılabilir veri sunmadığında meydana gelir. Örnek olarak, baskı sistemi üzerindeki lekeli baskılar, el geometrisi sisteminde yanlış el konumlandırma, retina veya iris sisteminde yanlış hizalama veya bir ses sisteminde mırıldanma sayılabilir. Denekler, kazayla ya da bilerek yaralama sorunlarına neden olurlar.

# 1.6. Yanlış Kabul Oranı

Genel olarak, kayıtlı olmayan kişilerin veya sahtekârların otantik olarak kabul edildiği bir yüzde olarak ifade edilen oran, bir biyometrik sistem tarafından kayıtlı kişilerin sahte kabul oranı olarak adlandırılır. Yanlış kabul bazen Tip II hatası olarak adlandırılır. Bu, genellikle bir biyometrik erişim kontrol sistemi için en önemli hata olarak kabul edilir.

# 1.7. Çapraz Hata Oranı (CER)

Bu aynı zamanda eşit hata oranı olarak da adlandırılır ve genellikle yanlış reddetme oranı ve yanlış kabul oranının eşit olduğu bir yüzde olarak ifade edilen noktadır. Bu, biyometrik sistem doğruluğunun en önemli ölçüsü haline geldi. Tüm biyometrik sistemler hassasiyet ayarlama özelliğine sahiptir. Yanlış kabul istenmediğinde, sistem kayıt verileri ve giriş verilerinin (neredeyse) mükemmel eşleşmesini gerektirecek şekilde ayarlanabilir. Bu yapılandırmada test edilirse, (yanlış) sıfır yanlış kabul oranı elde etmek için sistem doğru bir şekilde ifade edilebilir. Yanlış reddedilme istenmiyorsa, bu sistem yalnızca kayıt verileriyle eşleşmeye yaklaşan girdi verilerini kabul etmek için yeniden ayarlanabilir. Bu konfigürasyonda test edilirse, sıfıra yakın bir reddetme oranı elde etmek için sistem doğru bir şekilde ifade edilebilir. Ancak,Gerçek şu ki biyometrik sistemler aynı anda sadece bir hassasiyet ayarında çalışabiliyor.

Gerçek şu ki, sistem hassasiyeti yanlış kabulü en aza indirecek şekilde ayarlandığı zaman, yakından eşleşen veriler desteklenecek ve yanlış reddetme oranı belirgin şekilde artacaktır. Tersine, sistem hassasiyeti yanlış reddetmeleri en aza indirecek şekilde ayarlandığında, yanlış kabul oranı belirgin şekilde artacaktır. Böylece, yayınlanan (yani, doğru olan) veriler hikayenin sadece bir kısmını söyler. Alan işlemlerinde gerçek sistem doğruluğu kabul edilenden daha az olabilir. Bu, tek bir biyometrik sistem doğruluğu ölçüsü ihtiyacını yaratan durumdur. Çapraz hata oranı (CER), çeşitli sistemlerin performansını karşılaştırırken adil ve tarafsız olan tek bir ölçüm sağlar. Genel olarak, eşit hatayı üreten hassasiyet ayarı, sistemin ikinci çalışması için optimum olan ayara yakın olacaktır.Yüzde 2'lik bir CER sağlayan bir biyometrik sistem, yüzde 5'lik bir CER'ye sahip bir sistemden daha doğru olacaktır.

# 1.7. Hız ve verim oranı

Hız ve verim oranı, en önemli biyometrik sistem özellikleridir. Hız, genellikle sistemin veri işleme yeteneği ile ilgilidir ve kabul etme veya reddetme kararının ne kadar hızlı bir şekilde telaffuz edildiği olarak ifade edilir. Aslında, tüm kimlik doğrulama prosedürüyle ilgilidir: sisteme adım atmak; kartın veya PIN'inin girilmesi (bir doğrulama sistemi ise); bir el veya numara ekleyerek, bir gözü hizalayarak, erişim kelimelerini söyleyerek veya bir isim imzalayarak fiziksel verileri girmek; veri dosyalarının işlenmesi ve eşleştirilmesi; kabul etme veya reddetme kararının bildirilmesi; ve eğer bir portal sistem ise, kapıdan geçerek ve kapanarak.

Genel olarak kabul edilmiş standartlar, başlangıçtan karar vermeye kadar beş saniyelik bir sistem hızını içerir. Diğer bir standart, kapıdan altı ila on saniyeye / kişiye eşit olan altı ila on / dakikalık bir portal verimidir. Sadece son yıllarda biyometrik sistemler bu hız standartlarını karşılayabilecek hale geldi ve bugün bile bazı pazarlanan sistemler bu hızlılığı sürdürmüyor. Yavaş hız ve sonuçta ortaya çıkan bekleme hatları ve hareket gecikmeleri, biyometrik sistemlerin ve hatta biyometrik şirketlerin başarısızlığa uğramasına neden oldu.

# 1.7. Kullanıcılara Kabul Edilebilirlik

Kullanması gereken insanlara sistemin kabul edilebilirliği, biraz fark edildi, ancak biyometrik tanımlama işlemlerinde giderek daha önemli bir faktör oldu. Başlangıçta, az sayıda sistem varken, çoğu yüksek güvenlikli ve az sayıda kullanıcının sistemleri kullanmak için yüksek bir teşviği vardı; kullanıcı kabulü çok az ilgi çekiyordu. Ayrıca, ekran baskısı ve el sistemlerinde çok az kullanıcı tehdidi görülmüştür.

Biyometrik sistem kabulü, sistemi kullanması gerekenler - organizasyon yöneticileri ve herhangi bir sendika mevcutsa - hepsi korumaya ihtiyaç duyan varlıklar olduğu konusunda hemfikir olduklarında, biyometrik sistem bu varlıklara erişimi etkin bir şekilde kontrol ettiğinde, sistem kullanımının kullanıcı sağlığı için tehlikeli olmadığı durumlarda ortaya çıkar. sistem kullanımı, personel hareketini uygunsuz bir şekilde engellemiyor ve üretimde gecikmelere neden olmuyor ve sistem, yönetimin kullanıcılar hakkında kişisel veya sağlık bilgisi toplamasını mümkün kılmıyor. Taraflardan biri sistemin başarısını veya kaldırılmasını etkileyebilir. İşbirlikçi olmayan kullanıcılar, açık veya gizli bir şekilde sistem ekipmanlarını tehlikeye atacak, hasar verebilecek veya sabote edeceklerdir. Birliğin biyometrik sistemin sözleşmelerine dahil edilmesinin maliyeti çok maliyetli olabilir. Dahası, yönetim, biyometrik sistemin faydalarından faydalanıp yararlanmadığına dair karar vermiştir.

# 1.8. Biyometrik Organ ve Eylemin Tekliği

Biyometrik sistemlerin amacı, personelin pozitif tanımlanması olduğundan, bazı kuruluşlar (örneğin, hükümetin unsurları), yalnızca benzersiz (yani, dünyada yinelenmeyen) fiziksel özelliklere dayanan sistemler belirlemektedir. Bunun sebebi, tabanın benzersiz bir karakteristik olması durumunda, bir eşleşmenin, bunun doğru kişi olması ihtimalinin yüksek olduğu bir ifadeden ziyade pozitif bir tanımlaması olmasıdır. Biyometrik tanımlama için kullanılan sadece üç fiziksel özellik veya insan organı benzersizdir: etiket izi, gözün retinası (yani, göz küresinin arkasındaki kan damarı modeli) ve gözün irisi gözbebeği çevreleyen gözün renkli kısmında bulunan özellikler). Bu özellikler çilleri, halkaları, çukurları, şeritleri, damarları, koronatları ve kriptoları içerir.

# 1.9. Sahteciliğe Karşı Direnç

Sahte girdi verilerini algılama veya reddetme yeteneği, yüksek güvenlik gereksinimlerini karşılayan bir biyometrik erişim kontrol sistemi için hayati öneme sahiptir. Bunlar, el veya parmak izi sistemlerinde ölen kişinin kauçuk, plastik veya hatta ellerinin veya parmaklarının kullanımını ve ses sistemlerine kopyalanmış veya kaydedilmiş girişleri içerir. James Bond veya Terminator ms lms gibi eğlence medyası, ölen (ya da otantik) kişilerin kafalarının ya da gözlerinin korunan varlıklara ya da bilgilere erişim elde etmek için gözlerinin kullanıldığı durumlarda sık sık güvenlik sisteminin başarısız olduğunu göstermiştir. Erken biyometrik tanımlayıcı doğrulama sistemlerinin çoğu, yüksek güvenlikli erişim kontrol uygulamaları için tasarlandığından, sahte girdi verilerinin tespit edilmemesi veya reddedilmemesi, çeşitli sistem veya organizasyon arızalarının nedeni idi. Sahte verilere direnç, yüksek kaliteli, yüksek hassasiyetli sistemler için bir kriter olmaya devam etmektedir.Bununla birlikte, biyometrik sistemlerin diğer yüksek güvenlikli olmayan tip uygulamalara yayılması, sahteciliğe karşı direnç eksikliğinin gelecekte bir sistemin bozulmasına neden olmayacağı anlamına gelir.

# 1.10. Güvenilirlik

Biyometrik tanımlayıcı doğrulama sistemlerinin sürekli ve doğru operasyonda kalması hayati öneme sahiptir. Sistem, performans doğruluğu veya hızında bozulma veya bozulma olmadan diğerlerinin önüne geçerken yetkili kişilerin erişmesine izin vermelidir. Ek olarak, bu performans standartları, yüksek düzeyde bakım veya sık teşhis ve sistem ayarları yapılmadan sürdürülmelidir.

# 1.11. Data Storage Requirements

Veri depolama gereksinimleri, depolama ortamının çok pahalı olduğu önceki biyometrik sistemlerden çok daha az önemli bir konudur. Bununla birlikte, biyometrik veri dosyalarının büyüklüğü ilgi konusu olmaya devam etmektedir. Mevcut ultra yüksek hızlı işlemcilerde bile, büyük veri dosyalarının küçük dosyalardan daha uzun sürmesi, özellikle de tam tanımlama yapan ve giriş veri tabanındaki veri tabanındaki her bir dosyayla eşleşen sistemlerde daha uzun sürebilir. Biyometrik dosya boyutu 9 ila 10,000 bayt arasında değişmekte olup, çoğu 256 ila 1000 bayt arasında değişmektedir.

# 1.11. Kayıt Süresi

Kayıt süresi de günümüzde daha az önemli bir faktördür. Erken biyometrik sistemler bazen çok fazla tekrar gerektiren ve tamamlanması birkaç dakika gerektiren kayıt prosedürlerine sahipti. İki dakika yerine beş dakikalık bir kayıt gerektiren bir sistem, 1000 kullanıcı kayıt yaptırması gerekiyorsa 50 saatlik pahalı olmayan üretken zamana neden olur. Ayrıca, bekleme süresi göz önüne alındığında, maliyet birkaç kez artar. Kayıt süresi için kabul edilen standart kişi başına iki dakikadır. Bugün piyasadaki sistemlerin çoğu bu standarda uygundur.

# 1.12. Veri Toplamanın Saldırganlığı

Başlangıçta, bu faktör, vücudun içinden biyometrik verilerin toplanmasına ilişkin kaygılar nedeniyle, özellikle de göz küresinin içindeki retina nedeniyle geliştirilmiştir. Erken sistemler retinayı kırmızı ışık ışınıyla aydınlattı. Bununla birlikte, bu durum, lazerlerin halkın bilinçlendirilmesiyle aynı zamana denk gelmekte olup, bazen kırmızı ışık demeti çelik kesmektedir. Hiçbir zaman retina taramasından kaynaklanan bir kullanıcı yaralanması iddiası olmamasına rağmen, kullanıcı hassasiyeti, vücudun içine giren herhangi bir girintiyi içerecek şekilde vücuda giren kırmızı ışıklara dirençten genişledi. Bu kullanıcı hassasiyeti şimdi algılanan kişisel alana yapılan izinsiz girişlerle ilgili endişeleri artırdı.

# 1.12. Konu ve Sistem Temas Gereksinimleri

Bu faktör muhtemelen bir sonraki adım veya müdahaleci olmanın devamı olarak düşünülebilir. Endikasyonlar, biyometrik sistem kullanıcılarının yüzlerce başka bilinmeyen kişinin (kendilerine) biyometrik veri toplama için temas kurmaları gereken yüzeylerle fiziksel temasta bulunma zorunluluğuna giderek daha duyarlı hale geldiğidir. Bu kaygılar, dudaklara yakın bir el cihazında tutmayı ve konuşmayı gerektiren ses sistemlerini içerir. “Bir şeyi yapmayı seçersem sorun değil, bir kuruluş veya toplum aynı şeyi yapmamı isterse, yanlış olduğunu” hissediyor gibi görünen bir kullanıcı var gibi görünüyor. Bunun anlamlı olup olmadığı. Biyometrik sistemlerin kullanımı üzerinde etkisi olan toplumda yayılan bir tutum. Video kamera veri toplama kullanan sistemler bu kategoriye girmez.

# 1.13. Tarihsel Biyometrik Problemler

Son 25 yılda biyometrik sistemlerin kullanımında çeşitli sorunlar tespit edilmiştir. Bazıları üstesinden gelinmiştir ve bugün nadiren görülürler; diğerleri hala meydana gelir. Bu problemler arasında performans, donanım ve yazılım sağlamlığı, bakım gereklilikleri, sabotaj duyarlılığı, kullanım nedeniyle algılanan sağlık sorunları, yönetime sunulan özel bilgiler ve sistemi kullanmak için gereken beceri ve işbirliği sayılabilir.

# 1.14. Performans

Biyometrik tanımlayıcı doğrulama sistemlerinin saha performansı genellikle üreticilerin veya laboratuvar testlerindeki deneyimlerden farklıdır. Söz verilmiş performansı sağlamayan bir sisteme takılmamak için iki yol vardır. İlk olarak, bağımsız ve tarafsız bir test kuruluşu tarafından test edilen teknolojilere ve sistemlere yönelik düşünceleri sınırlandırın. New Mexico, Albuquerque'de bulunan Sandia Ulusal Laboratuvarları, Enerji Bakanlığı için uzun yıllardır biyometrik sistem testleri yapmıştır ve bazı raporları mevcuttur. İkincisi, herhangi bir sistem üreticisi veya satış temsilcisi, şu anda sistemlerini kullanan kuruluşların bir listesini sunabilmelidir. Uygulaması şu anda planlananlara benzeyen kullanıcıları belirtebilmelidirler (planlanan işlem yeni ve benzersiz bir uygulama değilse).Ayrıntılı tartışmalar ve belki de bir site ziyareti, benzer uygulama gereksinimlerine sahip mevcut kullanıcılar ile çoğu soruya cevap vermeli ve birçok sürprizle karşılaşmamalıdır.

