

**Bilgisayar-Bilgi Güvenliği ve Yönetimi/ BM-302**

**Prof.Dr. Abdulsamet HAŞILOĞLU**

**Hazırlayan**

**Fatih ALTIN**

**140757015**

**DIAL-UP SECURITY CONTROLS**

Alan Berman and Jeffrey L. Ott

**İçindekiler**

1. Doğrudan Arama ve Paket Anahtarlama İletimi,
2. Şifreler,
3. Mikrobilgisayar Erişimi,
4. Çevirmeli **/** Geri arama sistemleri
5. Şifreleme İzinsiz Girişi İzleme

**1.SORUNLAR ADRESLİ**

Bilgi sağlama ihtiyacı arttıkça, yetkisiz kullanıcıların çevrimiçi çevirmeli bilgisayar sistemlerine erişme kapasitesi artmıştır. Bu tehdit - ve böyle bir maruz kalmanın doğurduğu sonuçlar -, savunma bakanlığı bilgisayarlarına sızmadan büyük ağlara ya da paylaşılan bilgisayar tesislerine kadar yıkıcı sonuçlar doğurabilir. LAN tabanlı mikrobilgisayarlara duyulan güvenin artması, yalnızca yetkisiz kişilerin değiştirilmesine veya şirket kritik verilerinin silinmesine neden olma tehdidini arttırmaz, aynı zamanda ağ kullanıcılarına virüs bulaştırması olasılığını da arttırır. Dial-in erişimi sağlamak, sadece genel kullanıcı için şebeke veya sistem erişimi ile sınırlı değildir. Sunucular, yönlendiriciler, anahtarlar ve diğer ağ altyapısı aygıtlarındaki bakım bağlantı noktalarına bağlı modemlerde gizlenen daha büyük bir pozlama vardır. Bağlı bir modemi olan herhangi bir bilgi işlem aygıtı, kesilecek bir aygıt arayan biri için potansiyel bir hedeftir. Bakım portlarıyla ilgili problemler şunlardır:

• Bu limanlara çok az dikkat edilir, çünkü satıcı dahil yalnızca bir veya iki kişi kullanır.  
• Cihazdaki düşük düzeyli idari makama anında erişim sağlarlar.  
• Genellikle, hiç değiştirilmeyen varsayılan kullanıcı kimlikleri ve şifreleriyle birlikte verilir.  
• Bir satıcı tarafından kullanılıyorsa, satıcıların tüm makinelerinde aynı kimliği ve şifreyi kullanma alışkanlığı vardır.

Doğrudan ana sistemlere, sunuculara, anahtarlara, yönlendiricilere, PC'lere (hem iç hem de bilgisayar odasındaki), PBX'lere ve CBX'lere doğrudan bağlı modemleri arayın. Telekomünikasyon hizmetleri veren departmanı kontrol edin. Modemlere atanmış telefon numaralarının bir listesi olabilir. Ancak, buna güvenmeyin. En azından analog hatların bir listesini sunabilmeliler. Bunların çoğu faks makinesi olacak, ancak bazıları modem olacak. Son olarak, tüm modemlerin tanımlanmasını sağlamak için, borsadaki telefon numaralarına karşı bir savaşçı çalıştırın. Tehditler çok sayıda ve sonuçta mükemmel olsa da, çok az sayıda kuruluş bu sorunla mücadele etmek için eksiksiz güvenlik programlarına sahiptir. Bu makalede, çevirmeli hizmetlerin güvenliğini sağlamak için atılması gereken adımlar anlatılmaktadır.

**1.1 ARIZA ERİŞİM TÜRLERİ**

Çevirmeli bağlantı özelliği standart bir telefon hattı kullanır. Modemi, veri iletmek ve almak için telefonu kullanmak için gereken arayüz cihazı, bir dijital akışı bir analog sinyale çevirir. Kullanıcının sitesindeki modem, bitlerle kodlanmış bilgisayar verilerini analog sinyale dönüştürür ve bu sinyali bir telefon hattı üzerinden bilgisayar sitesine gönderir. Bilgisayar alanındaki modem, analog sinyali tekrar ikili kodlu verilere çevirir. Bilgisayar sitesinden kullanıcı sitesine veri gönderme prosedürü tersine çevrilmiştir. Çevirmeli bağlantı özelliği, standart telefon şirketi doğrudan arama servisi veya paket anahtarlama şebekeleri aracılığıyla sağlanır.

**1.1.1 Direkt Arama**

Doğrudan arama özelliği olan bir kullanıcı, kaynak cihazı ana bilgisayara bağlayan bir telefon numarasını çevirir. Bilgisayar sitesi, telefon hattını idare etmek için modemleri ve iletişim bağlantı noktalarını tutar. Standart çevirmeli hatlar, özellikle iletim yerel bir arama dışında bir şey içeriyorsa, pahalı olmayabilir. Örneğin, New York’taki bir aracı kurum veya banka hizmetine erişmesi gereken Kaliforniya’daki bir müşteri, günlük veya haftalık erişim ve iki yönlü iletim için yasak olan standart bir telefon şirketi çevirme hattı üzerinden iş yapmanın maliyetini bulur.

**1.1.2 Paket Anahtarlama**

Paket anahtarlama ağları, uzun mesafeli çevirmeli bağlantı servisinin yasaklayıcı telefon maliyetlerine bir çözüm sunar. Örneğin, Kaliforniya kullanıcısı doğrudan çevirmeli ağ sistemine yalnızca aynı tip telefon ve modemi kurmaya ihtiyaç duyar. Kullanıcı, New York alan koduyla bir numara çevirmek yerine, alandaki anahtarlama düğümü ile bağlantı kuran yerel bir telefon numarasını çevirir.

Dahili olarak, paket anahtarlama veri iletimi, doğrudan çevirmeli mesaj iletilmesinden farklı şekilde ele alınır. Doğrudan bir bağlantı oluşturmak ve ana bilgisayara ve bilgisayardan veri akışlarını göndermek ve almak yerine, paket anahtarlama ağları bir düğümde birkaç ileti alır. Mesajlar daha sonra veri paketlerine ayrılır. Her paketin bir boyut sınırlaması vardır ve bu boyutu geçen iletiler birkaç pakete bölünmüştür. Paketler atanan hedefe ulaşılana kadar düğümden ağdaki düğüme geçirilir. Mesajın hedefini belirtmek için kullanıcı atanmış bir kimlik kodu ve bir şifre girer. Girilen kodlar yetkilendirme ile ilişkilendirilir ve adreslenen bilgisayar sitesini belirtir. Kullanıcının amaçları doğrultusunda, ana bilgisayara bağlanma, bir çevirmeli bağlantı hattının kullanılmış olması ile aynıdır, ancak aramanın maliyeti büyük ölçüde azalır.

Hem çevirmeli ağ servisi hem de paket anahtarlama ağlarında, ana bilgisayar bilgisayarda depolanan verilere erişimi korumaktan sorumludur. Paket anahtarlama ağları bir düğüme bağlanmak için bir kullanıcı kimliği ve bir parola gerektirdiğinden, ek bir güvenlik önlemi sağladıkları görülüyor; ancak, bu her zaman böyle değildir ve bu, paket anahtarlama ağ satıcısına güvenlik sorumluluğunu iptal etmek için bir neden olmamalıdır.

Bir süredir, belirli satıcının paket anahtarlama ağ tesislerinin kullanıcıları, kullanıcı kimliğini ve şifre kontrolünü atlamanın mümkün olduğunu biliyorlar. Çok az deney yapıldığında, Amerika Birleşik Devletleri ve Kanada'daki çeşitli çevirmeli bilgisayar sitelerine herkesin erişebileceği keşfedildi, çünkü bu bilgisayar sitesi iletişim portlarının alan kodları ilgili telefon şebekesi alan kodlarının üç hanesiyle ön yüze yerleştirilir. . Bilgisayar adresinin geri kalanı üç sayısal karakter ve bir alfanümerik karakterden oluşur. Bu nedenle, alan kodunu içeren 10 basamaklı bir çevirmeli numara belirlemek yerine, bir hacker basit bir şekilde doğru sayısal kod sırası tanımlayıcıyı belirlemelidir. Alfabetik karakter araması, sayısal kümedeki ilk adresin doğru kodu girilene kadar A harfini, ikinci B'yi vb. Kullandığını varsayarak basitleştirilir veya elimine edilir. Bir bilgisayar sitesine erişmek yalnızca yerel bir düğüm numarası gerektirir ve bu numaralar genellikle paket anahtarlama ağ sitelerinde yayınlanır. Yerel düğüm numarasının kullanılması, yetkisiz kullanıcılar için çevirmeli erişim hattı maliyetlerini de önemli ölçüde azaltır. Paket anahtarlama ağ satıcıları bu soruna farklı derecelerde başarı ile yanıt verdiler, ancak bu ağlar kullanıldığında özel bir önlem alınmalıdır.

**1.2 RİSKLERİN AZALTMASI**

Bilgisayar korsanlarının bilgisayar sistemlerine erişebilmelerini sağlayacak telefon numaralarını edinmenin çeşitli yolları vardır. Belirli bir alan kodundaki telefon numaralarını rasgele çevirmek veya iblis çeviricileri veya savaş çeviricileri kullanarak telefonla değiş tokuş yapmak için girişimler yapılabilir. Bunlar 1980 filmi Savaş Oyunları'nda popülerdi. Bu bilgisayar korsanlığı programları, tesiste bulunan tüm yetkili ve yetkisiz modemleri bulmakta çok faydalı olabilir. Savaş çeviricileri, Procomm Plus iletişim yazılımı paketi tarafından sağlananlar gibi bir komut dosyası dili kullanılarak yazılabilir veya İnternet'teki çeşitli sitelerde birkaç kişi bulunabilir. Bu çeviricileri anlamak, çevirmeli bağlantıların güvenliğini sağlamak için gereken gereksinimleri anlamada çok yararlıdır.

Arayan kişinin inanılır ve kalıcı olması durumunda, bir şirketi aramak ve çevirmeli numarayı istemek gibi daha basit yöntemler başarılı olabilir. Operasyonel personeli günün en yoğun saatinde (örneğin, borsa veya banka kapanmadan önce, günün sonunda) aramak, acilen bilgisayar operatöründen veya katipten yanıt alması daha muhtemeldir.

