

Ağ Güvenliği (Donanım)

AĞ GÜVENLİĞİ
(DONANIM)

Prof.Dr. Resul DAŞ
Fırat Üniversitesi
Yazılım Mühendisliği Bölümü

Konu Başlıklarları

- Ağ Güvenliği
 - Ağ Güvenliği İçin Potansiyel Riskler
 - Ağlar İçin Güvenlik Tehditleri
 - Güvenlik Duvarı (Firewall) Cihazı
- Yedekleme
 - Yedekleme
 - Sunucu Yedekleme (Server NT Backup)
 - Aynalama (Mirroring)-Şeritleme (Striping)
- Sonuç
- Sorular
- Kaynaklar

Ağ Güvenliği

■ Amaç

Ağ güvenliğini tanıyarak, güvenliği tehdit eden unsurları tanıယacak ve gerekli güvenlik önlemleri seçimini yapabileceksiniz.

Ağ Güvenliği

Son yıllarda internetin, elektronik işletmelerin oluşması ve internet üzerinden ticaretin gelişmesiyle birlikte ağlar, oluşabilecek saldırılara karşı zayıflık göstermeye başlamıştır. Ve ağların bu zayıflıkları, kritik iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmuştur. Bilgisayar virüsleri, DoS saldırıları, şirket çalışanlarının hataları, bilgisayar ağları üzerinde hâlâ büyük bir tehlike oluşturmaktadır. Fakat bu ağ güvenlik açıklarını önlemek elbette ki mümkündür.

Ağ Güvenliği

Günümüzde internet, gerek kişisel gerekse iş ilişkileri arasındaki bilgi akışını sağlayan, dünyanın en büyük iletişim aracı hâline gelmiştir. Internetin tüm dünyada böylesine yaygın kullanımı, güvenlik tehlikelerini de artırmaktadır. Önemli bir bilgi kaybı olabilir, gizlilik ihlal edilebilir (kredi kartı numarasının bulunması gibi) veya saatler hatta günler süren yükleme zamanları ortaya çıkabilir. İnternetteki bu tür güvenlik açıkları, insanları internete karşı güvensizleştirebilir ve web tabanlı şirketlerin sonunu hazırlayabilir.

Ağ Güvenliği

Bu yüzden şirketler, güvenliklerini her geçen gün artırmakta ve yeni tehditlere karşı önlem almak amacıyla yatırımlarını sürdürmektedir.

Ağ Güvenliği

■ Ağ Güvenliği İçin Potansiyel Riskler

- Risk, bir olay olduğunda hasarın derecesi ya da olayın olma ihtimali olarak tanımlanabilir.
- Ağ açısından riskler; hata, kötü amaç ve virüsler gibi sisteme zarar verme potansiyeli olan olaylardır. Risk analizinin bir parçası olarak tehditlerin ihtimallerini ve firma mülklerine zarar verme potansiyellerini belirlemek gerekmektedir.
- Ağ açısından potansiyel riskleri, kısaca verinin çalınması, verinin yok edilmesi ve DoS atakları olarak ele alabiliriz.

Ağ Güvenliği

■ Veri Çalma (Data Theft)

Veri çalmanın ne olduğunu anlamak için öncelikle veri güvenliğini bilmek, verinin nasıl çalınabileceği bilgisine sahip olmak, tescilli bilginin çalınma yöntem ve tekniklerini kavrayarak bunlara ne gibi önlemler alacağımızı bilmemiz gerekmektedir.

■ Veri Güvenliği

Kurumların internet veya özel iletişim hatları üzerinden akan verilerinin güvenliğinin sağlanması amacıyla kullanılabilecek teknolojiler şunlardır.

Ağ Güvenliği

- **Fiziksel güvenlik:** Bilgisayarların fiziksel güvenliğinin gerek şifre gibi unsurlarla gerekse akıllı kart, güvenlik kartı türü araçlarla sağlanması.
- **Kullanıcı doğrulaması (authentication) yöntemleri:** Akıllı kart, tek kullanımlı parola, token ve Public Key Certificate gibi araçlar ve RADIUS gibi merkezi kullanıcı doğrulama sunucularının kullanılması.

