SAU Fen Bilimleri Enstitüsü Dergisi
8.Cilt, 1.Sayı (Mart 2004)



# BİLGİSAYAR AĞLARI VE GÜVENLİK

**Cüneyt BERGEL**

***Özet*** **– Bu tezde, bilgisayar ağlarının temelleri (veri haberleşme sistemleri, referans modelleri, TCP/IP protokol grubu, Lan ve Wan teknolojileri) hakkında bilgiler verilmiş ve bilgisayar ağlarında güvenliğin nasıl sağlanması gerektiği anlatılmıştır.**

***Anahtar Kelimeler*** **– OSI ve DoD modelleri, TCP/IP, LAN ve WAN teknolojileri,güvenlik.**

***Abstract*** **- In this thesis , It has been told information about basics of Computer Networks (Data Enformatic Systems, Reference Models, TCP/IP Protocol Stack, LAN&WAN Technologies) and how to secure Computer Networks.**

***Key Words*** **– OSI and DoD Models, TCP/IP,LAN and WAN Technologies,security.**

## I.GİRİŞ

Gelişmiş ve gelişmekte olan ülkelerde haberleşmenin artan öneminin iyice kavranması ve iş dünyasının iletişim ihtiyacındaki hızlı artış nedeni ile sağladığı mobilite (hareket kabiliyeti) açısından sayısal iletişim, gün geçtikçe vazgeçilemez bir haberleşme ortamı haline gelmektedir. Dünyadaki teknolojik gelişmelere paralel olarak daha iyi ses kalitesi ve sağladığı ek servisler (yüksek hızda veri iletimi, az data kaybı vs.) gibi nedenlerden dolayı iletişim analog yapıdan sayısal yapıya dönüştürülmektedir. Bilgi çağı, insanlar ve kuruluşlar arasında bilgi aktarımının hızlı ve etkin olarak yapılmasını gerektirmektedir.

Elektronik ve iletişimdeki hızlı gelişmeler dünyayı haberleşme açısından küreselleştirmektedir. Kişisel bilgisayarların ve iş istasyonlarının uygun fiyatla ve kullanımı rahat programlarla ortaya çıkması, yaşam biçimimizi değiştiren yeni teknolojileri ortaya çıkarmıştır.Bu teknolojik gelişmeler güvenlik sorunlarını da beraberinde getirmektedir.

Bilgisayar ağlarında güvenlik, vazgeçilmez bir unsur haline gelmiştir.Gizli tutulmak istenen kurumsal ve kişisel bilgiler veya web sitelerinin güvenliği çok önemlidir.Çünkü bu bilgilerin çalınması hem şirketlerin zarar etmesine, hem de prestijlerinin kaybolmasına neden olacaktır.

Bergel, SA.Ü Fen Bilimleri Enstitüsü, Elektrik ve Elektronik Mühendisliği Anabilim Dalı, Elektrik Bölümü, Adapazarı

## II.VERİ HABERLEŞME SİSTEMLERİ

Veri bir bilgisayarda saklanır ve bir haberleşme sistemi üzerinden ikilik tabanda iletilir.

Bir bilgisayardaki bitler elektrik işaretinin polarizasyon seviyeleri ile gösterilirler. Bir bilgisayardaki saklama elemanı içindeki yüksek seviye işareti 1'i ve alçak seviye işareti 0'ı gösterebilir. Bu elemanlar birlikte dizilerek belirlenmiş kodlara göre sayı ve karakterleri oluştururlar.

Veri, haberleşme yolu üzerinden bilgisayar yönlendirmeli cihazlar arasında elektrik işaretleri ve bit katarları ile iletilir. Bu elektrik işaretleri ve bit katarları harf ve karakterleri belirtir. Bazı durumlarda, veri ışık işaretleri ile gösterilir (fiber optik hatlarda). Bit dizileri kullanıcı verisini ve kontrol verisini tanımlar. Kontrol verisi, haberleşme ağını ve kullanıcı verisi akışını yönetmek için kullanılır[2].

## III. MODEL ve PROTOKOL KAVRAMLARI

### III.1 OSI Referans Modeli

OSI Referans Modeli International Standards Organization (ISO) tarafından sunulan bir model üzerine geliştirilmiştir. Bu model ISO OSI (Open Systems Interconnection) referans modeli olarak anılır.Açık sistemlerin yani diğer sistemlerle haberleşmeye açık sistemlerin bağlantısı ile ilgilenir. OSI modeli yedi tabakadan oluşur[5].