Diğer yöntemler, çevirmeli bilgisayarın sayısını açığa çıkarabilecek atılan telefon kayıtlarını bulmak için çöp kutusundan rumma işleminden oluşur. Bir hacker, doğru çizgiyi bulmayı umarak bu numaraları manuel olarak deneyecektir. Bu, muhtemelen en uzun süreli telefon görüşmesine sahip olan olacaktır.

Telefon numaralarının alınabileceği daha az ezoterik araçlar da vardır. E-posta, ürün siparişi, banka erişimi, hisse senedi alım satım ve ilan tahtaları gibi uygulamalar için çevrimiçi hizmetler genellikle numaralarını postaladıkları örnek materyalde yayınlamaktadır. Aslında, servisi gösteren birinin omzuna bakmak ve onu numarayı izlemek genellikle mümkündür. Gösteri otomatikleştirilmişse, numara ekranda görünebilir.

Numarayı telefon rehberinde listeleme ya da telefon şirketi bilgi operatörlerinin kullanımına izin verme uygulaması kısıtlanmış olsa da, bu potansiyel olarak etkili bir yöntem olmaya devam etmektedir.

Nasıl elde edilirse edilsin, telefon numarası hacker topluluğu boyunca yeraltı bülten panoları aracılığıyla hızlı bir şekilde yayılabilir. Numara dağıtıldıktan sonra, oyuncunun oyunu başlar. Artık kullanıcıların oturum açmasına izin veren güvenliği bozma meselesi.

Uzak bilgisayar sistemlerinin kullanıcılarını tanımlamak için kullanılabilecek fiziksel cihazlar (örneğin, kartlar, kartlar, PROMS) olmasına rağmen, bu sistemlerin hemen hepsi erişim kontrolü için geleneksel kullanıcı tanımlama ve şifre koruma mekanizmalarına dayanmaktadır.

**1.3 Kimlik**

Çevirmeli kullanıcıları tanımlamanın birincil yolu, kullanıcı kimlikleri atama uygulamasıdır. Geleneksel olarak, kullanıcı kimliği 6 veya 7 alfa sayısal karakterdir. Ne yazık ki, kullanıcı kimlikleri, bilgisayar korsanlarına bir avantaj sağlayan sıralı olma eğilimindedir (örneğin, USER001, USER002). Örneğin, hacker bülten panoları, XYZ’nin şirket kimliğinin XYZ001’de başladığını ve art arda çalıştığını bildiriyor. Notu yazan hacker, kimliği XYZ001'e saldırdığını açıklayacaktır. Bildirimi okuyan ilk bilgisayar korsanı, XYZ002 kullanıcısı olarak giriş yapmaya çalışacağını ve bir sonraki bilgisayar korsanının XYZ003'ü alacağını söyleyen bir not bırakacaktır. Net sonuç, her biri farklı bir kullanıcı kimliğini hedef alan birden çok bilgisayar korsanının aynı anda saldırı yapmasıdır. Bu, sisteme girme şanslarını önemli ölçüde artırıyor.

Bilinmeyen bir şekilde, bazı güvenlik yazılımları aslında geçerli kullanıcı kimliklerini belirlemeye yardımcı olabilir. Bir bilgisayar korsanı kullanıcı kimliğini ve şifreyi girmeye çalıştığında, sistem "Geçersiz Kimlik, Lütfen Yeniden Girin" mesajı ile geçersiz bir kullanıcı kimliğinin girilmesine yanıt verebilir. Bu, korsanın çabalarını geçerli bir kimliği girmeye odaklamasına izin verir Geçerli bir kimlik ve parola alma konusunda çok daha karmaşık bir çaba ile uğraşmak zorunda kalmak.

Aynı tip güvenlik sistemi, davetsiz misafirlere “Geçersiz Şifre, Lütfen Tekrar Girin” hata mesajını vererek geçerli bir kullanıcı kimliği bulduğunu her zaman söyleyecektir. Daha sonra kullanıcı kimliği dizisi desenini bulmaya (bülten panosuna yazı göndermeye) veya parola korumasını kırmaya çalışmasına odaklanmaya devam edebilir.

Parola istemeden önce geçerli bir kullanıcı kimliği isteyen girişler, sistem saldırganlarına da büyük bir avantaj sağlayabilir. En iyi güvenlik sistemi aynı anda hem kullanıcı kimliği hem de parola girilmesini gerektirir. Sistem kombinasyonu doğrulamaya çalışır; geçersiz bulunursa, “Kullanıcı Kimliği / Şifre Geçersiz, Lütfen Tekrar Girin” mesajı ile yanıt verir. Bu, hangi öğenin geçerli olmadığına bakılmaksızın gönderilen tek hata mesajıdır.

**1.4 Şifreler**

Parola kullanımı, bir bilgisayar sistemi kullanıcısının kimliğini doğrulamak için en yaygın kullanılan yöntemdir. Parolaların tasarımı kolaydır ve ek donanım gerektirmeden hızlı bir şekilde uygulanabilir. Uygun metodoloji kullanıldığında, şifre güvenliği, büyük bir harcama yapmadan yetkisiz sistem erişimine önemli bir engel teşkil eder.

Parola tanımlama ve kimlik doğrulamayı etkin bir güvenlik aracı yapmak için belirli kurallara uyulmalıdır:

• Parolaların manuel veya otomatik sistem saldırısı veya saf tahminde bulunmalarını engellemek için yeterli uzunlukta olması gerekir.  
• Parolalar o kadar uzun olmamalı, hatırlaması zor ve bu nedenle yazılmaları zor olmalıdır.  
• Şifreler algoritma tarafından türetilmeli veya tek yönlü şifreli bir dosyada saklanmalıdır.  
• Parolalar keyfi olarak atandığında en etkilidir.  
• Parolalar sıkı kontroller altında, tercihen çevrimiçi olarak dağıtılmalıdır.  
• Önceden verilen şifrelerin denetim izi oluşturulmalıdır. • Bireysel şifreler özel olmalıdır.  
• Taşınabilir belirteçle oluşturulan rastgele şifrelerin kullanımı teşvik edilmelidir. Jetonlar nispeten ucuz ve oldukça güvenilirdir.

Parola tanımlama metodolojisinin derinlemesine çalışılması için yeterli bir zaman mevcut değilse, rastgele seçilen ve şifrelenmiş bir dosyada depolanan altı karakterlik bir parola kullanılarak temel olarak sağlam bir parola yapısı yaratılabilir. Böyle bir prosedür bazı güvenlik önlemleri sağlar, ancak daha önemli bir metodoloji tasarlamak ve uygulamak için alınmalıdır.

Çeşitli güvenli verilere erişmek için birden fazla şifre kullanılabilir. Bu sistem, her giderek daha hassas veri seviyesi için kullanıcının farklı bir parolaya sahip olmasını gerektirir. Güncelleme ve sorgulama aktiviteleri için farklı şifreler kullanmak bile, tüm fonksiyonlar için tek bir şifreden çok daha fazla güvenlik sağlar.

Bilgisayar ve ağ güvenliği sistemleri son on yılda bazı kazanımlar elde etti. Bırakılan bir hatta erişmenin ve oturum açma güvenliğini atlarken yeniden bağlanmanın yol açtığı eski sorunlar giderildi. Doğrudan bağlantı bile (yani düğüme hitap etmek ve kullanıcı kimliğini ve parola doğrulamasını atlamak) bile düzeltildi.

Telefon numaralarını, kullanıcı kimliklerini ve diğer bilgisayar korsanlarının bülten panoları veya diğer yollarla şifre bilgilerini almasının yanı sıra, bilgisayar korsanlarının çevirmeli sisteme erişmek için gerekli bilgileri edinmenin üç temel yolu vardır:

• Manuel ve bilgisayar tarafından oluşturulan kullanıcı kimliği ve şifre tahmini  
• Kişisel iletişim  
• Tel Çekiciler

Bir kullanıcı kimliği verildiğinde, bilgisayar korsanı şifreyi iki yoldan biriyle tahmin etmeye çalışabilir: sık kullanılan şifreleri deneyerek veya bilgisayarı, sözlükteki kelimeleri kullanarak veya rastgele oluşturulmuş karakter kümelerini kullanarak şifre düzenine saldırmak için programlayarak. Bilgisayar korsanı, bilgisayara girmek istediği şirket sistemini otomatik olarak arayabilir ve geçerli bir kullanıcı kimliği ve şifre kombinasyonu bulmaya çalışabilir. Eğer ana bilgisayar sistemi bağlantısı kesilirse, bilgisayar tekrar arar ve doğru kombinasyon bulunup erişim sağlanıncaya kadar denemeye devam eder. Bu saldırı, bilgisayar sistemi müsait olduğu sürece kesintisiz olarak devam edebilir. Bu yaklaşımın sakıncası, denemeler keşfedilirse çağrının izlenebilmesidir.

Daha basit bir yaklaşım, hacker'ın saldırıya uğrayan bilgisayarın sitesini kişisel olarak ziyaret etmesidir. Bir çalışanla arkadaş olarak, sisteme erişmek için gereken tüm bilgileri elde edebilir. Bilgisayar korsanına yalnızca tesislerde izin verilse bile, terminalin yan tarafına yapıştırılmış, kullanıcının bülten panosunda taranan veya dikkat çekici bir şekilde görüntülenen bir kullanıcı kimliği ve şifresi bulacaktır. Kullanıcı kimliklerini ve şifrelerini korumak için temel özen gösterilmelidir. Örneğin, asla kimseyle paylaşılmamalı veya tartışılmamalıdır.

Potansiyel olarak geçerli kullanıcı kimliklerini ve şifrelerini belirlemenin en zarar verici yolu, telefon kayıtlarında telefon kayıtlarında tel çekme cihazlarının kullanımıdır. Düz metin bilgisi daha sonra kullanmak üzere kaydedilebilir. Telefon dinleme, bilgisayar korsanının ciddi bir işlem yapma niyetini gösterir. Bilgisayar korsanını, hırsızlık, zimmete alma veya casusluk ile ilişkilendirilme riskine maruz bırakır.