Ağ Güvenliği

- **Şifreleme:** Güvensiz ağlar üzerinden geçen verilerin güvenliği için Virtual Private Network veya şifreleme yapan donanımların kullanılması. Ayrıca web tabanlı güvenli veri transferi için SSL ve Public Key şifrelemenin kullanılması. Donanım tabanlı şifreleme çözümleri de mümkündür.
- **İnkâr edilmezlik ve mesaj bütünlüğü:** Sayısal imza teknolojisi kullanarak bunlar sağlanabilir.

Ağ Güvenliği

■ Bilginin Ele Geçirilmesi

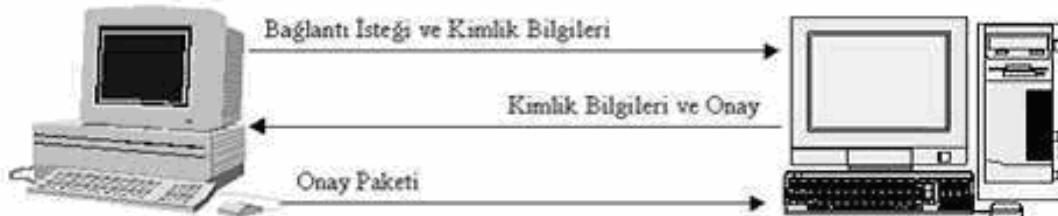
- Herhangi bir bilgisayar ağına gönderilen bilgi, o bilgiyi almaya yetkisi olmayan kişilerce ele geçirilebilir. Bu kişiler iletişimini gizlice gözetleyebilir ya da gönderilen bilgi paketini değiştirebilirler. Bunu birçok metot kullanarak yapabilirler. Örneğin IP spoofing yöntemi. Bilgi iletişiminde, bir alıcının IP numarasını kullanarak sanki o alıcıymış gibi gönderilen bilgileri istediği gibi kullanabilir.

Ağ Güvenliği

■ Tescilli Bilginin Çalınması

- Kimlik onayıyla birleştirilmiş güçlü şifreleme bu tür saldırılarla mücadelede etkilidir. Öncelikle bir ağ ortamında hacker'ların nasıl olup da kullanıcı bilgilerini kullanarak sistemlerden bilgi sızdırabildiğini inceleyelim. Bu iş aslında çok basit bir mantığa dayanmakta, değil mi? Hacker kendisini, kullanıcı bilgisayarından çıkan veriler ile bu verileri bekleyen sunucu bilgisayar arasında (Bu genellikle ana segment'tir) bulunacak şekilde yerleştirir. Bu işlemi yaparken tabii ki çeşitli yazılımlar hatta yazılımcıklar (Script de denilebilir.) kullanırlar.

Ağ Güvenliği



Şekil 1.1: Veri alma ve gönderme

Ağ Güvenliği

■ Veri Yoketme (Destruction of Data)

- Veri yok etmeyi anlayabilmek için öncelikle verinin nasıl kaybolduğunu anlamak gereklidir.
- Günümüzde gerek kişiler gerekse kurum ve işletmeler verilerini büyük oranda bilgisayar sistemlerinde işlemekte ve saklamaktadır. Bu veriler bilgisayar sistemlerinde genel hatlarıyla,
 - **Manyetik:** Hard diskler, disketler, teyp yedekleme kartuşları,
 - **Optik:** CD ve DVD,
 - **Elektronik:** Flash bellekler, bellek kartları, tabanlı ortamlarda depolanmaktadır.

Ağ Güvenliği

Depolanan bu verilerin normal yollarla erişilemez hâle gelmesi veri kaybı olarak değerlendirilmektedir. Veri kaybı nedenleri ve türleri ise genel hatlarıyla,

- Veri depolama ortamında verilerin dosyalar şeklinde düzenli bir şekilde yerleştirilmesine ve ihtiyaç duyulduğunda erişilmesine yarayan mantıksal düzenlemelerin (dosya sistemi) silinmesi veya hasar görmesi,

Ağ Güvenliği

- Veri depolama ortamındaki yapının yeniden oluşturulması (formatlama) veya dosyaların silinmesi,
- Ham veya belirli formatlara sahip dosyalarda (veri tabanı dosyaları, belgeler) dâhili bozulmalar olması,
- Veri depolama ortamının fiziksel olarak bozulması ya da hasar görmesi şeklinde özetlenebilir.

