ARAMA TEHLİKELERİNE KARŞI KORUMA: E-POSTA VE BİLGİ İLETİŞİMİ

İçerik:

Telekomünikasyon Gizlilik Politikası, Tailgating, Geri Arama Modemleri, Ana Bilgisayarı Koruma, Satıcı Çözümleri, İnternet Güvenliği, Güvenlik Duvarları, Yedekleme T1'leri.

Göçebe ve ev ofis ortamlarının ortaya çıkmasıyla birlikte, uzaktan erişim güvenliği bir kez daha güvenlik planlama faaliyetlerinde ön planda yer almaktadır. Herkes bir İnternet varlığı ve İnternet erişimi istiyor. Telekomünikasyon popülerliği kazanıyor. Dizüstü bilgisayarlar ile donanmış satış acentaları kırsal alanda dolaşıyor.

Göçebe ve ev ofislerinden gündelik erişime sistemlerin açılması çalışanlar, sistemler kritik öneme sahip ve gelir getirici hale gelmeden önce güvenlik prosedürlerinin uygulanmasını gerektirir. Bu makale, çevirmeli ve internet erişim sistemleri ile ilgili ele alınması gereken hususlara genel bir bakış sunmaktadır. Günümüzün mobil veri dünyasına yönelik hem fiziksel donanım hem de gizlilik politikaları için standartların nasıl sağlanacağına dair ipuçları da dahil edilmiştir.

TELEKOMÜNİKASYON GİZLİLİK POLİTİKASI

Başka birinin gizli e-postasını okursanız ne olur? Şirket seninkini okuyabilir mi? Bir çalışanın özel gizlilik hakkı var mı? Birçok kişi ve şirketin nasıl cevap vereceği konusunda hiçbir fikri yoktur.

Daha fazla işçi E-posta ve veri iletişimi kullandıkça, güvenliğin önemi artmakta ve sistemler gelir elde etmek için kullanılmadan önce sağlam bir şekilde kurulmalıdır. Sağlam bir telekomünikasyon gizlilik politikasından başlayarak, kuruluşlar çağrı sistemleri, geri arama modemleri ve kapsamlı satış sonrası ekipmanlardan güvenlik duvarlarını test etmek, tamamen gereksiz yapılandırmalar ve yedek T1'lere kadar çeşitli koruyucu önlemler almalıdırlar.

E-posta için benzer korumalar var mı? Genel olarak, bir şirketin E-posta gizliliği konusundaki çalışan politikası, genellikle bir telekomünikasyon gizliliği belgesinde, standardı belirler. Ne yazık ki, birçok kuruluşun böyle bir belgesi yok.

Her zaman, makaledeki bir hikaye, e-postaların savunmasızlığının uzmanlar tarafından binlerce kelimeden daha iyi olduğunu vurgulamaktadır.

Büyük bir çalışanın iki çalışanı arasında bir ofis romantizmi yaşanıyordu. Şirket, günlük işlerin yürütülmesinde büyük ölçüde elektronik postaya bağlı kaldı ve çalışanların bu E-postanın güvenli olduğuna inanmak için her türlü nedeni vardı. Genç bayan, görünüşte talihine fotoğraflı bir grafik e-posta mektubu göndermenin romantik olacağını düşündü. Mesajı gönderirken “Tüm Kullanıcılar” düğmesini tıklamamış olsaydı bu iyi olurdu. Bunun iyi bir dedikodu için yapıldığını ve herkese E-posta sistemlerinin kullanımı hakkında net bir mesaj gönderdiğini söylemek yeterlidir.

Bu tür insan hatalarına rağmen, E-posta sistemleri gerçekten güvenli mi? Bir işveren e-posta okuyabilir mi? Çalışanların mahremiyet hakkı var mı? Madde 5-04-41, faks iletimi gibi diğer iletişim biçimlerini tartıştı. Bir kişi başka birine yönelik bir faks veya e-posta alıp okuduğunda yasaları çiğniyor mu? Cevaplar sizi şaşırtabilir ve bu sistemler için güvenlik prosedürlerinin kapsamlı bir incelemesini isteyebilir.

Telekomünikasyon mahremiyetine ilişkin bir politika, sadece e-postaları değil, sesli postaları ve diğer ortamları kapsamalıdır. Politikalar genellikle yelpazenin aşağıdaki iki ucu arasında yer alır:

Bir kez daha, bu politikaları yazarken hukuk danışmanına başvurmak akıllıca olacaktır. Seçeneklerin çeşitliliğini göstermek için bu örneklerde bilerek rahat davrandım, ancak aynı zamanda hukuk danışmanına başvurulmaması risklere maruz kalan kuruluşları bırakabilir. Buna bir örnek, bir şirket sisteminden yasadışı bir bahisçilik operasyonu yürüten bir çalışandır. Kovuldu ama sonra işten çıkarıldı, çünkü şirketin işten çıkarmayı esas alacak mahremiyet politikası yoktu. Daha fazla bilgi için kurumsal hukuk departmanına, danışman dışına veya iç denetim bölümüne başvurmanız önemlidir. Gizlilik politikasının oluşturulmasına ek olarak, çevirmeli hatlar için koruyucu önlemlerin değerlendirilmesi, tehlikelerine genel bir bakışla başlamalıdır. Önerilen herhangi bir çözüm, asgari koruma seviyesini bile sağlayacaksa, aşağıdaki bölümlerde açıklanan izinsiz giriş türlerini ele almalıdır.

BİLGİSAYAR KORSANLARI

Bilgisayar korsanları, çoğu kez sistemi kırmaya çalışan, yetkisiz kullanıcılardır.

Bunlar ölümcül olabilir veya olmayabilir, ancak bazı temel önlemler bu ihlalleri önleyebilir. Bu kişiler sıklıkla modem hatlarını bulmak için her numarayı önek olarak çeviren iblis çeviricileri kullandıkları için (örneğin, 555-0000, 555-0001, vb.), Özellikle numaralar ise, sayıları bulmak zor değildir.Bunlar şunları içerir:

• Kullanıcıyı geri arayan modemler.

• Arayan tarafın CALLER Kimliğini görüntüleyen modemler.

• Başlangıçta sessizlikle cevap veren modemler veya donanımlar yerine bir modem tonu ile.

• “Hoş Geldiniz” gibi bir başlangıç ekranını boyamayan ekipman yetkilendirilmemiş bir kullanıcıyı daha fazla teşvik etmek için hizmet verebilecek olan ABC Widget Şirketi.

• Başarısız oturum açma girişimlerini kaydeden ve izleyen ekipman.

• Erişime izin vermek için özel bir donanım anahtarı gerektiren ekipman.

Bu yöntemler yetkisiz erişime karşı neredeyse olanaksız bir savunma sağlayabilir.

