Marmara İletişim Dergisi, Sayı:9, Ocak 1995
Marmara Journal of Communications, Number:9, January 1995

MODERN ŞİFRELEME TEKNİKLERİ VE GÜVENLİK TEKNOLOJİSİ

Doç.Dr.Emin Doğan AYDIN
MARMARA ÜNİVERSİTESİ
İletişim Fakültesi
(Bilişim Anabilim Dalı Öğretim Üyesi)

Şifre Güvenliği

En çok kullanılan bilgisayara erişim güvenliği yöntemi şifre, kullanıcı kimliği veya güvenlik kodları olarak bilinen gizli karakter dizileridir. Bu terimler birbirinin yerine kullanılabilir. Şifre; bireylerin yazılım, donanım ve veri de dahil bilgisayar kaynaklarına erişimini kontrol etmek için kullanılan ve gizli kalması amaçlanan bir karakter dizisidir. Özel bir şifre tipi erişimi kontrol için sayısal karakter katarı ve manyetik kodlu kart bileşimini kullanan kişisel tanımlayıcı numaradır (KTN).

Şifreler bilgisayar güvenliğinde önleyici bir görüş olabilirler. Şifre güvenliği bugün mümkün olan en iyi alternatif olmasına rağmen sistemin bütünlüğünü sağlamada en zayıf bağ olabilir. Geleneksel şifrelerin bir çok problemi vardır, çünkü:

* Bireylerce yanlış kullanılabilirler.

* Kullanım esnasında gözlenebilirler.

* Güvensiz hatlar dinlenerek alınabilirler.

* Başka bir bilgisayarca taklit edilebilirler.

* Tahmin edilebilirler.

* Değiş tokuş edilebilir veya ödünç verilebilir.

* Çalınabilir.

* Unutulabilir.

Şifrelerin yasaklama ve erişimi kontrol etme etkinliği şifrenin sadece bir kullanıcının bilmesine dayanmaktadır. Şifrenin gizliliğini sağlamak deşifre edilmesindeki güçlüğe ve kullanıcının bunu bir yere yazmadan hatırlayabilme yeteneğine bağlıdır. Bu, şöyle bir ikilem yaratır: Uzun ve karmaşık şifreler zor deşifre edilebilir ama hatırlanmak için mutlaka bir yere yazılması gerekir. Tam tersi, kısa şifreler rahatlıkla ezberlenebilir ancak kolayca deşifre veya tahmin edilebilir.

Belli uzunluktaki şifreler için muhtemel rastgele kombinasyonların sayısı aşağıda listelenmiştir. I ve O harfleri 1 ve 0 rakamlarıyla karışmaması için aradan çıkarılmıştır. Böylece 24 harf ve 10 sayı kalır.

Şifre Uzunluğu	Kombinasyonların Sayısı
1	34
2	1,156
3	39,304
4	1,336,336
5	45,435,424
6	1,544,804,416
7	52,523,350,144
8	1,785,793,904,896

Şifre Kaynakları

Şifre seçilebilir, dağıtılabilir veya aşağıdaki kaynaklarca sağlanabilir:

* Kullanıcı

* Merkezi yönetim fonksiyonu

* Bilgisayar

Kullanıcı - Seçimli Şifreler

Kullanıcı-seçimli şifrelerin avantajı, şifreyi sadece kullanıcının ve bilgisayarın bilmesidir. Eğer kullanıcı şifreyi açığa çıkarmazsa, gizliliği süreklidir. Kullanıcı-seçimli şifrenin dezavantajları:

* Rastgeleliğin olmaması ihtimali

* Değişim sıklığının olmaması

* Kullanıcının unutması halinde şifrenin tamamıyla kaybı

Genelde kişiye bir anlam ifade eden şifre seçimi eğilimi vardır. Bu yüzden kullanıcı-seçimli şifreler, bireyle çok yakın ilişkili olabilir; eşinin köpeğinin veya çocuğunun adı, adresi, telefon numarası, doğum tarihi, araba ruhsatı numarası veya kolayca hatırlanabilecek şeyler gibi. Fakat bu, bu tür şifrelerin kişiyi tanıyan birince bulunması ihtimalini artırır. Ortaya çıkan rastgelelik eksikliği şifre güvenliğini ortadan kaldırabilir.

Şifre değiştirme sıklığı gizliliği etkiler. Açığa çıkma ihtimali zamanla artar. Sıkça değiştirilmedikçe iş yerinde şifre herkesçe bilinebilir hale gelebilir.

Unutulmuş şifreler özel problemler yaratırlar. Erişim güvenliğini yeniden kurmak bu esnada kullanıcıya gerekli bilginin sağlanamayacağı uzun bir süre gerektirir.

Merkezi Yönetim Fonksiyonu

Merkezi yönetim fonksiyonu şifreyi rastgele bir temelde oluşturabilir, değiştirme sıklığını garanti edebilir ve unutulan şifreleri değiştirebilir. Bu yaklaşımdaki dezavantaj yönetici ve kullanıcının her ikisinin de şifreyi bilmesinden dolayı gizliliğin olmamasıdır. Diğer bir konu da bu ikisinin arasında şifrenin iletilmesi olmalıdır.

Bilgisayarca Üretilmiş Şifreler

Bilgisayar rastgele şifreler üretebilir ve değiştirme yöntemlerini uygular. Yeni şifreler eklemek ve şifre unutulduğunda erişimi yeniden kurabilmek için bir yönetici fonksiyon gereklidir.

Hiç bir şifre üretim sistemi mutlak güvenlik sağlamaz ve kendi içlerinde şifre sistemleri tam bir güvenlik sağlamaz. Toptan güvenlik ve kontrolün sadece bir yönüdürler.

Şifre Dağıtımı

Şifre güvenliği özellikle dağıtımı esnasında çok hassastır. Kullanıcılara sistemi kullanmaya izinli oldukları bildirilmeli ve şifrelerini almaları için bir yol belirlenmelidir. Şifreyi alacak kimsenin sistemi kullanmaya yetkili kimse olduğunu garanti etmek güç olabilir. Şifre dağıtımını güvenli yapma teknikleri:

Direkt temas: Bu metod çok etkili olabilir ancak büyük kuruluşlar içerisinde her kullanıcıyla yüz yüze temas kurmak zaman alıcı olabilir. Coğrafi olarak çok dağınık yerleşimler ek güçlükler yaratabilir.