# 1.15. Donanım ve Yazılım Sağlamlığı

Küçük ve orta ölçekli kullanıcı veritabanlarında çok etkili olan bazı sistemler ve teknolojiler, büyük veritabanlarında kabul edilemez olan bir performansa sahiptir. Ortaya çıkan sorunlar arasında sistem yavaşlaması ve hassasiyetin bozulması bulunur. Bazı biyometrik sistem kullanıcıları, sistemlerini atmak ve kuruluşlarının daha başarılı olması, beklenenden daha hızlı büyümesi ve eski sistemin büyümeyle başa çıkamaması nedeniyle baştan başlamak zorunda kaldı. Kuruluşla orijinal sistemlerini “büyütmeyi” umarlarsa, sistem yöneticileri en iyimser büyüme tahminini en az iki katına çıkarmalı ve bu yükü kaldırabilecek bir sistem için plan yapmalıdır. Bir diğer husus, beklenen şartlar altında genişletilmiş kullanıma dayanacak donanım yeteneğidir. Bir örnek, erken imza dinamik sistemleridir.Bu test sırasında ve erken gelişim döneminde yeterli bir şekilde gerçekleştirilmiştir. Ancak, vuruş yönü, hızı ve basıncı tespit etmek için kullanılan kalem ve ekran sensörleri çok küçük ve hassastır. Aylar veya bir yıllık normal kamusal kullanımdan sonra, sistem performansı, sistemlerin artık etkili tanımlayıcıları olmadığı noktalara düşmüştür.

# 1.16. Maintenance Requirements

Bazı sensörler ve sistemler, etkili işlemlere devam etmek için çok yüksek seviyede önleyici bakım veya teşhis ve ayar gerektirmiştir. Belirli işletme ve kullanıcı koşullarında (örneğin, tozlu alanlar veya sık sık el losyonu veya krem ​​kullananlar), bazı parmak izi sensörlerinin doğruluğun bozulmasını önlemek için her gün olduğu kadar sık ​​temizlenmesi gerekir. Diğer sistemler haftalık veya aylık olarak teşhis ekipmanlarının bağlanması, performans parametrelerinin değerlendirilmesi ve üretken performansı korumak için dikkatli ayar yapılmasını talep ediyordu. Bu insan müdahaleleri sadece normal güvenlik sürecini bozmakla kalmıyor, aynı zamanda işletme maliyetlerini de önemli ölçüde artırıyor.

# 1.17. Sabotaj Duyarlılığı

Duvarlardan uzaktaki ya da birçok hareketli parçadan çıkıntı yapan kaide üzerinde veri toplama sensörleri bulunan sistemler, genellikle hasarı sabote etmeye veya devre dışı bırakmaya duyarlıdır. Eğirme zemini cilalayıcı kulpları veya ceplerinden çıkan çekiçler göze çarpmayan veya yanlışlıkla sensörleri etkileyebilir. Bu olaylar, sıklıkla yaygın kullanıcı veya biyometrik sisteme sendika direnci olduğunda meydana gelmiştir.

# 1.18. Kullanım Nedeniyle Algılanan Sağlık Maladies

Yeni sistemler ve teknolojiler geliştirilip AIDS, Ebola ve E. coli gibi yeni virüs ve hastalıklara karşı halkın duyarlılığı büyüklük sırasına göre arttıkça, kabul edilebilirlik daha önemli bir konu haline geldi. Olası organ hasarı ve hastalığın biyometrik sistem kullanımından kaynaklanan potansiyel yayılma algıları, nihayetinde, bir sistemin satışları üzerinde tamamen yeniden tasarlanması gereken yıkıcı bir etki yarattı. Her ne kadar orjinal ünitelerin binlerce tanesi başarılı bir şekilde tanımlanmış olsa da, yeni paketlenmiş teknolojinin popülaritesini yeniden kazanıp kazanmadığı ya da hayatta kalmadığı görülüyor. Bunların tümü, bir sistemin tek kullanımlık bir sonucu olarak, sistem kullanımı sonucunda hastalanan veya yaralanan olduğu iddiası bile olmadı. Son zamanlarda ortaya çıkan bulaşıcı hastalıkların birçoğu kirlenmiş bir yüzeye basit temasla yayılabilir.Biyometrik sistemler birçok uygulamada daha geniş pazar penetrasyonu sağladığından, kullanıcı sayıları logaritmik olarak artmaktadır. Biyometrik verilerin alınması için kullanıcıların fiziksel olarak temasa geçilmesini gerektiren sistemler ve teknolojiler konusunda giderek daha hassas hale geldiğine dair göstergeler gelişmektedir.

# 1.19. Yönetime Sunulan Özel Bilgiler

Bazı sağlık olayları, göz küresi içindeki kan damarı paterninde (yani retinada) değişikliklere neden olabilir. Bunlar diyabet ve felç içerir. Retina bazlı biyometrik sistemin, yönetimin, sistem kullanıcılarının zararına kullanılabilecek sağlık bilgilerinin uygunsuz bir şekilde elde edilmesini sağladığına dair iddialar yapılmıştır. Senaryo, rutin bir kullanıcıyı tanımlayamayan sistemle başlar. Kullanıcı kolayca doğrulanır ve tekrar kaydedilir. Sonuç olarak, yönetimin yeniden kayıt raporunu not edeceği ve bu kullanıcının sağlıkla ilgili küçük bir olayı olduğu sonucuna varılacak (kullanıcı ertesi iş günü mevcut olduğu için küçük). Bu çalışanın bir sonraki sağlık olayının önemli bir tıbbi maliyete neden olacağı beklentisiyle, yönetim fesih nedeni bulabilir (veya yaratabilir). Bu iddia edilen senaryonun fiili bir oluşumu olmadığı gerçeğine rağmen,Bu folklor biyometrik endüstrisinde duyulmaya devam ediyor.

# 1.20. Kart Sistemlerine Göre Biyometrik Tanımlamanın Özellikleri

Biyometrik tanımlayıcı doğrulama sistemleri insanları kontrol eder. Doğru eli, gözü, yüzü, imzası veya sesi olan kişi bulunmuyorsa, tanımlama ve doğrulama yapılamaz ve istenen işlem (örneğin portal geçişi, veri veya kaynak erişimi) gerçekleşmez. Çoğu zaman gösterdiği gibi, rakipler ve suçlular PIN ekleme gerektiren kartlar bile olsa erişim kartlarını alıp başarılı bir şekilde kullanıyorlar. Bunun nedeni, bu sistemlerin insanlar yerine yalnızca plastik parçaları (ve bazen bilgileri) kontrol etmeleridir. Gerçek varlık ve kaynak koruması, kartlar ve bilgilerle değil insanlar tarafından gerçekleştirilebilir, çünkü yetkisiz kişiler kartları ve bilgileri alabilir. Ayrıca, yaşam döngüsü maliyetleri önemli ölçüde azalır, çünkü kart veya PIN yönetim sistemi veya personel gerekmez.Yetkili kişi fiziksel özelliklerini (yani eller, yüz, gözler, imza veya ses) kaybetmez, ancak kartlar ve PIN'ler sürekli olarak kaybolur, çalınır veya unutulur. Bu nedenle, kart erişim sistemlerinin, sistemlerin ve insanların (yeni) kartları ve PIN'leri yönetmesini, kontrol etmesini, kaydetmesini ve vermesini gerektirir. Üstelik, kartlar pahalı ve tekrar eden bir maliyettir.

# 1.21. Kart Sistemi Hata Oranları

Erişim kartı yanlış ellerde, kaybolduğunda veya çalındığında yanlış kabul oranı yüzde 100'dür. Sağ kart yanlış şekilde kaydırıldığında ya da sadece sistemi etkinleştirmediğinde yanlış bir reddetmedir. (Kapının kilidini açmak için otel odası erişim kartlarını tekrar denemek için kaç kere düşünün.) Aslında, bir kart unutulduğunda ve bu kişi kapıdan geçemediğinde yanlış bir reddetmedir.

# 1.22. Biyometrik Veri Güncellemeleri

Zaman içinde değişiklik gösterebilecek ölçüm özelliklerine ve özelliklerine dayalı teknolojiler kullanan bazı biyometrik sistemler, veritabanı her kullanımda güncellendiğinde en iyi şekilde çalışır. Bunlar öncelikle “yaptığımız” teknolojilerdir (ses, imza ve tuş vuruşu). Bütün sistemler bunu yapmaz. Bu sistemler tarafından ölçülen eylem zaman içinde kademeli olarak değişir. Ses insanlar yaşlandıkça değişir. Ayrıca ağırlıktaki değişikliklerden ve bazı sağlık koşullarından da etkilenir. Zaman içindeki imza değişiklikleri kolayca belgelenir. Örneğin, ilk başkanlığının başında Franklin D. Roosevelt imzasına bakın. Her isim ve başlangıç ​​açıkça görülebilir. Daha sonra, sadece sekiz yıl sonra üçüncü döneminde imza ile karşılaştırın. Kendisine aşina olanlar için, vuruşlar ve çizgiler açıkça başkanın imzasıdır; ama başkalarına,adıyla veya başka bir kelimeyle hiçbir ilişkisi yoktur. Tuş vuruş desenleri, zamanla, özellikle yazma sıklığına bağlı olarak benzer şekilde değişir.

Veritabanını güncelleyen sistemler, tanımlama işlemi tamamlandıktan sonra mevcut girdi verilerini veri tabanı şablonuna ortalar. Bazıları daha eski bir veri girişini de siler ve bu veritabanını hareketli bir ortalama yapar. Girdi verilerindeki bu kademeli değişiklikler, kullanıcı kimliğini aylarca veya yıllarca etkilemeyebilir. Bununla birlikte, veri tabanı dosyası ve giriş verileri birbirinden ayrıldıkça, giderek artan şekilde yanlış yapılan reddedilmeler, yeniden kaydolmanın dikte edilmesi için yeterince rahatsızlık yaratacaktır.

# 1.23. Farklı Biyometrik Sistem Çeşitleri ve Özellikleri

Bu bölümde farklı biyometrik sistemler açıklanmaktadır: ger ngerprint sistemleri, el geometrisi sistemleri, ses paterni sistemleri, retina paterni sistemleri, iris paterni sistemleri ve imza dinamiği sistemleri. Her sistem için, aşağıdaki özellikler açıklanmaktadır: kayıt prosedürü ve zamanı, şablon veya dosya boyutu, gereken kullanıcı eylemi, sistem yanıt süresi, herhangi bir sahteciliği önleme yöntemi, doğruluk, alan geçmişi, yaşanan sorunlar ve benzersiz sistem özellikleri .

Parmak İzi Sistemleri Bu bölümdeki bilgiler, teknolojisi parmak izine dayanan birkaç biyometrik tanımlayıcı doğrulama sistemi hakkındaki bilgilerin bir derlemesidir. Veri Toplama Parmak izi verileri, nesneler sık ​​sık camlarına veya polikarbonat plakalara bastırıldığında elde edilir. Ekranda görüntü kaydedilmemiş. Sırtların, genel hatların, çizgilerin, çatallanmaların ve kesişmelerin göreceli konumu ile ilgili bilgiler kayıtlı bir kullanıcı veri tabanı olarak depolanır ve daha sonra kullanıcı giriş verileri ile karşılaştırılır. Kayıt Prosedürü ve Zaman Belirtildiği gibi, konu tuş takımına bir ila dokuz haneli PIN girer. İşaretlendiği gibi, düğme okuyucu plaka üzerine yerleştirilir ve ardından çıkartılır. Dijitalleştirilmiş bir kod oluşturulur. İşaretlendiği gibi, kalibratör kalibrasyonu için cihaz dört kez daha yerleştirilir ve çıkarılır. Gerekli toplam kayıt süresi iki dakikadan az.Şablon veya Dosya Boyutu Parmak İzi kullanıcı dosyaları genellikle 500 ila 1500 bayt arasındadır. Kullanıcı Eylemleri Gerekli Neredeyse tüm parmak izi bazlı biyometri, doğrulama sistemleridir. Kullanıcı, klavyeden bir PIN girerek veya bir kart okuyucu kullanarak tanımlamayı belirtir ve ardından okuyucu plakasına bir numara yerleştirir. Sistem Tepki Süresi Onaylandı ve onaylanmadı kararının görsel ve sesli bir şekilde bildirilmesi, yedi saniyede gerçekleşir.Sistem Tepki Süresi Onaylandı ve onaylanmadı kararının görsel ve sesli bir şekilde bildirilmesi, yedi saniyede gerçekleşir.Sistem Tepki Süresi Onaylandı ve onaylanmadı kararının görsel ve sesli bir şekilde bildirilmesi, yedi saniyede gerçekleşir.

Doğruluk

Bazı parmak izi sistemleri, hatalı kabul oranını yüzde 0,0 olarak elde etmek için ayarlanabilir. Sandia National Laboratories, 1991 ve 1993 yıllarında en yüksek dereceli bir baskı sistemi testinde üç kez hatalı bir reddetme oranı olan% 9,4'ü ve% 5'lik bir çaprazlama hata oranını üretti. Alan Tarihi Örneğin, devlet yararlarının ödenmesi için erişim kontrolü ve kimlik doğrulaması için binlerce birim belirlenmiştir. Sorunlar Büyük kullanıcı popülasyonuna sahip deneyimli Sistem operatörlerinin, derinin derisini ve sistem doğruluğunu olumsuz yönde etkileyen kiri temizlemek için sensör plakalarını sık sık temizlemek için sık sık ihtiyaç duyulur. Eşsiz Sistem Yönleri Kir birikmesi probleminden kaçınmak için yeni geliştirilen bir baskı sistemi, baskı görüntüsünü ultrasonla elde eder. Bu sistemin lateks eldivenli bir cerrahın baskı iznini alabildiği iddiaları yapılmıştır.Bir dizi şirket, baskıya dayalı biyometrik tanımlama sistemleri üretiyor.<br>El Geometrisi Sistemi El geometrisi verisi, el ve uzunlukların uzunluk, genişlik ve yüksekliğinin üç boyutlu kaydıdır, aynı anda dikey ve yatay kamera görüntüleri ile elde edilir.