Sabotajcı

En rahatsız edici saldırı türleri, çevre hakkında bilgi sahibi olanlardan gelir. Mesela hoşnutsuz çalışanlar, diğerlerinden daha fazla hasara neden olabilir, çünkü en çok hangi saldırının en fazla zarar verebileceğini biliyorlar. Birçok kuruluş yüksek düzeyde çalışan güvenine sahiptir ve çalışanların yüksek derecede sisteme erişimine izin verme politikasına sahiptir. Bu övgüye değer, ancak özen gösterilmesi gerekiyor, çünkü en sıkı sıkıya bağlı firmalar bile bir çalışanın kişisel bir yakınlık nedeniyle kritik bir sistemi ne zaman tahrip edeceğinden asla emin olamıyor. Önerilen asgari önlemler şunları içerir:

• Bir çalışanın giriş yapmasını engellemek için basit bir işlem şirketi terk eder.

• Herhangi bir çalışan sonlandırıldığında oturum açma erişimini engellemek için zorunlu bir süreç.

TAILGATING

Tailgating, bir sisteme erişmek için kullanılan eski bir çağrıdır. Bu böyle devam ediyor:

1. Bir süper kullanıcı veya sistem yöneticisi uzak bir sisteme arar.

2. Hacker numarayı çevirir (bir iblis çeviriciden elde edilir) ve yoğun bir sinyal alır.

3. Hacker 0'ı arar ve yerel telefon operatöründen hattı doğrulamasını ister.

4. Operatör, genel olarak yetkilendirilmiş hattan düşen hattı keser. Süper kullanıcı

5. Bu sırada bilgisayar korsanı aynı anda başka bir hatta arama yapıyor. Mükemmel bir şekilde zamanlanmışsa, modem taşıyıcı damlasını geçici bir çizgi vuruşu olarak görür ve korsanın modemiyle oturumu yeniden kurar.

6. Hacker süper kullanıcı erişimi ile çevrimiçi; sırayla süper kullanıcı çoğu zaman onun düşürüldüğünü bile bilmiyor. Sistemin sadece kilitlendiğini düşünüyor.

7. Hızlı bir şekilde çalışan hacker, şifre dosyalarını alır ve süper kullanıcı bir şeyin yolunda gitmediğini fark etmeden önce, bir sonraki denemesi için sistemi tehlikeye atar. Güvenlik günlükleri kontrol edildiğinde, oturumu asla sonlandırılmadığı için yalnızca süper kullanıcı günlüğe kaydedilir.

Zekice zekice mi? Aslında, diğer bazılarına göre

hileler, bu ilkedir. Uygulanan ek güvenlik önlemlerinin kurumsal varlıklar için daha fazla iç huzur ve koruma sağladığının altını çizer. Unutmayın, güvenlik düzinelerce veya yüzlerce çalışanın kamuya açık telefon şebekesi üzerinden kritik sistemlere erişmesi büyük bir sorundur. Dikkatli planlama daha sonra büyük zorlukları önleyebilir.

ÖNLEYİCİ TEDBİRLER

Gelen Çağrı Muhasebe Sistemleri

Önerilen her bir çözüm, çevirmeli erişimin bir kağıt izi yapmak için yapılan tüm arama girişimlerinin bir muhasebe kaydını sağlamalıdır. Bu bilgilerin taranması, raporlanması ve sunumundaki güç, herhangi bir koruyucu sistemde ana seçim kriteri olmalıdır. Bir gece 350 başarısız oturum açma girişimi gösteren bir sistem açık bir sinyal gönderiyor.

Çağrı Sistemleri:

Yüksek düzeyde güvenlik gerektiren bazı sistemler otomatik çağrı bildirimi sağlar. Bir kullanıcı oturum açtığında, bir sistem yöneticisinin çağrı cihazı kapanır. Bunlar, başka türlü hesaba katılmayan gizemli giriş denemelerini bildirme prosedürleriyle birleştirilebilir. Sistem yöneticisine anında anormallik bildirildiği göz önüne alındığında çok pahalı değildir.

Donanım Anahtarları:

Donanım anahtarları gibi donanım aygıtları, kritik görev sistemleri için tüm güvenlik önerilerine dahil edilmelidir. Paralel bir bağlantı noktasına takmak gibi kullanım kolaylığı ve düşük maliyet, bu cihazların kullanımında hem öncelikli kriterler olmalıdır. Anahtarlar, genellikle bir dizüstü bilgisayarın paralel bağlantı noktasına takılan bir donanım cihazıdır. Görevli yazılım ile birlikte oldukça kurşun geçirmez bir çözüm sunarlar çünkü bir davetsiz misafir sisteme daha da yaklaşmak için hem şifreleme yazılımına hem de donanım anahtarına sahip olmak zorunda kalır.

Arayan kimliği:

Arayan kimliği birçok şehirde bulunur. Telefon teli merkezlerinde bile mümkün olduğu yerde, sınırlamalar vardır. Arayan Kimliği daha fazlası için kullanışlıdır. Sadece akşam yemeği sırasında can sıkıcı aramaların tanımlanmasından ibaret değil. Uygun şekilde kullanıldığında, yetkisiz kullanıcıları telefon numaralarıyla ve çoğu zaman adlarıyla tanımlayabilir. Daha da güzel olan arayan kimliği, birçok modem ve ISDN (tümleşik hizmetler dijital ağı) terminal adaptörleri için yerleşik bir özelliktir. Numaralar, daha önce açıklanan arama günlüğünün bir parçası olarak arama bazında kaydedilebilir.

Arayan kimliği servisinin pek çok alanda kullanılamaması nedeniyle, bu hizmeti koruyucu sistemin tek temeli olarak kullanan modemler veya diğer donanımlar dikkate alınmayabilir. Arayan kimliği mevcut olsa bile, güvenlik kaygıları var, yani:

• Arayan numara verileri her zaman değişmeli aktarıcılar tarafından aktarılmayabilir. AT&T, MCI ve Sprint gibi. Şirketiniz bir anlamda, bunu geçmeyen taşıyıcıları kullanan uzun mesafe arayanlara karşı savunmasız olacaktır. (Bu, taşıyıcılar mümkün olduğunca arayan kimliği verilerini aktarmak için FCC düzenlemelerine uydukları için hızla değişmektedir.)

• Değişim taşıyıcıları bu verileri iletecek şekilde donatılmış olsalar bile, uzak yerel merkez ofisi olmayabilir. Bir şirket, başka yöntemler kullanılmadığı sürece hala izinsiz kullanıma açık olacaktır.

• Ülkenin bazı bölgelerinde bulunan yerel merkez ofisleri, yerel ya da şehirlerarası aramalar için arayan kimliği değildir.

Geri arama modemleri:

Günümüzde piyasada pek çok geri arama modem bulunmaktadır. Bu cihazlar kullanıcıların oturum açmasını ve ardından gelen arayanı önceden belirlenmiş bir numaradan kapatıp tekrar aramalarını gerektirir. Bunlar oldukça kusursuz, ancak uygunsuz. Bir oteldeki göçebe bir kullanıcının yetkili bir numarası olmayacak ve bir geri arama modem bankasını arayamayacak. Bununla birlikte, potansiyel davetsiz misafirlere özel vurgu ve tarama yaparak bu amaç için özel modem bankaları ve sayıları belirlenebilir.