**Yedi Tabakalı Model:**

7)Uygulama: Uygulamalara değişik servisler sağlar.
6)Sunum: Bilgi formatını çevirir.
5)Oturum: Haberleşme ile ilgili olmayan problemlerle ilgilenir.
4)Taşıma: Uçtan uca haberleşme kontrolünü sağlar.
3)Ağ: Ağ üzerinde bilgiyi yönlendirir.
2)Veri Bağlantısı: Bağlı uçlar arasında hata denetimini sağlar.
1)Fiziksel: İletim ortamına bağlantıyı sağlar.

### III.2 DoD Referans Modeli

TCP/IP protokol grubu, OSI referans modeli hazırlanmadan önce oluşturulmuştur.

TCP/IP protokol grubu DoD modelini referans alır ve verilen bu model OSI modelinden farklı yapıdadır.

DoD modeli 4 ayrı katmandan oluşur. Bu katmanların OSI modelindeki karşılıkları aşağıdaki şekildedir. [5]

OSI'nin Uygulama,Sunum,Oturum katmanları DoD'un Uygulama katmanına, OSI'ini Aktarım katmanı, Aktarım katmanına ,OSI'nin Ağ katmanı, İnternet katmanına ve OSI'nin Veri-Bağlantı ve Fiziksel katmanı , Ağ arayüzü katmanına karşılık gelir.

## IV. TCP/IP PROTOKOL GRUBU

### IV.1 İnternet Katmanı Protokolleri

IP'nin sorumluluğu üst katmandan gelen segment ya da datagram'ları birbirine bağlı ağlar üzerinden iletmektir. IP bu segment ve datagram'ları TCP veya UDP'den alır.

IP (İnternet Protokolu): Temel olarak veri paketleri için bir iletim yolu belirleme işlevini yerine getirir[5].

IP'nin sağladığı fonksiyonlar :

- Global adresleme yapısı,
- Servis isteklerini tiplendirme,
- Paketleri iletim için uygun parçalara ayırma,
- Hedef hostta paketleri tekrar birleştirme.

### IV.2 Aktarım Katmanı Protokolleri

TCP (Transport Control Protocol): Uçtan-uca (End-to-end) veri dağıtım (akış) fonksiyonu sağlar. Verinin güvenli iletimi için gerekli mekanizmaları içerir.

Bu mekanizmalar Hata denetimi (checksum), Sıra numarası (sequence number), Onay (acknowledge) ve yeniden gönderim (retransmit) fonksiyonlarını içerir.

TCP güvenli ve sıralı hale getirilmiş veriyi uygulama katmanına sunar.

UDP(User Datagram Protocol):Güvenli bir iletişim fonksiyonuna gerek duyulmadığı durumlarda, uygulamalar için TCP den daha iyi bir performans sağlar.

### IV.3 Uygulama Katmanı Protokolleri

OSI referans modelindeki Uygulama, Sunum ve Oturum katmanlarının bütününe karşılık gelir.

TCP/IP Protokol grubundaki Uygulama protokolleri:

Telnet,FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System )[5]

## V. BİLGİSAYAR AĞLARINDA KULLANILAN TEKNOLOJİLER

Yerel alan ağları (LAN), aynı çalışma ortamında birbirleriyle ilgili işlerde çalışan bir topluluk içinde veri alış verişi ve bilgisayarların CPU, disk gibi kaynaklarının ve yazıcı, çizici gibi cihazların paylaşılması amacıyla geliştirilmiştir. LAN'lar da temel özellik, sistemlerin aynı ortamda veya birbirlerine yakın mesafede olmasıdır. Bu nedenle sistemler arasında kullanılacak kabloların seçiminde büyük esneklik vardır ve kablolama alt yapısı bir kez kurulduktan sonra maliyetsiz bir iletişim ortamı sağlar. Ethernet, Jetonlu Halka ( Token Ring), Jetonlu Yol (Token Bus ), 100VG-AnyLAN , ATM ve FDDI bilgisayar ağlarında kullanılan teknolojilerdir[4].

### V.1 Ethernet

Ethernet ilk olarak, deneysel çalışmaların sonucu olarak ortaya çıkmıştır. İlk Ethernet LAN 2.94 Mbps hızında idi. Ancak günümüzde bilgisayar haberleşmesine olan gereksinim artması ve mikroelektronik teknolojinin gelişmesine paralel olarak daha yüksek hızlara 10 Mbps, 100 Mbps ve 1000 Mbps gibi hızlara kadar çıkılmıştır. Günümüzde Ethernet ve türevleri olan Fast Ethernet, Gigabit Ethernet LAN tarafında vazgeçilmez bir standart haline gelmiştir[3].