Kayıt Prosedürü ve Zaman Konu, elinizi between parmakların arasına mandallara karşı yerleştirilmiş bir ızgara plakasına yerleştirmek üzere yönlendirilir. Dört konumlu lamba, ellerin uygun şekilde konumlandırılmasını sağlar. Dijital kamera, yan görünüm için 45 derecelik bir ayna kullanarak üstten bir yandan ve yandan bir görünüm kaydeder. Konu çekilmeye ve daha sonra eli iki kez daha konumlandırmaya yönlendirilir. Okunan değerlerin tek bir kodda ortalaması alınır ve bir PIN verilir. Toplam kayıt süresi iki dakikadan az. Şablon veya Dosya Boyutu El geometrisi kullanıcı boyutu dokuz bayttır. Gerekli Kullanıcı İşlemleri El geometrisi sistemi sadece bir tanımlayıcı olarak çalışır. Kullanıcı bir tuş takımına bir PIN girerek veya bir kart okuyucu kullanarak kimlik belirleme sağlar. Ünite ekranında “el koy” mesajı göründüğünde, kullanıcı elini plaka üzerine mandallara yerleştirir. Dört ışık da doğru el pozisyonunu doğruladığında, veriler elde edilir ve “el kaldır” mesajı görüntülenir. Sistem Müdahale Süresi Onay ya da onaylama kararının görsel ve sesli uyarısı üç ila beş saniye içinde gerçekleşir. Rekabet Karşıtı Metod Üretici, “sistem, canlı bir elin kullanılmasını sağlamak için kontrol eder” diyor. Accuracy Sandia National Laboratories testleri, tek denenmiş bir yanlış kabul oranını% 0,1'den daha az, üç denemeli bir yanlış kabul oranını% 0,1'den daha az ürettiğini belirtti. ve yüzde 0.2 ve 2.2 çaprazlama hata oranları (yani iki test). Alan Tarihi Erişim kontrolü, kolej kafeteryaları ve yurtlar ve devlet tesisleri için binlerce birim seçildi. El geometrisi, Enerji Bölümü ve Göçmenlik ve Vatandaşlığa Kabul Hizmeti'nin tercih ettiği orijinal biyometrik sistemdi. Ayrıca, Atlanta'daki 1996 Olimpiyatları'nda Sporcunun Köyü'nü korumak için de kullanıldı.

Deneyimli Sorunlar Bazı uygulamalardan bazıları ilk Sandia testinin doğruluk sonuçlarına ulaşmamıştır. Kullanıcı veritabanları yüzlerce olduğunda, doğrulama doğruluğunun, veritabanları binler arasında büyüdüğü zaman kötüleştiğine dair göstergeler olmuştur. Eşsiz Sistem Yönleri Dokuz baytlık el geometrisi kullanıcı kodu, şu ana kadar mevcut biyometrik sistemlerin en küçüğüdür. El geometrisi tanımlama sistemleri Recognition Systems, Inc. Tarafından üretilir. İki geometri tanımlama sistemi olan bir varyasyon BioMet Partners tarafından üretilir.

Ses Düzeneği Sistemleri Yedi nazal ton parametresi, gırtlak ve boğaz titreşimleri ve ses kaynaklı hava basıncı, ses ve diğer sensörler tarafından yakalanır. Kayıt Prosedürü ve Zaman Çoğu ses sistemi, standart bir telefona benzer ekipman kullanır. Belirtildiği gibi, konu ahizeyi kaldırır ve telefon tuş takımında bir PIN girer. Telefon ahizesinde işaretlendiğinde, kişi kendi PIN'ini, adını veya diğer dört ila altı kelimelik bir cümle olabilen erişim cümlesini konuşur. Geçiş işareti ve erişim ifadesi dört defa tekrarlanır. Gerekli toplam kayıt süresi iki dakikadan az. Şablon veya Dosya Boyutu Sesli kullanıcılar sistem üreticisine bağlı olarak 1000 ila 10.000 bayt arasında değişir. Kullanıcı İşlemleri Gerekli Şu anda, ses sistemleri yalnızca tanımlayıcılar gibi çalışır. Kullanıcı, telefon tipi tuş takımındaki PIN kodunu girerek tanımlama yapar. Telefon ahizesinde işaretlendiği gibi (“lütfen erişim cümlenizi söyleyin” diyen kaydedilmiş ses), telefon ahizesi sensörlerine konuşur. Sistem Yanıt Süresi Sesli cevap (yani, “kabul edildi, lütfen girin” veya “yetkili değil”) ahize ile sağlanır. Bazı sistemler görsel uyarı içerir (örneğin, kırmızı ve yeşil ışıklar veya LED'ler). Toplam işlem süresi 10 ila 14 saniyeye kadar sürebilir. Sahteciliğe Karşı Yöntem “p” veya “t” sesleri söylendiğinde artan hava basıncını ölçmek de dahil olmak üzere çeşitli yöntemler kullanılır. Bazı karmaşık sistemler, kullanıcının her kullanımında, on veya daha fazla kayıtlı kelime listesinden farklı sözcükleri farklı bir sırada konuşmasını gerektirir. Doğruluk Sandia National Laboratories, test ettikleri iki sistem için yüzde 10'dan daha büyük çaprazlama hatalarını bildirdi. Diğer ses testleri planlanmaktadır. Alan Tarihçesi 100'den fazla sistem kurulmuş olup, 1000'den fazla kapı erişim ünitesi, kolejlerde, hastanelerde, laboratuvarlarda ve merkezlerde. Sorunlar Tecrübeli Arka Plan gürültüsü ses sistemlerinin doğruluğunu etkileyebilir. Erişim sistemleri, yoğun, yüksek trafikli ve yüksek gürültü seviyeli sitelere girme eğilimindeki girişlerde, koridorlarda ve girişlerde bulunur. Eşsiz Sistem Yönleri Bazı ses sistemleri, dahili sistem olarak veya diğer sistem kullanıcıları için mesaj bırakmak için de kullanılabilir. Ses tabanlı biyometrik tanımlama sistemleri üreten birkaç şirket var.

Retina Desen Sistemi Sistem, görüntüyü elde etmek için bir kamera kullanarak göz küresinin iç arka kısmında retinadaki kan damarı deseninin elemanlarını kaydeder. Kayıt Prosedürü ve Süresi Konu gözünü sistem açıklığından bir ya da iki cm uzağa yerleştirerek, açıklıkta ortalanmış ünite içinde yanıp sönen yeşil bir nokta tutmaya ve hareketsiz kalmaya yönlendirilir. Ultra düşük yoğunluklu görünmez ışık, retinanın üzerinde 450 derecelik bir dairede 320 nokta okumanızı sağlar. Birimin tuş takımına bir PIN girilir. Gerekli toplam kayıt süresi iki dakikadan az. Şablon veya Dosya Boyutu Retina deseni sayısallaştırılmış dalga biçimi 96 baytlık bir şablon olarak saklanır. Kullanıcı İşlemleri Gerekli Doğrulanıyorsa, kullanıcı tuş takımındaki PIN'i girer. Bir göz açıklığın önüne getirildiğinde ve darbeli yeşil nokta üzerine ortalandığında sistem otomatik olarak veri alır. Kabul veya kabul edilmeme, LCD ekranda gösterilir. Sistem Tepki Süresi Doğrulama sistemi karar süresi yaklaşık 1,5 saniyedir. Tanınan karar süresi, 1.500 katmanlı bir veri tabanı ile beş saniyeden daha kısa. Ortalama işlem süresi dört ila yedi saniyedir. Rekabet Karşıtı Yöntem. Üreticiye göre, sistem “kalıp verilerini elde etmek için canlı, odaklanmış bir göz gerektiriyor”. Doğruluk Sandia Ulusal Laboratuvarları’nın önceki retina modelinde yaptığı test, yanlış kabul ve% 1,5’lik çapraz hata oranı vermedi. Yeni model olan System 2001'de de benzer bir performans sergiliyor. Alan Tarihçesi Yüzlerce orijinal dürbün tipi ünite, bu modeller kesilmeden önce hazırlandı. Kolejlerde, laboratuvarlarda, devlet tesislerinde ve hapishanelerde erişim kontrolü ve tanımlanması için kullanılmıştır. Yeni model, System 2001 şimdi satışta.

Yaşanan Sorunlar Terleyen ya da sulanan kişilerin önceki modellerin gözlerine nem bırakabileceği için, bazı kullanıcılar vücut sıvılarının transferi yoluyla bir hastalık edinmekten endişe duyuyorlardı. Önceki modeller model verilerini elde etmek için kırmızı ışık ışını kullandıklarından, bazı kullanıcılar “lazer” den olası göz hasarı konusunda endişe duyuyorlardı. Herhangi bir kullanıcının gerçekten bu sistemleri kullanarak yaralandığını ya da hastalandığını iddia etmiyordu. Diyabet ve kalp krizi gibi bazı fiziksel koşullar, bu sistem tarafından tespit edilebilecek retina düzeninde değişikliklere neden olabileceğinden, bazı kullanıcılar yönetimin zararlarına kullanabilecekleri yetkisiz tıbbi bilgi alacağından endişe duyuyorlardı. Retina sistemi bilgilerinden kaynaklanan hiçbir çalışan personel eylemi vakası rapor edilmemiştir. Eşsiz Sistem Yönleri Bazı potansiyel sistem kullanıcıları, yeni Sistem 2001'i kullanmaktan kaynaklanan potansiyel göz hasarı konusunda endişe duymaya devam ediyorlar. Bunu göremeseler bile, sistemin retina modelini okumak için gözün içine bir ışın yansıttığını söylüyorlar. Retina bazlı tanımlama patentleri, EyeDentify Inc. şirketine aittir. İris Desen Sistemi İris (yani, öğrenciyi çevreleyen gözün renkli kısmı), zengin ve eşsiz desen, çukur, çil, çentik, çentik, ilmek, halka, koronlar, oluklar ve damarlar. Görüntüler, bir kameraya benzer şekilde saniyede 30 görüntü yakalayan standart 1/3 inç CCD video kamera ile elde edilir.

Kayıt İşlemi ve Süresi Konu, gözünün aynaya benzeyen bir LCD ekranı kullanaraküne bakar, görüntüyü yönlendirildiği şekilde merkezler ve odaklar. Sistem, iris planlamaunda analiz bölgeleri yaratır, bölgelerin bulunduğu yerlerde bulunur ve bir IrisCode sitesinde. Sistem üç görüntü işliyor, en çok temsilci seçiyor ve operatörün onayı üzerine yönlendirer. Yönetici veri tabanına bir PIN eklenir (yani isim, adres). Gerekli toplam kayıt süresi iki dakikadan az.

Şablon veya Dosya Boyutu IrisCode, 256 byte kaplar.

Kullanıcı İşlemleri Gerekli İriScan sistemi bir kontrol cihazı olarak çalışabilir, ancak normalde tam işlevlerde olduğundan bu durumda bu konuda doğru olanlarınız daha hızlı gerçekleştirir. Kullanıcı başlatıldığında basar, bilgisayarda açılıp kapatılmamış, optik bir üniteyi yatırır ve gözünün LCD'sini geri ayarlayarak, bakar, görüntüyü ortalar ve odaklar. Sistem bir onaylayıcı olarak bağlanabiliyor, bir tuş takımı veya kart okuyucu bağlanabiliyor.

Sistem Tepki Süresi Belirlenen ya da kararsız görsel ve sesli uyarısı, özellikinin boyutuna bağlı olarak bir ila iki saniye içinde oluyorir. Toplam çıkış süresi (diğer bir sözcük, başlatıldı).

Sahteciliği Önleme Yöntemi Sistem, gözün doğal olarak birleşik fiziksel faktörlerini kullanarak veri girişini canlı bir kişiden yapıyoruz.

Doğruluk Sandia National Laboratories'in bir hazırlık modelinin testinde yanlış bir kabul, düşük hatalı reddedilme ve “son derece iyi performans göstermiş” bir sistem burada. Sandia şu anda testte olan bir üretim lideri sahip. İngiliz Telekomünikasyon sistemi son sistemi çeşitli modlarda test etti ve mühendislik günlüğünde bir rapor yayınlayacak. 250.000'den Fazla IrisCode karşılaştırmasında Yüzde 100 doğru performans rapor ettiler. “İris tanıma güvenilir ve sağlam bir biyometrik. Sunulan onu gözüne kaydetdi. Yanlış kabul edilmedi ve verilen her şey başarılı bir şekilde tanımlandıdı. “Diğer testler Yüzde 0,5'ten düşük Bir çaprazlama hata rate bildirmiştir.

Saha Tarih Birimleri, askeri ve devlet kuruluşlarında, bankalarda, telekomünikasyon şirketlerinde, cezaevlerinde ve hapishanelerde, eğitim kurumlarında, imalat şirketlerinde ve güvenlik şirketlerinde yönetim ve personel tanımlaması için orada. Deneyimli Sorunlar Bu kamera tabanlı bir sistemde, optik ünite güneşin doğrudan açıklığa parlamayacağı şekilde konumlandırılmıştır. Eşsiz Sistem Özellikleri Gözün iri, yaşam boyunca bir yaşından itibaren zaten hiç değişmeyen sabit bir organdır. Buradaki, bir kez kaydolduktan sonra, belli göz yaralanmaları veya hastalıkları bulunmayan bir kişi her zaman verilecektir. IRIScan Inc., dünya çapında iris tanıma Teknolojisi Konusunda Patent sahibidir.

İmza Dinamiği Sistemleri İmza darbesi hızı, konumu ve basıncı, kalem, ekran rengi veya yazı tabletindeki küçük sensörler olduğu sırada. Kayıt İşlemi ve Süresi Belirtildiğinde, konuya göre belirle, plan veya hassas tableti kullanarak normal bir imza imzalar. Beş imzalayarak. Bazi Sistemler, şablon Olarak zamana Karşı üç koordinat setini yazdıklarınız kaydedilecek.

Şablonlar, imza çoğaltılmasını engellemek için şifrelenir. Bir tuş takımı kullanarak bir PIN eklenir. Gerekli toplam kayıt süresi iki dakikadan az. Şablon veya Dosya Boyutu Kayıt imzası girişinin 1000 ila 1500 bayt bir şablona ortalaması alınır. Kullanıcı İşlemleri Gerekli Kullanıcı, bir tuş takımındaki veya kart okuyucusundaki PIN girişi yoluyla tanımlamayı sağlar. İmza daha sonra verilen araç ya da tablet kullanılarak yazılır. Bir kayıt için imzanın bir kopyası gerekli değilse, bazı sistemler kağıdın kullanılmadan kalemin kullanılmasına izin verir. Sistem Tepki Süresi Doğrulanmış veya doğrulanmamış kararın görsel ve sesli uyarısı yaklaşık bir saniye sonra telaffuz edilir. Toplam çıkış süresi, imzayı yazmak için gereken zamana bağlı olarak beş ila on saniye aralığındadır. Rekabet Karşıtı Yöntem Bu özellik imza dinamiği sistemleri için geçerli değildir. Doğruluk Veri toplama pilot projelerde ve beta test alanlarında devam etmektedir. Mevcut imza dinamikleri biyometrik sistemleri henüz bağımsız bir kuruluş tarafından test edilmemiştir. Alan Tarihçesi Medikal, ilaç, bankacılık, imalat ve devlet alanlarındaki kuruluşlar tarafından işletilen bir düzine sistemde yaklaşık 100 birim kullanılmaktadır. Sorunlar Daha önce laboratuvar ve kontrollü testler sırasında iyi performans gösteren tecrübeli imza dinamiği sistemleri, zorlu operasyonel kullanımlara dayanmıyordu. Başlangıçta kabul edilebilir doğruluk ve güvenilirlik oranları aylarca sistem kullanımından sonra bozulmaya başladı. Kesin arıza bilgisi bulunmamakla birlikte, kalem hızı, basıncı ve yönündeki dakika değişikliklerini ölçmek için gereken küçük, süper hassas sensörlerin halkın sert kullanımına dayanmadığına inanılmaktadır. Mevcut imza sistemleri neslinin bu eksikliklerin üstesinden gelip gelmediğini söylemek için çok erken. Benzersiz Sistem Yönleri Çeşitli biyometrik kimlik sistemleri arasında, bankacılar ve avukatlar imza dinamiklerini savunuyorlar çünkü yasal belgeler ve finansal taslaklar tarihsel olarak imza ile doğrulandı. İmza dinamikleri tanımlama sistemleri, erişim kontrolü ve diğer güvenlik uygulamaları için aday olarak görülmemektedir. İmza dinamiği sistemleri üreten birkaç şirket var.