Ana Bilgisayarı Sabitleme:

Pek çok kullanıcı, çevirmeli ağ için güvenlik seçeneklerinin en iyi ihtimalle marjinal olduğu eski anabilgisayar ortamlarını korumaya çalışırken sıkıştı. IBM, ana bilgisayar için zarif ve basit bir çözüme sahip olmamakla birlikte, protokol dönüştürücüyü bir çevirmeli sunucu ile sonlandırarak ek bir güvenlik düzeyi sağlayabilir. IBM 8235 çevirmeli sunucu, bir adaydır. Gerekli muhasebe, geri arama yeteneği sağlar ve maksimum sekiz port kapasitesiyle gelecekteki herhangi bir büyüme için doğru boyutlandırılmış görünmektedir. Ancak, biraz pahalıdır.

Yazılım Tabanlı Çözümler:

Çevirmeli kullanıcılar için şeffaflık bir sorun olduğu için (farklı bölümler çevirirken genellikle çeşitli yazılım paketleri kullanırlar), çevirmeli yazılım emülasyon paketlerinin toptan değişimini düşünmek istemeyebilirsiniz. Bu, mevcut işletim ortamınız için zararlı olabilir. Mevcut donanım paketini güçlendiren veya geliştiren yazılım alternatifleri en çok tercih edilir, çünkü yeni paketler hakkında eğitim ihtiyacı asgari düzeydedir.

Bunları veya başka bir ürünü değerlendirirken, aşağıdakileri arayın;

Özellikler:

1. Ünite güvenlik cihazı ve modem yöneticisi olarak görev yapmalıdır. Arama yaparken, art arda “cevap yok” diye isabet eden herkes modem havuzu bu özelliği takdir edebilir. Sistemin yapabildiğinden emin olun bu satırları otomatik olarak meşgul et, sonra sizi problemle ilgili uyar.

2. Ünite, modem tarafından cevap süresi bilgisi sağlamalıdır. Telefon hattı ve limana göre. Örneğin, kişisel bir arayüze arayüz gerekir. Etkili performans yönetimi için bilgisayar. Bu, kullanıcılar bağlantı kurmayı bildirmek için aradıklarında bir yardım masasına iyi bir bilgi kaynağı sağlar.

3. Ürün etkili bir yükseltilebilirlik sunmalıdır. Ek güvenlik için, ürünün, kullanıcının paralel bağlantı noktasına arayüz sağlayan token donanım aygıtları sunması gerekir. Yazılım belirteci de mevcut olmalıdır. DOS veya Windows yazılımının her ikisi de desteklenmelidir.

4. Yazılım ve donanım anahtarları. Kullanıcılar için ekipman şeffaflığı genellikle bir sorun olduğu için, uzak kullanıcılar tarafından kullanılan donanımdaki büyük değişiklikleri göz önünde bulundurmamaya çalışın. Bu durum için çok rahatsız edici olabilir. Mevcut çalışma ortamı. Bu bakım ve eğitimde daha sonraya mal olabilir.

İNTERNET GÜVENLİĞİ SORUMLULUKLARI

İzinsiz veri erişim tartışması, İnternet'ten bahsetmeden tamamlanmaz. İnternet, çoğu şirket için, en azından gelir getirici bir sistem olarak nispeten yeni bir fenomendir ve birçok şirket, güvenlik sorumluluklarıyla ilgili çözülmemiş organizasyon sorunlarına sahiptir. İnternet erişimi için kullanılan ekipmanı kim korur? Tarihsel olarak, bu tür işlemler genellikle Orta Kademe bilgisayar hizmetleri gibi İD departmanında özel bir ünitenin altına düşmüştür. Ancak, bugün birçok şirket İnternet güvenlik duvarının ve diğer bileşenlerin fiili olarak işletilmesinden sorumlu ayrı bir teknoloji grubuna sahiptir. İnternet güvenliğinden sorumlu her zaman net bir iş birimi yoktur.

Kimin hangi sistemden ve hangi şartlar altında kimin sorumlu olduğunu belirten net bir politika bulunmamasından dolayı sistemde geçici olarak açık bırakılmalıdır. Bu sorumluluk nihayetinde bir BT güvenlik grubuna (bugünkü LAN ve anabilgisayar hizmetleri gibi) çekecek olsa da, teknoloji “tweaking and tinkering” aşamasındayken, güvenlik açıkları derhal devam edecek.

Başka bir konu personel ve kaynak tahsisidir. Birçok şirket, çok küçük bir uzman havuzu oluşturmamak ve daha iyi bir derinlik sağlamak için insan gücündeki nominal bir artışı düşünmelidir. İnternet erişimi sağlandığı ve olası güvenlik kuşakları veya boşlukları kapatıldığı zaman, organizasyon değişiklikleri okunabilir. Bir şirketin kolayca Internet gurusu olarak tanımlanan bir kişisi varsa, not alın. Bu millet çok rağbet görüyor ve başka iş kabul ettikleri takdirde çantayı tutmanıza izin verebilir. Ayrıca, asılsız ve az çalışan personelin güvenlik ihlallerini araştırmak için çok az zamanları vardır.

Test Güvenlik Duvarı Kurulumu

Çoğu şirket, test ve yedekleme için özel olarak ayrılmış güvenlik duvarı platformuna sahip değildir. Tüm amaç ve amaçlar için, mevcut teknoloji hemen hemen her şekilde tek dişlidir. Bu henüz büyük bir endişe değil, güvenlik duvarı tam olarak çalışmaya başladığında ve sistem gelir getirdiğinde olur.

Ana karelerde ve yerel alan ağlarında olduğu gibi, üretim uygulamalarına doğrudan yeni uygulamalar getirmeyen bir protokol ve prosedür oluşturmak önemlidir. Bu ders 25 yıllık anabilgisayar operasyonları sırasında ortaya çıktı ve hatta en yenilen yerel ağ yöneticileri bile ihtiyatlı bir operasyon müjdesi olarak benimsemeyi öğrendi. Pek çok yeni teknoloji gibi, bu protokoller henüz pek çok firma için İnternet alanında yetişmedi.

Yine sistem tamamen gelir getirici hale geldiğinde. İnternet birçok firma için nispeten yeni bir teknoloji olduğundan, personelin uğraşmaya teşvik edilmesi gerekir. Bir üretim platformunda deneme yapmak akıllıca olmasa da, yedek güvenlik duvarı yapılandırması pratik bir seçenek sağlayabilir. Yedekleme, personeli işletmeyi işletmeyi tehlikeye atmadan denemeye, iyileştirmeye ve iyileştirmeye teşvik ederek daha da haklı çıkarılabilir. Özet olarak, bir yedek güvenlik duvarı özelliğinin ekstra maliyeti, ağın sağladığı esneklik için haklı gösterilebilir ve çünkü temel teknolojistler yeni süreçleri denemeye teşvik edildiğinde eğitim eğrisini kısaltır.

