Internet'te Veri Güvenliği

Data Security on the Internet

Umut AL*

Öz

Bu makalede Internet'te veri güvenliği hakkında genel bilgiler verilmekte, kriptografi, kriptografinin uygulama şekilleri ve şifreleme konuları özetlenmektedir. Ayrıca, ağ üzerinde veri güvenliği için kullanılan bir araç olan ateş duvarları, kavramsal olarak incelenmektedir.

Anahtar sözcükler: Veri güvenliği, Kriptografi, Şifreleme, Ateş duvarları.

Abstract

This article gives general information about data security on the Internet, summarizes topics of cryptography, application types of cryptography and encryption. In addition, firewalls, that are used as a means for data security on the network, are examined conceptually.

Keywords: Data security, Cryptography, Encryption, Firewalls.

Arş. Gör.; Hacettepe Üniversitesi Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bölümü (umutal@hacettepe.edu.tr)

Giriş

Yaşamdaki önemli olgulardan bir tanesi güvenliktir. İnsanlar güvenlik bakımından herhangi bir sorunla karşılaşmak istemezler. Olayın elektronik ortamdaki boyutu ise veri güvenliğidir. Internet'in devreye girmesiyle verilerin güvenliği konusu daha fazla önem kazanmıştır. Daha önceleri verilerin bozulması veya kaybolması gündemdeyken, internet ile birlikte verilerin başkaları tarafından kullanılması, kopyalanması veya değiştirilmesi konuları ön plana çıkmaktadır.

İnsanlar verilerini kaybetmemek için önlemler almaktadırlar. Değişik yollarla alınan önlemler insanları rahatlatsa da, bu işin uzmanları tarafından kabul edilen gerçek, ağ ortamında güvenliği yüzde yüz sağlanmış bir bilgi yığını olmadığı şeklindedir. Çünkü her geçen gün, bu konuyla ilgili yeni teknolojiler üretilmektedir. Söz konusu teknolojilerin belirli kişi ya da kuruluşların elinde bulunması ve ticaretinin yasalarca yasaklanmış olması karamsarlığa düşülmemesi için mantıklı bir neden gibi gözükse de, asıl sorun; söz konusu teknolojiler, gücü olan herkesin eline geçtiği zaman ortaya çıkacaktır.

Elektronik ortamda şifre kırmak veya şifre çözmek, gerçek hayattakinden daha kolaydır. Bu alandaki uzmanların amacı, genellikle kendilerinin neleri başarabileceğini göstermektir. Fakat madalyonun diğer yüzünde bu işi ticari çıkar ve hatta başkalarına zarar vermek için yapanlar vardır ki; asıl korkutucu olan da budur.

Bilgilerin Doğruluğu ve Güvenliği

Internet aracılığı ile erişilen bilgi kaynaklan ile ilgili en önemli sorunlardan birisi de bilgilerin doğruluğu ve güvenliğinin sağlanmasıdır. Internet'ten sağlanan bilgilerin doğrulanabilmesi ve aslına uygun olup olmadığının araştırılması (authentication), elektronik ortamdaki bilgilerin, aradan geçen zaman içinde günlenmesi ya da transfer anında kolayca değiştirilebilmesi, veri bütünlüğü ve veri güvenliği ile ilgili sorunları da beraberinde getirmektedir. Bu tür sorunlara çözüm bulmak ve elektronik belgelerin aslına uygun olup olmadığım belirlemek amacıyla, çeşitli algoritmalar ve elektronik damgalama (time stamping) teknikleri geliştirilmektedir. Gerek bilimsel belgelerin, gerekse kişilere ait finans ya da sağlık bilgileri içeren veri tabanlarının kolayca değiştirilebilmesi insanları endişelendirmektedir (Kurbanoğlu, 1995; Tonta, 1996, s. 223).

Yücel (1997, s. 2) iletişimin güvenli olarak yapılabildiği elektronik bir ortamın kullanıcıya sağlaması gereken üç niteliğin bulunduğunu ifade etmektedir. Bunlar:

1. **Kimlik:** Alıcı olan taraf, bilgiyi gönderenin kimliğinden emin olabilmelidir. Diğer bir deyişle, kimlik bilgisini içeren elektronik imza taklit edilemez olmalıdır.
2. **Bütünlük:** Bilgiyi gönderen ve alan taraflar, bilginin bütünlüğüne, yani üçüncü bir kişi tarafından en ufak bir değişikliğe uğratılmamış olduğuna güvenebilmelidir.
3. **Gizlilik:** Eğer istenirse, gönderilen bilgi, yalnız bilgiyi alan kişi tarafından çözülecek ve üçüncü kişilerden gizlenebilecek şekilde şifrelenebilmelidir.