Telefon iletişimi: Bu metod sıkça kullanılır ve nispeten ucuzdur. Fakat telefon kullanımında açığa çıkma ihtimali çok yüksektir.

Yönetici tarafından dağıtım : Birçok işletme dağıtım sürecinde bilinen ve güvenilen yöneticilerini kullanır. Bu yöntem kullanıcılarla direk teması ortadan kaldırır ve yönetim güvenirliliğini kurar. Şifreler tek tek mühürlü zarflar içinde yöneticilere gönderilir. Bu yaklaşımın dezavantajı güvene dayalı olması ve güvenlik sürecindeki insan sayısını artırmasıdır.

Kendini postalayan zarflar : Bu metod şifreyi, fişi ve geri gönderme zarfını kullanıcıya gönderir. İmzalı olarak geri dönen fiş kullanıcının şifreyi aldığını gösterir. Bu yaklaşımın ana dezavantajı, postanın sıkı kontrolü olmaması durumunda açığa çıkma ihtimalinin muhtemel oluşudur.

Şifre Güvenliği ve Kontrol Teknikleri

Şifre güvenlik sistemlerinin sağladığı koruma seviyesi ve derecesi organizasyonlar ve bilgisayar sistemleri arasında oldukça değişir. Bir kimse, eğer şifreyi bulursa, kullanıcının yerine sadece o kullanıcıya izin verilmiş fonksiyonları kullanabilir. İyi bir şifre güvenliği sistemi:

* Şifre değişimlerinin güvenlik yöneticisince mi yoksa kurulum esnasında kullanıcı tarafından mı yapılacağı konusunu yönetimin belirlemesine izin vermeli.

* Şifre güvenliğini kullanıcıyla, uygulamayla, uygulama içindeki fonksiyonlarla ve uygulama dahilinde etkileşimle sağlamalı.

* Her kullanıcı için son şifre değiştirme tarihini saklamalı ve raporlamalı.

* Kullanıcı isteği üzerine otomatik olarak şifre üretmeli.

* Kullanıcı veya güvenlik görevlisinin şifreyi daha önce kullanılmış bir şifreye dönüştürmesini engellemeli.

* Giriş esnasında şifreleri saklamalı.

* Eğer bir menü tanımlandıysa, kullanıcıyı uygun girişten sonra önceden tanımlanmış menüye yönlendirmeli.

* Terminalce belli işlemlere girişimi sınırlamalı (mesela sadece belli terminallere mali işlemler yapma izni vermeli).

* Kullanılmayan veya aktif olmayan şifreleri izlemeli.

* Çok kullanılan şifreleri izlemeli.

* Giriş/çıkış saatlerini, erişilen sistemi ve her terminal kullanıcısının yaptığı faaliyetleri belirten terminal aktivite raporu hazırlamalı.

* Sisteme tüm yetkisiz erişim girişlerini gösteren güvenlik ihlalleri raporu hazırlanmalı.

* Şifreleri rastgele üretmeli.

* Şifreleri kodlamalı.

* Dosyaya, programa, menüye ve kütüphaneye dayalı şifre seviye leri kurmalı.

* Daha önceden belirlenmiş sayıda geçersiz erişim girişiminden (genellikle üçtür) sonra terminali otomatik olarak sistemden çıkmalı.

* Terminalleri belirlenmiş bir süre boyunca faaliyetsiz kaldığında kullanıcıları sistemden çıkmalı. Bu kontrol metodu başında yetkili kimse bulunmayan açık terminallerle ilgili riskleri azaltır.

* Her açılışta kullanıcıyı, kullanıcının bir önceki başarılı girişinden veya bu esnadaki başarısız giriş denemelerinden haberdar etmeli. Kullanıcı böylece şüpheli olayları bildirebilecektir.

* Terminalleri, giriş esnasında operatörün tuşa basmasının görüleme yeceği şekilde yerleştirmeli.

* Kullanıcının bir sistemde aynı anda çalışabileceği terminal sayısı nı sınırlamalı. Genelde bir kullanıcı bir anda sadece bir terminali kul lanabilmelidir.

* Kullanıcıların giriş işlemine ayrılan süre sınırlanmalı.

* En az altı karakterlik bir şifre zorunlu olmalıdır. Şifreler tüm kombi nasyonları denemeyi zorlaştıracak kadar çok olmalıdır.

* Belli bir süre sonucunda kullanıcıları şifrelerini değiştirmek için otomatik olarak uyarmalı ve bunu zorunlu kılmalı.

* Tüm şifre değişimlerini izleyebilmeli.

* Belli özel işlemleri terminalle, günün zamanıyla ve haftanın günüyle sınırlamalı.

* Şifrelerin görüntülenmesini engellemeli.

* Başarılı giriş işlemi için deneme sayısının en fazlasını belirlemeli. Hatalar oluşabileceğinden kullanıcılara şifrelerini doğru girmeleri için birden çok şans tanınmalıdır. Fakat sisteme otomatik şifre dene me saldırılarını ve şifrenin rastgele bulunmasını engellemek için en fazla deneme sayısı belirlenmelidir. Bu deneme sayısı aşıldığında ter minaller veya iletişim kapıları kapatılmalıdır.

* Sisteme giriş için başkaları tarafından zorlanan kullanıcılara yar dım için bir alarm sistemi kurulmalı.

* Tüm erişim girişimleri için zaman ve tarih damgası kullanılmalıdır.

* Tüm erişim girişimlerini takip edecek bir sistem kurulmalıdır.

* Özellikle önemli bilgiye erişim için çok seviyeli şifreler zorunlu tu tulmalı. Çok seviyeli yazılım güvenliği, yetkisiz kullanıcının bir şe kilde baş edebileceği tek seviyeden daha çok koruma sağlar. Çok sevi yeli şifreler normalde meşru kullanıcıyı geciktirmez ve önemli oranda koruma sağlar.

* Programlanabilir fonksiyon veya terminal fonksiyon tuşlarının giriş aşamasında kullanılmasını yasaklamalı. Giriş işlemlerinde bu tuşla rın kullanımı şifre güvenliğini ve sistem bütünlüğünü bozar.