### V.2 Yüksek Hızlı Ethernet (Fast Ethernet ,Gigabit Ethernet)

Ethernet ilk olarak kalın koaksiyel kablo üzerinden 10 Mbps hız için tanımlanmıştır. Daha sonra bazı sınırlamalar dahilinde, daha ekonomik olan ince koaksiyel uyarlaması yapılmıştır. Ancak, bakır büklümlü çift ( UTP veya STP ) ve fiber optik (FO) kabloların veri iletişiminde kullanılması, fiziksel olarak yıldız topolojinin yaygınlaşması ve her geçen gün daha yüksek hızlara olan gereksinimden dolayı yüksek hızlı Ethernet teknolojileri ortaya çıkmıştır. Fast Ethernet ve Gigabit Ethernet olarak adlandırılan bu teknolojiler sayesinde, 100 Mbps ve 1 Gbps hızlara çıkılmaktadır.

### V.3 100VG –AnyLAN

100VG-AnyLAN, IEEE'nin 802.12 komitesi tarafından tanımlanmış yüksek hızlı bir LAN teknolojisidir. 100Base–T gibi 100Mbps'lik bir iletim ortamı sunar. Bu teknolojide yola erişim için Ethernet'te olduğu gibi CSMA/CD yöntemi kullanılmaz. CSMA/CD'ye göre erişim zamanı daha öngörülebilir bir yöntem olan DPMA (Demand Priority Access Medhod ) yöntemi kullanılır. DPAM, CSMA/CD'de çatışmalardan dolayı oluşan zaman kaybını yok eden ve portlara merkezi denetimli erişim sağlayan bir yöntemdir.

### V.4 Jetonlu Halka (Token Ring)

İlk olarak IBM firması tarafından (1970'li yıllarda) geliştirilen Jetonlu Halkada (Token Ring , TR) düğümler birbirlerine halka biçiminde bağlanırlar. Aktarım hızı olarak 4 ve 16 Mbps olan iki uygulaması vardır[3].

### V.5 FDDI (Fiber Distributed Data Interface)

FDDI, iki yollu halka topolojiye sahip türevine göre 100 ile 2 Mbps'e kadar band genişliği sunan ve temelde fiber optik kablo kullanılmasına dayanan bir ağ teknolojisidir. Bir LAN teknolojisi olarak geliştirilmesine karşın, Ethernet ve Jetonlu Halka tabanlı LAN'ların daha ucuz çözüm sunmaları ve uygulamada baskın olmalarından dolayı, FDDI daha çok büyük LAN uygulamalarında veya kampus uygulamalarında Omurga (Backbone) ağ oluşturmak için kullanılmıştır[1].

## VI. BİLGİSAYAR AĞLARINDA GÜVENLİK

Son yıllarda intemetin ve internet üzerindeki ticaretin gelişmesiyle birlikte, ağlar oluşabilecek saldırılara karşı zayıflık gösterıneye başlamıştır.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 hala büyük bir tehlike oluşturmaktadır.

Günümüzde internet gerek kişisel gerekse iş ilişkileri arasındaki bilgi akışını sağlayan, dünyanın en büyük letişim aracı haline gelmiştir. İnternetin tüm dünyada öylesine yaygın kullanımı, güvenlik tehlikelerini de rtırmaktadır. Önemli bir bilgi kaybı olabilir, gizlilik lal edilebilir (kredi kartı numarasının bulunması gibi) eya saatler hatta günler süren yükleme zamanları rtaya çıkabilir. İnternetteki bu tür güvenlik açıkları, sanları internete karşı güvensizleştirebilir ve web tabanlı şirketlerin sonunu hazırlayabilir. Bu yüzden şirketler, güvenliklerini her geçen gün arttırmakta ve yeni tehditlere karşı önlem almak amacıyla yatırımlarını sürdürmek zorundadırlar.

### VI.1 Güvenlik Mimarisinin Kurulması

Güvenlik mimarisinin merkezinde kurumun güvenlik politikası olmalıdır ve bu politikalar kurumun yöneticileri tarafından desteklenmelidir.Politikaların tanımının ardında, onun nasıl uygulanacağını anlatan prosedür ve kılavuzlar hazırlanmalı, çalışanların politikalara uymamasının bir karşılığı olacağını ve şirketin konu üzerinde ne kadar titizlikle durduğunu anlamalıdırlar[6].

### VI.2 Güvenlik Politikalarının Belirlenmesi

Kurumların kendi kurmuş oldukları ve internet'e uyarladıkları ağlar ve bu ağlar üzerindeki kaynakların kullanılması ile ilgili kuralların genel hatlar içerisinde belirlenerek yazılı hale getirilmesi ile ağ güvenlik politikaları oluşturulur. Güvenlik politikasının en önemli özelliği yazılı olmasıdır ve kullanıcıdan yöneticiye kurum genelinde tüm çalışanların, kurumun sahip olduğu teknoloji ve bilgi değerlerini nasıl kullanacaklarını kesin hatlarıyla anlatmasıdır. Güvenlik politikası olmadan güvenli bir bilgisayar ağı gerçekleştirilemez[8].