# 1.24. Information Security Applications

Bilgi ve fonlar, bu alanlardaki kayıplar, fiziksel hırsızlık ve sahtekarlıktan kaynaklanan zararları hızla aştı. Hayati programlara ve verilere erişen ve hayati fonksiyonlar yerine getiren bilgisayar operatörlerinin pozitif tanımlanması, bu kayıpları ortadan kaldırmanın tek yolu olduğu için zorunlu hale geliyor. Bilgisayarın açılmasını ve programlanmasını kontrol etmek için parolaların ve PIN'lerin kullanımı ve veri araması, kontrol edilmekten daha iyidir, ancak daha önce tartışılan tüm eksikliklere tabidir. Basit, hatırlaması kolay kodlar, “kötü adamları” çözmek için kolaydır. Rasgele veya geniş kodlar hatırlamak zordur ve neredeyse her zaman rahat ve savunmasız bir yere yazılır. Ek olarak ve en önemlisi, bu kontrollerin yalnızca operasyonun başında veya programa veya dosyalara erişim sırasında etkin olmasıdır. İhtiyaç duyulan şey, bilgisayar klavyesinde oturan kişinin sürekli, şeffaf ve pozitif bir şekilde tanımlanmasını sağlayabilen bir biyometrik sistemdir. Bu sistem, operatör bu bilgisayarı veya terminali kullanmaya yetkili bir kişi olarak pozitif bir şekilde tanımlanana kadar bilgisayar açılışını keser. Bu sistem aynı zamanda, operatör bu tür erişime izin verilen bir kişi olarak pozitif olarak tanımlanıncaya kadar kontrollü programların veya verilerin kullanımını engelleyecektir. Bu sistem aynı zamanda, bu kontrollü programlar veya dosyalar kullanımda olduğu sürece operatörün sürekli, periyodik (örneğin, her 30 saniyede bir) pozitif tanımlamasını sağlayacaktır. Bu sistem periyodik bir kontrol sırasında yetkili operatörün varlığını doğrulamazsa, ekran verilerden temizlenebilir. Bu sistem yetkisiz veya tanımlanmamış bir operatörün varlığını doğrularsa, alan ve program kapatılabilir. Açıkçası, böyle bir sistemin uygulanabilirliği, kurcalamayı, yetkisiz tanımlayıcı dosyaların yerleştirilmesini veya baypas edilmesini önlemek için etkili duvarları ve programcı erişim kontrolleri olan yazılıma bağlıdır. Ancak, böyle bir yazılım zaten var. Ayrıca, oturum açma şifresini değiştiren bir biyometrik tanımlama sistemi zaten mevcuttur. Henüz mevcut değil, uygulanabilir, bağımsız bir şekilde test edilmiş, devam eden ve şeffaf bir operatör tanımlama sistemidir. Şu Anda Kullanılabilen Sistem Identix’in TouchSafe ™’si, bilgisayarda oturum açan veya kapatılan kayıtlı kişilerin onayını sağlar. IBM uyumlu bir eklenti elektronik kartı ve kablo içeren 5.4 ¥ 2.5 ¥ 3.6 inç ger ngerprint okuyucu ünitesi ile birlikte gelir. Bu ünitenin daha kontrollü bir çalışma ortamı ve sınırlı bir kullanıcı listesi nedeniyle daha önce tarif edilen normal parmak izi erişim kontrol sistemlerinden daha doğru olması beklenebilir. Ancak, devam eden veya saydam bir tanımlama sağlamaz. Tanımlama her gerekli olduğunda, operatör aktiviteyi durdurmalı ve okuyucuya bir numara yerleştirmelidir. Geliştirilmekte Olan Sistemler Sadece kamera tabanlı bir sistem gerekli devam eden ve saydam tanımlamayı sağlayabilir. Bilgisayar monitörünün üst köşesine yerleştirilmiş küçük bir video kamera ile sistem, operatör kimliğini her 30 veya 60 saniyede bir kontrol etmek üzere programlanabilir. Operatörün ekrana sık sık bakması beklenebileceğinden, bir yüz veya iris tanımlama sistemi, operatörün çalışmasını hiç kesmeden etkili olacaktır. Böyle bir sistem, kabul edilebilir bir görüntü elde etmek ve operatörü tanımlamak için 15 saniyelik bir gözlem penceresine sahip olacak şekilde ayarlanabilir. Operatör ekrana bakmadıysa veya 15 saniye boyunca mevcut olmasaydı, ekran ekran koruyucusu ile silinirdi. Sistem gözlem modunda kalır, böylece operatör klavyeye geri döndüğünde veya ekrana bakıp tanımlandığında ekran geri yüklenir. Klavyedeki operatöre yetki verilmemiş veya tanımlanmamışsa, program ve dosyalar kaydedilir ve kapatılır. Bu yetenekleri sağlama potansiyeli olan ilk gelişme sistemi Miros Inc.'in yüz tanıma sistemidir. Miros, TrueFace adlı bir ürün grubu üzerinde çalışmaktadır. Şu anda, Miros’un gelişen sistemlerinin performansı ve doğruluğu ile ilgili bağımsız bir test verisi mevcut değildir. Yüz tanıma araştırması uzun yıllardır sürmekte ancak başarılı bir sistem henüz pazara ulaşmamıştır. Ayrıca, biyometrik tanımlama endüstrisi, alan kullanımında kabul edilebilir sonuçlar verememiş umut verici gelişmelere sahiptir. Miros’un gelişmeleriyle ilgili sonuçlar tanınmış bir bağımsız kuruluş tarafından yapılan performans ve doğruluk testlerini beklemelidir. IriScan Inc., istenen bilgisayarı veya bilgi erişim kontrolü yeteneklerini sağlayabilen bir iris tanıma sistemi geliştirmenin ilk aşamalarındadır. IriScan’ın ispatlanmış doğruluğu, bu gelişime en doğru bilgi kullanıcı tanımlama sistemi olma potansiyeline sahiptir.

# 1.25.Özet

Hızlı, doğru, uygun maliyetli biyometrik tanımlama sistemleri dönemi geldi. Toplumsal faaliyetler bireylerin ve kuruluşların varlıklarını, bilgilerini ve hatta bazen varlıklarını bile tehdit ediyor. Anlık, olumlu kişisel kimliklendirme, toplumun kaynaklarına erişimin kontrol edilmesinde ve korunmasında kritik öneme sahip bir adımdır. Etkili araçlar şimdi mevcuttur. Günümüzde önemli sayıda biyometrik tanımlama sistemi üreten ve satan bir düzineden fazla şirket vardır. Daha da fazla organizasyon biyometrik araştırma ve geliştirme çalışmaları yürütüyor ve pazara girmeyi umuyor ya da zaten az sayıda birim satıyor. Tüm biyometrik sistemler ve teknolojiler genel olarak eşit derecede etkili değildir ve özellikle tüm uygulama gereksinimlerini karşılamada etkili değildir.Güvenlik yöneticilerinin, seçim yapmadan önce aday biyometrik sistemleri araştırırken dikkatli ve dikkatli olmaları tavsiye edilir. Bağımsız test sonuçları ve benzer uygulamalara sahip mevcut kullanıcıların raporları tavsiye edilir. Yerinde testler istenmektedir. Biyometrik tanımlama sisteminin seçiminde ve kurulumunda özenli ve titiz olanlar, varlık koruma seviyelerinde büyük artışlar gerçekleştireceklerdir.

# 2. Kuruluş için Tekli Oturum Açma

Her yerdeki şirketler ana bilgisayar merkezli veri işleme ortamından müşteri / sunucu yapılandırmasına işlevsel geçiş yaptılar. Bu dönüşümle birlikte yeni ekonomiler, daha çeşitli operasyonel seçenekler ve yeni bir dizi zorluk ortaya çıktı. Ana bilgisayar merkezli kurulumda, sistem yönetimi genellikle bilgisayar kompleksinin kendisinin idari ikizi idi: sistemin bileşenleri, sistemin yönetimini yapanlar gibi bir alana bağlandı. Dağıtılmış istemci / sunucu düzenlemesinde, sistemleri yönetenler yine benzer bir şekilde düzenlenir. Bu dağıtılmış altyapının, karmaşık işlemlerde basit bir günlük tutma eylemini gerçekleştirmesine rağmen, karmaşık işlemleri vardır. Kullanıcıların, çalışmalarını gerçekleştirmek için birçok farklı sisteme ve uygulamaya erişmeleri gerekir. Bunları basit ve kolay bir şekilde yapmalarını sağlamak, zaman alıcıdır ve birden fazla sistemdeki birkaç kişi arasında koordinasyon gerektirir. Ana bilgisayar ortamında, bu sistemler ve uygulamalar arasında geçiş yapmak, ana menüye dönmek ve yeni bir seçim yapmak anlamına geliyordu. İstemci / sunucu dünyasında bu tamamen farklı bir sisteme giriş yapmak anlamına gelebilir. Yeni oturum açma, yeni şifre ve önceki sistem için kullanılanlardan her ikisi de büyük olasılıkla farklıdır - kullanıcı bunlarla doludur ve başarısız oturum açma girişimlerini önlemek için kafalarını karıştırmama sorunu. Bu ve bununla ilgili problemlerden dolayı Tek SignOn veya SSO kavramının doğması gerekiyordu.

# 2.1. Evrim

Hesaplama platformlarının, işletim sistemlerinin ve erişim kontrol yazılımlarının (ve bunlarla birlikte gelen birçok giriş ve şifrenin) çeşitliliği göz önüne alındığında, bir defada ve aynı anda tek bir işlemle birden fazla sistemde oturum açma kabiliyetine sahip olmak, bir duanın yanıtını verir . Böyle bir dua, kullanıcılar tarafından sunulan ve her yerde erişim kontrol yöneticileridir. Kavramı, bunu başarmak için bir yöntem ortaya çıktığında, onu farklı sistem erişim kontrol biçimleriyle bütünleştirmenin birçok engelde göz korkutucu bir meydan okumaya yol açacağı açıkça ortaya çıktı. Uygulama yazılımının ana bilgisayarın ilk günleri gibi tek bir platformda çalıştığı günlerde, varsayılan olarak kullanıcıların gerçekleştirmesi gereken tek bir oturum açma vardı. Uygulamanın parti odaklı veya etkileşimli olmasına rağmen, kullanıcının hatırlaması gereken yalnızca bir giriş ve şifre kombinasyonu vardı. Parola değiştirme zamanı geldiğinde, kullanıcı sıklıkla kendi ifadesini oluşturabilir. Karşılaşılan en kötü şey, sayı / harf kombinasyonları sunan bazı şirketler tarafından uygulanan rastgele şifre üreticisi yazılımıydı. O zaman bile, onlardan sadece biri vardı. Bir sonraki adım, aynı ağ üzerinde aynı türden birden fazla bilgisayarın eklenmesiydi. Bu makineler her zaman birbirleriyle iletişim kurmazken, kullanıcının tüm veri gereksinimlerini karşılamak için birden fazlasına erişmesi gerekiyordu. Aynı tipte bile olsa birden çok sistem farklı kullanım kurallarına sahipti. Veri işleme departmanındaki farklı gruplar genellikle bu farklı sistemleri kontrol eder ve bazen aynı şirketle organizasyonları tamamen ayırır. Tabii ki, her bir sistem aynı terminalden erişilebilir olmasına rağmen, her biri için farklı bir oturum açma ve parola olması gerekiyordu.

Sonra, “bölüm bilgisayarı” denildi. Bu daha küçük, daha az güçlü işlemciler, o bölüme özgü benzersiz uygulamalar yürütmek için şirketteki belirli gruplara hizmet etti. Örnekler arasında malzeme yönetimi, muhasebe ve finansman uygulamaları, merkezi kelime işlem ve işletme uygulamaları sayılabilir. Bu alanların kısıtlı ihtiyaçları ve sık sık kendi içlerinde elektronik olarak kendileri ile iletişim kurmaları, bu sistemleri aynı ağ üzerinde birbirine bağlamaları gerektiği için gereksizdi. Bu durum uzun sürmedi. Yakında bu sistemleri birbirine bağlamanın ve onların ağ üzerinden birbirleriyle iletişim kurmasına izin vermenin bir alandan diğerine bilgi akışını hızlandıracağı ortaya çıktı. Dahili posta yoluyla bir rapor almak için ayın son haftasına kadar beklemek yerine, satın alma kayıtları, satın alma işlemine gönderilen toplu raporlardan aynı hafta alınan malzemeler için stok kayıtları ile haftalık olarak birleştirilebilir. Bilgi akışındaki bu sonraki aşama da uzun sürmedi. Sistemler daha az, daha az parti odaklı ve daha etkileşimli hale geldikçe ve malların, hizmetlerin ve paraya bağlı hareketlerini kaydetmek için iş baskıları arttıkça, daha hızlı erişim talep edildi. Bir alandaki kullanıcıların diğerlerindeki bilgilere doğrudan erişmeleri gerekiyordu. Bu senaryoda tek bir sorun vardı - ve küçük bir problem değildi. Bilgisayarlar neredeyse her zaman ağırlıklı olarak iki farklı alana girmiştir: genel amaçlı makineler ve özel amaçlı makineler. Başlangıçta “iş işleme sistemleri” ve “bilimsel ve mühendislik sistemleri” olarak adlandırılan bu bilgisayarlar, bugün devam eden tek bir protokol ve tek işletim sisteminden ayrılmaya başladı. Tek bir kullanıcının her ikisine de erişebilmesi için, genellikle her biri farklı bir protokolde çalışan iki ayrı ağ gerekir. Elbette bu, kullanıcının masasındaki iki farklı terminal anlamına geliyordu. Tüm sistemlerin aynı üreticiden gelmesi önemli değildi: sistemler aynı tel veya iş istasyonunda birleştirilemedi. Evrimdeki bir sonraki aşama, çeşitli adaptörler, çoklu ekran “pencereli” ekranlar, protokol dönüştürücüler, vb. Takmaktı. Bu cihazlar bazen ikinci terminali elimine etti. Ardından şimdiki her yerde bulunan kişisel bilgisayar veya “PC”, 12 Ağustos 1981'de IBM tarafından tanıtıldığı zaman ilk çağrıldığı haliyle geldi. Birkaç yıl içinde, bu vazgeçilmez cihazın neredeyse her yerden bilgi bağlamasına ve görüntülemesine izin veren adaptörler ortaya çıktı. Her tür ana bilgisayar daha sonra hizmete girer. Başka bir nimettir son kullanıcıya çarptı! Bu evrim günümüze kadar devam etmiştir. Çoğu özel protokol, yünlü Mamut'un yolunda ilerlemiş ve neredeyse hepsi TCP / IP konuşan bir şekilde değerli bir azınlığa ulaşmıştır. Bu yakınsama son derece önemlidir: tüm bu farklı hesaplama platformlarını aynı kablo üzerinde ortak bir protokolle birbirine bağlamanın temel yöntemi mevcuttur. Microsoft Windows'un gelişi bu yakınsamayı bir adım daha ileriye itti. Protokollerin bir araya geldiği gibi, farklı bilgisayarlarla oturumları görüntüleme kabiliyeti de gerçekleşiyordu. Durumla birlikte, grafiksel kullanıcı arayüzü (“GUI” - aşırı duygusal ile aynı) farklı ana bilgisayarlardan eşzamanlı gösterimleri etkinleştirdi. Sanal bellek PC'de gerçek oldu mu, bu eşzamanlı aktif ekranlara ve işlemlere izin vererek hala bu zarfı itti. Kullanıcılar yıllarca istedikleri ve ihtiyaç duydukları yetenekleri alıyorlardı. Şimdi imkansız son tarihlere sahip imkansız görevler normal, hatta rutin hale getirildi. Ancak, kaydedilen tüm ilerlemelere rağmen, asıl mesele henüz ele alınmamıştı. Biçimlendirmeye uygun, kullanıcılar tüm yeni oyuncaklara ve söz verdikleri kullanım kolaylığına minnettarlardı… uyanıp bu yeniliklerin hiçbirinin en fazla ve en çok şikayet ettikleri şeyi, birden fazla logini ve şifreyi desteklemediğini tespit edene kadar. Peki, tek oturum açma nedir?