Şifreleme bile telefon dinleme hacker'ını engellemeyebilir. Bilgisayar korsanı, şifreli verileri tekrarlama adı verilen bir teknik kullanarak yorumlamanın yetersizliğini giderebilir. Bu taktik, şifre metnini yakalamayı ve daha sonra yeniden iletmeyi içerir. Sonunda, hacker oturum açma dizisi şifresini yakalar ve tekrar eder. Veri akışı geçerli olarak kabul edilir ve bu nedenle bilgisayar korsanına sisteme erişim izni verilir. Bir tekrarlama saldırısıyla mücadele etmenin tek yolu, şifrelenmiş verinin zamanlanması veya dizinin damgalanmasıdır. Bu, oturum açmanın yalnızca bir kez kullanılabildiğinden ve tekrar oynatılmayacağından emin olmanızı sağlar.

Telefon dinlemeye karşı en iyi savunma, fiziksel güvenliktir. Telefon dolapları ve odalar, kartlı anahtar erişimi ile korunmalıdır. Kapalı devre kameralar erişimi izlemeli ve kaydetmelidir. Eğer bilgisayar korsanı iletişim hatlarına erişemezse, telefonla konuşamaz ve bilgi kaydedemez.

**1.5 Mikrobilgisayar Parola Sorunları**

Mikrobilgisayar ve iletişim yazılım paketlerinin kullanılması, güvenlik için şifrelere dayananlara başka bir sorun ortaya çıkardı. Bu paketler kullanıcının telefon numaraları, kullanıcı kimliği ve şifreler gibi kritik bilgileri saklamasını ve iletmesini sağlar.

Microsoft Windows 95 Çevirmeli Ağ programı veya Symantec’in PCANYWHERE gibi birçok uzaktan erişim programı, kullanıcıya kullanıcı kimliğini, şifreyi ve telefon numarasını ileride kullanmak üzere kaydetme seçeneği sunar. Bu uygulama özellikle dizüstü bilgisayarlarda kesinlikle önerilmemelidir. Dizüstü bilgisayarlar, hem fiziksel eşya hem de içerdiği bilgiler için hırsızlık için ana hedeflerdir. Bir hırsız, çevirmeli ağ oturum bilgileri (telefon numarası, kullanıcı kimliği ve şifre) kaydedilmiş bir dizüstü bilgisayarı çalsa, sahibinin hangi sisteme erişebildiğini anında tam olarak görebilir.

Dizüstü bilgisayar güvenliği tartışması başlı başına bir bölüme layıktır; Ancak, bu tartışmanın amaçları doğrultusunda, kullanıcıların çevirmeli bağlantı uygulamalarını kullanma ve güvenceye alma konusunda tam olarak eğitilmeleri gerektiğini söylemek gerekir.

Güvenliği arttırmanın etkili ancak daha zahmetli bir yolu, varış yerinin görünür tanımını ve tespit bilgisini gizlemektir. Kullanıcı artık görünmeyene kadar ekran yoğunluğunu azaltabilir veya oturum açma tamamlanıp tüm güvenlik bilgileri ekrandan silinene kadar monitörü kapatabilir. Bazı yazılım paketleri, oturum açma işlemi tamamlandığında bilgisayarın sesli bir uyarı vermesini sağlayarak kullanıcıyı uyarır. Sesli sinyal vermeyen yazılım paketleri bile bu karartma tekniği ile geliştirilebilir. Oturum açma işlemini tamamlamak için gereken zaman miktarının tahmini, bilgilerin tekrar ne zaman görünür hale geleceği konusunda fikir verebilir.

**1.6 KISA BİR YETKİ GEREKLİLİKLERİ İNCELEME**

İnsanlık tarihi ve irfan boyunca, aşağıdakilerden birini göstererek bir kişinin kimliği doğrulandı:

• bildiğiniz bir şey  
• Sahip olduğun bir şey  
• olduğunuz bir şey

Ali Baba'nın “Açıl Susam” (bildiğiniz bir şey) dediği gibi, Indiana Jones kadrosundaki kristaliyle (sahip olduğunuz bir şey) veya “Binici geliyor… Bu Dusty !! Kapıları açın! Kapıları açın !! ”(fiziksel tanıma - olduğunuz bir şey), bir kişi bu“ kimlik belirleme faktörlerinden ”birini karşılayarak başka birine erişim izni verdi veya reddetti.

Parola bilme (bildiğiniz bir şey) gibi yalnızca bir faktörün yerine getirilmesi kolayca yenilebilir. Güvenli ortamlarda, üç tanımlama faktöründen en az ikisini karşılamak daha iyidir. Bu en iyi bir banka ATM kartı başvurusunda görülebilir. Kartı kullanmak - bir hesaba erişmek için - birinin bir ATM kartı (sahip olduğunuz bir şey) olması ve o karta atanan PIN kodunu (bildiğiniz bir şey) bilmesi gerekir. Ne zaman ve sadece bir kişi her iki tanımlama faktörünü karşılayabiliyorsa, hesaptaki paraya ulaşılabilir.

Üçüncü tanımlama faktörü, retinal taramalar, parmak izleri ve sesli izler gibi biyometri kullanımıyla bugün temsil edilmektedir.

Günümüz piyasasında güvenli arama, bu üç tanımlama faktöründen en az ikisini karşılayabilme yeteneğidir.

**1.7 Fiziksel Cihazlar**

Parolalar, çevirmeli ağ ortamında kimlik doğrulama ve kimlik doğrulama güvenliği sağlama açısından nispeten ucuz bir yöntem olsa da, fiziksel cihazlar sermaye harcamasını gerektirir. Maliyet, cihazın karmaşıklığına bağlıdır. Hangi cihazın belirli bir ortama en uygun olduğunu belirlemek, yetkisiz çevirmeli penetrasyonun sonuçlarının dikkatlice analizini gerektirir.

Piyasa, mevcut teknoloji ve piyasa güçlerine cevap olarak sürekli değişiyor. Şu anda, çevirmeli kaynakların korunmasında bir teknoloji baskın: dinamik şifre üreticileri. En temel şekliyle, dinamik parola üreteci kimlik doğrulama sistemine iki bileşen vardır: satıcı tarafından sağlanan uzaktan erişim kodunu yürüten bir sunucu olabilecek ana bilgisayar sistemi veya üreticinin sağladığı donanım / yazılım ön uç ve bir el cihazı, genellikle bir hesap makinesine veya kredi kartına benzer. Bu alanda iki zamanlama var, zaman senkronlu ve meydan okuma / cevap.

**1.8 Zaman Senkron**

Bir satıcı bu pazarda, Security Dynamics Technologies, Inc. şirketine aittir (http://www.securid.com/). Ürün serileri, kısmen Greenwich Ortalama Saati'ne (GMT) dayanan, her 60 saniyede bir yeni altı basamaklı şifre üreten özel yazılım içermektedir. Bir kullanıcıya, uzaktan erişim cihazında merkezi bir veri tabanında kayıtlı küçük bir kredi kartı boyutunda "belirteç" verilir. Bir kullanıcı aradığında, kullanıcı kimliğine ve o anda ekranda beliren şifreye göre kullanıcının kimliğini doğrulayan uzaktan erişim cihazına ulaşır. Kimlik doğrulamasından sonra, kullanıcıya hedef cihaza veya ağa erişim izni verilir. Güvenlik Dinamiklerinin belirteçlerinin çeşitli türleri ve uygulamaları (kredi kartı boyutunda, anahtarlıklar, PCMCIA kartları ve yazılım tabanlı) ve kimlik doğrulamalarının “çekirdeği” veya kodlarının birçok farklı uygulamasına sahiptir. Ek olarak, birçok üçüncü taraf ürünü uzaktan erişim / kimlik doğrulama ürünlerinde Security Dynamics kodunu lisanslamıştır.

**1.9 Sınama / Yanıt**

Birkaç satıcı, elde tutulan belirteçleri ve PC yazılımını kullanan başka bir çevirmeli kimlik doğrulama yöntemi uygulamıştır. Zaman eşzamanlı belirteçler mevcut GMT'ye göre oluşturulan bir şifreye dayanırken, meydan okuma / yanıt belirteçleri paylaşılan bir algoritma ve benzersiz bir "tohum" değeri veya anahtarı kullanır. Bir arama kullanıcısı bir meydan okuma / yanıt belirteci kullanarak bir uzaktan erişim cihazına eriştiğinde, kullanıcının belirteci tarafından oluşturulan belirli bir "meydan okuma" için beklenen "yanıt" temelinde kimliği doğrulanır. Meydan okuma / cevap teknolojisi ayrıca farklı tiplerde ve belirteçlerin, yazılımların ve donanımların uygulamalarında da gelir. Başlıca meydan okuma / yanıt teknolojisi satıcıları arasında AssureNet Pathways, Inc. (http://www.assurenetpathways.com/) ve LeeMah Datacom Security Corporation (http://www.leemah.com/) bulunmaktadır.

**1.10 Çevirmeli / Geri Arama Sistemleri**

Yalnızca önceden kodlanmış tanımlayıcılar kullanıldığında mümkün olan sistem sızma türüne karşı koruma sağlamak için, üreticiler çevirmeli / geri arama sistemleri geliştirmiştir. Bu teknikle erişim izni verilmeden önce iki telefon görüşmesi yapılmalıdır. Ana bilgisayarı çevirdikten sonra, kullanıcı geçerli bir şifre girmelidir. Şifrenin alınmasından sonra, ana bilgisayar bağlantıyı sonlandırır ve şifre ile ilişkilendirilmiş olan telefon numarasına otomatik olarak bir arama yapar. Yetkili bir terminal kullanılıyorsa, bağlantı kurulur ve kullanıcı devam edebilir. Bazı çevirmeli / geri arama sistemleri, geri dönüş çağrısını yerel hatlarda, WATS hatlarında ve diğer genel taşıyıcı tesislerinde en düşük maliyetli rotalama yoluyla yapar, böylece geri arama prosedürünün maliyetini düşürür.

Çevirmeli / geri arama sistemleriyle ilgili sorunlardan biri, yetkili arayan kişinin önceden belirlenmiş tek bir yerle sınırlı olmasıdır. Bu kısıtlama, seyahat atamaları için taşınabilir terminallerin kullanılmasını yasaklar. Ayrıca farklı sitelerde kullanım için birden fazla kimlik gerektirir.