Ağ Güvenliği

- **Servis Reddetme (Denial of Service, DoS Attack)**
 - **DoS Attack Nedir?**

Bir tür bilgisayar ağı saldırısı olarak bilinen DoS saldırılarında bilgisayar korsanları, istedikleri Web sitesini çalışmaz hâle getirebilmektedir.

Korsanlar bu saldırıları, kişisel bilgisayarları kullanarak yapmakta ve özellikle büyük web siteleri bu tür saldırılar nedeniyle büyük zararlar görebilmektedir.

Ağ Güvenliği



- Ağlar İçin Güvenlik Tehditleri

- Dış Tehditler
- İç Tehditler

Ağ Güvenliği

- Dış Tehditler
 - Servis Reddetme (DoS)

Genellikle kullanılan yöntemler üç sınıf altında toplanabilir:

- Bant Genişliğine Yönerek Ataklar
- Protokol Atakları
- Mantıksal Ataklar

Ağ Güvenliği

■ DoS Ataklarının Türleri

- **Service overloading:** Bu atak tipi belirli host ve servisleri düşürmek için kullanılır. Atak yapan kişi özel port ve host'a bir çok ICMP paketi gönderir. Bu olay network monitör ile kolayca anlaşılır.
- **Message flooding:** Service overloading'den farkı sistemin normal çalışmasını engellemez. Yine aynı şekilde gönderilen paketler bu sefer normal olarak algılanır. Örnek Nis server'ında flood yapılrsa (Unix network) Nis bunu şifre isteği gibi görür ve saldırganın host'a hükmetsesi sağlanır.

Ağ Güvenliği

- **Clogging:** Saldırganın SYN gönderip ACK alıp ondan sonra da gelen ACK'ya cevap vermeyip sürekli SYN göndermesinden oluşur. Bu durum defalarca kez tekrarlanırsa server artık cevap veremez hâle gelir. Bu paketler sahte IP ile gönderildiğinden sistem bunu anlayamaz ve hizmeti keser. Anlasa ne olur? Anlasa aynı IP' den gelen o kadar istege cevap vermez. Kurtuluş yolu bunları tarayan firewall'lardır.

Ağ Güvenliği

■ Dağıtık Servis Reddetme (DDoS)

- Bir saldırgan daha önceden tasarladığı birçok makine üzerinden hedef bilgisayara saldırısı yaparak hedef sistemin kimseye hizmet veremez hâle gelmesini amaçlayan bir saldırısı çeşididir. Koordineli olarak yapılan bu işlem hem saldırının boyutunu artırır hem de saldırıyı yapan kişinin gizlenmesini sağlar. Bu işlemleri yapan araçlara Zombi denir.

Ağ Güvenliği

- Bu saldırı çeşidinde saldırganı bulmak zorlaşır. Çünkü saldırının merkezinde bulunan saldırgan aslında saldırıya katılmaz. Sadece diğer ip numaralarını yönlendirir. Eğer saldırı bir tek ip adresinden yapılrsa bir Firewall bunu rahatlıkla engelleyebilir. Fakat saldırının daha yüksek sayıdaki IP adresinden gelmesi Firewall'un devre dışı kalmasını sağlar(Log taşıması firewall servislerini durdurur.). İşte bu özelliği onu DoS saldırısından ayıran en önemli Özelliğidir.

Ağ Güvenliği

■ DDoS Atakları İçin Kullanılan Programlar

- Trinoo
- TFN
- Stacheldraht
- Shaft
- TFN2K
- Mstream

Ağ Güvenliği

- **Sömürücüler (Exploits)**
 - **Windows Null Session Exploit:** Windows işletim sistemi, dışarıdaki kullanıcılarla network üzerinde hiç bir hakkı sahip olmadan oturum, kullanıcı ve paylaşım bilgilerini (session, user ve share) verir. Ve ne kadar ilginçtir ki, bu exploit, Windows Network API'sinde belgelenmiş ve feature (özellik) olarak gösterilmiştir. Kötü niyetli birisi bu exploit'i kullanarak sistem hakkında çok kritik bilgilere sahip olabilir.