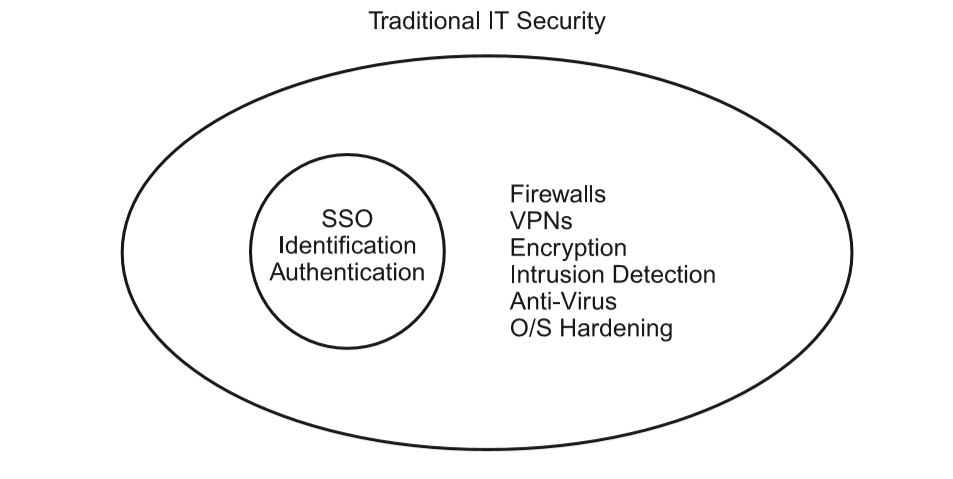
# 2.2. Tekli Oturum Açma Nedir: Başlangıç

Yaklaşık 50 yıl önce başlayan sistem tasarımcıları, bilgisayar sistemleriyle etkileşimin izlenmesi için bir yönteme ihtiyaç duyulduğunu fark ettiler ve bu nedenle bir kimlik belirleme şekli (loginid) tasarlandı. Neredeyse eşzamanlı olarak bununla aynı anda parola geldi - bu bazen kullanıcının kimliğini doğrulayan ya da onaylayan oturum açma işlemine eşlik eder. Geçtiğimiz on yıllar boyunca, tek bir oturum açma ve ilgili şifre, kullanıcının kullanabileceği neredeyse tüm bilgi işlem gücüne ve kullanabileceği tüm uygulamalara ve sistemlere erişmesine yardımcı olmak için yeterliydi. Evet, o günlerdi… basit, anlaşılır ve yönetimi kolay. Ve şimdi hepsi bitti, tıpkı kulüp yosunu, vakum tüpü ve MS / DOS (belki) gibi.

Günümüz ortamı hem coğrafya hem de platform açısından daha dağılmıştır. Bazıları tartışsa da, bir işletim sistemini diğerinden ayıran özellikler hem ağ erişimi hem de grafiksel kullanıcı arayüzleri (her yerde bulunan GUI) tarafından engelleniyor. Her geliştirici, kendi uygulamalarını her bilgisayar platformunda sunmayı seçmediğinden (ve ağlar bu çeşitlilikten habersiz göründüğü için gelişti), kullanıcılar artık daha fazla platforma yayılmış daha geniş bir araç yelpazesine erişebiliyor, daha fazlası Geçmişte herhangi bir zamanda şeffaf olarak. Ve yine de hepsi cennet değil. Bu güç ve fayda zenginliği ile birlikte öncekiyle aynı gereksinim gelir: kullanıcıyı tanımlamak ve doğrulamak. Fakat şimdi bu, tüm bu çeşitli sistemler ve platformlar arasında yapılmalıdır ve hepsinin bunu başarmak için farklı mekanizmaları vardır. Sonuçta, kullanıcılar artık her biri kendi benzersiz şifresiyle yönetilen ve muhtemelen de kendilerine özgü benzersiz kurallarla yönetilen birden fazla oturum açmaya sahip. CISSP, kullanıcıların bu durumdan acı bir şekilde şikayet ettiklerini biliyor ve genellikle ne gerekiyorsa onu atlatmaya çalışır. Bunu önlemek için CISSP bir çözüm bulmak zorundaydı. Bunu kolaylaştırmak ve bir pazarlama fırsatından yararlanmak için, yazılım satıcıları hayati bir ihtiyaç gördüler ve bu nedenle tek oturum açma (SSO) tasarlandı. Ek 7.1, göründüğü zaman genel güvenlik programında SSO'nun nerede bulunduğunu göstermektedir. Bir erişim kontrol yöntemi olarak, SSO birden fazla platformda (kullanıcı kimliği ve kimlik doğrulaması) önemli ihtiyaçları ele aldı. Genel olarak, genel bilgi koruma ve kontrol yapısına katkısı bakımından zor ve uygulanması zor olan ve şüpheli değeri olan bir "kullanıcı rahatlığı" olarak kabul edildi.

# 2.3. Temel Sorun

En basit ifadeyle, çok fazla giriş ve şifre ve diğer kullanıcı erişim yönetimi sorunlarının bir ana bilgisayarı. Çalışanların çalışmasını denetlemek için coğrafi olarak dağılmış bir matris yaklaşımı gerektiren karmaşık yönetim yapılarıyla, operasyonel hedefleri ve raporlama gereksinimlerini karşılamak için dağıtılmış ve çoğu zaman çok farklı sistemler gerekir. Büyük ölçüde anabilgisayar tabanlı sistemler günlerinde, bu tür bir sorun neredeyse yoktu. Standartlar yapıldı ve yaptırım karmaşık değildi. Bu günlerde, bu koşullar çeşitli sistem standartlarının oluşturulması ve uygulanması için aynı görevi yerine getirmektedir. Ancak şimdi, bu koşullar ve bunlarda ortaya çıkan sistemler, doğal olarak buna elverişli değillerdir. Yukarıda bahsedildiği gibi, bu tür sistemler kullanıcı aktivitesini izlemek için farklı yerleşik sistemlere sahiptir. Temel kavramlar benzer: Denetim izi, erişim kontrolü kural kümeleri, Erişim Kontrol Listeleri (ACL'ler), sistem ayrıcalık seviyelerini düzenleyen parametreler, vb. Sonunda, teoride sağlam olsa da, bir kural ve standart kümesinin ortaya çıkabileceği anlaşılıyor. Yönetilemez bir karmaşıklık oluşturmadan tüm platformlarda uygulama yapmak için fazlasıyla zor olun. Ancak, işletme seviyesindeki kullanıcı yöneticilerinin aradığı “Kutsal Kase” dir.

****

Bu sorunun görünen basitliğine rağmen, kullanıcı yönetimi ile ilgili bir dizi sorunun sadece ucunu temsil ediyor. Bu tür sorunlar, kullanıcıların kaynaklara erişimini denetleme zorunluluğu getirildiği her yerde mevcuttur: yerel kurum içi, uzak WAN düğümleri, uzaktan içeri arama ve Web tabanlı erişim. Exhibit 7.1 ile karşılaştırıldığında Exhibit 7.2, SSO'nun daha fazla işlevselliğe sahip daha geniş kapsamlı bir ürüne nasıl geliştiğini göstermektedir. Sadece bir "kullanıcı rahatlığı" olarak kabul edildiğinde, SSO diğer geleneksel güvenlik ürünleri ve yetenekleriyle daha sıkı bir şekilde bütünleştirildi. Bu evrim, SSO’nun imajını ölçülebilir bir şekilde iyileştirdi, ancak uygulamasını basitleştirmedi. Yukarıda belirtilen soruna ek olarak, bu tür yeteneklere duyulan ihtiyaç, bazıları aşağıdakileri içeren çeşitli yollarla kendini gösterir:

1. Giriş noktalarının sayısı arttıkça (İnternet dahil), geliştirilmiş ve denetlenebilir güvenlik kontrolleri uygulamasına ihtiyaç vardır. 2. Çok sayıda iş istasyonunun yönetimi, virüslerden kaçınmak, kullanıcı tarafından girilen sorunları sınırlamak, yardım masası kaynaklarını en aza indirmek, vb. İçin bazı kontrollerin yerleştirilmelerini zorunlu kılmaktadır. Son kullanıcıların elektronik masaüstlerine ulaşmak için çalışma yolları boyunca çeşitli iş istasyonlarını kullanabilmelerine ihtiyaç duyulmaktadır. 4. Uygulamaların çoğalması, şifreler otomatikleştirildikten sonra bile zor, çok hantal veya çok zaman alan tüm bilgilere ulaşılmasını sağlamıştır. 5. Güvenlik yönetimi, endüstri kurallarına uyumu arttırmak ve verimliliği artırmak için bir uygulama odağından küresel bir odağa geçmelidir.

# 2.4. Mekanizmalar

SSO'yu uygulamak için kullanılan mekanizmalar zamanla değişmiştir. Bir yöntem Kerberos ürününü, kullanıcıları ve kaynakları bir “biletleme” sistemi aracılığıyla birbirlerine doğrulamak için kullanır; bunlar, sistemlere ve kaynaklara yetki verildiği araç olan biletlerdir. Diğer bir yöntem, kabuklar ve komut dosyaları olmuştur: kabukta birincil kimlik doğrulaması, daha sonra hedef platformlarda hesap ve kaynak erişimini etkinleştirmek için çeşitli platform spesifik komut dosyaları başlattı. Kerberos uygulamasına dahil olan zaman ve çabayı harcamak istemeyen kuruluşlar için, nihai çözüm, kabuk ve senaryo yaklaşımının bir çeşitlemesi olabilirdi. Bunun birkaç dezavantajı vardı. Her platformda ayrı ayrı kullanıcı hesapları kurma ihtiyacını ortadan kaldırmadı. Ayrıca parola senkronizasyonu veya diğer yönetim özelliklerini sağlamadı. Kabuk ve komut dosyası en iyi şekilde yarım adımdı ve kullanıcı oturumunu basitleştirmesine rağmen, bu kolaylaştırdığı otomasyonun kapsamıydı. “Öyleydi”. Bugün, bir SSO platformu uygulanırken farklı yapılandırma yaklaşımları ve seçenekleri mevcuttur ve önceki girişimlerin dezavantajları büyük ölçüde ele alınmıştır. Ne olursa olsun, güvenlik mühendisliği perspektifinden, uygulama planı için tasarım ve hedeflerin (yani, çözmeye çalıştığı sorun) bir risk analizinde değerlendirilmesi ve daha sonra garanti edildiği şekilde azaltılması gerekir. SGK durumunda, operasyonel endişeler aşağıda tartışıldığı gibi değerlendirilmelidir.

Bir uygulama şekli, kullanıcının oturumu kapatıncaya kadar yetkili kaynaklarının tümüne aktif olarak bağlı kalmasıyla sonuçlanan bir oturum açma oturumuna izin verir. Bu tür yapılandırma, zamana dayalı yeniden doğrulama yapılmasını sağlar (her… dakika veya saatte bir) veya olaya dayalı olabilir (yani, sistem sınır geçişi). Bu yapılandırma ile ilgili bir endişe kaynak kullanımıdır. Bunun nedeni, oturum açma sırasında birçok ağ trafiğinin üretilmesi, dizin / ACL erişimlerinin gerçekleştirilmesi ve birkaç uygulama / sistem oturumu kurulmasıdır. Bu aktivite seviyesi, özellikle birkaç kullanıcı aynı anda giriş yapma girişiminde bulunursa, genel sistem performansını önemli ölçüde azaltacaktır. Seans kaybının önlenmesi (etkin olma zaman aşımına uğraması nedeniyle), eğer özelliğin kendisi devre dışı bırakılamazsa, bunu önlemek için ara sıra "ping" yapılması gerekebilir. Bu da ek ağ trafiği olan kaynakları tüketir. Bu yaklaşımla ilgili diğer önemli endişe, kullanıcının belirli bir uygulamada aktif olup olmamasına bakılmaksızın “açık oturumların” mevcut olmasıdır. Bu, veri akışının istila edilmesi, nüfuz edilmesi veya yeniden yönlendirilmesi durumunda “oturum çalmayı” mümkün kılabilir. Başka bir potansiyel yapılandırma, şebeke servisine ilk tanımlamayı / doğrulamayı gerçekleştirir, ancak kullanıcı açıkça talep edene kadar belirli bir sisteme veya uygulamaya erişimi başlatmaz (yani ilgili masaüstü simgesine çift tıklayın). Bu ağ trafiği seviyesini düşürür ve yalnızca istendiğinde yeni oturumlar başlatır. Periyodik yeniden doğrulama hala geçerli olacaktır.