Elde Taşınan Şifre Üreticileri

Elde taşınan şifre üreticileri bilgisayar ağlarında ilave güvenlik sağlayabilir. Kullanıcı tarafından taşınan cihaz bir seferlik ve tek olan bir şifre üretir. Her cihazda farklı olan kullanıcı verisine ve her giriş denemesinde değişen veriye bağlı olarak şifre üreten bir algoritma kullanılır.

Bilgisayar da cihazda bulunan veriyi ve aynı algoritmayı kullanır. Bilgisayar kullanıcıdan sayısal kodu girmesini ister. Cihazca üretilen şifre bilgisayarca üretilen şifreyle karşılaştırılır ve buna bağlı olarak izin verilebilir.

Kişisel Tanımlama Numarası/ları

İşaret tabanlı tanımlama erişim için anahtar gibi fiziki bir cihaza ihtiyaç duyar. KTN'leri iki çeşit tanımlama; plastik bir kart (sahip olduğunuz bir şey) ve bir şifre (bildiğiniz bir üye) kullanan İşaret tabanlı sistemin özel bir tipidir.

Otomatik vezne makinaları kart kullanıcısını tanımak için bir plastik kart ve gizli bir kod (KTN) kullanırlar. Otomatik vezneler deneme yanılma yoluyla suç işlenmesini engellemek için bir kaç başarısız denemeden sonra kartı reddetmeye veya karta el koymaya programlanmışlardır. Dört haneli bir KTN için 10000, altı hanelik bir KTN için ise 1000000 seçenek vardır. Kart sahiplerinden şifrelerini ezberlemeleri ve bunu kartın üstüne veya kartla birlikte taşınan bir belgenin üstüne yazmamaları istenir.

Bilgisayar sistemi ve iletişim ağı da güvenli olmalıdır. Bilgisayar sistemi KTN'leri güven altına almak için tipik olarak çeşitli genel kontrol ve uygulama kontrolleri kullanır. İletişim ağını dinlemeye karşı korumanın ana yöntemi kodlamadır.

KTN'lerin güvenliğini sağlamak;

* Vericinin ve müşterinin

* Verici ve ağ hizmeti sunanın

* Ağ hizmeti sunan ve bağlantı hizmetinin

* Bağlantı hizmeti ve diğer ağ hizmeti sunanın

* Ağ hizmeti sunanın ve alıcının

* Alıcı ve diğer bir ağ hizmeti veya terminal hizmeti sunanın sorumlu luğundadır.

DİĞER TESPİT ve KORUNMA YÖNTEMLERİ

Uygulama Kontrolları

Uygulama kontrolları yatırımlar, bordro, talep toplama muhasebesi ve borç sistemleri gibi bilgisayar uygulamalarına özel güvenlik teknikleridir. Uygulama kontrolları girdi, işleme ve çıktı kontrolları olarak sınıflandırılırlar.

Girdi Kontrolları

Girdi kontrolları işlemlerin izni ve kaynağını, işlemlerle ilgili kayıt ve hata yönetimi ve dosyalama veya diğer kaynak doküman saklama metodlarına hitab eder. Girdi kontrolları genellikle kullanıcı bölümü seviyesinde bulunur çünkü kullanıcılar genellikle kaynak doküman kontrolü ve uygulama için veri girişinden sorumludurlar.

Girdi kontrolları bilgisayarda işlemek için alınan veriye uygun şekilde izin verildiğinden, makinaca anlaşılabilir forma dönüştürüldüğünden ve kontrol edildiğinden ve verinin (iletişim hatlarından gönderilen veriler de dahil) kaybolmadığından, veriye ek yapılmadığından, çoğaltılmadığından veya uygunsuzca değiştirilmediğinden yeterince emin olabilecek şekilde tasarlanmalıdır. Girdi kontrolları, daha önceden yanlış olan verinin reddi, düzeltilmesi ve yeniden yayımını da kapsar.

Kontrol edilmesi gereken dört temel girdi kategorisi vardır:

1. İşlem girişi : İşlem girişi normal olarak en büyük hacmi temsil etti ğinden en çok hataya sebep olan da budur.

2. Dosya bakımı işlemleri : Dosya bakımı (güncelleştirme) çoğu za man sınırlı bir miktarda veriyi kapsar, yasaklanmış kaynaklardan or taya çıkar ve güncelleştirilen dosyalar üzerinde nispeten uzun süreli etkisi olur.

3. Sorgulama işlemleri : Bu işlemler kaynak dosyayı değiştirmezler ama diğer işlemlere veya girdilere götüren kararlara sebep olabilirler.

4. Hata düzeltme işlemleri : Hata düzeltme çok karmaşık bir yöntem dir. Geri alma, orijinal işlemlerin ayarlanması, orijinal işlemin yeni den girilmesi veya bunların bir bileşiminden oluşabilir. Hata düzelt me genellikle ilave hata yapma ihtimalini ortaya çıkaran ve orijinal iş lemin yenilenmesinden daha karmaşık bir işlemdir.

Basit bir bilgisayar suçu tekniği bilgisayar sistemine girmeden önce veya giriş esnasında veriyi değiştirmektir. Hatalı veri girişi veya veri aldatması olarak bilinen teknik, suçu işleyen için oldukça güvenlidir çünkü hatalı veri girişi olarak algılanabilir. Suç, görünürde işlem girişi ve hata düzeltme yetkileri olan bir kimse tarafından işlenmiş olabilir. Bu, kaynak belgelerin sisteme girilmeden önce uygun şekilde izinlendirilmesinin ve işlem girişini takip eden izleme yolunun gözden geçirilmesinin önemli bir sebebidir. Toplu kontrol toplamlarını kullanmanın ve bunları işlem girişini takiben bilgisayar sistemince üretilen kontrol toplamlarıyla karşılaştırılmasının önemini vurgular.

Ne yazık ki yanlış veri girişinin, kuruluşun yeterli görev ayırımı yoksa fark edilmesi çok zordur - ve bir çok küçük organizasyonda durum böyledir. Genellikle sadece izlemede kullanılan işlemleri kaynak belgeleriyle karşılaştırma yöntemi ile tespit edilebilirler. Fakat izleme yöntemleri genellikle az sayıda işlemleri temsil ederler ve yüksek hareketli veya büyük dolar işlemleri olan istisna hesaplara bakabilirler.