Internet'te Genel Güvenlik Sorunları

Internet'te güvenlik denince akla ilk olarak yetkisiz kişilerin paylaşımlı bilgisayarlara sızıp bilgi hırsızlığı yapması veya bilgilere zarar vermesi gelmektedir. Gerçekten de en ciddi zararlar bu şekilde verilmektedir. Ancak buradaki sorun, iletişim ağından çok kullanılan uygulama katmanı yazılımlarının (telnet, ftp, http vb.) ve sunucu (server) tarafindaki işletim sisteminin tasarım hatalarıdır. Bu tür güvenlik sorunları "uzaktan erişim" sorunları olarak adlandmlmaktadır. Günümüzde bu sorunların çözümü olarak ateş duvarları (firewall) yaygın oiarak kullanılmaktadır. Ateş duvarı, iç ağı dış ağdan, bir başka ifadeyle Internet'ten ayıran bir duvar olarak düşünülebilir. Ateş duvarlarının temel işlevi güvenlik gediği olan uygulamalara ait veri paketlerinin iç ağa ulaşmasını engellemektir. Böylelikle, iyi veya kötü niyetli olduğuna bakılmaksızın, hiç kimse ağ dışından ağ içine izin verilen uygulamalar dışında erişim sağlayamayacaktır (Levi ve Çağlayan, 1997).

Bir bilgisayar sisteminin en önemli parçaları; yazılım, donanım ve veridir. Bilgisayar sisteminin güvenliğini tehdit eden 4 öğe bulunmaktadır:

- Düzenini bozma (interruption): Bu işlemin sonucunda bilgisayar sistemindeki veriler kaybolur, erişilemez veya kullanılamaz hale gelir.
- Durdurma (interception): İzin verilmeyen grupların, ulaşmaması gereken verilere erişim hakkı kazanmasıdır. Bu çeşit bir tehdide örnek olarak, ağ ortamındaki bir programın veya dosyanın kanuna aykırı bir şekilde kopyalanması gösterilebilir.

- Değiştirme (modification): Sadece erişimle kalmayıp, bir değiştirme olayı söz konusu olursa, bu da sistem güvenliğini tehdit eder. Örneğin bir kişi, izni olmadan herhangi bir veri tabanındaki değerleri değiştirebilir.
- Fabrikasyon (fabrication): İzin verilmeyen grup ya da kişiler bilgisayar sistemi üzerindeki nesnelerin taklidini yapabilirler. (Pfleeger, 1997, s. 3-4)

Genel olarak ağ güvenliğinden söz edildiğinde akla gelen diğer bir sorun da açık kanallarda dolaşan bilginin gizliliği ve bütünlüğüdür. Bilgi gizliliği, verinin alıcısı dışında hiç kimse tarafından okunamaması, bilgi bütünlüğü ise, verinin değişmeden alıcısına ulaşması anlamına gelmektedir. Kimlik kanıtlama sistemleri, oluşturdukları oturum anahtarları ile bu sonardan çözebilmektedir. İlk bakışta pek önemsenmeyen, ama bazı uygulamalarda gerekli olan diğer bir güvenlik sorunu ise, inkar edememedir (non-repudiation). Özellikle doğrudan doğruya parayla ilgili uygulamalarda ortaya çıkan bu sorun, göndericinin gönderdiği bir mesajı daha sonra inkar edememesi, etse bile alıcının, gönderenin mesajı gönderdiğini üçüncü kişilere ispat edebilmesi zorunluluğundan kaynaklanmaktadır. (Levi ve Çağlayan, 1997).

Kriptografi

Kriptografinin Türkçe karşılığı şifre yazımdır. Kriptografi terimi, Yunanca gizli anlamına gelen "kript" ve yazı anlamına gelen "graf"dan türetilmiştir. Kriptoloji ise şifrebilimdir. Şifre kelimesi ise Fransızcadaki "chiffre" yani sayı kelimesinden gelmektedir (Türkiye Kriptografi Sayfaları, 1997).