# 2.5. Tekli Oturum Açma Ne Sağlar?

SSO ürünleri, son uç nokta sistemlerinin merkezi yönetimini, son kullanıcıların büyük popülasyonlarının etkilenmesini sağlayan rol tabanlı bir bakış açısıyla yönetmeyi içeren daha karmaşık sorunlara basit son kullanıcı kimlik doğrulama ve parola yönetiminin ötesine geçmiştir. tek sistem yönetimi değişikliği (örneğin, tüm çalışanlara yeni bir uygulama eklenmesi) ve son kullanıcıların hassas uygulamaları kullanmasının izlenmesi. Bir sonraki bölümde, ideal bir tek oturum açma ürününün sunabileceği birçok özellik ve özellik açıklanmaktadır. Maliyetten bahseden öğelerin bazıları, işlevi yerine getiren yazılıma değil, yapılan noktaya atıfta bulunur. Burada tartışıldığı gibi bir ürünün yaşam döngüsü maliyeti, bir kurulumdan diğerine geniş ölçüde değişebilir ve değişebilir. Bu çeşitliliğin derecesi birçok faktöre dayanır ve bu tartışmanın kapsamı dışındadır. SSO ürününün potansiyel ekonomilere ulaşmak için uygulanmasıyla ilgili büyük bir endişe, ürünün maliyeti dikkate alındığında ve bunu, SSO öncesi yapılan işlemlerin maliyeti ile karşılaştırırken ve bunu, bunun işler durumunun maliyetiyle karşılaştırmasıyla ortaya çıkar. SSO'dan sonra, SSO'yu koymanın maliyeti ve projenin tamamlanması sürecinde harcanan diğer tüm dolarlar yapılacaktır. Öncesi ve sonrasındaki harcamaları karşılaştırarak, SSO'yu kurmak için yatırım getirisi (yatırım getirisi) hesaplanabilir ve proje gerekçesinin bir parçası olarak kullanılabilir. Bunun, herhangi bir proje düşünülürken işletmenin uyguladığı eşdeğer formül, kısıtlamalar ve yatırım / yatırım getirisi hedefleri kullanılarak yapılması önerilir. Analiz ve sonuçlar sunulacaksa (bu girişimi desteklediklerini varsayarsak), izleyici, yatırımın sağlamlığı hakkında gerçek maliyetler ve gerçek değer katkısı açısından daha iyi bir anlayışa sahip olacaktır. Bu tür bir içgörü, onaylamayı teşvik eder ve önemli bir maliyet ve uzun uygulama zaman çizelgesinin ne olacağı konusunda daha fazla kabul görmeyi destekler. Ne olursa olsun, bu teknolojinin edinmenin ve sürdürmenin ucuz olmadığını söylemek makul bir şekilde doğrudur. Ek olarak, herhangi bir sorun çözme setinde olduğu gibi, “Bu sorun çözümün fiyatına değer mi?” Sorusu sorulmalıdır. Bir sonraki bölümde, böyle bir kararın alınmasına yardımcı olacak özelliklerden bazıları tartışılmaktadır.

# 2.6. Dahili Yetenek Vakfı

GUI tabanlı merkezi yönetime sahip olmak, basitleştirilmiş kullanıcı yönetimi için potansiyel sunar ve bu nedenle düşük eğitimde, düşük yönetimsel çabada ve kullanıcı yönetimi için daha düşük yaşam döngüsü maliyetinde önemli ölçüde maliyet tasarrufu sağlar. Bunun altında, bazı DBMS motorlarına ve bir dizi rapor oluşturma aracına dayanarak, SSO ürünü aracılığıyla elde edilen etkinlik raporlaması ve adli analiz için veri azaltma sürecini geliştiren ve kolaylaştıracak bir kayıt tutma özelliği olacaktır. Temel destek yapısı doğrudan (standart geleneksel giriş) ve Web tabanlı erişimi içermelidir. Bu, özellikle İnternet artık çok özel bir hale geldi ve aynı zamanda artan sayıda uygulama bir tür Web etkin / bilinçli arayüz kullanıyorsa, bu standart olacaktır. Bu, SSO uygulamasının, doğrudan çevirmeli veya Web üzerinden uzaktan erişimi pratik hale getirmek için oturum açma işleminin kapsamını veya derinliğini mutlaka sınırlayacağı anlamına gelir. Endişenin bir yönü, uygulamanın müdahaleci olmamasıdır. Saldırganlık, ürünün işlevselliğini sağlamak için çalışma ortamının ne derece değiştirilmesi gerektiğidir. Bir diğeri ise eski sistemlerin ve uygulamaların güçlendirilmesidir. SSO ürününün kuruluştaki çeşitli platformlara kurulması genellikle özel kod seviyesini en aza indirgemek için API'ler aracılığıyla yapılır. Şaşırtıcı olmayan bir şekilde, çoğu SSO çözüm satıcısı, ürünlerini eski sistemleri göz önünde bulundurarak geliştirmiştir. Örneğin, Platinum Technologies (şimdi CA) ürünü AutoSecure SSO, RACF, ACF2 ve TopSecret destekli - hepsi eski sistemler dünyasında doğup büyüyen erişim kontrolü uygulamaları. Ayrıca, Windows NT, Novell ve TCP / IP ağ destekli sistemleri destekler. Bu nedenle günümüzden günümüze kadarki mirası kapsar.

# 2.7. Genel Özellikleri

Doğru SSO ürünü, gerekli tüm özellikleri sağlamalı ve bir kurumsal üretim ortamında kendisini korumalıdır. Açık sistemler dağıtılmış bir bilgi işlem ortamında faaliyet gösteren ve paralel ağ sunucuları ile birlikte çalışan ürünler, kurumsal ihtiyaçları karşılamak için daha dar NOS tabanlı SSO ürünlerinden daha iyi konumlandırılmıştır. Öyleyse, bu teknolojinin vaadi gerçekleşecekse, SSO ürünlerinin oldukça geniş bir dizi sistemi, cihazı ve arayüzü destekleyebilmesi gerektiği açıktır. Bu göz önüne alındığında, bazı ortamların diğerlerinden daha fazla değişiklik gerektireceği açıktır; yani, SSO yapılandırması daha karmaşıktır ve çalışma ortamını büyük ölçüde değiştirir.

Aşağıdaki sorularla elde edilen bilgiler uygulama öncesi analizine yardımcı olacaktır:

1. SSO müdahaleci değil midir? yani, uygulamaları herhangi bir şekilde değiştirmeye gerek kalmadan tüm uygulamalara erişimi yönetebilir mi? 2. SSO ürünü tüm uygulamalar için tek bir ortak oturum açma ve şifre belirliyor mu? 3. SSO ürünü hangi iş istasyonlarını desteklemektedir? 4. SSO ağ sunucuları hangi işletim sistemlerinde çalışabilir? 5. Hangi fiziksel tanımlama teknolojileri desteklenir (örneğin, Güvenli Kimlik kartı)? 6. Çevirmeli son kullanıcılar destekleniyor mu? 7. İnternet erişimi destekleniyor mu? Öyleyse, kimlik doğrulama ve şifreleme zorunlu mu? 8. SSO masaüstü isteğe bağlı olarak belirli iş istasyonlarının kullanımını (örneğin üretim alanında) daha yakından kontrol etmek için standart masaüstünü değiştirebilir mi? 9. Şifreler, bir son kullanıcının SSO ürününün kontrolünde bir uç nokta uygulaması kullandığı ilk kez otomatik olarak yakalanabilir mi? 10. SSO masaüstünün görünümü, özel bir siteye özgü masaüstü görünümüyle değiştirilebilir mi? 11. SSO zaten kurulmuş olan PKI çerçevesi ile nasıl çalışacak?

# 2.8.Son Kullanıcı Yönetim Tesisleri

Bu özellikler ve seçenekler hesap oluşturma, parola yönetimi vb. İçin normal işlevler grubunu içerir. Son kullanıcı kimliği ve kimlik doğrulamasının performansı açıktır. Parola yönetimi tüm normal özellikleri içerir: parola yaşlandırma, geçmiş ve sözdizimi kuralları. Resmi tamamlamak için, özellikle uzaktaki son kullanıcılar SSO ürününü kullanacaksa, çeşitli simge tipindeki aygıtları (Secure-ID kartlar), biyometrik aygıtları ve benzerlerini destekleyin. En azından bu desteği sağlayan isteğe bağlı modüller bulunmalı ve mevcut olmalıdır.

Kullanılması gereken bazı ek özellikler şunlardır:

• Rol bazlı ayrıcalıklar. Bu işlevsellik, büyük sayıda son kullanıcı tarafından paylaşılan sınırlı sayıda rolü yönetmeyi mümkün kılar. Bunun mutlaka bu rolün yetki alanı dışında çalışan bireysel kullanıcılar üzerinde bir etkisi olmayacaktır.

  • Masaüstü kontrolü. Bu, yerel masaüstünün SSO tarafından yönetilen bir masaüstüyle değiştirilmesine izin verir, böylece son kullanıcıların iş istasyonunu destek sorunları yaratacak şekilde kullanmalarını önler (ör. Yetkisiz yazılımlar sunmak). Bu yetenek, iş istasyonlarının son kullanıcılar tarafından paylaşıldığı alanlarda özellikle önemlidir (örneğin üretim alanları).

• Uygulama yetkilendirmesi. Bu, başlatılan herhangi bir uygulamanın SSO ürünü tarafından kaydedilmesini ve silinmesini ve kayıtların bireysel uygulama kullanımında tutulmasını sağlar.

• Mobil kullanıcı desteği. Bu özellik, son kullanıcıların konumlarından veya kullandıkları iş istasyonundan bağımsız olarak masaüstlerine erişmelerini sağlar. Ayrıca, uygulamaların başlatılmasından önce uygun etki alanı sunucusuna erişmek için iş istasyonunu yapılandırmayı ve bireyin tercihlerini iş istasyonuna getirmeyi de içermelidir.

# 2.9. Uygulama Yönetimi Olanakları

SSO bağlamındaki uygulama yönetimi, bir uygulamanın kullanıcıları yönetme veya işleme biçimine benzer şekilde ele alınmasını ifade eder. Ek 7.2'de gösterildiği gibi, SSO'nun gelişmiş durumu, kullanıcıların basit bir şekilde tanımlanmasının / onaylanmasının ötesine geçmiştir ve şimdi uygulama yönetiminin bazı yönlerini kapsamaktadır. Bu yönetim kabiliyeti, uygulama fonksiyonlarının bakımı ve yükseltilmesinden ziyade, kullanıcı masaüstlerinin görünüşü ve uygulama menüleri ve arayüzleri arasında gezinme ile ilgilidir. Bağlam yönetimi, ortak bir konuyla ilgili olan birden fazla oturumun aynı anda etkin olması durumunda, ilgili başka bir oturumun konumu değiştiğinde her oturumun otomatik olarak güncellenmesini sağlar (örneğin, bir sağlık bakımı ortamında, klinisyen doktorun eczane oturumlarının aynı hasta üzerinde olması gerekir) klinik bir karara varırken iki hastanın kayıtlarını karıştırmamaktan kaçınmaktır).

Uygulama izleme, belirli bir bilgi satırının kullanımını, bu tür bir bilgi sağlamak için programlanmamış bir uygulamada (örneğin, belirli bir kurucuların bir devlet ortamındaki kayıtlarına erişim gibi) kullanımını izlemek istendiğinde özellikle yararlıdır. Uygulama konumlandırma kişiselleştirilmiş ancak merkezi olarak kontrol edilen masaüstleriyle ilgili bir özelliktir. Bu, başlangıçta bir uygulamayı açmak için (muhtemelen bir dizi seçenek arasından seçilen) bir son kullanıcı başlatma betiğinin yapılandırılmasını ve hangi ekranın yükleneceğini bile belirtmesini sağlar. Uygulamaları birbirine bağlayan bir başka özellik de uygulama kaynaştırmasıdır. Bu, uygulamaların birlikte çalışarak son kullanıcının yalnızca tek bir oturumdan haberdar olacağı şekilde çalışmasını sağlar. Son kullanıcıya bakış, uygulamalar arasında son kullanıcı için tamamen yeni bir görünüm oluşturmak da dahil olmak üzere uygulamalar arasında basit bir otomatik geçiş arasında değişebilir.

# 2.10. Uç Nokta Yönetim Olanakları

Son nokta yönetimi, bir SSO ürününün temel bir bileşenidir; çünkü onsuz uygulama, aynı bilgiyi iki kez girmek zorunda kalır; Bir kez SSO'da ve bir kez son noktada ise SSO veritabanında bir değişiklik yapılır. Son noktaya iki giriş yöntemi desteklenmelidir: (1) Bir API'yi destekleyen uç nokta sistemlerini güncellemek için API tabanlı aracılar ve (2) API'yi desteklemeyen son nokta sistemlerini güncellemek için oturum animasyonu aracıları. Bu idari hedefi gerçekleştirmek için SSO tarafından sağlanan hizmetler şunları içermelidir:

• Giriş kontrolu. Bu, son kullanıcılar tarafından uygulamalara erişmek ve her uygulamanın yeteneklerine bağlı olarak, uygulamaya son kullanıcının kendi ayrıcalıklarını tanımlamak için kullanılan araç. Hem API tabanlı hem de oturum tabanlı uygulamalar desteklenmelidir.

• Denetim hizmetleri. Bunlar, SSO ürününün kayıt sistemine bilgi yayınlamak isteyen uygulamaları son noktaya getirmek için bir API ile sağlanmalıdır.

• Oturum şifreleme. Bu özellik, uygulamalar ve son kullanıcılar arasında hareket ederken bilgilerin ifşa ve kurcalamaya karşı korunmasını sağlar. Bu özellik, hassas uygulamaların yalnızca açık metin olanakları sağladığı durumlarda bir gereklilik olmalıdır.

# 2.11. Mobil Kullanıcılar

Son kullanıcıların bilgi kaynaklarına ulaşmak için mevcut herhangi bir iş istasyonunu kullanma kabiliyeti, son kullanıcıların çok sayıda farklı konumda çalışması beklenen ortamlarda zorunludur. Bu tür kullanıcılar arasında seyahat eden çalışanlar, sağlık hizmeti sağlayıcıları (mobil hemşireler, doktorlar ve teknisyenler), danışmanlar ve satış personeli bulunur. Günümüz dünyasının son derece hareketli işgücünde, bu özelliği sunmayan bir ürünün başarılı olması muhtemel değildir. Başka bir olası özellik iş istasyonu paylaşımını kolaylaştıracaktır; yani, cihazın eşzamanlı olarak birden fazla kullanıcı tarafından paylaşılması, her birinin kendi aktif oturumunun diğerlerinden ayrı olması. Bu özellik, oturum açma ve şifreler paylaşılmayacak şekilde bir ekran değiştirme biçiminin kullanılmasını gerektirir.

Bu konudaki potansiyel ihtiyaçları araştırırken, kendinize ve bu tür ürünlerin satıcılarına sormanız gereken sorular şunları içermelidir:

 1. Ortak bir alandaki bir iş istasyonu birçok son kullanıcı tarafından paylaşılabilir mi (örneğin üretim alanı)?

 2. Birisi zaten başka bir son kullanıcı tarafından kullanılmakta olan bir iş istasyonunu kullanmak istiyorsa, SSO ürünü mevcut son kullanıcının uygulamalarını (açık belgelerin kapatılması dahil) inceleyerek kapatabilir ve kontrolü yeni son kullanıcıya devredebilir mi?

3. Son kullanıcılar masaüstlerinin organizasyonunu ayarlayabilir mi ve öyleyse, kullandıkları iş istasyonundan bağımsız olarak onlarla birlikte seyahat ediyor mu?