Yedek T1'ler:

Dikkate alınması gereken bir diğer husus, çoğu büyük kullanıcının, bir güvenlik açığı oluşturan İnternet Servis Sağlayıcıya (ISS) yalnızca bir T1 yüklemesidir. Daha akıllıca bir yaklaşım, ISS'ye geniş alan ağı bağlantısında daha fazla esneklik için “Round Robin DNS” ile birlikte ikinci bir T1 eklemeyi düşünmektir. Birçok yerel telefon şirketi de T1 erişimini çeşitlendirmek için tasarlanmış hizmetler sunmaktadır. Güneybatı Bell bölgesinde, hizmete oldukça farklı bir oranda tamamen farklı bir T1 devresi sunan SecureNet ™ adı verilir. CSU'lar ve DSU'lar gibi diğer bileşenler, artıklık olmadan tek dişlidir. Arızalı bileşenlerin hızlı bir şekilde değiştirilebilmelerini sağlamak ve işletmeler üzerindeki etkiyi en aza indirgemek için satıcılarla yedek parça tutulması veya depo düzenlemeleri yapılmalıdır.

İnternet, bir şirketin faaliyetlerinin ayrılmaz bir parçası haline geldikçe (gelir veya diğer geçerli ölçümler üzerindeki etkilerle tanımlandığı gibi), sabit diskler de dahil olmak üzere yedek parçaların depolanması, yedek denetleyici kartları, yedek teyp sürücüleri ve güç kaynakları dikkate alınmalıdır.

Özetle, gelir getirici uygulamalarla aynı seviyede bir sistem sağlamak için şirketler, aynı anda ISP ve “Round Robin DNS” ile ikili bağlantılarla birleştirilmiş 5000 veya 6000 yönlendiriciye (veya eşdeğerine) yükseltmelidir. Yedek parçalar için depo düzenlemeleri yapılmalı, Southwestern Bell SecureNet ve T1 erişimini çeşitlendirmek için diğer yöntemler gibi hizmetler göz önünde bulundurulmalıdır. Bu tür önlemler, hızlı bir şekilde gelir getirici bir sistem haline gelecek olanlara ucuz bir sigorta sağlayacaktır.

TAVSİYE EDİLEN EYLEM KURSU:

Her ne kadar gelir getiren arama sistemleri birçok şirket için çok uzak gibi görünse de, deneyimler bunun gibi sistemlerin yakalanmanın bir yolunu olduğunu göstermektedir. Sigorta şirketleri, dial-in dizüstü bilgisayarlarla fitil talep ayarlayıcıları fikrine bayılıyor. Herkes evde çalışmak istiyor.

Ticaret internette canlanıyor. Bir başarısızlığın bir kuruluşun potansiyel olarak ticari açıdan zayıflatıcı bir sistemin korunmasına ayak uydurmaya çalışmanın reaktif modunda neredeyse kalıcı olması için istifa etmesinden sonra gelir etkisi yaşanmasını beklemek.

Oldukça İyi Gizlilik Kullanarak E-posta Güvenliği

Ödemek

Çoğu kullanıcı, E-posta iletilerinin tamamen herkese açık olduğunu ve başkaları tarafından izlenebileceğinin farkında değildir. Bu makalede, kullanıcıların gizli dinlemeden güvenli ve orijinal oldukları garanti edilen mesajları göndermelerini sağlayan bir E-posta güvenlik paketi olan Pretty Good Privacy açıklanmaktadır.

Giriş

Ticari posta veya kişisel iletişim için elektronik posta kullananlar dikkat etmelidir. Bir ağ üzerinden gönderilen mesajlar gizlice dinlenmeye maruz kalır. Mesajlar bir dosyada saklanırsa, aylarca hatta yıllarca sürebilir. Aynı zamanda kimliğe bürünme tehdidi de vardır ve bir mesajın, olduğunu iddia ettiği partiden gelmeyebilir. Koruma, güçlü, neredeyse kırılmaz ve kullanımı kolay bir paket sağlamak için gizliliği ve dijital imza özelliklerini birleştiren Phil Zimmermann tarafından geliştirilen bir E-posta güvenlik paketi olan Pretty Good Privacy (PGP) şeklinde mevcuttur.

PGP Tanımlı:

Bu E-posta güvenlik programının en önemli özellikleri şunlardır:

· İnsanların gizlice dinlemekten korunan e-posta mesajları göndermesini sağlar. Sadece alıcı alıcı oldukça iyi bir gizlilik mesajı okuyabilir.

· İnsanların orijinal garantili e-posta mesajları göndermelerini sağlar. Alıcının, PGP mesajının, onu yarattığını iddia eden kişi tarafından yaratılması ve mesajı oluşturulduğundan beri hiç kimsenin değiştirmemesi sağlanır.

· İnternette, birçok elektronik bülten panolarında ve CompuServe gibi çoğu ticari hizmette ücretsiz olarak bulunur.

· Disk isletim sistemi, Macintosh, UNIX, Amiga, OS / 2, VMS ve diger isletim sistemleri için versiyonlarda mevcuttur.

· Güvenli e-posta mesajları oluşturmak için herhangi bir e-posta paketi ile çalışır.

E-posta Riskleri:

PGP, gizli dinleme tehlikesinden korunma sağlar. İnternet üzerinden gönderilen bir mesaj bir avuç posta ileticisinden ve düzinelerce paket değiştirme düğümünden geçebilir. Bir sistem yöneticisi veya bu aktarma noktalarından herhangi birine ayrıcalıklı erişim kazanmış biri bu mesajları okuyacak konumdadır.

E-posta kullanıcıları saklayacak bir şeyleri olmadığını düşünmelerine rağmen, bir gün İnternet'i kullanan avukatlarına veya muhasebecilerine danışmak isteyebilirler veya İnternet üzerinden özel bilgi göndermek isteyen şirketler için çalışabilirler. Birçok kişi Internet'i zaten kişisel veya hassas mesajlar göndermek için kullanıyor.

Endişelenecek bir sivil özgürlük sorunu da var. Hükümetin polis, istihbarat ve diğer güvenlik güçleri dijital ve bilgisayarlı e-posta mesajlarını kolayca izleyebilir, anahtar sözcükleri, adları ve değiş tokuş kalıplarını arayabilir. Herhangi bir kullanıcı masum bir şekilde böyle bir ağa yakalanabilir.

Mesajların doğruluğu başka bir potansiyel risk teşkil eder. Şebekenin kimliğe bürünmesini sağlayacak şekilde yanlış bir dönüş adresi içeren bir mesaj göndermeye zorlamak zor değildir. Bir mesajı yolu boyunca yakalamak, içeriği değiştirmek ve ardından yoluna göndermek de oldukça kolaydır.

Örneğin, bir kullanıcı İnternet'e bağlanan UNIX sistemi gibi paylaşılan bir sistemdeyse, taklit eden kişi sistemde “süper kullanıcı” ayrıcalıklarına sahip bir kişi olabilir. Böyle bir kişi, gelen ve giden tüm trafiği şüphesiz posta kutusundan özel bir dosyaya yönlendirebilir. Taklitçi, kullanıcı ve muhabir arasındaki tüm trafiğin geçmesi gereken bir yönlendiriciye, posta köprüsüne veya başka bir ağ geçidine de erişebilir. Bu kimliğe büründürücüler, postaları durdurmak ve sahte bir dönüş adresi içeren postalar göndermek ve göndermek için ağ geçidi üzerindeki ayrıcalıklı durumlarını kullanabilir.