Ağ güvenliğinin sağlanması için gerekli olan temel politikalar aşağıda sıralanmıştır:

1-Erişim politikası,

2-Ağ güvenlik duvarı (firewall) politikası,

3-İnternet politikası,

4-Şifre yönetimi politikası,

5-Fiziksel güvenlik politikası,

6-Sosyal mühendislik politikası.

### VI.3 Güvenlik Cihazları

**Firewall (Ateş Duvarı):** Bir güvenlik duvarı, şirketlerin özel ağları ile internet gibi herkesin kullanımına açık ağ arasında güvenlik sağlar. Bu iki ağ arasındaki tüm trafik güvenlik duvarı tarafından incelenmelidir.Güvenlik duvarından sadece izin verilen trafik geçebileceğinden internet ile özel ağlar arasındaki haberleşmenin serbestlik seviyesini kontrol etmede kullanabilir[7].

**IDS (Saldırı Tesbit Cihazı):** IDS ürünü network ve

host tabanlı olmak üzere iki çeşidi vardır.Network tabanlı IDS ağdan geçen tüm trafiği inceler, host tabanlı IDS ise kendi üzerinden geçen tüm trafiği inceler.Her iki IDS'in de çalışma mantığı aynıdır.Gelen-giden tüm data trafiğini dinleyerek, üzerinde tanımlı bulunan ataklar ile tüm data paketleri karşılaştırır. Eğer tanımlı bulunan bir atakla incelediği paketi eşleştirirse, o atağa atanmış olan görevi yerine getirir.Örneğin, atak yapan host'u bir saat boyunca bloklama yaptırılabilir[8].

## VII. SONUÇ

Bilgisayar ağlarının yaygınlaşması toplumu oluşturan çeşitli bireyler arasında hızlı, zahmetsiz iletişim ve bilgi paylaşımı sağlamaktadır.

Bilgisayar iletişimi, bilgi ve servislerin bir iletişim ortamı üzerinden belirli kurallar çerçevesinde paylaşımıdır.

Bilgisayar ağları, bilgisayar kaynakları ve elektronik nesne paylaşımını amaçlayarak başladı ve bir iletişim, paylaşım, dayanışma ve ortak çalışma ortamına dönüştü.

Bu gelişmelerle beraber bilgisayar ağlarında güvenliğe ihtiyaç duyulmaya başlandı.

Bilgisayar ağlarında kullanıcıların kullanımından kaynaklanan hatalardan, kullanılan işletim sistemlerinden veya ağ protokollerinden kaynaklanan güvenlik açıkları gün yüzüne çıkmaya başladı. Eğer güvenli bir bilgisayar ağı isteniyorsa, mutlaka güvenlik politikaları oluşturulmalı, alınacak güvenlik cihazları ihtiyaçlara göre belirlenmeli ve ona göre konfigürasyon edilmelidir.

Bunun yanında kişilere gerektiği kadar erişim sağlamalı ve kişiler bu konular hakkında bilinçlendirilmelidir.

## KAYNAKLAR

[1]. Tanenbaum A. S., Computer Networks(3.Edition), Prentice-Hall, 1996
[2]. Stallings W.,Data And Computer Communications, Prentice-Hall, 1997
[3]. Çölkesen R.,Bilgisayar Haberleşmesi ve Ağ Teknolojileri, Papatya Yayıncılık-Ekim 2000,2. Baskı
[4]. Derfler F. J.,Network Sistemleri Ve Bilgisayar Bağlantı Kılavuzu,Sistem Yayıncılık, Şubat 1998 2.Baskı
[5]. UTKU S., Internetworking & TCP/IP,Armada Yayıncılık 2000,3.Baskı
[6]. Yelkenci İ.,Güvenlik Politikasız Güvenlik NereyeKadar?,2002, http://www.guvenlikhaber.com/koseyazisi.asp?ID=8
[7]. Holbrook J.P., Reynolds J.K., The Site Security Handbook,RFC-1244,Jul-01-1991, http://rfc.net/rfc1244.html
[8]. Acceptable Use Policy Template, SANS Enstitute, http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf
[9].Karaaslan E.,Ağ Güvenlik Duvarı Çözümü Oluşturulurken Dikkat Edilmesi Gereken Hususlar, Akademik Bilişim,2003