Girdi kontrol yöntemleri şunları kapsar:

* İşlemlerin belirlenmiş bir sırada girilmesine izin veren ve aynı bi çimde kontrolları ve alan onaylamalarını her işlemde yapan yapısal veri girişi.

* Hata düzeltmesi esnasında girilen her işlemin, orijinal işlem gibi ayrı girdi kontrollarına maruz kalmasını garantileyen yapısal hata düzeltmesi.

* Belli işlem grupları için bazen dolar toplamları, tekrar toplamları ve ya kayıt sayıları şeklindeki kontrol toplamları.

* Veriyi işleme sokmadan önce inceleme ve değiştirme imkanı tanıyan özellik düzenleme yöntemleri, girdi hatalarını veya istisnaları tespit etmek ve yazdırmak için kullanılmalıdır. Örnekler:

* İşlem sınırı testleri.

* Kayıt dosyaları arasında kayıtların tamlığı ve kabul edilebilir ilişkileri onaylamak için çapraz kontrol.

* Önceden numaralandırılmış belgelerin sıra kontrolları.

* Bütünlük testleri.

* Mantık testleri.

* Girdi belgelerinde kullanılan tüm kod değerlerinin onaylanması.

* Müşteri hesap numaralarını onaylamak için hane kontrol yöntemleri.

* Beklenti kontrolları.

* Uygunluk testleri için bir değerler dağılma aralığıyla karşılaştırılması.

* İlişkili alanların çapraz tabanlı.

* Geçersiz sayılar testi.

* Uygun matematiksel işaret testi.

* Tarih kontrolları.

Hane kontrol yöntemleri, hesap numaralarını değerlendirmek için

önemli bir girdi kontrol tekniğidir. Hesap numaralarının girişi esnasında sistem bu numaralar üzerinde bir modülo kontrolü yapmalıdır. Hesap numaraları için kullanılan modülo, modülo 10 veya modülo 11 olabilir.

Modülo 11 yöntemi aşağıdaki işlemlerden oluşur:

- Hesap numarasının birler hanesini 1 ile, onlar hanesini 2 ile, yüzler hanesini 3 ile,... 11. haneyi 11 ile çarp.

- Eğer bu çarpımların toplamı 11'e tam olarak bölünebilir ise sayı geçerlidir.

Aşağıda bir sayının modülo 11 bir sayı olup olmadığını inceleyen iki örnak bulunmaktadır.

ÖRNEK SAYI : 123528

1	2	3	5	2	8
x 6	x 5	x 4	x 3	x 2	x 1
6	10	12	15	4	8

6 + 10 + 12 + 15 + 4 + 8 = 55
55 : 11 = 5

123528 GEÇERLİ SAYI

ÖRNEK SAYI : 123529

1	2	3	5	2	9
x 2	x 1	x 2	x 1	x 2	x 1
6	10	12	15	4	9

6 + 10 + 12 + 15 + 4 + 9 = 56
56 : 11 = 5.09

123529 GEÇERSİZ SAYI

Modülo 10 yöntemi aşağıdaki işlemlerden oluşur:

- Hesap numarasının birler hanesi kontrol hanesidir.

- Onlar hanesini 2 ile, yüzler hanesini 1 ile, binler hanesini 2 ile çarpın...

- Bu çarpımların birler hanelerini toplayın

- Üçüncü adımda elde edilen toplama 9 ekleyin ve son haneyi sıfırlayın

• Eğer üçüncü adımdaki toplamla dördüncü adımdaki dönüşümün sonucunun farkı kontrol hanesi ile aynıysa sayı geçerli bir Modülo 10 sayısıdır.
İki sayı için örnek hesaplamalar şunlardır:

ÖRNEK SAYI : 123528

1	2	3	5	1
x 2	x 1	x 2	x 1	x 2
2	2	6	5	2

2 + 2 + 6 + 5 + 2 = 17
17 + 9 = 26
İlk hane sıfırlanır 0 : 20
20 - 17 = 3
123513 GEÇERLİ SAYI

ÖRNEK SAYI : 123529

1	2	3	5	1
x 2	x 1	x 2	x 1	x 2
2	2	6	5	2

2 + 2 + 6 + 5 + 2 = 17
17 + 9 = 26
İlk hane sıfırlanır 0 : 20
20 - 17 ≠ 4
123514 GEÇERSİZ SAYI

İşleme Kontrolları

İşleme kontrolları uygulama programlarına yerleştirilmiş otomatik kontrollar ve aşağıdakilerce meydana getirilen hatalı şartların ihtimalini azaltan işlem akışlarıdır.

* İşleme esnasında kasıtlı veya kazara hata oluşumu ile ilgili program hataları ve eksikleri

* Hatalı veri, kayıp işlemler gibi olaylara sebep olabilen donanım arızaları

* İşleme esnasında tespit edilen hataların düzeltildiği ve orijinal işlem gibi kontrolların aynı seviyesinin etkisi altında olduğunu garanti eden hata yönetimi.

Bilgisayarca üretilmiş işlemler, kullanıcılar ve dahili/harici denetleyicilerin özel ilgisine haizdir. Bu işlemler başka bir işlemin girişi ile veya bu işlemce sağlanan özel koşullara dayalı olarak oluşabilir. Özel program parçalarının çalışmasının sonucudurlar ve işlemin özel bir değer veya izin belirten kaynak belgesi olmadığından test edilmelidir. Bilgisayarca üretilen işlemler bilgisayarla işlemenin, bilgisayar suçunun bir çok kez tespit edildiği, en çok yara alan bölgelerinden biridir.

İşlem kontrolları verinin iki kez işlenmesini veya hatalı işlenmemesini garanti edebilecek yeniden başlama/kurtarma yeteneğini de dikkate almalıdır.