PGP'nin Tarihçesi: Gizlilikle İlgili Sorun

PGP, sıradan vatandaşlar tarafından meşru sebeplerden dolayı kullanılabilecek meşru bir araçtır, ancak bazı kullanıcılar biraz şüpheli olduğunu düşünür.

Phil Zimmerman 1980'lerde Pretty Good Privacy üzerinde çalışmaya başladı ve 1991'de ilk versiyonunu yayınladı. PGP'nin gelişmesi için en önemli motive edici faktörlerden biri FBI'nın belirli güvenlik algoritmalarını ve kuvvetlerini yasaklayacak bir yasanın geçişini güvence altına alma çabasıydı. bilgisayar üreticileri, devlet kurumları tarafından atlanabilecek e-posta güvenlik özelliklerini uygulamak için. Zimmerman bunu gizlilik ve özgürlük için bir tehdit olarak gördü. Bu nedenle PGP, e-posta gizliliğini ve özgünlüğünü sağlamak için ortalama bir kişi tarafından küçük bir sistemde kullanılabilecek bir paket olarak tasarlandı.

· Bu algoritmaları, işletim sisteminden ve işlemciden bağımsız ve küçük, kullanımı kolay komutlar kümesine dayanan genel amaçlı bir uygulamaya entegre etmek.

· Kaynak kodu da dahil olmak üzere paketi ve belgelerini ücretsiz ve yaygın olarak kullanılabilir hale getirmek.

PGP şifreleme algoritması kullandığı için ihracat kontrollerine tabi tutulmuştur. Bir şifreleme algoritması, kullanıcıların bir mesajı yalnızca amaçlanan alıcının şifresini çözmesine izin verecek şekilde karıştırmasını sağlar.

Şifreleme algoritmaları ABD hükümeti tarafından silahlanma sınıfı olarak sınıflandırılmakta ve Uluslararası Silahlanma Yönetmeliği (ITAR) kapsamına girmektedir. ITAR, kullanıcıların silahları ihraç etmek için Dışişleri Bakanlığı'ndan ihracat lisansı almalarını gerektirir. Uygulamada

Dışişleri Bakanlığı, güçlü şifreleme algoritmaları için bu tür bir lisans vermeyecek ve PGP en güçlerinden ikisini kullanmaktadır.

ABD’de PGP kullanımına karşı bir yasa bulunmadığından, bu sorunun ortalama bir kullanıcıyı ilgilendirmesine gerek yoktur. Ayrıca ABD dışında yasa dışı bir şekilde ihraç edilen bir ürünün kullanımını önlemek için ABD dışında bir kanun yoktur. Ayrıca, PGP'nin daha yeni sürümlerinden bazıları aslında ABD dışından kaynaklanmış ve problemi tamamen ortadan kaldırmıştır.

İkinci bir problemin patentlerle ilgisi var. PGP'deki iki şifreleme algoritmasından biri Rivest-Shamir-Adleman (RSA) olarak bilinir. ABD’de PGP kullanan herkes, bir süre için, potansiyel olarak Rivest\_Shamir-Adleman patent ihlali için dava açacaktı.

Geleneksel Şifreleme:

PGP iki güçlü güvenlik fonksiyonundan yararlanır: geleneksel şifreleme ve açık anahtarlı şifreleme. Geleneksel şifreleme, eski Roma’ya ve daha da eskilere dayanan gizli kodlara verilen klasik yaklaşımdır. Geleneksel bir şifreleme şeması (bkz. Ek 1) aşağıdaki beş bileşeni içermektedir:

· Düz metin. Bu, algoritmaya girdi olarak beslenen okunabilir mesaj veya veridir.

· Şifreleme algoritması. Şifreleme algoritması, düz metin üzerinde çeşitli ikameler ve dönüşümler gerçekleştirir.

· Gizli anahtar. Gizli anahtar ayrıca algoritmaya girdidir. Algoritma tarafından gerçekleştirilen tam ikameler ve dönüşümler anahtara bağlıdır.

· Şifreli Metin. Bu çıktı olarak üretilen şifreli mesajdır. Bu, düz metne ve gizli anahtara bağlıdır.

· Şifre çözme algoritması. Bu aslında şifreleme algoritmalarının tersine çalışmasıdır. Şifreyi ve aynı gizli anahtarı alır ve orijinal düz metni oluşturur.

Geleneksel Şifreleme

Julius Caesar tarafından kullanılan Sezar şifresi, basit bir şifreleme örneğidir. Sezar şifresi, alfabenin her harfini, alfabenin altında üç basamakta duran harfle değiştirir.

Alfabe, Z'yi takip eden harf A olacak şekilde etrafına sarılır. Şifre çözme algoritması, sadece şifreli metni alır ve her harfin, alfabenin önceki bölümlerinde yer aldığı harfle değiştirir. Genel bir Sezar şifresi, k'nin 1'den 25'e kadar değiştiği k harflerinin kaymasını içerir. Bu durumda, k, algoritmanın gizli anahtarıdır. Sezar şifresi çok güvenli değil. Kodu deşifre etmek isteyen herkes, 1'den 25'e kadar olan her olası geçişi deneyebilir. Pretty Good Privacy, Uluslararası Veri Şifreleme Algoritması veya Etkileşimli Veri Çıkarma ve Analizi olarak bilinen çok daha güçlü bir algoritma kullanır.

Uluslararası Veri Şifreleme Algoritması

IDEA, 1990 yılında İsviçre Federal Teknoloji Enstitüsü'nden Xuejia Lai ve James Massey tarafından geliştirilen blok odaklı geleneksel şifreleme algoritmalarıdır. IDEA şifrelemesi için genel şema Ek 2'de gösterilmektedir. IDEA, 64 bitlik bloklardaki verileri şifrelemek için 128 bitlik bir anahtar kullanır.

Genel FİKİR Yapısı

DEA algoritması, son bir dönüşüm fonksiyonunu takip eden sekiz tur veya yinelemeden oluşur. Algoritma, girişi dört adet 16 bitlik alt bloklara böler. Her yineleme turu, giriş olarak dört adet 16 bitlik alt blok alır ve dört adet 16 bitlik çıkış bloğu üretir. Son dönüşüm ayrıca 64 bit şifreleme metnini oluşturmak üzere birleştirilmiş dört adet 16 bit blok üretir. Her yinelemede altı adet 16 bitlik alt anahtar kullanılır, oysa son dönüşümde toplamda 52 adet alt anahtar için dört adet alt anahtar kullanılır. Serginin sağ tarafı, bu 52 alt anahtarın hepsinin orijinal 128 bit anahtarından üretildiğini gösterir.