**1.11 Diğer Teknolojiler**

Bu alan değişiyor. Bir kuruluş, örgütsel gereksinimlerine bağlı olarak daha yeni veya daha az popüler olan teknolojileri araştırmak isteyebilir. Bir PC veya dizüstü bilgisayarın seri veya paralel bağlantı noktasına, PCMCIA kartlarına ve biyometriye bağlanan cihazlardır.

Dinamik şifre üreticileri bugün seçimin doğrulanması ise, biyometri yarın seçimin doğrulanması olacaktır. Son gelişmeler güvenilirliği önemli ölçüde arttırmış ve maliyetleri düşürmüştür. Önümüzdeki birkaç yıl içinde biyometrik kimlik doğrulamasında daha fazla ürün teklifi görmeyi bekleyin.

Bu cihazlardan herhangi birini satın alma kararı, donanımın izlenmesi için kurulum maliyeti ve işçilik maliyeti gibi faktörlere bağlıdır.

**2. ŞİFRELEME**

Yetkilendirilmemiş bir çevirmeli bağlantı kullanıcısı bir bilgisayar sisteminin tanımlamasına ve onaylama savunmasına girerse, veri değişikliğini ve hırsızlığı önlemezse, şifreleme zarar verebilir. Şifreleme, saf bir güvenlik önlemi yerine teknik olarak bir gizlilik önlemidir. Bilginin, uygun şifre çözme yeterliliği olmayan (anahtar, algoritma veya şifre çözme cihazı) kimseye anlaşılmaz olmasını sağlamak amaçlanmıştır. Bu, bir sisteme erişen yetkisiz personelin değiştirmek, yok etmek veya dağıtmak isteyebilecekleri verileri okuyabilmesini önler.

Veri iletişimi için, mesajlar iletim noktasında şifrelenir ve yalnızca şifreleme işleminde kullanılan anahtarla birlikte verilen bir terminalde şifresi çözülebilir. Çeşitli şifreleme algoritmaları mevcuttur ve algoritmanın karmaşıklığı korunmakta olan verinin değerine bağlı olmalıdır. Federal Hükümetin sivil kurumları tarafından kullanılacak tek şifreleme yöntemi olan Ulusal Standartlar ve Teknoloji Enstitüsü'nün Veri Şifreleme Standardı (DES) yaygın olarak kullanılmaktadır ve otomatik saldırılara karşı oldukça dirençlidir. Şifreleme, mikrobilgisayar iletimleri için, özellikle hücresel iletişimlerin kullanılması muhtemel olduğunda dikkate alınmalıdır. Bu, açık hava dalgaları üzerinden açık metin gönderimini ortadan kaldırır.

Şifreleme ve şifre çözme işlemi öncelikle veri aktarımında kullanılsa da, kritik dosyaları ve programları dış tehditlerden koruyabilir. Şifreleme verileri ve program kaynak kodu, yetkisiz bir kullanıcının dosyada hangi bilgileri veya kodları içerdiğini belirlemeyi zorlaştırır. Şifreleme dosyaları ayrıca, bu dosyaları kullanan programların kaynak kodunu okuyarak tespit edilebilecek dosya ilişkilerini de korur. Davetsiz misafir için bir kuruluşun veri bileşenlerini bilmediği ve bundan dolayı, böyle bir engel herhangi bir yetkisiz faaliyeti engelleyebilir. Yetkili kullanıcılar için bile, şifreli dosyalar, kullanıcıların görmeye alıştıkları bilgilerle hiçbir ilgisi yoktur. Ayrıca, yalnızca anahtar dosyalar ve programlar için kullanılırsa, şifreleme önemli miktarda depolama alanı içermez.

**2.1 NİHAİ SAVUNMA**

Bilgisayar korsanları, durdurma çabalarına rağmen bilgisayar sistemlerine erişmede gittikçe daha fazla önem kazanıyor. Herhangi bir sistemin güvenliğinin ihlal edilme olasılığı çok yüksektir. Bu durumda, bilgisayar korsanını tanımlamak ve aramayı izlemek veya bağlantıyı kesmek için etkili güvenlik önlemlerinin alınması zorunludur. İzinsiz erişim durdurulduktan sonra, güvenlik yöneticisinin erişimin nasıl kazanıldığını ve hasarın niteliğini ve kapsamını belirlemesi gerekir. Bu, hasarı onarmak ve savunmaları ilerideki saldırılara karşı güçlendirmek için gereklidir.

Yetkisiz bir kullanıcıyı tanımlamanın yollarından biri, kullanıcıların güvenlik süreçlerinde bulunmayan işlemlere, dosyalara ve verilere erişme girişimlerini izlemektir. Tekrarlanan ihlaller varsa (örneğin, art arda reddedilen erişimler), bazı güvenlik önlemleri alınmalıdır. Bu, hattın bağlantısını kesmek, kullanıcı kimliğini geçersiz kılmak veya en azından kullanıcıyla daha fazla görüşmek üzere ihlalleri günlüğe kaydetmek şeklinde olabilir.

Büyük bir kredi referans şirketi, bir kullanıcının bilgiye nasıl eriştiğine ilişkin normal bir aktivite modeli oluşturmak için yapay zekaya sahip post-inüzyon izleme yazılımı kullanır. Örneğin, XYZ001 kullanıcısı genellikle sosyal güvenlik numarasına göre arama yaparak müşteri bilgilerine erişebilir. XYZ002 kullanıcısı, bir kişinin adını ve adresini kullanarak bilgilere erişebilir. Bir kullanıcı oturum açtığında, o kişinin etkinlik düzeni izlenir ve kullanıcının normal faaliyet alanıyla karşılaştırılır. Büyük tutarsızlıklar ortaya çıktığında, şirket taleplerinin geçerliliğini sağlamak için müşteri ile iletişim kurmaya çalışır. Bu tür faaliyet izleme yetkisiz birçok kullanıcıyı engelledi.

Sonuç olarak, sistemleri yetkisiz erişime karşı korumaya yardımcı olmak her kullanıcının sorumluluğundadır. Yardım etmenin en iyi yolu dikkatli olmaktır. Son kullanıcılar başarılı bir oturum açma sırasında görüntülenen son oturum açma zamanını ve tarihini kontrol etmelidir. Kullanıcının bunun geçerli bir oturum açma olduğuna dair herhangi bir şüphesi varsa, uygun yetkiliye başvurmalıdır. Bu sadece sistemi korumakla kalmaz, aynı zamanda bir davetsiz misafir başka birinin kimliğini kullandığında yarattığı sorumluluğun yetkili kullanıcısına da yardım eder.

**2.2 TAVSİYE EDİLEN EYLEM KURSU**

Merkezi veri kaynaklarını korumak için seçilen güvenlik yönteminin kurumun kaynakları ve prosedürleri üzerinde büyük etkisi vardır. İlk maliyetler, uygulama süresi, müşteri tepkisi ve ilgili faktörler ancak mevcut ve gelecekteki ihtiyaçları inceleyen kapsamlı bir risk analizi yapılarak ele alınabilir. Bu makalede açıklanan önlemler, izole edilmiş bir dizi önlem olarak değil, organizasyonu tüm iç ve dış tehditlerden korumak için tasarlanmış genel bir güvenlik şemsiyesinin bileşenleri olarak yorumlanmalıdır. Veri güvenliği yöneticisi, ilk adımın, tüm çevirmeli bağlantı kullanıcıları ile ilgilenmek için daha güvenli bir ortam yaratacak kurumsal bir farkındalık oluşturmak için bir temel oluşturmasını sağlamalıdır. Özellikle, yönetici şunları sağlamalıdır:

• Geçerli çevirmeli bağlantı kullanıcılarının ve mevcut durumlarının tam bir listesi tutulur, böylece artık şirkette bulunmayan ya da konumu artık erişim gerektirmeyen tüm çalışanlar ortadan kalkar.  
• Tüm şifre şemaları ve dosyalar için koruma sağlanır.  
• En az iki tanımlama faktörü sağlanmıştır.  
• Yeni indirilen yazılımı doğrulamak için bir test makinesi (herhangi bir ağa bağlı değil) kullanılır  
• Tüm kullanıcılara düzenli olarak güvenlik politikaları hatırlatılır ve bu politikaların mevcut sürümleri çalışanlara dağıtılır.

Kapsamlı bir dizi politika ve eğitimli bir kullanıcı topluluğunun bir araya geldiği bu adımlar, bir çevirmeli ağın güvenliğini önemli ölçüde artırabilir.

**SNMP hakkında bu kadar basit olmayan nedir?**

Chris Hare, CISSP, CISA

Basit Ağ Yönetimi Protokolü veya SNMP, Yorum İsteği (RFC) 1157'de açıklandığı gibi, İnternet Mühendisliği Görev Gücü tarafından belirlenmiş bir İnternet standardıdır. Bu bölüm, SNMP'nin ne olduğunu, nasıl kullanıldığını ve ağ yönetiminin karşılaştığı zorlukları ele almaktadır. ve kullanımıyla ilgili güvenlik uzmanları.

Bu bölümde birçok SNMP uygulaması belirtilmiş olsa da, bu uygulamaların hiçbir desteği veya önerisi yapılmamakta veya ima edilmemektedir. Herhangi bir uygulamada olduğu gibi, kurum SNMP uygulamasını kendi gereksinimlerine göre seçmelidir.

1. **SNMP Tanımı**

SNMP dünyadaki ağ ve bilgisayar cihazlarını izlemek için kullanılır. Basitçe belirtildiği gibi, ağ yöneticileri, ağ yönetimi istasyonu ve ağ cihazlarındaki SNMP aracıları arasında hem durum hem de yapılandırma olan yönetim bilgilerini iletmek için SNMP'yi kullanır.

Protokol uygun olarak adlandırılmıştır, çünkü bir ağın karmaşıklığına rağmen, SNMP'nin kendisi çok basittir. Mimariyi incelemeden önce, kullanılan terminolojinin gözden geçirilmesi gerekmektedir.