İşleme kontrolları, bilgisayar işleminin belli uygulamalar için istendiği şekilde yerine getirildiğini, mesela tüm işlemlerin izin verildiği şekilde yapıldığı, izin verilen hiç bir işlemin atlanmadığını ve izin verilmemiş işlemlerin eklenmediğini makul bir garanti sağlayacak şekilde tasarlanmalıdır. Bu tür kontrollar aşağıdaki tip hataları tespit etmek ve önlemek için tasarlanmalıdır.

* Tüm girdi işlemlerini uygulamamak veya aynı girdiyi birden çok uygulamak

* Yanlış dosya veya dosyaları işleme ve güncelleştirme

* Mantıksız veya uygun olmayan girdiyi işleme

* İşleme esnasında veri kaybı veya bozulması

Çıktı Kontrolları

Çıktı kontrolları, bir uygulamayı dengeleme veya telif kontrolu, çıktı dağıtımı kontrolu ve kayıt saklama ve düzenlenebilen maddelerle ilgili kontrollardır.

Çıktı kontrolları işlem sonucunun kesinliğini (hesap listeleri, KIT(CRT) görüntüleri, raporlar, manyetik dosyalar gibi) ve çıktıyı sadece yetkili personelin almasını garanti etmek için tasarlanmalıdırlar. Çıktı kontrolları tüm girdinin işlenmesini, işlemenin doğru olduğunu ve çıktının yetkili personele dağıtımını sağlamalıdır.

Bu alanla ilgili bazı potansiyel sorunlar ve konular şunlardır:

Çıktı dengeleme ve telif işlemlerinin doğru ve tamamıyla yapılması nı sağlama

Çıktı dağıtımı: Yazılı kopya, manyetik ortam ve mikrofiş dahil çıktı ların taşınmasının ve dağıtımının kontrol edilmesi ve yetkili alıcılara yönlendirilmesini

Gizlilik: Kuruluş veya birey hakkındaki bilginin kasti veya kazara dağılmamasını

Düzenlenebilir maddeler : Düzenlenebilir maddelerin (çekler, se netler vb) açıklanmasını ve yatırımların korunmasını.

Kayıt saklanmasını ve atılması : gerekli iş faaliyetleri kayıtlarının kanuni gerekliliklere uygun olarak saklanmasını ve saklama ve atık yoketme yöntemlerinin bilginin gizliliğini korumasını sağlamak.

Atık toplamak izinsiz olarak bilgisayar çıktısından bilgi elde etmeyi kapsayan bir bilgisayar suçu tekniğidir. Bazı atık toplama teknikleri çöp kutularını karıştırmak, karbon kopyaları kullanmak veya kazınmış manyetik ortamda kalan bilgiyi almak için gözden geçirmektir.

Veri sızdırma, bir bilgisayar tesisinden veya depolama alanından bilgi çalmayı kapsayan diğer bir bilgisayar suçudur.Birçok kuruluş, raporların ve/veya manyetik ortamın eski veya günümüz kopyalarının saklandığı yere girme iznini tüm çalışanlarına verir.Bu malzemenin çok kısa bir süre için bile yerinden alınması, bilginin gizliliğini ortadan kaldırabilir.

Veri yönetiminde zayıf kalan elle kontrollar bilgisayar üzerindeki zayıf kontrollardan daha büyük suç olaylarına sebep olabilmektedir ve genellikle bilgisayar ortamının dışındaki herşeye bilgisayar içinde olanlardan daha kolay erişilebilmektedir.İyi erişim kontrolları, depolama yöntemleri ve atık imha teknikleri bu kontrol yetersizliklerini azaltıp kuruluşun kötü olaylara maruz kalma riskini artırabilir.

Hem genel hem de uygulama kontrolları bilgisayar suçuna karşı korunmada önemlidirler. Fakat bir dahili kontrol yönteminin maliyeti sağlanacak muhtemel yarardan çok fazla olmamalıdır. Elektronik bilgi işlem kontrolu maliyet-etkin olmadığı zaman yerine geçebilecek elle kontrol sistemleri kurulabilir. Dahası, yeterli miktarda önleyici, tespit edici ve düzeltici kontrol tekniklerinin bir karışımının kurulması ve sağlanması önemlidir.

Ağ Güvenliği

Ağ güvenliği, ağ bilgisini koruma ihtiyacı duyan mali kurumlar için önemi gittikçe artan bir konudur. Kontrolu artırmanın bir yöntemi erişimi kontrol etmek ve bilgiyi korumak için güvenlik modemleri kullanmaktır. Modem bir telefon hattı gibi bir iletişim ortamından yayın yapması için bilgisayarın sayısal verisini analog yapıya çeviren bir cihazdır. Hattın diğer ucundaki başka bir modem bu analog sinyali alıp diğer bilgisayarın kullanabileceği sayısal yapıya dönüştürür.

Modemlerin çalışma hızı, baud hızı veya saniyede bit cinsinden tanımlanır. Düşük hızlı modemler 1200 baud da ve yüksek hızlı modemler 9600 baud veya üzerindeki hızlarda çalışırlar.

Modemler geri arama, şifre koruması ve kodlama gibi birçok güvenlik özelliği ve yeteneklerine sahip olabilirler. Mesela geri arama yeteneğine sahip bir sistem kullanıcı yetkisini teyid etmek için güvenlik dizinindeki yerden kullanıcıyı arar. Bu cihazlar genelde aşağıdaki gibi çalışır.

1. Bir uzak kullanıcı klavye veya tuşlu telefon kullanarak bilgisayarı arar.

2. Erişim isteğini geri arama ünitesi karşılar.

3. Geri arama ünitesi kullanıcı tanımlama numarasını ve şifreyi ister.

4. Uzak kullanıcı istenilen veriyi girer.

5. Geri arama ünitesi uzak kullanıcıyı devreden çıkarır ve kullanıcı tanımlamasını dizinde arayarak bir telefon numarası bulur.

6. Eğer kullanıcı tanımlama bilgisi yetkili bir kullanıcıya ait ise cihaz kullanıcının numarasını çevirir. Eğer bilgi tutmuyorsa cihaz sistemi yetkisiz erişim isteğinden haberdar eder.

Bu yaklaşımın ana güvenlik avantajı cihazın arayan kişiyi hem doğru tanımlama bilgisi ile hem de belli bir yerleşimle ilişkilendirmesidir. Bu yüzden güvenlik sadece değişik harf ve sayı bileşenlerinin denenmesiyle aşılamaz.