Her IDEA yinelemesi, üç farklı matematiksel işlem kullanır. Her işlem, tek bir 16 bit çıktı üretmek için iki 16 bit giriş üzerinde gerçekleştirilir.

Aynı zamanda birbirleriyle uyuşmuyorlar çünkü üç operasyondan hiçbiri ortak bir kanunu yerine getirmiyor. Örneğin:

Bu üç ayrı işlemin bir arada kullanılması, kriptanalizi çok zorlaştıran girdilerin karmaşık bir dönüşümünü sağlar. Sergi 3, tek bir yineleme için algoritmayı göstermektedir. Aslında, bu sergi ilk yinelemeyi göstermektedir. Daha sonraki yineleme işlemleri aynı yapıya sahiptir, ancak farklı alt anahtar ve düz metin türevli giriş ile. Yineleme, birleştiren bir dönüşümle başlar.

Tek IDEA İterasyonu (İlk İterasyon):

Son olarak, üst dönüşümden dört çıkış bloğu, bu yineleme için dört çıkış bloğunu üretmek üzere XOR kullanarak MA yapısının iki çıkış bloğuyla birleştirilir. İkinci ve üçüncü girişler (X2 ve X3) tarafından kısmen üretilen iki çıkış, ikinci ve üçüncü çıkışların (W12 ve W13) üretilmesi için değiştirilir, böylece işlenen bitlerin karışımını arttırır ve algoritmayı kriptanalize karşı daha dirençli hale getirir. Algoritmanın dokuzuncu aşaması, Ek 2'deki çıktı dönüşüm aşamasını etiketledi.

Tek fark, ikinci ve üçüncü girişlerin operasyonel birimlere uygulanmadan önce birbirleriyle değiştirilmeleridir. Bu, sekizinci yinelemenin sonunda değişimin geri alınması etkisine sahiptir. Bu ekstra değişim, şifre çözme işleminin şifreleme ile aynı yapıya sahip olması için yapılır. Bu dokuzuncu aşama, ilk sekiz aşamadan her biri için altı alt tuş girişi ile karşılaştırıldığında yalnızca dört alt anahtar girişi gerektirir. Her yineleme için alt anahtarlar, orijinal 128 bit anahtarındaki bir dizi vardiya tarafından üretilir. IDEA, eski geleneksel şifreleme tekniklerine göre avantajlara sahiptir. 128 bit anahtar uzunluğu, kaba kuvvet anahtar arama saldırılarına karşı dayanıklı olmasını sağlar. FİKİR de çok yüksek kriptanalize karşı dayanıklıdır ve hem yazılım hem de donanım uygulamalarını kolaylaştırmak için tasarlanmıştır.

Genel-Anahtar Şifreleme:

Etkileşimli Veri Çıkarma ve Analizin temel özelliklerinden biri ve tüm geleneksel şifreleme algoritmaları, iki tarafın kimsenin bilmediği bir gizli anahtarı paylaşma ihtiyacıdır. Bu, özellikle bir e-posta uygulaması için çok büyük bir sınırlamadır.

Oldukça İyi Gizlilik yalnızca IDEA'nın kullanımına bağlı olsaydı, bir kullanıcı herhangi biriyle temasa geçmeden önce, o kullanıcı bir şekilde mesaj alıcısıyla gizli bir 128-bitlik sayıyı paylaşmak zorunda kalacaktı. Güvenli iletişim kurmanın bir yolu yoksa, anahtarı göndermek zorlaşır. Genel anahtar şifreleme olarak bilinen şifrelemeye yeni bir yaklaşım bu soruna bir çözüm sunar. 1976 yılında Whitfield Diffie tarafından geliştirilen bu yöntemle, bir gizli anahtar iletmeye gerek yoktur. Bunun yerine, her bireyin özel bir anahtarı ve eşleşen bir ortak anahtarı vardır. Şifreleme bu iki anahtardan biriyle yapılır ve şifre çözme diğerini kullanır. Özel anahtar, sadece sahibinin bildiği gizli tutulur. Eşleşen ortak anahtar, sadece budur - genel. Özel anahtar sahibi, eşleşen ortak anahtarı yayınlayabilir. Açık anahtarlı şifreleme, gizliliği sağlamak için aynı şekilde kullanılabilir

Kullanıcılar şifreleme algoritmalarına düz metin ve hedeflenen alıcının genel anahtarını koyarlar. Algoritma şifreli metin üretmek için düz metin ve genel anahtarı kullanır. Alıcı uçta, şifreleme algoritmalarının tersi olan şifre çözme algoritması kullanılır. Bu durumda, giriş şifreli metin ve alıcının özel anahtarıdır. Bu mesaj gizlice dinlemekten korunmaktadır, çünkü yalnızca alıcı şifre çözme için gerekli özel anahtara sahiptir. Alıcının genel anahtarının bir kopyasına sahip olan herkes sadece bu alıcı tarafından okunabilecek bir mesaj oluşturabilir.

Kimlik doğrulama, şifreleme algoritmalarına düz metin ve gönderenin özel anahtarını koyarak da yapılabilir. Algoritma, şifreli metin üretmek için düz metni ve özel anahtarı kullanır. Alma sonunda, kodun tersi olan şifre çözme algoritması

RSA Algoritması

İlk anahtar programlardan biri 1977'de MIT'de Ron Rivest, Adi Shamir ve Len Adleman tarafından geliştirildi ve ilk olarak 1978'de yayınlandı. Yaratıcıları için adlandırılan Rivest-Shamir-Adleman (RSA) programı o zamandan beri hüküm sürdü. yalnızca açık anahtarlı şifrelemeye yaygın olarak kabul edilen ve uygulanan bir yaklaşım. RSA, düz metin ve şifreli metnin bazı n'ler için 0 ile n - 1 arasında tam sayı olduğu bir blok şifredir. Şifreleme ve şifre çözme, bazı düz metin blok M ve şifreli metin blok C için aşağıdaki formu alır:

C = M*e* mod *n*

M = C*d* mod *n* = (M*e*)*d* mod *n* = M*ed* mod *n*

Hem gönderenin hem de alıcının n değerini bilmesi gerekir. Gönderen e'nin değerini bilir ve yalnızca alıcı d'nin değerini bilir. Dolayısıyla, bu, KU = {e, n} genel anahtarına ve KR = {d, n} özel anahtarına sahip genel anahtar şifreleme algoritmalarıdır. Bu algoritmanın ortak anahtar şifrelemesi için tatmin edici olması için aşağıdaki şartların yerine getirilmesi gerekir:

Ek 5, RSA algoritmasını özetlemektedir. Algoritmayı anlamak için kullanıcılar, iki asal sayıyı, p ve q seçerek ve şifreleme ve şifre çözme için modül olan n ürünlerini hesaplayarak başlamalıdır. Daha sonra, n'nin Euler totienti olarak adlandırılan, n'den daha az pozitif tamsayıların sayısı olan ve n'nin nispeten asal olan miktarları (n) belirlenmelidir. Daha sonra, f (n) 'nin göreceli olarak asal olan bir tamsayı d (yani, d ve f (n)' nin en büyük ortak böleni 1'dir) seçilmelidir. Son olarak, d, modulo f (n) 'nin çarpımsal tersi olarak hesaplanmalıdır. D ve e'nin istenen özelliklere sahip olduğu gösterilebilir.