• Ağ elemanı: ana bilgisayarlar, ağ geçitleri, sunucular, terminal sunucular, duvarlar, yönlendiriciler, anahtarlar ve etkin hub'lar dahil olmak üzere ağa bağlı herhangi bir cihaz.  
• Ağ yönetim istasyonu (veya yönetim istasyonu): ağ öğelerini izlemek ve kontrol etmek için SNMP yönetim yazılımına sahip bir bilgi işlem platformu; ortak yönetim istasyonlarına örnek olarak HP Openview ve CA Unicenter verilebilir.  
• SNMP ajanı: yönetim istasyonundan alınan ağ yönetimi işlevlerini yerine getirmekten sorumlu bir yazılım yönetimi temsilcisi.  
• SNMP isteği: yönetim istasyonundan ağ cihazındaki SNMP aracısına gönderilen bir mesaj.  
• SNMP tuzağı alıcısı: ağ istasyonundaki SNMP aracısından olay bildirimi mesajlarını alan yönetim istasyonundaki yazılım.  
• Yönetim bilgi tabanı: SNMP veri tabanındaki elemanları tanımlayan standart bir yöntem

Ağ cihazlarının yönetimi için SNMP'ye yapılandırılmış bir ağ, en az bir SNMP ajanı ve bir yönetim istasyonundan oluşur. Yönetim istasyonu ağ elemanlarını yapılandırmak ve bu elemanlardan SNMP tuzakları almak için kullanılır.

SNMP aracılığıyla, ağ yöneticisi çeşitli ağ elemanlarının durumunu izleyebilir, uygun konfigürasyon değişikliklerini yapabilir ve ağ elemanlarından alınan uyarılara cevap verebilir (bkz. Ek 23.1). Ağların büyüklüğü ve karmaşıklığı arttıkça, merkezi bir izleme ve yönetim yöntemi şarttır. Ağ yapısını bölümlere ayırmak veya ağın operasyonlarını bölgeselleştirmek için birden fazla yönetim istasyonu bulunabilir ve kullanılabilir.

SNMP, cihaz hataları veya uyarılara ek olarak belirli bir ağ elemanı için yapılandırma bilgilerini alabilir. Hata koşulları bir SNMP aracısından diğerine değişecektir ancak ağ arayüzü arızalarını, sistem arızalarını, disk alanı uyarılarını vb. İçerecektir. Cihaz yönetim istasyonuna bir uyarı verdiğinde, ağ yönetimi personeli sorunu çözmek için araştırma yapabilir. Sistemlere erişim, bir şifre ile karşılaştırılabilen bir topluluk dizgisinin bilgisi ile kontrol edilir. Topluluk dizeleri, bölümün ilerleyen kısımlarında daha ayrıntılı olarak ele alınmaktadır, ancak kendi başlarına bir kimlik doğrulama şekli olarak değerlendirilmemelidir.

Zaman zaman yönetim istasyonunun cihaza yapılandırma istekleri göndermesi gerekir. Doğru topluluk dizesi sağlanırsa, cihaz yapılandırması uygun şekilde değiştirilir. Bu basit açıklama bile SNMP'den elde edilen değeri kanıtlar. Bir kuruluş tüm ekipmanlarının durumunu izleyebilir ve uzaktan sorun giderme ve yapılandırma yönetimi gerçekleştirebilir.

1. **Yönetim Bilgi Tabanı (MIB)**

MIB, ağ elemanının alınması veya yapılandırılması için mevcut bilgilerin kapsamını tanımlar. Tüm cihazların desteklemesi gereken standart bir MIB vardır. Cihazın üreticisi ayrıca ek yapılandırma parametrelerini desteklemek için cihaza özel uzantılar tanımlayabilir. MIB uzantılarının tanımlanması, yönetim istasyonlarının MIB'yi doğru bir şekilde anlamaları ve yorumlamaları için belirlenmiş bir sözleşmeye uymalıdır.

MIB, ASN.1 dili kullanılarak ifade edilir; ve farkında olmak önemli olsa da, MIB için özel olarak yeni unsurlar tasarlamadığınız sürece, bu önemli bir sorun değildir. Tüm MIB nesneleri, İnternet standardı MIB'ye veya tanımlanmış bir isimlendirme kuralı ile açıkça tanımlanmıştır. Tanımlanan adlandırma kurallarının kullanılması, ürün satıcılarının belirli bir ağ cihazı için MIB elemanının bireysel örneklerini oluşturma yeteneğini sınırlar. Çok sayıda SNMP özellikli cihaz ve nispeten küçük izleme istasyonu ekipmanı yelpazesi göz önüne alındığında, bu önemlidir.

MIB'nin bu noktadan daha iyi anlaşılması, yalnızca kendilerini gerçek MIB yapısı ve temsilleriyle ilgilenmesi gereken ağ tasarımcıları için gereklidir. Bu tartışma için MIB bileşenlerinin İngilizce tanımlayıcılar kullanılarak temsil edildiğini söylemek yeterlidir.

1. **SNMP İşlemleri**

Tüm SNMP aracıları, MIB değişkenlerinin hem muayenesini hem de değiştirilmesini desteklemelidir. Bu işlemlere SNMP almak (alma ve inceleme) ve SNMP seti (değiştirme) denir. SNMP geliştiricileri, desteklemesi gereken temel yönetim işlevlerinin sayısını en aza indirmek ve diğer zorunlu yönetim komutlarının kullanılmasını önlemek için sadece bu iki işlemi kurdu. Çoğu ağ protokolü, hem istemcide hem de sunucuda bulunması gereken çok çeşitli potansiyel komutları destekleyecek şekilde geliştirilmiştir. Dosya Aktarım Protokolü (FTP), 74 komuttan daha fazlasını içerecek şekilde geliştirilen basit bir komut setine iyi bir örnektir.

SNMP yönetim felsefesi, ağ elemanlarını uygun bilgi için yoklamak için yönetim istasyonunu kullanır. SNMP, izlenen sistemde çalışan aracıdan izleme istasyonuna mesaj göndermek için tuzakları kullanır ve daha sonra oylamayı kontrol etmek için kullanılır. Temsilci ile izleme istasyonu arasındaki mesaj sayısının sınırlandırılması, basitlik hedefine ulaşır ve ağ yönetimi işlevleriyle ilişkili trafik miktarını en aza indirir.

Belirtildiği gibi, komut sayısının sınırlandırılması protokolün uygulanmasını kolaylaştırır: işletim sistemine bir arayüz geliştirmek, sistemin yeniden başlatılmasına neden olmak veya belirli bir süre geçtikten sonra yeniden başlatmayı zorlamak için değişkenlerin değerini değiştirmek gerekmez.

SNMP ajanı ile yönetim istasyonu arasındaki etkileşim, protokol mesajlarının değişimi yoluyla gerçekleşir. Her mesaj, tek bir Kullanıcı Datagram Protokolü (UDP) paketi içinde bulunmak ve böylece yönetim yapısının ağ üzerindeki etkisini en aza indirecek şekilde tasarlanmıştır.

1. **İdari ilişkiler**

Ağ elemanlarının yönetimi, elemanın kendisinde ve bir yönetim istasyonunda bir SNMP ajanı gerektirir. SNMP temsilcilerinin bir yönetim istasyonuna gruplandırılması topluluk olarak adlandırılır. Topluluk dizesi, aynı ağdaki toplulukları ayırt etmek için kullanılan tanımlayıcıdır. SNMP RFC, ağ cihazına yönetim istasyonundan doğru topluluk dizesinin sağlandığı mesaj olarak gerçek bir mesaj belirtir. Kimlik doğrulama şeması, topluluk dizesinden ve iletinin gerçekten orijinal olup olmadığını belirlemek için bir dizi kuraldan oluşur. Son olarak, SNMP kimlik doğrulama servisi, oluşturulan kimlik doğrulama şemalarına göre otantik bir SNMP mesajını tanımlayan bir işlevi tarif eder.

Topluluklar adı verilen idari ilişkiler, izlenen bir aygıtı yönetim istasyonuyla eşleştirir. Bu program sayesinde, idari ilişkiler aygıtlar arasında ayrılabilir. Bir topluluk içinde belirlenen temsilci ve yönetim istasyonu SNMP erişim politikasını oluşturur. Yönetim istasyonları doğrudan aracıyla veya ağ tasarımı durumunda bir SNMP proxy aracısıyla iletişim kurabilir. Proxy aracı, izlenen cihaz ile yönetim istasyonu arasındaki iletişimi iletir.

Proxy ajanlarının kullanımı, modemler, çoklayıcılar ve farklı yönetim çerçevelerini destekleyen diğer cihazlar dahil olmak üzere tüm ağ elemanları ile iletişime izin verir. Proxy aracısı tasarımından elde edilen ek faydalar, ağ elemanlarını erişim politikalarına karşı korumalı ve karmaşık olabilir.

Topluluk dizesi, kullanılacak erişim politikası topluluğunu oluşturur ve şifrelerle karşılaştırılabilir. Topluluk dizesi, aracıya genel topluluk olarak da adlandırılan salt okunur modda veya özel topluluk olarak bilinen okuma-yazma modunda erişmek için parola oluşturur.

1. **SNMP İstekleri**

SNMP içinde iki erişim modu vardır: salt okunur ve salt okunur. Kullanılan komut, değişken ve topluluk dizesi erişim modunu belirler. Erişim moduyla ilgili olarak, her erişim modu için bir tane olmak üzere iki topluluk dizesi bulunur. Değişkene ve ilişkili eyleme erişim aşağıdakiler tarafından kontrol edilir:

• Değişken, erişim tipi yok olarak tanımlandıysa, değişken hiçbir koşulda kullanılamaz.  
• Değişken erişim tipinde salt okunur veya salt okunur olarak tanımlanırsa, değişken uygun alma, ayarlama veya bindirme komutları için erişilebilirdir.  
• Değişken tanımlanmış bir erişim tipine sahip değilse, alma ve bindirme işlemleri için kullanılabilir.