Ağ Güvenliği

- **PHF Exploit:** Bu exploit oldukça eski olmasına rağmen hâlen karşılaşabileceğiniz bir güvenlik açığıdır. Phf.cgi yardımı ile sistemdeki dosyalara admin olarak erişebilirsiniz.
- **ASP Exploit:** Active server page (ASP) özelliği kullanan Web sunucularda URL'nin sonuna bir nokta (.) ya da ::\$DATA yazarak ASP'nin içeriğini (source code) görebilirsiniz. Eğer ASP'nin içerisinde herhangi bir şifre varsa bu exploit çok tehlikeli olabilir.

Ağ Güvenliği

- **Sendmail Exploit:** Eski “send mail” sürümlerinde bir kaç basit hile ile sistemin şifrelerinin tutulduğu dosyayı çekmeniz mümkündür. Ayrıca sistem kullanıcıları hakkında bilgi almak (EXPN) ya da bir kullanıcı isminin o sunucuda olup olmadığını da öğrenmek mümkündür (VRFY).
- **ICQ Tabanlı Exploitler:** Son derece zayıf bir mimariye sahip olan ICQ sistemi, kolayca taklit edilebilen hatta gerçek “spoofing” bile yapmanıza gerek kalmayan bir sistemdir.

Ağ Güvenliği

- **İç Tehditler**

- **Firma Casusluğu (Corporate Espionage)**

- Firmanız hangi ağ çözümünü uygularsa uygulasın güvenlik son derece önemlidir. Bilgisayar güvenliği bilgi, donanım ve yazılım gibi firmanın kaynaklarını koruyacak şekilde dizayn edilir. Firma casusluğunu, çalışanlardan kaynaklı servis kullanımının engellenmesi ve sistemin zarara uğratılması olarak adlandırabiliriz.

Ağ Güvenliği

■ Servis Kullanımını Engellemeye

- Bir kullanıcı veya firma, internet güvenliğinin aşıldığı bir durumda çeşitli tehditlerle karşılaşabilir. Bu tehditlerin sonuçları kullanıcının iş alanına bağlıdır. Örneğin bazı kullanıcılar servislerin tutarlılığı ve hızı konusunda endişelenirken diğerleri bilgisayarlarındaki gizli bilgilerin gizliliği konusunda endişe duyabilirler.

Ağ Güvenliği

■ Şirket Çalışanları

- Çoğu güvenlik uzmanları, güvenlik açıklıklarını, ağı veya bilgisayarı kullanan şirket çalışanlarının başlattıklarını iddia etmektedirler. Şirket çalışanları, çoğunlukla ya şakaya ya kötü niyetle ya da yanlışlıkla kendi şirketlerinin ağına veya önemli bilgilere zarar verirler. Şirketler genelde şubelerine de ağlarına erişim hakkı verirler ve şubede çalışan insanlar da, aynı şekilde güvenlik açıklarına yol açabilirler. Bu yüzden, şirket güvenliğini sürekli kontrol etmek zorundadır.

Ağ Güvenliği

■ Kötü Amaçlı Kullanıcılar (Rebellious Users)

- Kötü amaçlı saldırılar genelde bir firma ya da kullanıcıya kayıp ya da hasar vermeye yönelikir. Eğer internete doğru güvenlik önlemlerini almadan bağlanırsanız bilgi sistemlerinizi risk altına alıdığınızı bilmelisiniz. Ağınıza bir web sunucusu kurduğunuzda potansiyel olarak tüm internetin yerel ağınıza erişebileceği bir pencereye açıyorsunuz. Sitenizin çoğu ziyaretçisi web sunucunuza amaçlandığı şekilde kullanacaktır. Fakat bazıları ağınızdaki özel bilgilere erişmeye çalışacak hatta dâhili ağınıza erişim için sistemde güvenlik açığı arayacaktır. Sistem güvenliğinizin kimlerin aşmaya çalışabileceğinden her zaman haberdar olmalısınız.