Şifreleme Teknikleri

Elektronik dinleme her türlü bilgi iletişimini ve depolamayı tehdit etmektedir.Mali kuruluşlar hergün elektronik ortamlarda yüzlerce milyon dolar transfer ederler. Hiç bir ortam tam güvenli değildir. Elektronik fon transfer ağları işlem verisi korunmadığı sürece suça maruz kalabilir. Koruma olmaksızın mesajlar engellenebilir, silinebilir veya hattın herhangi bir yerinde ve herhangi bir zamanda değiştirilebilir. Pratik olarak hattın tamamının fiziksel korunması mümkün değildir. Bu yüzden veri ağ içerisinde aktıkça korunmalıdır. Ağa verilmiş bir verinin korunmasında kanıtlanmış bir metod, veriyi karıştırarak anlamsız bir hale getirecek bir algoritma kullanan veri şifrelemedir..

Veri şifreleme, veriyi izleyen kimselerin anlayamayacağı şekilde ağdaki veriyi saklar. Şifreleme teknikleri veriyi değiştirmek için yapılan herhangi bir girişimi tespit etmek için kullanılabilir. Bu yüzden veri şifreleme müşteri KTN' nın gizliliğini korumak ve mali işlemlerdeki veri bütünlüğünü gözlemek için kullanılır.

Tarihçe

Şifrelemenin 4000 yıllık bir geçmişi vardır. Şifreleme; 'kod ve şifre tasarımı ve analizi ' olarak tanımlanır. İlk 3000 yılında şifreleme Mısır, Hindistan ve Mezopotamya gibi antik kültürlerde birbirinden bağımsız olarak gelişmiştir. Antik yazımda şifrelemenin en eski kanıtı MÖ 1900 yılında bir mısır mezarının ana odasında duvara oyulmuştur. Sıradan semboller yerine olağandışı hiyeroglif sembolleri kullanılmıştır. Yazı, şifrelemenin önemli yöntemlerinden birini- metnin dönüştürülmesi- kullanmasına rağmen gizli bir yazı değildir. Amacı yazıya otorite ve haysiyet kazandırmaktır. Babil ve Asur yazıları da kil tabletlerini imzalamak ve tarihlemek için olağandışı semboller kullanmaktadır.

Yunanlıların en savaşçıları olan Spartalılar ilk askeri şifreleme sistemini kurdular. Romalılar da işlerinde şifrelemeyi kullanmışlardır. Askeri bilgileri saklamak için Julius Caesar 2000 yıldan daha fazla zaman önce basit bir şifre tekniği kullanmıştır. Bu sistemde düz metnin her harfi alfabede kendisinden belli bir sayı sonra gelen harfle değiştirilmektedir. Mesele a, c ile, her b, d ile...

Normal A B C .....Y Z
Şifre C D E .....A B

Bu sistem kullanılarak 'MUTLU YILLAR' mesajı şifrelenirse sonuç 'OVöNV AJNNŞ' olur.

Bu süre içerisinde geliştirilen diğer basit sistemler şunlardır:

* Gizli mesajları dikey veya tersten yazmak

* Sesli harflerin yerine nokta koymak

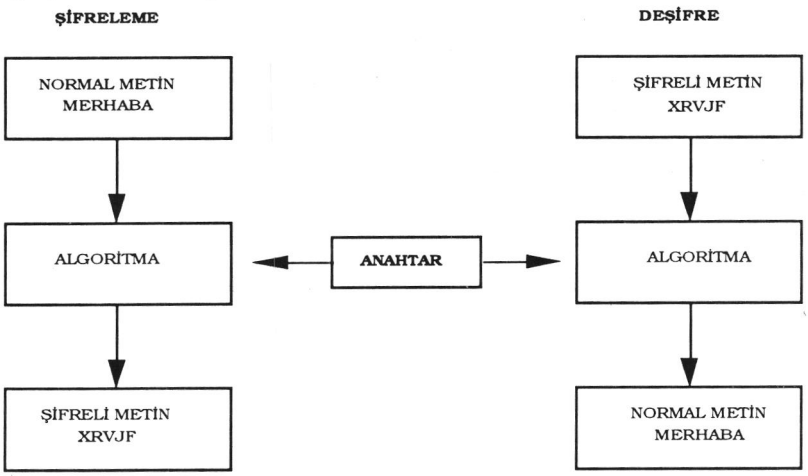
* Yunan veya İbrani alfabesi gibi yabancı alfabeleri kullanmak

* Harfler yerine özel işaretler yerleştirmek

Modern şifreleme tabloları eskilerine göre matematik olarak daha karmaşık ve daha zahmetlidir. Hassas bölgelerini korumak için askeri ve kamuya ait birimler son derece gelişmiş sistemler kullanırlar. Mali sektör ise bilgisayar sistemlerini ve veri iletişimlerini korumak için benzer sistemler kullanırlar.

Modern Şifreleme Teknikleri

Modern şifreleme bilgiyi (modern metni) güvenli olmayan kanallar üzerinden gönderebilmek için anlaşılamaz bir hale (şifreli) çevirme işlemidir. Çevirme işlemi anahtar adı verilen bir veri katarı ile yürütülür. Güvenli olmayan hat üzerinde mesajı önleyen bir kimsenin mesajı deşifre edebilmesi için (normal metne geri çevirebilmek için) uygun anahtara sahip olmalıdır. Mesajı alacak kimsenin bu anahtara sahip olduğu varsayılır. Bu metod aşağıdaki şekilde gösterilmiştir. Bugün kullanılan iki temel tip şifreleme sistemi özel ve kamu anahtarı sistemleridir. Özel anahtarlı bir sistem gönderici ve alıcının ortak bir anahtara sahip olmalarını gerektirir. Şifreli bilginin güvenliği için bu anahtar gizli (özel) tutulmalıdır.



Kamu anahtarı şifre tekniğinde biri metni şifrelemek, diğeri de deşifre etmek için kullanılan anahtar çiftleri bulunur. Şifreleme anahtarı herkesçe bilinir ve mesajını şifrelemek isteyen bu anahtarla şifreler gönderir. Fakat sadece alıcı gizli deşifre anahtarına sahiptir. Bu tip yöntem yönetim problemlerini azalttığı gibi büyük ağlar için de caziptir.