· İki asal sayı, p = 7 ve q = 17 seçili.

· Hesapla n = pq = 7 x 17 = 119.

Kodu Kırmak Ne Kadar Zor?

RSA algoritmasını yenmek için iki olası yaklaşım vardır. Bunlardan ilki, bruteforce yaklaşımı: tüm olası özel anahtarları denemek. Böylece d ve d'deki bit sayısı arttıkça, algoritma daha güvenli olur. Bununla birlikte, hem anahtar üretme hem de şifreleme / şifre çözme işlemlerinde yer alan hesaplamalar karmaşık olduğundan, anahtarın boyutu ne kadar büyükse, sistem o kadar yavaş çalışacaktır.

RSA'nın kriptanaliziyle ilgili tartışmaların çoğu, iki ana faktör olarak p'yi faktoring görevine odaklanmıştır. Yakın zamana kadar bu, yaklaşık 300 veya daha fazla bit olan 100 ondalık basamak aralığında sayılar için olanaksızdı. Üç geliştiricisi olan Rivest-Shamir-Adleman’ın gücünü göstermek için, 129 ondalık basamaklı bir sayıyı kamu modülü olarak kullanarak şifrelenmiş bir mesajın şifresini çözme mücadelesi verdi. Yazarlar mevcut teknoloji ile kodu kırmanın 40 katrilyon yıl alacağını tahmin ediyorlardı. Son zamanlarda, İnternet üzerinden işbirliği yapan ve yalnızca sekiz aylık çalışmadan sonra 1.600'den fazla bilgisayarı kullanan dünya çapında bir ekip tarafından kod kırıldı. Bu sonuç, RSA kullanımını geçersiz kılmaz; bu sadece daha büyük anahtar boyutlarının kullanılması gerektiği anlamına gelir. Şu anda, 1.024 bitlik bir anahtar boyutu (yaklaşık 300 ondalık basamak), hemen hemen tüm uygulamalar için yeterince güçlü olarak kabul edilir.

PGP Nasıl Çalışır?

Rivest-Shamir-Adleman, güvenli bir E-posta tesisi için gerekli olan tek şey gibi görünebilir. Pretty Good Privacy kullanmak isteyen herkes eşleşen bir anahtar çifti oluşturabilir (PGP gerekli hesaplamayı yapar) ve sonra genel anahtarı dağıtabilir. Bir mesaj göndermek için, önce gerçekliğini garanti altına almak için önce özel anahtarla şifrelenmiş olması gerekir. Daha sonra, hiç kimsenin mesajı okuyamayacağından emin olmak için birinci adımın sonucunun alıcının genel anahtarı ile şifrelenmesi gerekir.

Bu şema teknik olarak geçerlidir ancak pratik değildir. Sorun, RSA'nın ve diğer tüm ortak anahtar programlarının çok yavaş olmasıdır. Keyfi uzunlukta mesajları şifrelemek çift için çok fazla zaman alıyor. Kullanıcılar, PC'lerinin sayıları arttırmalarını beklerken dakika ve hatta saat gecikmeleri yaşayabilirler.

Bunun yerine, PGP geleneksel ve açık anahtarlı şifrelemenin güçlü yanlarından yararlanır. Bir mesaj gönderildiğinde, güvenlikle ilgili iki işlem aşamasından geçer: dijital imza ve şifreleme.

Dijital imza, açık anahtarlı şifreleme çalışmalarından çıkan en akıllı yeniliklerden biridir. Dijital imza kullanmak için kullanıcılar, 128 bitlik sabit uzunlukta bir kodla göndermek ve eşlemek istedikleri mesajını alır. Bunu yapmak için algoritma denir

MD5 (mesaj özeti sürüm 5). 128 bitlik mesaj özeti bu mesaj için benzersizdir. Birisinin bu mesajı değiştirmesi ya da başka bir mesajı değiştirmesi ve hala aynı özeti bulması neredeyse imkansız olurdu.

PGP daha sonra RSA'yı ve gönderenin özel anahtarını kullanarak özeti şifreler. Sonuç, mesaja eklenen dijital imzadır. Bu mesajı alan herkes mesaj özetini yeniden hesaplayabilir ve RSA'yı ve gönderenin ortak anahtarını kullanarak imzanın şifresini çözebilir. İmzadaki mesaj özeti, hesaplanan mesaj özeti ile eşleşiyorsa, imza geçerlidir. Bu işlem yalnızca 128 bit bloğun şifrelenmesini ve şifresini çözmeyi gerektirdiğinden, çok az zaman alır.

Şifreleme aşaması için, PGP rastgele 128-bit bir gizli anahtar oluşturur ve mesajı ve ekli imzayı şifrelemek için Etkileşimli Veri Çıkarma ve Analiz'i kullanır. Alıcı, RSA'yı kullanarak gizli anahtarı bulabilir. PGP, alıcının genel anahtarını kullanarak gizli anahtarı RSA'ya girdi olarak alır ve mesaja eklenmiş şifreli bir gizli anahtar üretir. Alıcı tarafta, PGP gizli anahtarı kurtarmak için alıcının özel anahtarını kullanır ve ardından düz metin mesajı artı imzasını kurtarmak için gizli anahtarı ve IDEA'yı kullanır.

Genel Anahtarları Alma

Genel anahtar şifreleme teknikleri, her kullanıcı için iki anahtar kullanır: yalnızca bir kullanıcı tarafından bilinen özel bir anahtar ve tüm kullanıcılar tarafından bilinen bir ortak anahtar. Bu iki anahtarla, orijinalliği garanti eden dijital imzalar oluşturmak mümkündür.

Bir mesajın ve bir mesajın yalnızca amaçlanan alıcının okuyabileceği şekilde şifrelenmesini desteklemek.

Bununla birlikte, her kullanıcının sadece özel anahtarını gizli tuttuğu ve ilgili ortak anahtarı yayınladığı konusunda yaygın bir yanılgı vardır. Ne yazık ki, bu basit bir çözüm değil. Bir sahtekâr, bir kamu ve özel anahtar çifti oluşturabilir ve genel anahtarı başka birinin sanki yayabilir. Örneğin, A kullanıcısının B kullanıcısına güvenli bir mesaj göndermek istediğini varsayalım.

Bu sorunun üstesinden gelmenin bir yolu, kamu anahtarlarının güvenli bir şekilde değiştirilmesinde ısrar etmektir. Örneğin, B kullanıcısı ve A kullanıcısı birbirlerini kişisel olarak tanıyorlarsa ve yan yana yaşıyorlarsa, disketlerdeki anahtarları fiziksel olarak değiştirebilirler. Ancak PGP'nin genel amaçlı bir E-posta güvenlik aracı olarak yararlı olması için, yaygın olarak dağıtılmış sitelerdeki kişilerin, daha önce tanışmadıkları ve hatta tanımadıkları başkalarıyla anahtar alışverişinde bulunmaları mümkün olmalıdır.