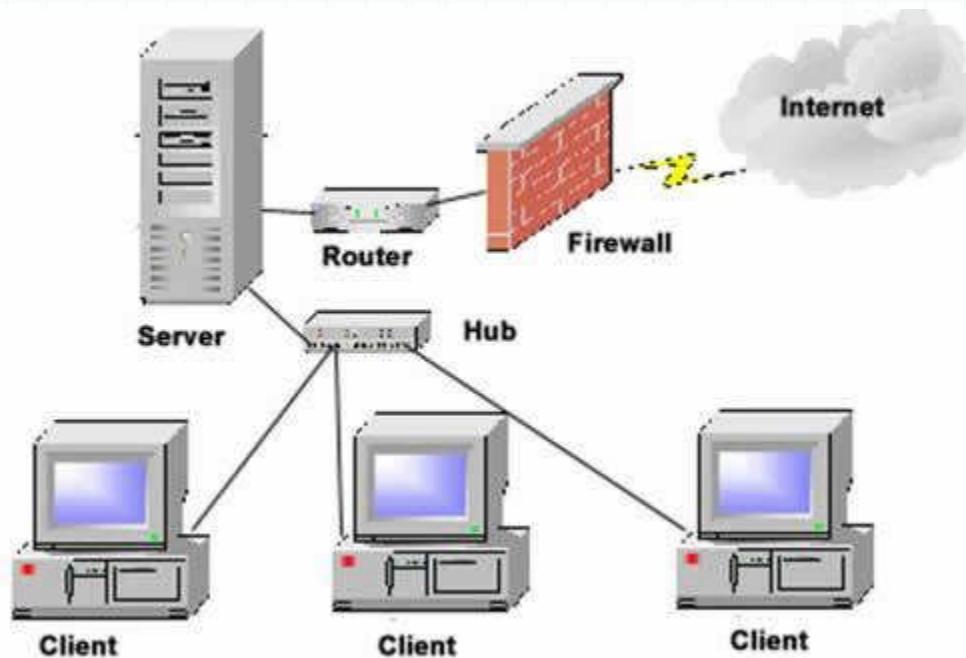
Ağ Güvenliği

- **Güvenlik Duvarı (Firewall) Cihazı**

- **Güvenlik Duvarı Nedir?**

- Güvenlik duvarı, bir sistemin özel bölümlerini halka açık (public) bölümlerden ayıran, kullanıcıların ancak kendilerine tanıyan haklar düzeyinde sistemden yararlanmasını sağlayan çözümlerdir.

Ağ Güvenliği



Şekil 1.2: Tipik bir güvenlik duvarı

Ağ Güvenliği

■ Güvenlik Duvarı Bileşenleri

- Paket-filtreleme router`ları (packet-filterin routers)
- Devre ağ-geçitleri (circuit gateways)
- Uygulama ağ-geçitleri (application gateways)

Ağ Güvenliği

■ Güvenlik Duvarı Çeşitleri

■ **Packet-Filtering Firewall**

- Bu yöntem Firewall oluşturmanın en kolay yoludur. Paketlerin başlık alanı içindeki bilgilere bakılarak istenmeyen paketler karşı tarafa geçmez. OSI modelinde 3 katman olan network katmanında çalışır.

■ **Circuit-Level Gateway**

- OSI modelinde 4 katmanı olan session katmanı düzeyinde çalışır. Bu sistemde oturum bir kez kabul edilip kurulduktan sonra, her paket için denetim yapılmaz. Paketler kurulan sanal devre üzerinden geçer.

Ağ Güvenliği

■ Application-Level Gateway

- En sık koruma yapan Firewall tekniğidir. OSI modelinde uygulama katmanı düzeyinde çalışır. Bu nedenle tam denetim yapma imkânı sunar. Bu tür düzenlemede oturum kurulduktan sonra bile paketlerin sınaması yapılmaktadır. Bundan dolayı beklenmedik saldırılara karşı korumayı güçlendirir.

Yedekleme

■ Yedekleme Nedir?