Bununla birlikte, bu kurallar sadece MIB değişkeninde hangi eylemlerin gerçekleştirilebileceğini belirler. SNMP ajanı ile izleme istasyonu arasındaki gerçek iletişim, mesaj alışverişi için belirlenmiş bir protokolü izler. Her mesaj şunları içerir:

• SNMP sürüm tanımlayıcısı  
• Topluluk dizesi  
• Protokol veri birimi (PDU)

SNMP sürüm tanımlayıcısı, kullanımda olan SNMP sürümünü - Sürüm 1, 2 veya 3'ü belirler. Daha önce belirtildiği gibi, topluluk dizesi, hangi topluluğa genel veya özel olarak erişildiğini belirler. PDU, gerçek SNMP tuzağı veya isteğini içerir. UDP bağlantı noktası 162'de bildirilen tuzaklar hariç olmak üzere, tüm SNMP istekleri UDP bağlantı noktası 161'den alınır. RFC 1157, protokol uygulamalarının 484 bayttan daha uzun mesajları kabul etmemesini gerektirmesine rağmen pratikte daha uzun bir mesaj uzunluğu destekledi.

SNMP'de desteklenen beş PDU var:  
1. GetRequest-PDU  
2. GetNextRequest-PDU  
3. GetResponse-PDU  
4. SetRequest-PDU  
5. Trap-PDU

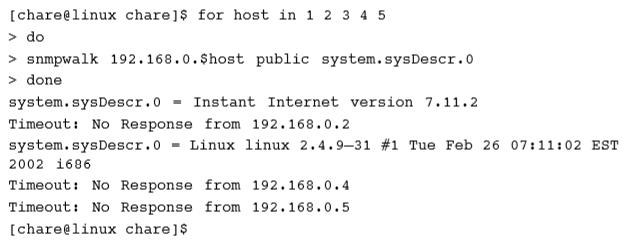
Geçerli bir SNMP isteği iletilirken, PDU, ASN.1 notasyonundaki MIB değişkeni uygulanan işlev kullanılarak oluşturulmalıdır. ASN.1 notasyonu, kaynak ve hedef IP adresleri ve UDP portları topluluk dizgisine eklenir. İşlendikten sonra ortaya çıkan talep alıcı sisteme gönderilir.

Kod çözme başarısız olursa, mesaj atılır. Doğru uygulanırsa, bu silme işlevi alıcı sistemin hatalı biçimlendirilmiş SNMP isteklerini görmezden gelmesine neden olmalıdır. Benzer şekilde, SNMP sürümü kontrol edilir ve bir uyuşmazlık varsa, paket de düşürülür. İstek daha sonra topluluk dizesi kullanılarak doğrulanır. Doğrulama başarısız olursa, bir doğrulama hatası olduğunu belirten bir tuzak oluşturulabilir ve paket bırakılır.

Mesaj kabul edilirse, gerçek isteği bir araya getirmek için nesne yeniden ayrıştırılır. Ayrıştırma başarısız olursa, mesaj bırakılır. Ayrıştırma başarılı olursa, uygun SNMP probu adlandırılmış topluluk kullanılarak seçilir ve mesaj işlenir. Ortaya çıkan veriler, isteğin kaynak adresine döndürülür.

1. **Protokol Veri Birimi**

Belirtildiği gibi, desteklenen beş protokol veri birimi vardır. Her biri, SNMP ajanı ve yönetim istasyonunda belirli bir istek uygulamak için kullanılır. Her biri amaç ve işlevselliği gözden geçirmek için kısaca incelenecektir. *GetRequest PDU* uzak cihazdan alınacak bilgileri ister. Yönetim istasyonu, çeşitli ağ öğelerinin sorgularını yapmak için *GetRequest PDU*'yu kullanır. Belirtilen MIB değişkeni MIB ağ elemanında tam olarak eşleşiyorsa, değer *GetResponse PDU* kullanılarak döndürülür. Linux sistemlerinde yaygın olarak bulunan *snmpwalk* komutunu kullanarak *GetRequest* ve *GetResponse* mesajlarının doğrudan sonuçlarını görebiliriz:

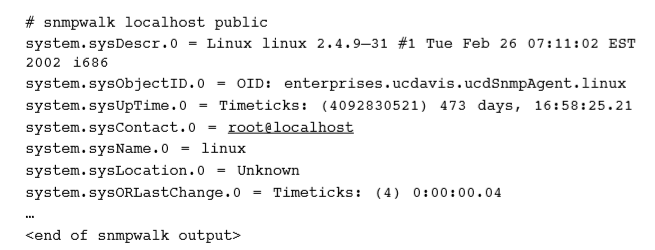


Bir cihazın yukarıdaki aralıktaki tüm IP adreslerinde bulunmasına rağmen, yalnızca iki tanesi yanıt vermesi için onaylanmıştır veya belki de sağlanan SNMP topluluk dizesi hatalıydı.

*Snmpwalk*'un kurulu olmadığı sistemlerde, komutun birçok ağ havuzunda bulunan net-ucb-snmp kaynak kodunda mevcut olduğunu unutmayın.

*GetResponse PDU*, yönetim istasyonu tarafından verilen talebe yanıtı içeren protokol türüdür. Her *GetRequest PDU*, isteğin geçerliliği ne olursa olsun, *GetResponse* kullanarak bir yanıtla sonuçlanır.

GetNextResponse PDU, önceki bir istekten ek bilgi almak için kullanılması dışında, *GetResponse PDU* ile aynıdır. Alternatif olarak, MIB üzerinden tablo geçişleri tipik olarak *GetNextResponse PDU* kullanılarak yapılır. Örneğin*, snmpwalk* komutunu kullanarak, aşağıdaki komutu kullanarak tüm tabloyu geçebiliriz:



Örneğimizde, tüm MIB değişkenlerinin ve bunlarla ilişkili değerlerin yazdırılmasına neden olan belirli bir MIB değişkeni talep edilmez. Bu *snmpwalk*'tan büyük miktarda çıktı üretir. Alınacak ek bilgi bulunmadıkça her değişken alınır.

Bilgi alma taleplerinin yanı sıra, yönetim istasyonu seçilen değişkenleri yeni değerlere de ayarlayabilir. Bu *SetRequest PDU* kullanılarak yapılır. *SetRequest PDU*’yu alırken, alıcı istasyonun birkaç geçerli yanıtı vardır:

• Eğer belirtilen değişken değiştirilemezse, alıcı istasyon bir hata kodlu bir *GetResponse PDU* döndürür.  
• Değer, belirtilen değişken tipiyle eşleşmezse, alıcı istasyon, hatalı değer göstergeli bir *GetResponse PDU* döndürür.  
• Eğer talep yerel boyut sınırlamasını aşıyorsa, alıcı istasyon bir *GetResponse PDU*’ya çok büyük bir gösterge ile cevap verir.  
• Eğer belirtilen değişken değiştirilemez ve yukarıdaki kurallara uymazsa, *GetResponse PDU*'yu kullanan alıcı istasyon tarafından genel bir hata mesajı döndürülür.

İstekte hata yoksa alıcı istasyon adlandırılmış değişkenin değerini günceller. Tipik okuma-yazma topluluğuna özel denir ve bu erişim için doğru topluluk dizesi sağlanmalıdır. Değer değişirse, alıcı istasyon “Hata yok” göstergesi olan bir *GetResponse PDU* döndürür.

Bu bölümde daha sonra tartışıldığı gibi, SNMP okuma-yazma topluluğu dizesi varsayılan ise veya başka bir iyi bilinen değere ayarlanmışsa, herhangi bir kullanıcı MIB parametrelerini değiştirebilir ve böylece sistemin çalışmasını etkileyebilir.

1. **SNMP Traps**

SNMP tuzakları bir olayı izleme istasyonuna geri göndermek için kullanılır. Tuzak, ajanın isteği üzerine iletilir ve SNMP yapılandırmasında belirtilen cihaza gönderilir. Tuzakların kullanımı SNMP uygulamalarında evrensel olmakla birlikte, SNMP aracısının tuzağı nereye göndereceğini belirleme aracı SNMP aracı uygulamaları arasında farklılık gösterir.

İzleme istasyonuna gönderilecek birkaç tuzak var:

•coldStart

• warmStart

• linkDown

• linkUp

•authenticationFailure

• egpNeighborLoss

•enterpriseSpeciﬁc

Tuzaklar, daha önce tartışılan diğer mesaj türlerine benzer şekilde PDU kullanılarak gönderilir.

*ColdStart* tuzağı, sistem kapalı durumdayken başlatıldığında ve aracı yeniden başlatıldığında gönderilir. Bu tuzak, izleme istasyonuna SNMP uygulamasının değiştirilmiş veya değiştirilmiş olabileceğini gösterir. *WarmStart* tuzağı, sistem yeniden başlatıldığında aracının yeniden başlatılmasına neden olarak gönderilir. *WarmStart* trap etkinliğinde, ne SNMP aracısının uygulaması ne de yapılandırması değiştirilmez.

Çoğu ağ yönetim personeli, *linkDown* ve *linkUp* tuzaklarını bilir. *LinkDown* tuzağı, SNMP aracısındaki bir bağlantı SNMP aracısının yapılandırmasındaki bir veya daha fazla ağ bağlantısının arızasını algıladığında üretilir. Benzer şekilde, bir iletişim bağlantısı geri yüklendiğinde, *linkUp* tuzağı izleme istasyonuna gönderilir. Her iki durumda da, tuzak, hatanın veya restorasyonun gerçekleştiği ağ bağlantısını gösterir.

Çoklu ağ arayüzlerine sahip bir yönlendirici olan bir cihazı göstermektedir. Kırmızı arabirimin arızası, yönlendiricinin yönetim istasyonuna bir *linkDown* tuzağı göndermesine ve nesnenin renginin değişmesine neden oldu. Yeşil nesneler şu anda işlevsel arayüzleri temsil eder.

*AuthenticationFailure* tuzağı, SNMP aracısı yanlış topluluk dizesiyle bir ileti aldığında oluşturulur; bu, SNMP topluluğuna erişme girişiminin başarısız olduğu anlamına gelir. SNMP aracısı Dış Ağ Geçidi Protokolü (EGP) ilişkisinde iletişim kurduğunda ve eşe artık erişilemediğinde, yönetim istasyonuna bir *egpNeighborLoss* tuzağı oluşturulur. Bu tuzak, diğer ağ bağlantılarını etkileyebilecek olan EGP eşinden alınabilecek yönlendirme bilgilerinin artık mevcut olmadığı anlamına gelir.

Son olarak, SNMP temsilcisi bir kuruluşun Özel tuzağı oluştuğunu algıladığında *enterpriseSpeci enterprise c* tuzağı oluşturulur. Bu, uygulamaya bağlıdır ve izleme istasyonuna geri gönderilen mesajdaki özel tuzak bilgilerini içerir.