 4. Bireysel uygulama tercihleri ​​son kullanıcıyla diğer iş istasyonlarına (örneğin, MS Word tercihleri) gidebilir mi?

 5. Mevcut uygulamaların seti, son kullanıcının ağa giriş noktasına göre değişiklik gösterebilir mi?

 6. Bir Novell son kullanıcısı, farklı bir Novell etki alanına atanmış bir iş istasyonunda oturum açarsa, son kullanıcı kendi etki alanına nasıl geri döner?

7. Kimlik doğrulama için Windows 95 ve Windows NT yerel olarak depolanmış bir şifreye güvenirse, son kullanıcı başka bir iş istasyonuna giriş yaptığında ne olur?

 8. Son başarılı oturum açmanın tarihi ve saati, son kullanıcının izinsiz oturum açmaları için imzaladığı tarihte gösterilir mi?

9. İş istasyonlarının diğer son kullanıcılar tarafından istemeden kullanılmasını önlemek için, oturum açan son kullanıcının adı belirgin bir şekilde gösteriliyor mu?

# 2.12.Doğrulama

Kimlik doğrulama, kullanıcıların iddia ettiği kişi olduklarını sağlar. Ayrıca, tüm işlem ve işlemlerin yalnızca yetkili son kullanıcılar tarafından başlatılmasını da sağlar. Kullanıcı kimlik doğrulaması, kullanıcı adı ve parolayı birleştirerek kullanıcı için bir tanımlayıcı, erişim ayrıcalıklarını atama mekanizması ve sisteme erişim, işlem başlatması ve diğer eylemler gibi tüm etkinliklerin izleneceği bir denetim "işaretçisi" sağlar. (örneğin, oturum açma girişimi). Bu nedenle, kimlik doğrulama sürecinde, “kim” ve “neyi” kontrol etmek ve izlemek için araçlar vardır. SSO ürünleri bu süreci alır ve oturum açma uygulamalarını geliştiren ve genişleten ek hizmetler için kullanılmasını sağlar. / şifre kombinasyonu. Bu uygulamaların bazıları, güvenliği de artıran kullanıcıya kolaylık sağlar: İş istasyonunu kısa bir süre önce terk etmeden hemen önce iş istasyonunu kilitleme yeteneği, iş istasyonunu başka bir kişi tarafından kötüye kullanım için açık bırakmak yerine, kullanıcının iş yapma olasılığının daha yüksek olduğu anlamına gelir. Bazıları denetim araçlarının uzantılarıdır: son giriş girişiminin görüntülenmesi ve tüm girişlerin günlük girişi. Bu özellikler kesinlikle SSO'ya özgü değildir, ancak işlevselliğini genişletir ve geliştirir ve böylece daha kullanıcı dostu hale getirir.

Genel Anahtar Altyapısı (PKI) kurulumunun bir parçası olarak, SSO dijital sertifika kimlik doğrulamasını destekleme yeteneğine sahip olmalıdır. SSO, çeşitli yöntemlerle (belirteç, şifre girişi, muhtemelen biyometri), kullanıcı için sistemin daha sonra Kerberos biletine benzer bir şekilde hem onaylayıcı hem de erişim lisansı “lisansı” olarak kullandığı bir dijital sertifika sağlar. Buradaki hayati nokta, bu işlevselliğin gerçekte nasıl gerçekleştirildiği değil (başka bir uzun tartışma), ancak SSO'nun bir PKI ile desteklediği ve bütünleştiği ve bunu yaparken geniş çapta tanınmış standartlar kullandığıdır. Bununla birlikte, daha yaygın erişim kontrol programları yoluyla elde edilebilen standart özellikler grubundan daha az teklif sunan herhangi bir SSO ürününün göz önünde bulundurulmaması gerektiğine dikkat edilmelidir. Böyle bir ürün, “daha ​​iyi olan” öncülünde daha zengin özellikli SSO ürünlerine bir alternatif olarak sunulabilir. Bu durumda daha basit değildir, çünkü etkinliği düşürür.

 Adayların ölçüp ölçmeyeceğini bilmek için, bu hususlarla ilgili olarak bir araştırma yapılmalıdır:

1. Kimlik doğrulama bir ağ sunucusunda mı yoksa iş istasyonunda mı?

2. Doğrulama kanıtlanmış ve kabul edilmiş bir standartla (ör. Kerberos) yapılıyor mu?

3. Tüm oturum açma girişimleri kaydedildi mi?

4. Sitede belirtilen sayıda başarısız oturum açma girişiminin ardından, gelecekteki tüm oturum açma girişimleri koşulsuz olarak reddedilebilir mi?

5. Bir süre etkinlik olmadığında masaüstünü kilitlemek veya kapatmak için etkin olmayan bir zamanlayıcı var mı?

6. Birisi bir iş istasyonunu terk ettiğinde (örneğin, tek bir tuşa basılması), masaüstü kolayca kilitlenebilir veya kapatılabilir mi?

7. Son başarılı oturum açmanın tarihi ve saati, son kullanıcının izinsiz oturum açmaları için oturum açtığı tarihte mi gösteriliyor?

# 2.13.Şifreleme

Şifreleme, son kullanıcılar ve güvenlik sunucuları / sunucuları ve eriştikleri uç nokta uygulamaları arasında bulunan bilgilerin casusluk, satır dokunma veya başka bir gizli dinleme yöntemiyle engellenmemesini sağlar. Birçok SSO ürünü, son kullanıcı ile güvenlik sunucusu arasındaki trafiği şifreler ancak son kullanıcı ile son nokta uygulamaları arasında açık metin geçişi sağlayarak potansiyel bir güvenlik açığının ortaya çıkmasına neden olur. Bazı ürünler varsayılan olarak iş istasyonu ile sunucu arasındaki tüm trafiği şifreler, bazıları yoktur ve yine de bazıları bu özelliği kurulumda seçilebilecek bir seçenek olarak sunar. Her kurulum kendi ortamında ve gereksinimlerinde farklıdır. Aynı şey, riskler ve güvenlik açıkları söz konusu olduğunda da geçerlidir.

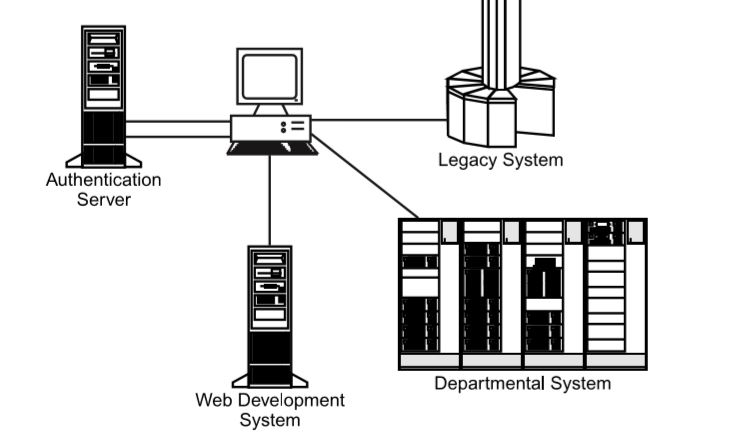
Bu adresi kapsayacak noktalar şunları içerir:

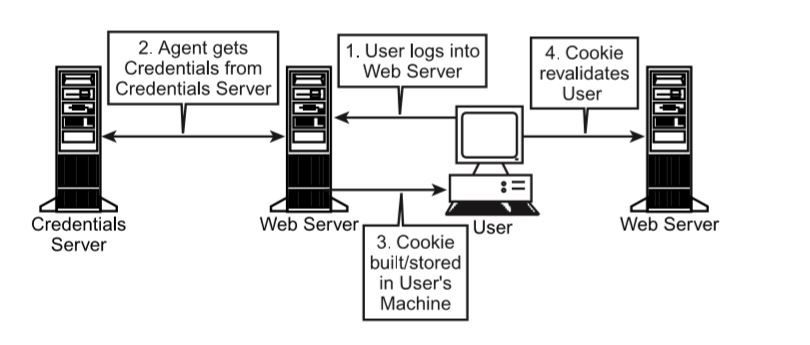
• İş istasyonu ile SSO sunucusu arasındaki tüm trafik şifrelenmiş mi? • SSO ürünü, uç nokta uygulamalarında değişiklik yapılmasını gerektirmeden uç nokta uygulamalarına (örneğin bilgisayar odası) kadar şifreleme sağlayabilir mi?

• Veri akışı kabul edilmiş ve kanıtlanmış bir standart algoritma (örneğin, DES, Triple DES, IDEA, AES veya diğer) kullanılarak şifreleniyor mu?

# 2.14. Giriş Kontrolü

Son kullanıcılara yalnızca erişme yetkisi olan uygulamalar sunulmalıdır. Bu uygulamaları başlatmak için gereken faaliyetler dikkatle değerlendirilmelidir, çünkü birçok SSO ürünü yalnızca API tabanlı uç nokta uygulamalarının katılabileceğini ya da SSO'nun tüm uç nokta uygulamalarının uyması gereken tek bir şifrenin sahibi olduğunu varsaymaktadır. Bu aktiviteler, uygulama şifrelerini süresi dolduklarında otomatik olarak girmeyi ve güncellemeyi içerir. Sergi 7.3, SSO'nun bir kullanıcının yetkilendirildiği tüm kaynakların otomatik oturum açmayı ve edinilmesini nasıl kolaylaştırdığını göstermektedir. Kullanıcı kimlik doğrulama sunucusunda oturum açar (ağda merkezi olarak konumlandırılmıştır). Bu daha sonra kullanıcıyı ve erişim haklarını doğrular. Sunucu daha sonra doğrulanmış kimlik bilgilerini gönderir ve kullanıcıyı oturum açmak ve kaynaklarını başlatılan oturuma eklemek için gerekli komut dosyalarını etkinleştirir.





Otomatik olarak oluşturulan şifrelerin kullanıcının hayatını kolaylaştıracağı kesin olarak doğru olsa da, mevcut en iyi uygulama, kullanıcıların kendi şifrelerini oluşturmalarını ve kullanmalarını sağlamaktır. Bununla birlikte bu şifrelerin sözdizimini düzenleyen bir kural olmalıdır; örneğin, sözlük kelimeleri, sayı ve harflerin bir kombinasyonu, harflerin arasına bir harf karışımı, belirli sayıda parola neslinde tekrarlama yapmama, özel karakterlerin yasaklanmış kullanımı (#, $, &,?,%, vb.) ) ve diğer kurallar. SSO, bu fonksiyonu, sistemler ve uygulamalar için amaçlanan tüm arayüzlerde desteklemelidir. Sergi 7.4, SSO'nun çerezleri kullanarak web üzerinden ileri ve geri gönderilen küçük bilgi paketlerini kullanarak Dünya Çapında Ağ (WWW) üzerinden giriş yapmayı nasıl kolaylaştırdığını göstermektedir. Kullanıcı ilk Web sunucusunda oturum açar (1), bu durumda kullanıcının kimlik bilgilerini kimlik bilgileri sunucusundan (2) alan bir aracı etkinleştirir. Bu sunucu, bir isim sunucusuna veya bir LDAP sunucusuna benzer şekilde çalışır, ancak bu cihazın özel olarak yetkilendirme ve erişim ayrıcalıkları bilgisi vermesi dışında. Tanımlama bilgisi daha sonra kullanıcının makinesinde (3) oluşturulur ve saklanır ve bir sayfa geçişi yapıldığında kullanıcıyı yeniden doğrulamak için kullanılır. Bu işlem, bir DBMS içindeki uygulama düzeyinde yetkilerin doğrulanmasına benzer. Veri tabanı sistemi içinde hareket ederken, kullanıcı yeni bir bölgeye veya işleme her eriştiğinde, doğru yetkilendirmeyi sağlamak için erişim ayrıcalıklarının yeniden düzenlenmesi gerekir. Web’deki sayfa geçişleri, DBMS içindeki yeni bölgelere veya işlemlere eşittir.

Bu alanda aşağıdaki hususlar ele alınmalıdır:

1. Platformdan bağımsız olarak tüm uygulamalar müdahaleci bir şekilde desteklenemez mi (yani, kapsamlı ya da hiç değiştirmeden)?

2. Bireysel uygulamaları ayarlamak zorunda kalmadan uygulama başlatma işlemini mekanikleştirmek için ne tür adaptörler mevcuttur? API tabanlı, OLE tabanlı, DDE tabanlı, komut dosyası tabanlı ve oturum uyarlama bağdaştırıcıları mevcut mu?

3. Tüm uygulama aktivasyonları ve devre dışı bırakmalar kaydediliyor mu?

4. Uygulama şifrelerinin süresi dolduğunda, SSO ürünü otomatik olarak süresi dolan yeni şifreleri oluşturur mu veya kullanıcılar kendi seçimlerini seçip girebilir mi?

5. Bir uygulama etkinleştirildiğinde, bilgi uygulamadaki doğru konuma gitmek için kullanılabilir (örneğin, sipariş girişi uygulaması sipariş girişi ekranına konumlandırılmış)?

6. Uygulama aktivasyon prosedürü son kullanıcıdan gizlenebilir mi yoksa son kullanıcının mekanize işlemi ilerledikçe görmesi gerekiyor mu?

7. Bir süre için faaliyet eksikliği olduğunda, bir uygulamayı sonlandırmak için etkinlik dışı kalma zamanlayıcıları var mı?

# 2.15.Uygulama Kontrolü

Uygulama kontrolü, son kullanıcıların uygulamaları yalnızca belirli bir uygulama içindeki belirli ekranların görülebileceği şekilde sınırlandırır, yalnızca belirli kayıtlar talep edilebilir ve uygulamaların özel kullanımları denetim amacıyla, son nokta uygulamalarına şeffaf bir şekilde kaydedilebilir. dahil olan uygulamalarda herhangi bir değişiklik yapılması gerekmez.

Kullanıcı navigasyonunun kontrol edilmesinin bir yolu olarak, bu, kurulumun genel güvenlik duruşunun geliştirilmesine yardımcı olabilecek başka bir özelliktir. Yine, bu bir ek özellik olarak olurdu - anahtar yöntem değil. Bu kabiliyetin kullanışlılığının belirlenmesi aşağıdaki sorularla yapılabilir.

1. Küçük uygulamalar masaüstünün sunum alanına dahil edilebilir mi (örneğin, ana hesapların listesi)?

2. Bir uygulama içindeki doğru konuma gitmek için uygulama bilgileri (örneğin, belirli bir hesap) kullanılabilir mi (örneğin, belirli bir müşteri için bekleyen siparişlerin listesi)?

 3. Her uygulamanın görünümü yalnızca belirli bir son kullanıcı için uygun bilgileri gösterecek şekilde ayarlanabilir mi?

4. SSO ürünü, son kullanıcıların uygulamalardaki etkinliklerini kaydedebilir mi (örneğin, hangi hesaplara erişilmiş)?

 5. Uygulama ekranları, uygulamaları kendileri değiştirmek zorunda kalmadan yeni yeteneklerle geliştirilebilir mi (örneğin, yakalanan girdilerin ek doğrulaması)?