Her iki sistemde de anahtarların seçimi ve korunması (kamu anahtarının bile) sistemin toptan güvenliği için kritiktir.

Her şifreleme sistemi normal metni şifreli metne ve şifreli metni yeniden normal metne dönüştürecek iyi tanımlanmış işlemlere (algoritmalara) ihtiyaç duyarlar. Şifreleme sisteminin gücünün algoritmanın gizliliğine dayandırılmaması kabul görmüş bir şifreleme prensibidir. Bu anlayış algoritmayla ilgili sistemlerin tasarımı ve üretimini gerekli bilgi değişimini mümkün kılar.Ayrıca algoritmanın kritik analizini mümkün kıldığı gibi belgeler ve cihazların fiziki olarak korunması gerekliliğini de ortadan kaldırır.

Çeşitli şifreleme ürünleri (hem özel hem de kamu sistemleri) özel (gizli) şifreleme algoritmaları kullanırlar. Bu algoritmalar genellikle kamu anahtarı kullanan algoritmalardan daha yüksek hızlarda çalışmak üzere tasarlanmışlardır.

Şifreleme algoritmaları hem donanım hem de yazılımla gerçeklenebilir. İlk seçenek elbette daha hızlı ve daha iyi doğrulukla işler.İkinci yaklaşım daha az masraflıdır ve daha esnektir. Bir tek tümleşik devre içerisinde algoritmaların donanım uygulamaları mevcuttur ve bir çok şifreleme ürününde kullanılmaktadırlar. Şifreleme algoritmalarının yazılım versiyonları da mevcuttur.

Gelişen Güvenlik Teknolojisi

Biyometrik tanımlama eşsiz fiziksel özelliklerin veya davranışların analizi temeline dayanan kişisel kimlik belirleme yöntemidir. Biyometrik tanımlamanın geleneksel yöntemi yüz tanımadır, mesela sürücü ehliyeti üzerindeki resmi tanımak gibi. Diğer sık kullanılan tanımlama yöntemleri:

* Yaralar veya diş izi gibi belirleyici vücut yapıları.

* Kardeşçe el sıkışmaları gibi belirleyici hareketler.

* Manyetik kodlu bir kart veya taşınan bir sembol

* Şifreler

* Kişisel tanımlama numaraları

Şifreler ve kişisel tanımlama numaraları geleneksel yöntemlerden daha güvenli koruma teknikleridir. Ama onlarında sınırlamaları vardır:

* Şifreler ve KTN ları sahibinin haberi olmadan çalınabilir.

* Kullanıcı-seçimli şifreler rastgele seçilmediğinden, bulunabilme riski artar.

* Şifre güvenlik sistemleri üstüste rastgele denemelerle bulunabilir (özellikle şifrede kullanılan hane sayısı altıdan azsa)

* Şifreler sıklıkla değiştirilmediğinde iş ortamında bilinir hale gelirler.

Karmaşık bilgisayar ağlarında büyük uzaklıklar arasında mali işlemleri yürütme ihtiyacı daha yüksek güvenlik ve gelişmiş tanımlama tekniklerine özel ihtiyaç duyar. Biyometrik tanımlama teknolojileri pozitif kişisel tanımlama ihtimalini artırmak için geliştirilmişlerdir.

Biyometrik tanımlama yöntemleri biyolojik veya davranışsal teknikler olarak sınıflandırılırlar. Biyometrik teknolojinin ana tipleri:

Biyolojik: El geometrisi, parmak izleri veya retina taraması

Davranışsal : Ses tanımlaması, imza teknikleri, tuş basma dinamikleri

Son zamana kadar biyometrik ürünler yüksek fiyatlardan, uzun cevap verme sürelerinden ve kullanıcıların hoşlanmamasından dolayı pek kabul görmediler.

Biyolojik Teknikler

El geometrisi: Herkesin elinin eşsiz olduğu tespit edilmiştir. Kendi başına ölçülebilen özellikler parmak uzunluğu, deri saydamlığı, el kalınlığı ve avuç içi şeklidir. El geometrisi teknolojisi bu fiziksel boyutları ölçmek ve kaydetmek için özel bir cihaz kullanır.

El geometrisi biyometrik erişim kontrol sistemi olarak uzun süre kullanılmamasının sebebi teknolojisinin pahalılığı ve biyometrik özelliklerin hissedilebilmesi için gerekli sürenin fazlalığıdır. Kullanıcılar bir donanıma veya bilgisayarda depolanan veriye ulaşmak için bu kadar uzun süre beklemeyi istemezler.

Parmak izleri : Parmak izlerinden kimlik tesbiti kanuni çalışmalarda sıkça kullanılmış bir yöntemdir. Parmak izi tanıma donanımlarının hem kul-

lanımı kolaydır hem de diğer biyometrik erişim kontrol sistemlerinden daha ucuzdur. Tanınmak için, kullanıcılar KTN lerini girerler ve parmaklarını cam bir yüzeyin üzerine koyarlar. Camın alt yüzeyinden bir donanım optik olarak parmağı tarar ve görüntüsünü sayısallaştırır. Bir algoritma dosyadaki ile bu şekli karşılaştırır.

Parmak izi tanıma sistemlerinin kullanımında, hassaslıklarından ve izin yanlış okunmasından kaynaklanan muhtemel hataları vardır. Fazla baskı uygulamak, cihaza parmağı yanlış yerleştirmek, parmaktaki aşırı nem veya yağ veya yaralı doku sorun yaratabilir.

Bir çok satıcı parmak izi erişim kontrol sistemleri pazarlamaktadır. Bazı tolerans seviyelerinde kontrol süresi 5 saniyenin altına indirilmiş olduğundan bu teknolojinin yayılması hızlanıştır. Yeni bir parmak izinin kaydı bir dakikadan az sürmektedir. Dahası hatalı reddetme oranı yüksek teknoloji kullanımı ile indirgenmiştir.

Retina Taraması : Tek yumurta ikizleri de dahil olmak üzere herkesin farklı ve değiştirilemez bir retina yapısı vardır. Buna rağmen tanımlamada retina tabakasının kullanımı diğer biyometrik tanıma yöntemlerinden daha pahalıdır.