- Sabit Disk
- Yedek Sabit Disk
- RAID Sabit Disk
- Disket
- CD-R / CD-RW
- DVD-R / DVD-RW / DVD+R / DVD+RW
- Zip Disk / LS Disk
- Harici Sabit Disk
- USB Bellek

Yedekleme

- Yukarıdaki yedekleme donanımlarından herhangi biri veya birkaçını kullanarak bilgisayarınızdaki bilgilerin periyodik zamanlarda birer kopyasının alınmasına yedekleme denir. Bu işlem için günümüzde en çok CD ve disketler kullanılmaktadır.
- Periyodik zamanlarda (genelde haftada bir) bilgilerin disketlere yedek alınması gerekmektedir. Daha sonra ayda bir bu yedek alınan disketler, disketlerdeki bozulmaları önlemek için formatlanmalı (biçimlendirilmeli) ve daha sonra yeniden yedekleme işlemi yapılmalıdır. Disketler kesinlikle manyetik ortamlarda ve güneşte bırakılmamalıdır.

Yedekleme

■ Yedekleme Çeşitleri

■ Tam (Full) Yedek

- Bu yöntem, seçilen kaynağın tüm içeriğini yedekler. En güvenilir yöntemdir, ancak zaman ve kapasite ihtiyacı yüksektir. Diğer yöntemler uygulanmadan önce, en az bir kez tam yedek alınmalıdır.

■ Adımlı (Incremental) Yedek

- Bu tip yedeklemede, sadece son yedekten bu yana yedeklenmemiş olduğu tespit edilen Archive (arsiv) attribute dosyalar yedeklenir. Kurtarma sırasında önce tam yedek, sonra sırayla tüm adımlı yedekler kurtarılmalıdır. Bu nedenle güvenirlilik düşer.

Yedekleme

■ Fark (Differential) Yedeği

- Bu tip yedeklemede, son tam yedekten bu yana yedeklenmemiş olduğu tespit edilen dosyalar yedeklenir. Kurtarma sırasında önce tam yedek, sonra son fark yedeği kurtarılmalıdır. Güvenirlilik orta düzeydedir. Bazı yedekleme yazılımları, istek üzerine yapılan yedekleme işlemleri dışında, ayarları kaydedilen bir yedekleme işlemini istenen aralıklarla tekrar edecek özellikler de taşır.

Yedekleme

- **Sunucu Yedekleme (Server NT Backup)**

- Yedekleme işlemlerini, komut isteminde veya ntbackup komutu ile birlikte çeşitli parametreler kullanarak toplu iş dosyasından gerçekleştirebilirsiniz.

Kaynaklar

- ÇÖLKESEN Rıfat, **Bilgisayar Haberleşmesi ve Ağ Teknolojileri, Papatya**
- Yayıncılık, Ekim 2000.
- ÇÖLKESEN Dr.Rıfat, **Bilgisayar Haberleşmesi ve Ağ Teknolojileri,**
- ISBN:975-6797-00-2, 2002.
- DERFLER Frank J, **Network Sistemleri ve Bilgisayar Bağlantı Klavuzu,**
- Sistem Yayıncılık, Şubat 1998.
- TANENBAUM Andrev S., **Computer Networks (3. Edition), Prentice-Hall,1996**

Kaynaklar

- UTKU Selim, **Internetworking & TCP/IP**, Armada Yayıncılık 2000.
- http://www.asistbilisim.com \Ağ_Güvenliği.htm
- www.bilgisayardershanesi.com
- <http://www.bilisimsurasi.org.tr/ e-turkiye/docs/güvenlik07042004.doc,2002>
- <http://www.microsoft.com/turkiye/girisimci/themes/sgc/checklist/articles/zararlı.mspx>
- http://www.olympos.org/article/articleview/128/1/10/internet_güvenliği__bölüm_2

Kaynaklar

- http://www.olympos.org/article/articleview/1351/1/10/voip_security
- <http://www.pcnet.com.tr/>
- http://silifke.meb.gov.tr/egitim/Windows%20NT/NT_yedekleme.htm
- http://www.tepum.com.tr/secura_guvenlik_duvari.htm
- <http://www.veritim.com.tr/security.htm>