 6. SSO ürün günlüğü izin verilen alanların ötesine geçen uygulama alanlarına ulaşmaya çalışabilir mi (örneğin, gizli hasta bilgileri)?

7. Son kullanıcıların her bir uygulamayı öğrenme gereksinimini ortadan kaldırmak için birden fazla uygulama tek bir son kullanıcı oturumunda birleştirilebilir mi?

8. Başvurular bir uygulamadaki (örneğin faturalandırma) son kullanıcı hareketi otomatik olarak alt uygulama oturumlarını (örneğin, mevcut siparişler, alacak hesapları) yeniden konumlandıracak şekilde koordine edilebilir mi?

# 2.16 Yönetim

SSO tarafından sunulan merkezi yönetim yetenekleri - ana cazibe değilse - daha önce bahsedilen “Kutsal Kase” dir. Bir SSO ürünü aracılığıyla kullanıcı hesaplarının ve kaynak yöntemlerinin yönetimi (değiştirilmesi, değiştirilmesi, silinmesi) bir kurum veya kuruluştaki bu işlevi kolaylaştırabilir ve basitleştirebilir. Yönetim araçlarının gücü çok önemlidir, çünkü büyük bir son kullanıcı popülasyonunu yönetmenin maliyeti, SSO ürününün maliyetini kolayca gölgeleyebilir. Ürün analizi aşağıdaki özellikleri dikkate almalıdır:

1. SSO ürünü tüm uç nokta sistemlerinin merkezi yönetimine izin veriyor mu? (Yani, merkezi yönetim veritabanında yapılan değişiklikler otomatik olarak uç nokta sistemlerine yansıtılır.)

2. Yönetim “son kullanıcı” veya “işletme içindeki bir rol” düzeyinde mi yapılır? (Bu bir son kullanıcı odağı orantısız yönetim çabasıyla sonuçlanabileceği için kritik bir unsurdur.)

3. Her iş istasyonunun ayrı olarak kurulması gerekiyor mu? Öyleyse, tahmini süre nedir?

4. Kuruluştaki son kullanıcıların rolleri kolayca değiştirilebilir mi (karma roller oynayan insanlarla başa çıkmak için)?

5. Son kullanıcının rolleri değiştirilirse, masaüstü otomatik olarak ayarlanıyor mu, yoksa masaüstü görünümünün manuel olarak mı ayarlanması gerekiyor?

6. Bir yönetici, uygulamaya göre etkin son kullanıcıların listesini görebilir mi?

7. Bir yönetici belirli uç nokta uygulamalarına verilen tüm şifrelere erişebilir mi?

8. Ürün, ağ sunucusu hatalarını incelikle ele alıyor mu?

# 2.17. Masaüstü Duyarlı Uygulamalar için Hizmetler

Mevcut uç nokta uygulamalarını değiştirmenin mümkün olduğu durumlarda, sorumluluklarını masaüstüyle işbirliği içinde paylaşma kabiliyeti çok çekicidir. Gerekli olan yayınlanmış bir masaüstü API ve ilgili hizmetlerdir. Bu durum, son kullanıcının, sadece onu etkileyecek ve temel uygulamanın kendisini değiştirmeyecek şekilde kendi kullanımına yönelik kurumsal bir üründeki standart bir ürünü kişiselleştirmek istediği durumlarda ortaya çıkabilmektedir. Bu özelleştirme, ekran kullanıcı formatlarını, komut dosyalarını ve bireysel kullanıcının sunucu tarafından sağlanan uygulama ile birlikte kullanmak istediği veya kullanması gereken belirli görevlerle ilgili işlemleri içerebilir. Sağlanan API ile, kullanıcı engellemeden gerekli özel değişiklikleri yapabilir ve bu, diğer kullanıcıların kendilerini veya iş istasyonlarını etkilemeden devam etmelerini sağlar. Bu gibi durumlarda, değişiklikleri isteyen kullanıcı, diğer kullanıcıları kilitlemek için özel erişim ve diğer kontroller gerektirebilir. Bir örnek, değişiklikleri gerektiren kullanıcının hassas veya kısıtlı bilgiler üzerinde çalıştığı ve aynı alandaki diğerlerinin çalışmadığı ve bunlara erişimine izin verilmediği bir örnek olabilir. Bu daha sonra, ek güvenlik gereksinimlerini karşılamak için masaüstünü değiştirmek için kullanılan komut dosyalarına gömülü erişim denetimlerinin kullanılmasını gerektirebilir. Bu durumda, API, SSO'ya erişim olanağı sunmalı ve SSO erişim / ayrıcalık veritabanına doğrudan erişimi olan kullanıcı (yerel değişiklikleri yapan kişi) olmadan erişim / ayrıcalık kontrolünü yapmalıdır. Bu, yerel iş istasyonunun kullanımını izlemek için erişim girişimlerinin, işlemlerin ve veri erişim yetkilerinin kaydedilmesini kolaylaştırmak için de aynı şekilde geçerli olmalıdır. Bu tesisin SSO'daki varlığını belirlemek için, bu hizmetler, API'ler ve aşağıdakiler gibi ilgili yeteneklerle ilgili sorular sorulmalıdır:

1. Masaüstünü tanıyan uygulamalar, SSO ürünü tarafından yönetilen son kullanıcı izinlerini sorgulayabilir mi?

2. Masaüstünü tanıyan uygulamalar, SSO ürününün kayıt olanaklarını kendi kullanımları için kullanabilirler mi?

3. Masaüstü özelleştirmesini sağlayan API hizmetleri var mı?

4. Bu API'ler, yerleşik güvenlik bilgi veritabanına "arka kapı" erişimi sağlayarak genel sistem bütünlüğünden ödün vermeden bunu kolaylaştırıyor mu?

# 2.18. Güvenilirlik ve Performans

Bir SSO ürününün, zorunlu olarak, son kullanıcılar ile işlerini yapmak için erişmeleri gereken uygulamalar arasında konumlandırılması nedeniyle, işletme içinde çok yüksek bir görünürlük vardır ve beklenmeyen güvenilirlik veya performans sorunlarının ciddi sonuçları olabilir. Bu sorun doğrudan ürünü haklı çıkarmak için yapılan orijinal iş davasına işaret ediyor. Güvenilirlik ve performans ile ilgili endişeler genellikle bir yazılımın diğerine (“başka bir katman”) eklenmesi, SSO ve dokunduğu diğer erişim kontrol programları arasındaki arayüzler, bu etkileşimlerin karmaşıklığı vb. endişe, bu yeni katmanın ortaya çıkardığı gecikme süresidir. Açılıştan giriş ekranına kadar geçen süre yıllar içinde istikrarlı bir şekilde artmıştır ve SSO'nun eklenmesi yine bunu artırabilir. Bu kullanıcı hayal kırıklığını daha da arttırabilir. Güvenilirlik sorunu, SSO ile diğer güvenlik cephesi arasındaki etkileşim dikkate alındığında ortaya çıkar. Arayüzlerin karmaşıklığı, çok büyükse, artan servis sorunlarına yol açabilir; Kod ne kadar karmaşık olursa, başarısızlık o kadar sık ​​sonuçlanır. Bu, şifreler ve senkronizasyon kaybetme, güvenilir şekilde geçmeme veya ayrıcalık atama dosyalarının aynı şekilde veya hızlı bir şekilde güncellenmemesi gibi değişikliklerle kendini gösterebilir. Bunlar gibi sorunlar, SSO'nun gerçekten de olsa iyi bir fikir olup olmadığını sorguluyor. Karmaşık kod bakımı masraflıdır ve SSO karmaşık değilse hiçbir şey değildir. En iyi programlama bile düzgün yapılmazsa etkisiz hale getirilebilir veya daha da kötüsü üretken olabilir. Bir SSO ürünü, özellik bakımından zengin karmaşıklığından dolayı bu türden daha fazla dikkat gerektirir. SSO'nun amacının erişim kontrolü olduğu ve bu bağlamda diğer tüm erişim kontrol sistemlerinde olduğu gibi aynı gizlilik, bütünlük ve erişilebilirlik hedeflerine ulaşıldığı açıktır. SSO ürünleri daha fazla işlevsellik sağlamak üzere tasarlanmıştır, ancak bu şekilde kullanılması, kurulu oldukları ortamları olumsuz yönde etkileyebilir. Bunu yaparlarsa, etkiler büyük olasılıkla güvenilirlik, bütünlük ve performans faktörlerine karşı görünecektir; ve eğer yeterince büyükse, etkiler SSO'nun başka bir yerde sağladığı faydaları olumsuz etkileyecektir.

# 2.19. Gereksinimler

Bu bölüm, bir SSO uygulamasında görmek istedikleriyle ilgili olarak Georgia Area RACF Users Group'un (GARUG) bir araya getirdiği bir gereksinim belgesinin içeriğini sunmaktadır.

# 2.20. Hedefler

Bu listenin odağı, güvenilir bir tek oturum açma ve güvenlik yönetimi ürününün tasarımı ve geliştirilmesi için bir dizi işlevsel gereksinim sunmaktır. Bunun, güvenlik uygulayıcıları tarafından incelenebilecekleri güvenlik ürünlerinin etkinliğini belirlemek için kullanılması niyetindedir. Deneyimli güvenlik kullanıcılarının çok platformlu sistemlerin başarılı bir şekilde korunmasında çok önemli olduğunu düşündükleri birçok gereksinimi içerir. Ayrıca, şu anda hemen bulunamayacak birkaç işlevsel gereksinim de içerir. Bu listenin bir araştırma ve geliştirme aracı olarak kullanılabileceğini, çünkü gereksinimlerin gerçek dünyadaki sorunlara yanıt olarak deneyimli, çalışan güvenlik uygulayıcıları tarafından benimsendiğini söyledi.

Bu konu, profesyonel güvenlik camiasındaki birçok kişi ve bu listeyi cevap olarak hazırlayan GARUG üyeleri tarafından öne çıkarıldı. Bu, güvenlik ürünleri arayışında kullanılacak bir yemek kitabı değildir. Birçok yönden, bu liste vizyonerdir; bu, burada belirtilen gereksinimlerin çoğunun mevcut olmadığını söyler. Ancak sadece şu anda var olmadıkları için şimdi dahil olmalarını engellemiyor. Bir üyenin belirttiği gibi, “İstemediğimiz takdirde, alamayacağız”.

# 2.21. İşlevsel gereksinimler

Aşağıdakiler, piyasadaki ideal bir güvenlik ürününün işlevsel gereksinimlerinin bir listesidir. Listede, güvenlik uygulayıcılarının gelecekteki ürünlere dahil edilmesini görmek istedikleri birçok özellik de var. Gereksinimler dört ana kategoriye ayrılmıştır: güvenlik yönetimi yönetimi, tanımlanması ve yetkilendirilmesi, erişim kontrolü ve veri bütünlüğü / gizliliği / şifrelemesi. Her kategoride gereksinimler en kritik ve en kritik sıraya göre listelenmiştir.

# 3.Ek Konu : Kötü amaçlı yazılım saldırısı

Kötü Amaçlı Araçlar; otomatik olarak virüs, solucan veya Trojan oluşturmak, uzak sunuculara DoS saldırıları düzenlemek, başka bilgisayarlara saldırıda bulunmak ve benzeri işlemler için tasarlanmış kötü amaçlı yazılım programlarıdır.

# 3.1. Kötü Amaçlı Araçlar Sizi Nasıl Etkileyebilir?

Kötü Amaçlı Araçlar alt sınıfındaki kötü amaçlı yazılımlar, virüslerin, solucanların ve Truva atlarının aksine çalıştıkları bilgisayara doğrudan bir tehdit oluşturmaz ve programın kötü amaçlı yükü yalnızca kullanıcının doğrudan emriyle bırakılır.

Constructor : Constructor programları, yeni virüsler, solucanlar ve Truva atları oluşturacak şekilde tasarlanmıştır. Kötü amaçlı program kaynak kodu, nesne modülleri ve/veya kötü amaçlı dosyalar oluşturabilirler.

DoS :Bu programlar, bir kurban bilgisayara karşı Hizmet Reddi (DoS) saldırıları düzenleyecek şekilde tasarlanmıştır. Programlar, hedeflenen kurban bilgisayara çeşitli istekler gönderir ve bilgisayarın tüm istekleri işleyecek kadar kaynağının bulunmaması halinde hizmet reddi durumu oluşur.

Email-Flooder :Spam gönderenler, bazı durumlarda bu programları e-posta kanallarını anlamsız mesajlarla doldurmak için kullanır.

Flooder : Flooder programları, spam gönderenler tarafından bazı durumlarda IRC (İnternet Üzerinden Sohbet) gibi diğer ağ kanallarını doldurmak için kullanılır.

IM-Flooder : Spam gönderenler bazen bu programları kullanarak ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype ve benzeri anlık mesajlaşma kanallarını anlamsız mesajlarla doldurur.

SMS-Flooder : SMS-Flooder programları, spam gönderenler tarafından bazen kısa mesaj kanallarını gereksiz mesajlarla doldurmak amacıyla kullanılır.

HackTool : Bu programlar, izin verilen sistem ziyaretçileri listesine yeni kullanıcılar eklemek, ayrıca sistem günlüklerindeki bilgileri silerek kötü amaçlı kullanıcının sistemdeki varlığını gizlemek için kullanılır. Kötü amaçlı kullanıcılar yerel veya uzak bilgisayarlara yönelik saldırılar düzenlerken HackTool programlarından yararlanır.

Hoax : Hoax programları bilgisayarınıza zarar vermez. Bunun yerine zararın oluştuğunu veya oluşacağını bildiren mesajlar gönderir ya da aslında var olmayan bir tehdit hakkında uyarılarda bulunur.

Spoofer : Spoofer programları, mesaj veya ağ istekleri gönderen tarafın adresinin yerini alır. Bunlar, alıcının mesajı gönderenin kimliğini belirlemesini engellemek gibi çeşitli amaçlarla kullanılır.

VirTool :Bu programlar, diğer kötü amaçlı programları değiştirmek ve antivirüs çözümünün kötü amaçlı yazılımı algılamasını engellemek için kullanılabilir.

# 3.2.Kötü Amaçlı Araçlara Karşı Korunma

Cihazlarınıza bir kötü amaçlı yazılımdan koruma yazılımı yüklemeniz ve bu yazılımı bilgisayarınızda sürekli olarak bulundurmanız büyük önem taşır. Kaspersky Lab, ödüllü internet güvenliği teknolojileri geliştirmiştir ve şu cihazları koruyabilecek ürünler sunar:

Windows PC'ler

Linux bilgisayarlar

Apple Mac bilgisayarlar

Akıllı telefonlar

Tabletler

# 4.Kaynakça

https://www.kaspersky.com.tr/resource-center/threats/malicious-tools

Information Security Management HandBook