Kullanıcılar bir merceğe bakarlar ve giriş işlemini başlatmak için bir tuşa basarlar. Bu teknoloji retinayı taramak için kızıl ötesi ışınları kullanır ve yansıyan ışık bilgisini sayısallaştırır. Bilgisayar ilk kaydı daha sonraki erişim isteklerini onaylamak amacıyla kullanır.

Geçmişte göze hasar veren bir teknoloji kullanıldığından bahsedilmekteydi. Fakat satıcılara göre tarama cihazının çok alçak yoğunlukta ışık kaynağı kullanmasından dolayı böyle bir şey söz konusu değildir. Yetkili kimlik kodları dosyası ne kadar uzun olursa arama süresinin o kadar uzamasına rağmen, retina tarama sistemleri KTN ları ile birlikte veya onlarsız kullanılabilir.

Davranışsal Teknikler

Ses tanımlama: Ses tanımlama teknolojisi bir telefon ahizesi veya mikrofon ve KTN tuş cihazını beraber kullanır. Bu sistemler kişinin ilk kayıt yaptırdığı gün alınan ses örneklerini konuşmacının ses kalitesi ile karşılaştırır. Tanımlama işlemi kullanıcı sisteme giriş yapmak istediğinde kendisinin kayıtlarında bulunan kelimelerden rastgele birkaç tanesini söylemesi istenir.

Önceki sistemlerin, sesin ölçülebilecek birçok özelliği olmasından (mesela gülme, nezle veya o andaki halden dolayı değişen) tanımlama için güvenilebilir bir temel oluşturmamasından dolayı hata oranları çok yüksek. Bu problemleri aşmak için, teknolojik gelişmeler sesin, kafa ve boğazın daha az değişken yapıları ile ilgili özelliklerine yüklenmişlerdir. Günlük ses sapmaları da kullanıcının gelişimini güncelleştirmek için kullanılır.

Diğer bir problem de harici sestir. Fakat gelişmiş teknoloji sadece kullanıcının sesini kaydeden çok hassas bir mikrofon kullanarak bu sorunu azaltmıştır.

Bu sistemler çoğunlukla kapı giriş kontrol sistemlerinde kullanılmakla birlikte bilgisayar ve terminal erişim kontrol sistemlerinde de uygulanabilirler. Ses tanımlama, KTN ları ile veya onlarsız kullanılabilir.

İmza Dinamikleri : İmza kontrolu özellikle çek imzalama ve kontrolünde kullanıldığından genellikle bir erişim kontrol metodu olarak kabul görmektedir. Fakat statik imzalar kolaylıkla taklit edilebileceğinden sıkı güvenliğin gerekli olduğu yerlerde tanımlama için kullanışlı değildirler.

İmza dinamikleri, imza atılırken kalem hareketlerinin ölçümü ve elektronik algılayıcılara dayalı yeni bir tekniktir. İmzalar sayısallaştırılır, şifrelenir ve karşılaştırmalar için saklanır. Birçok profesyonel taklitçi kendi davranışsal özelliklerini ortadan kaldırabilmek için imzayı tersten atarlar. Fakat imza dinamikleri incelendiğinde, olaya katılan imzanın parçaları arasında kalemin durma süreleri, ismin belirli yerlerini yazma süreleri ve kalemle uygulanan basınç miktarı gibi refleksif hareketlerin çeşitliliğinden dolayı imzayı taklit etmek zordur.

Geliştirilen ilk sistemlerde hareket algılayıcılarına bağlı bir kalem kullanılamaktaydı. Bu konudaki son teknoloji algılayıcıları kalemde bulundurmak yerine, yazı tabanı üzerinde bulundurur. Böylece sistem daha hassas ve kullanışlı hale gelir.

İmza dinamikleri kontrolu trafiğin yüksek olduğu alanlarda imza atma işleminin çok uzun olmasından dolayı fiziki erişim kontrol yöntemi olarak tavsiye edilmez. Aynı kimselerin gün içerisinde sıklıkla girip çıktığı ortamlarda da verimli değildir. İmza dinamiklerinin tesislerde veya terminallerde uygulanmasının en uygulanabilir olduğu ortam, yüksek güvenlik gerektiren yerlerdir.

Tuş basma dinamikleri: Tuş basımı dinamikleri klavyeyle yazma yapılarını ve ritimlerini tanımlamada kullanan oldukça yeni bir yöntemdir. Bu biyometrik tanımlama yönteminin önemli avantajı ucuz olmasıdır. Tuşa basım dinamikleri testi kullanıcı için saydamdır yani test giriş işleminin doğal bir parçasıdır. Terminallere erişim için çok uygundurlar çünkü ek bir adım gerektirmezler.

Fırtına Kalkanları

Bilgisayar suçu işleyenlerce bilgisayar sistemlerinden yayılan radyo dalgalarını alabilecek özel donanımlar kullanılabilir. Bu yüzden özellikle kritik veya hassas bilgiler için bilgisayar dışına radyo frekans yayılımlarını önleyecek koruyucu kalkanlar (fırtına diye adlandırılan) kullanılabilir. Fırtına kalkanlarının dezavantajı ek maliyettir.

Radyo frekans yayılımlarını önlemenin diğer bir yolu, elastömerlerin kullanılmasıdır. Bu yaklaşım radyo dalgalarını emen elektrik-iletken plastikleri kullanır.

YARARLANILAN/YARARLI KAYNAKLAR

Brandstand, D.; **Standard on Password Usage**, FIPS-Pub-112, March 1985.

____:**Guideline on User Authentication Techniques for Computer Net works Access Control**, FIPS-Pub-83, September 1980.

____: **Guideline on Evaluation of Techniques for Automated Personal Identification**, FIPS-Pub-48, April 1977.

Smid, M.; **Standard on computer Data Authentication**, FIPS-Pub-113, March 1985.

U.S. Department of the Treasury, **Electronic FundsStransfers (EFT)**, Directive Number 16-02, 3. October 1986.

Wood, H.; **The Use of Passwords for Controlled Access to Computer Resources**, NBS Special Pub 500-9, May 1977.