1. **SNMP Güvenlik Sorunları**

SNMP'nin önceki kısa tanıtımı, güvenlik uzmanı için birkaç sorun yaratmalıdır. Belirtildiği gibi, varsayılan SNMP topluluk dizeleri salt okunur erişim için genel ve okuma yazma için özeldir. Çoğu sistem ve ağ yöneticisi bu değerleri değiştirmez. Sonuç olarak, yetkili olan veya olmayan herhangi bir kullanıcı



cihazla ilgili SNMP yoluyla bilgi almak ve potansiyel olarak değerleri değiştirmek veya sıfırlamak. Örneğin, okuma yazma topluluk dizesi varsayılan ise, herhangi bir kullanıcı cihazın IP adresini değiştirip ağdan çıkarabilir.

Bunun, özellikle cihazın kullanılabilirliğini çevreleyen önemli sonuçları olabilir. Kurumsal bilgilere veya sistem şifrelerine erişmek veya SNMP kullanarak komut satırı veya terminal erişimi elde etmek tipik olarak mümkün değildir. Sonuç olarak, herhangi bir değişiklik, izleme istasyonunun cihazı kullanılamaz olarak tanımlamasına ve hizmetin geri yüklenmesine yönelik düzeltici eylemin yapılmasına neden olabilir.

Ancak, yaygın SNMP güvenlik sorunları şunları içerir:

• İyi bilinen varsayılan topluluk dizeleri  
• SNMP aracısının çalıştığı sistemdeki yapılandırma bilgilerini değiştirebilme  
• Aynı cihazı yöneten birden fazla yönetim istasyonu  
• Hizmet reddi saldırıları

Pek çok güvenlik ve ağ uzmanı, şüphesiz Şubat 2002'de yayınlanan Bilgisayar Acil Durum Müdahale Ekibi (CERT) CA-2002-03 Tavsiye Belgesine aşinadır. Bu, bugün ağ ve güvenlik toplulukları için özellikle ilgi çekici olsa da, söz konusu diğer sorunları gölgelememelidir. Yukarıda çünkü CA-2002-03'teki sorunların birçoğu diğer güvenlik sorunlarından dolayı mümkün olabilir.

1. **İyi bilinen varsayılan topluluk dizeleri**

Daha önce belirtildiği gibi, sırasıyla genel ve özel topluluk topluluk dizelerini kullanan salt okunur ve salt okunur iki SNMP erişim ilkesi vardır. Birçok kuruluş varsayılan topluluk dizelerini değiştirmez. Varsayılan değerlerin değiştirilmemesi, yetkisiz bir kişinin cihazla ilgili yapılandırma parametrelerini değiştirmesinin mümkün olduğu anlamına gelir.

Sonuç olarak, SNMP topluluk dizeleri parola olarak değerlendirilmelidir. Parolanın kalitesi ne kadar yüksek olursa, yetkisiz bir kişi topluluk dizesini tahmin edebilir ve yapılandırmayı değiştirebilir.

**10. SNMP aracısının çalıştığı sistemdeki yapılandırma bilgilerini değiştirebilme**

Birçok sistemde, yönetici ayrıcalıklarına sahip kullanıcılar, yetkisi olmasa bile, sistemlerinin yapılandırmasını değiştirebilirler. Yerel SNMP ajanı konfigürasyonunu değiştirme yeteneği sistemin çalışmasını etkileyebilir, ağ yönetimi sorunlarına neden olabilir veya cihazın çalışmasını etkileyebilir.

Sonuç olarak, SNMP konfigürasyon dosyaları kontrol edilmeli ve mümkünse, konfigürasyon değişikliklerini tanımlamak ve düzeltmek için merkezi olarak yönetilmelidir. *Tripwire* gibi araçlar da dahil olmak üzere çeşitli şekillerde yapılabilir.

**11. Aynı cihazı yöneten birden fazla yönetim istasyonu**

Bu, kendi başına bir güvenlik sorunu olmasa da, aynı cihazı seçen çok sayıda yönetim istasyonu, düşük performanstan, farklı SNMP yapılandırma bilgilerine, görünür hizmet kaybına kadar değişen sorunlara neden olabilir.

Ağınız birden fazla yönetim istasyonu gerektirecek kadar büyükse, bu olayların gerçekleşmesini önlemek için ayrı topluluklar kurulmalıdır. Unutmayın, ağda kullanılabilecek SNMP topluluklarının sayısı konusunda herhangi bir kısıtlama yoktur; sadece sınırları uygulayan şebeke mühendisidir.

**12. Hizmet reddi saldırıları**

Hizmet reddi, yetkili veya yetkisiz yapılandırmalar nedeniyle hizmet kullanılabilirliği kaybı olarak tanımlanır. Yetkili ve yetkisiz değişiklikler konusunda net olmak önemlidir. Yapılandırmasını değiştiren, işinin bir parçası olan ve hizmet kaybına neden olan sistem veya uygulama yöneticisi, uzaktan hizmet kaybına neden olan bir program yürüten saldırganla aynı etkiye sahiptir.

SNMP ile ilgili önemli bir problem, servis kesintisine neden olan sistemin konfigürasyonunu değiştirme veya SNMP konfigürasyonunu değiştirme ve izleme istasyonu tarafından bildirildiği şekilde servis reddi taklit etme yeteneğidir. Her iki durumda da, nedenden bağımsız olarak, yapılandırma sorununu gözden geçirmek ve muhtemelen düzeltmek zorundadır. Yetkili bir kişi değişikliği yapsa bile, bunun şirkete maliyeti vardır.

**13. CERT CA-2002-03'ün Etkisi**

Çoğu ekipman üreticisi, işletmesi ve bireyi, Carnegie Mellon Yazılım Mühendisliği Enstitüsü (CM-SEI) Bilgisayar Acil Müdahale Ekibi Koordinasyon Merkezi (CERT-CC) tarafından yayınlanan CERT danışmanlığının etkisini hissetti. Danışma, Oulu Üniversitesi Güvenli Programlama Grubu, SNMP Sürüm 1'in mesaj işleme yeteneklerinin çok kapsamlı bir analizini yaptıktan sonra yayınlanmıştır. Danışma, SNMP Sürüm 1 için özel olarak belirtilmiş olsa da, çoğu SNMP uygulamaları, PDU’nun kodunu çözmek için aynı program kodunu kullanır. potansiyel olarak tüm SNMP sürümlerini etkilemektedir.

Danışmada SNMP'yi etkilediği için belirtilen başlıca konular, yetkisiz ayrıcalıklı erişim, hizmet reddi saldırıları veya diğer dengesiz davranış potansiyelini içerir. Özellikle, Oulu Üniversitesi tarafından yapılan çalışma, SNMP yönetim istasyonu tarafından alınan tuzak mesajlarının çözülmesi ya da ağ cihazındaki SNMP aracısının aldığı taleplerin çözülmesiyle ilgili problemler buldu.

Ayrıca, SNMP uygulamasında bulunan güvenlik açıklarının bazılarının doğru topluluk dizesini gerektirmediği tespit edilmiştir. Sonuç olarak, satıcılar SNMP uygulamaları için yamalar yayınlamaktadır; ancak daha önemlisi, işletmeler ağlarındaki güvenlik açıklarını test ediyorlar.

On yıllardır kullanılmakta olan kodlardaki güvenlik açıkları, güvenlik açıklarını gidermek, doğrulamak ve düzeltme eklerini kaldırmak için geliştiricilere milyonlarca dolara mal olacak. Bu ürünlerin kullanıcıları, potansiyel riskleri sınırlamak için diğer kontrolleri yamalamak ve uygulamak için milyonlarca dolar harcarlar.

CERT tarafından sorunu gidermek için verilen önerilerin çoğu, SNMP kullanırken ortak güvenlik sorunlarına yönelik çözümlerdir. SNMP bir ağ servisi olarak değerlendirilmeli, çünkü CERT tarafından sağlanan tavsiyeler sağduyulu sayılabilir.

• SNMP'yi devre dışı bırakın. Söz konusu cihaz SNMP kullanılarak izlenmiyorsa, servisi devre dışı bırakmak muhtemelen güvenlidir. Unutmayın, cihazı izliyor ve yanlışlıkla SNMP'yi devre dışı bırakırsanız, yönetim istasyonunuz cihazı aşağı olarak bildirir.  
• Çevre ağı filtreleme uygulayın. Çoğu işletme, yetkisiz kişilerin veya kuruluşların ağ cihazlarınızla ilgili SNMP bilgilerini almalarını engellemek için harici ağlardan gelen SNMP taleplerini doldurmalıdır. İşletmenize nasıl saldırılacağına dair iyi bir görüş sağlamak için SNMP verilerinde yeterli bilgi bulunmaktadır. İkincisi, SNMP isteklerinin ağınızdan ayrılmasını ve başka bir işletmeye yönlendirilmesini önlemek için giden filtreleme uygulanmalıdır. Buradaki istisnalar, sizin dışınızdaki başka bir ağı izliyorsanız veya bir dış kuruluş ağınız için SNMP tabanlı izleme sistemleri sağlıyorsa.  
• Yetkili SNMP ana bilgisayar filtresini uygulayın. İsteyen her kullanıcı, SNMP sorgularını ağ cihazlarına gönderemez. Sonuç olarak, SNMP taleplerinin kaynak ve hedef adreslerini sınırlandırmak için yönlendiriciler ve anahtarlar gibi ağ cihazlarına filtreler takılabilir. Ek olarak, acentenin SNMP yapılandırması, yetkili SNMP yönetimini ve tuzak istasyonlarını sınırlandırmak için uygun detayları içermelidir.  
• Varsayılan topluluk dizelerini değiştirin. Çoğu işletmede büyük bir sorun olan, varsayılan kamu ve özel topluluk dizeleri karmaşık bir dizeyle değiştirilmelidir ve bu ipin bilgisi mümkün olduğu kadar az insanla sınırlı olmalıdır.  
• Ayrı bir yönetim ağı oluşturun. Bu, birçok işletmenin üstlenemediği uzun, ilgili ve pahalı bir işlem olabilir. Ayrı bir yönetim ağı, ağ kısmında bir arıza olsa bile ağ cihazlarına bağlantıyı sürdürür. Bununla birlikte, tamamen ayrı bir altyapıya ihtiyaç duyar, bu da uygulanması pahalı hale getirir ve geriye doğru zorlaştırır. Yeni bir ağ oluşturuyorsanız veya kritik operasyonel gereksinimleri olan mevcut bir ağınız varsa, ayrı bir yönetim ağı şiddetle tavsiye edilir.