Açık Anahtar Sertifikaları ve Dağıtılmış Güvenlik

PGP'nin yaygın şekilde kullanılmasına izin veren temel araç ortak anahtar sertifikasıdır.

ortak anahtar sertifikasının temel unsurları şunlardır:

· Anahtar sahibinin adı ve e-posta adresini içeren bir kullanıcı kimliği.

· Genel anahtar ve kullanıcı kimliği için bir veya daha fazla dijital imza.

Bilgi İşlem Güveni

Oldukça İyi Gizlilik, sertifikalandırma makamlarını oluşturmak veya güven oluşturmak için herhangi bir şartname içermemesine rağmen, güven kullanmanın, güven ile ortak anahtarların ilişkilendirilmesinin ve güven bilgilerinin kullanılması için uygun bir yol sağlar.

Her kullanıcı bir dizi imzalı anahtar toplayabilir ve ortak anahtar halkası olarak bilinen bir PGP dosyasında saklayabilir. Her girişle ilişkilendirilmiş, PGP'nin bu kullanıcı için geçerli bir ortak anahtar olduğuna ne kadar güveneceğini belirten anahtar bir meşruiyet alanıdır; güven seviyesi ne kadar yüksek olursa, bu kullanıcı kimliğinin bu anahtara bağlanması o kadar güçlü olur. Bu alan Pretty Good Privacy tarafından hesaplanmıştır. Ayrıca girişle ilişkilendirilmiş, anahtarlık sahibinin bu sertifikayı imzalayan topladığı top sıfır veya daha fazla imza. Sırasıyla, her imza onunla, bu PGP kullanıcısının imzalayanları ortak anahtarların sertifikalandırılması için ne kadar güvendiğini belirten bir imza güven alanıyla ilişkilendirmiştir. Kilit meşruiyet alanı, girişteki imza güven alanlarının toplanmasından türetilir. Son olarak, her giriş belirli bir sahiple ilişkilendirilmiş bir ortak anahtar tanımlar ve bu ortak anahtarın diğer ortak anahtar sertifikalarını imzalamak için ne kadar güvenileceğini belirten bir sahip güven alanı bulunur; Bu güven seviyesi kullanıcı tarafından belirlenir. İmza güven alanları, başka bir girişten sahip güven alanının önbellek kopyaları olarak düşünülebilir.

Güven İşleme

A kullanıcısı, ortak anahtar halkasına yeni bir ortak anahtar eklerse, PGP'nin bu ortak anahtarın sahibi ile ilişkilendirilmiş olan güven bayrağına bir değer ataması gerekir. Sahibi aslında A ise ve bu ortak anahtar ayrıca özel anahtarlıkta da görünürse, o zaman nihai güven değeri otomatik olarak güven alanına atanır. Aksi takdirde, PGP A kullanıcısından bu anahtarın sahibine verilecek güveni değerlendirmesini ister ve A kullanıcısı istenen seviyeye girmelidir. Kullanıcı bu sahibin bilinmeyen, güvenilmeyen, marjinal olarak güvenilir veya tamamen güvenilir olduğunu belirtebilir.

Yeni ortak anahtar girildiğinde, ona bir veya daha fazla imza eklenebilir. Daha sonra daha fazla imza eklenebilir. Girdiye bir imza eklendiğinde, PGP bu imzanın sahibinin bilinen ortak anahtar sahipleri arasında olup olmadığını görmek için ortak anahtarlıkta arama yapar. Öyleyse, bu sahibin OWNERTRUST değeri, bu imza için SIGTRUST alanına atanır. Aksi takdirde, bilinmeyen bir kullanıcı değeri atanır.

PGP Güven Modeli Örneği

“Siz” etiketli düğüm, bu kullanıcıya karşılık gelen halka açık anahtarlıktaki girişi ifade eder. Bu anahtar geçerlidir ve OWNERTRUST değeri nihai güvendir. Anahtar halkasındaki her diğer düğüm, kullanıcı tarafından başka bir değer atanmamışsa, tanımlanmamış bir OWNERTRUST değerine sahiptir. Bu örnekte, kullanıcı, diğer anahtarları imzalamak için her zaman D, E, F ve L kullanıcılarına güvendiğini belirtti. Bu kullanıcı ayrıca, diğer anahtarları imzalamaları için A ve B kullanıcılarına kısmen güveniyor.

Ek 7'deki düğümlerin gölgelendirilmesi veya olmaması, bu kullanıcı tarafından verilen güven seviyesini gösterir. Ağaç yapısı, hangi anahtarların başka hangi kullanıcılar tarafından imzalandığını gösterir. Bir anahtar aynı zamanda bu anahtarlığa sahip olan bir kullanıcı tarafından imzalanırsa, ok, imzalayan anahtarı imzalayana bağlar. Anahtar, bu anahtarlıkta bulunmayan bir kullanıcı tarafından imzalanırsa, ok, imzalayan anahtarı kullanıcı için bilinmediğini belirten bir soru işaretine bağlar.

Sonuç

PGP zaten yaygın olarak kullanılıyor. Oldukça İyi Gizlilik, eski Komünist ülkelerde özgürlük için mücadele edenler için önemli hale geldi. Dünyadaki sıradan insanlar alt güvenlikten aktif katılımcılardır. PGP USENET haber grubu. PGP yaygın bir ihtiyacı doldurduğu ve makul bir alternatif olmadığı için geleceği güvende. PGP elde etmek için en iyi konum listelerinden biri, getpgp.asc dosya adıyla, Internet'teki iki Dosya Aktarım Protokolü sitesinde bulunur: ftp.csn.net/mpj ve ftp.netcom.com/pub/mp/mpj .

**Kaynakça;**

William Stallings

William Stallings bağımsız bir danışman ve Comp-Comm Consulting’in Başkanı Brewster MA.

<https://www.muhendisbeyinler.net/kriptoloji-ve-sezar-sifreleme-algoritmasi/>

<https://www.google.com/search?q=sezar+algoritmas%C4%B1+%C3%B6rne%C4%9Fi&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiW__LK-a_iAhUC_aQKHedpDJoQ_AUIDigB&biw=1366&bih=657#imgrc=yqb_UT-2uEazBM:>

<http://bilgisayarkavramlari.sadievrenseker.com/2009/06/11/idea-uluslar-arasi-sifreleme-algoritmasi/>

<http://bilgisayarkavramlari.sadievrenseker.com/2008/03/19/rsa/>

<https://www.sanfoundry.com/cpp-program-implement-rsa-algorithm/>

<https://www.google.com/search?biw=1366&bih=608&tbm=isch&sa=1&ei=l8XrXNDVIqHHrgSGsrkQ&q=pgp+&oq=pgp+&gs_l=img.3..35i39l2j0l2j0i30l6.747.747..994...0.0..0.206.206.2-1......0....1..gws-wiz-img.eszA-KbO4sU>