Burada tanımlanan öneriler, tüm ağ cihazlarında en son yamalara sahip olsa bile, birçok işletme tarafından uygulanmalıdır. Bu tekniklerin SNMP'ye ek olarak diğer ağ protokolleri ve hizmetleri için uygulanması, yetkisiz ağ erişimi ve veri kaybı riskini büyük ölçüde azaltabilir.

**14. ÖZET**

SNMP'nin amacı yapılandırmayı değiştirmek ve sistemlerin ve ağ cihazlarının durumunu ve kullanılabilirliğini izlemek için basit ama güçlü bir mekanizma sağlamaktır. Ancak, diğer ağ protokollerinde olduğu gibi SNMP'nin doğası da ağ yöneticileri, sistem yöneticileri ve güvenlik personeli tarafından saldırıya ve uygunsuz kullanıma maruz kalmasını sağlar.

SNMP'nin temellerini ve burada açıklandığı şekilde kullanımını etkileyen ana güvenlik konularını anlamak, güvenlik yöneticisinin ağ tasarımı ve uygulamasıyla ilgili endişeleri ağ yöneticisi veya ağ mühendisiyle iletmesine yardımcı olur.

**15. TRUVA ATI (TROJAN)**

Truva atı (veya “Trojan”), gerçek amacını gizlemek için çeşitli yöntemler kullanan zararlı yazılımları açıklayan geniş bir terimdir. Bununla birlikte, bir virüsün aksine, tek başına çoğalamaz veya dosyaları enfekte edemez. Bu zararlı yazılım mağdurun cihazına sızmak için indirme, güvenlik açıklarından yararlanma, diğer zararlı kodlar ya da sosyal mühendislik teknikleri gibi yöntemleri kullanır.

**15.1. (Dijital) Truva atı nedir?**

Eski Greko-Romen hikayelerinden bilinen Truva Atı'na benzer şekilde, bu tür kötü niyetli yazılımlar, gerçek amaçlarını saklamak için gizleme veya yanlış yönlendirme metodları kullanır. Hedeflenen makineye ulaştıktan sonra, genellikle kullanıcı tarafından veya etkilenen sistemdeki diğer yazılımlar tarafından yürütülecek çeşitli teknikler kullanılır.

Truva atları şu anda en sık rastlanan zararlı yazılım kategorisidir. Arka kapılar açmak, etkilenen cihazın kontrolünü ele geçirmek, kullanıcı verilerini süzmek ve saldırgana göndermek, etkilenen sisteme diğer zararlı yazılımları indirmek ve çalıştırmak ve diğer birçok kötü amaç için kullanılırlar.

**15.1 Kısa Tarih**

“Truva atı” terimi, Yunanlılar tarafından Truva kentinin fethedilmesini anlatan klasik antik dönem tarihinden türetilmiştir. Yunanlılar, Truva şehrinin savunmasını ele geçirmek için, masif bir tahta at yaptılar ve en iyi askerlerini içine gizlediler. Truva muhafızlarını bu “armağan” ile kandırıp atı şehrin içine çektikten sonra içerideki askerler gece olmasını beklediler ve sonrasında şaşkınlık içinde kalan şehrin savunmasını yenmeleri zor olmadı. Bu terim ilk kez [1974 ABD Hava Kuvvetleri raporunda](https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/karg74.pdf) zararlı kodları tanımlamak için kullanıldı. Bilgisayar sistemlerinde güvenlik açıklarının analizi üzerinde duruldu. Ancak, terim 1980'lerde, özellikle de [Ken Thompson'ın](https://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf) dersi [sonrasında](https://www.ece.cmu.edu/~ganger/712.fall02/papers/p761-thompson.pdf) ACM Turing Ödülleri 1983 resepsiyonunda popüler oldu.

**15.2 İyi Bilinen Örnekler**

Yaygın olarak bilinen ilk Truva atlarından biri de fidye yazılımıydı: **AIDS Truva Atı** 1989 ”. Bu kötü amaçlı kod, AIDS hastalığı ile ilgili etkileşimli bir veritabanı içerdiği iddia edilen disketlerde posta yoluyla dağıtıldı. Yüklenen, program 90 açılış döngüsünü bekledi ve daha sonra makinenin kök dizinindeki dosya adlarının çoğunu şifreledi. Yazılımın “lisans sözleşmesi”, kurbanların verilerini geri almak için Panama'daki bir postane kutusuna 189 dolar veya 378 dolar göndermelerini istedi.

Kötü şöhretli casus yazılımlar **FinFisher** (FinSpy olarak da bilinir) Truva atının başka bir örneğidir. Kapsamlı casusluk yetenekleri ve web kameralarının ve mikrofonların gizlice kullanımı, klavye hareketlerinin çalınması ve dosyaları süzme yetenekleri ile bilinir. Geliştiriciler tarafından bir yasa uygulama aracı olarak pazarlanmaktadır, ancak baskıcı rejimler tarafından da kullanıldığı düşünülmektedir. FinFisher gerçek amacını gizlemek için çeşitli yöntemler kullanır. ESET tarafından keşfedilen [kullanımlarından](https://www.welivesecurity.com/2017/09/21/new-finfisher-surveillance-campaigns/))birinde, tarayıcılar ve medya oynatıcılar gibi popüler ve meşru programlar için bir yükleyici olarak ortaya çıktı. Ayrıca sahte ekler veya sahte yazılım güncellemeleri ile e-posta yoluyla dağıtıldı.

Ancak, Truva atları masaüstüne veya dizüstü bilgisayarlara özel bir tehdit değildir. Günümüzün mobil (ve özellikle Android) kötü amaçlı yazılımlarının büyük bir kısmı da bu kategoriye ait. **DoubleLocker** Adobe Flash Player güncellemesi olarak gizlenmiş yenilikçi bir fidye ailesiydi. Mobil cihaza Erişilebilirlik hizmetleri aracılığıyla sızdı, verilerini şifreledi ve rasgele bir PIN kodu kullanarak ekranını kilitledi. Ardından, saldırgan, aygıtın ve verilerin kilidini açmak için bitcoin olarak ödeme talep etti.

**15.3 Nasıl Korunulur?**

Truva atı adı altında çeşitli kötü amaçlı yazılımlar bulunur bu nedenle yalnızca iyi bir siber temizlik ve güvenilir bir güvenlik çözümünün kullanılmasıyla önlenebilir.

Birçok Truva atı, kurbanların sistemlerine sızmak için güvenlik açıklarından yararlanır. Bu güvenlik açıklarını azaltmak için, kullanıcılara yalnızca işletim sistemlerini değil, kullandıkları tüm yazılımları düzenli olarak güncellemeleri ve yamalamaları önerilir.

Truva atları ayrıca sosyal mühendislik teknikleri kullanarak kullanıcıları kandırmaya çalışırlar. Kullanıcıların ve işletmelerin bu tekniklerin farkına varabilmeleri için hem uyanık hem de en son tehditlerden haberdar olmaları gerekmektedir. Düzenli siber güvenlik eğitiminin yanı sıra güvenilir siber güvenlik haberlerini ve kaynakları takip etmek çok işinize yarayacaktır.

Güvenilir ve çok katmanlı bir güvenlik çözümü, kullanıcının siber savunmasının önemli bir parçasıdır. Truva atları, bir cihaza veya ağa girmek için birkaç kanal kullanabilir. Bu nedenle, modern güvenlik yazılımlarının çoğu, saldırı girişimlerini tespit etmek ve mümkün olan en iyi güvenlik düzeyini sağlamak için sanal alan, emülasyon ve makine öğrenimi gibi çeşitli teknolojiler kullanır.

**16. REFERANSLAR**

İnternet Mühendisliği Görev Gücü (IETF) Yorum İsteği (RFC) belgeleri: İnternet Mühendisliği Görev Gücü (IETF) Yorum İsteği (RFC) belgeleri:

RFC-1089 SNMP over Ethernet

RFC-1157 SNMP over Ethernet

RFC-1187 Bulk Table Retrieval with the SNMP

RFC-1215 Convention for Deﬁning Traps for Use with the SNMP RFC-1227 SNMP MUX Protocol and MIB

RFC-1228 SNMP-DPI: Simple Network Management Protocol Distributed Program

RFC-1270 SNMP Communications Services

RFC-1303 A Convention for Describing SNMP-Based Agents

RFC-1351 SNMP Administrative Model

RFC-1352 SNMP Security Protocols

RFC-1353 Deﬁnitions of Managed Objects for Administration of SNMP

RFC-1381 SNMP MIB Extension for X.25 LAPB

RFC-1382 SNMP MIB Extension for the X.25 Packet Layer

RFC-1418 SNMP over OSI

RFC-1419 SNMP over AppleTalk

RFC-1420 SNMP over IPX

RFC-1461 SNMP MIB Extension for Multiprotocol Interconnect over X.25

RFC-1503 Algorithms for Automating Administration in SNMPv2 Managers

RFC-1901 Introduction to Community-Based SNMPv2

RFC-1909 An Administrative Infrastructure for SNMPv2

RFC-1910 User-Based Security Model for SNMPv2

RFC-2011 SNMPv2 Management Information Base for the Internet Protocol

RFC-2012 SNMPv2 Management Information Base for the Transmission Control Protocol

RFC-2013 SNMPv2 Management Information Base for the User Datagram Protocol

RFC-2089 V2ToV1 Mapping SNMPv2 onto SNMPv1 within a Bi-Lingual SNMP Agent

RFC-2273 SNMPv3 Applications

RFC-2571 An Architecture for Describing SNMP Management Frameworks

RFC-2573 SNMP Applications

RFC-2742 Deﬁnitions of Managed Objects for Extensible SNMP Agents

RFC-2962 An SNMP Application-Level Gateway for Payload Address

CERT Advisory CA-2002–03