Kriptografı, bilgiyi şifrelemek ve şifresini çözmek için kullanılan bir matematik bilimidir. Çoğu kişi için kriptografi, sadece haberleşmeyi gizli tutmakla ilgilidir.

Kriptografi, önemli bilgilerin depolanmasını veya güvenli olmayan ağ ortamında yollanmasını, bilgilerin alıcıdan başkası tarafından okunamayacak ve anlaşılamayacak şekle getirilmesini sağlamaktadır. Kriptografi, bilgi güvenliği bilimi iken, kriptoanaliz, güvenli iletişimi analiz etme ve onu kırma, bir başka ifadeyle, farklı amaçlar için şifresini çözme bilimidir. Kriptoanalizle uğraşan kişilere kriptoanalist adı verilmektedir. Kriptoanalistler, aynı zamanda elektronik ortamdaki bilgilere saldırıda bulunan kişiler (attacker) veya daha güncel ismiyle hackerlar olarak bilinmektedirler (Erdun, 2000, s. 206).

Kriptografik algoritma, şifreleme ve şifre çözüm İşlemlerinde kullanılan matematikse! bir işlev topluluğudur. Kriptografik algoritmalar, sade-metni şifrelemek İçin bir anahtar (kelime, rakam veya değişik uzunluktaki sözcük) ile birlikte çalışır. Bu anahtar, genellikle kişiye özel ve gizlidir. Her kişinin farklı anahtarları olabilir. Farklı anahtarın kullanımı ile sade-metin aynı olsa bile, birbirinden farklı şifreli metinler elde edilebilir. Şifrelenmiş bilginin güvenliği tamamen iki şeye bağlıdır; kriptografik algoritmanın gücü ve anahtarın gizli tutulması. Kriptografik algoritma ne kadar güçlü olursa olsun, gizli anahtar açığa çıkartıldığı anda çok fazla bir anlamı kalmayacaktır. Algoritma bilinip anahtar bilinmiyorsa, kriptoanalistlerin yapacağı tek şey onu tahmin etmektir. Günümüzde kullanılan anahtarlar çok büyük olduklarından, hesap yoluyla tahmin etmek çok zordur; fakat imkansız değildir. (Erdun, 2000, s. 206-208)

Bugünün kriptografisi, şifreleme ve şifre çözmeden çok daha fazlasını içermektedir. Kriptografı bazı mekanizmalara sahiptir. Bu mekanizmalar, kaynaklara erişimi kontrol altına almak için kullanılmaktadır. Yeni ifadesiyle kriptografi, farklı problemlerin varlığına bağlı olan teknik ve uygulama çalışmaları olarak nitelendirilebilir. Kriptoanaliz ise, yukarıda verilen tanımından daha masum bir ifade ile, kriptografık mekanizmanın anlaşılması ve çözümü çalışmalarım içermektedir. Doğal olarak böyle çalışmalar sonucunda bir bilim dalı ortaya çıkmıştır ki, bu kriptolojidir. Modern kriptografi gittikçebüyürken, bunu algoritmanın temelinde "çözülmesi zor problemler"i kullanarak gerçekleştirir. Şifreli metnin şifresinin doğrudan çözülmesi, ancak bu fonksiyonun tersinin bilinmesiyle mümkündür. Şu ana kadar böyle bir çözüm bulunmadığından, şifreli metnin çözümü ancak tahminlerle yapılabilir. (Erdun, 2000, s. 208)

Kriptoanaliz, kodlan kırma, sırları deşifre etme, doğru düzenleri bozma ve genelde kriptografık protokolleri kırma bilimidir. Güçlü bir şifreleme algoritmasının veya kriptografik protokolün tasarımım yaparken, onun herhangi bir zayıf yönünü bulmak ve düzeltmek için kriptoanaliz kullanmak gereklidir. Bu durum, en güvenilir şifreleme algoritmalarıyla, genel güvenliği sağlamlaştırmak şeklinde özetlenebilir (Erdun, 2000).

Erdun (2000) kriptografının, dünyadaki mevcut güvenin, elektronik ortama taşınmasında önemli bir rol oynadığını ifade etmektedir. Bu bakış açısıyla, kriptografi olmasaydı, kriptoanalistler veya modern adıyla "hacker"lar, elektronik postaların içine girerek özel mesajları okuyabilir; kredi kart numaralarını alarak kullanabilir, cep ve diğer

telefonlarım dinleyebilir, banka hesaplarına girerek parayı sahibinin adına harcayabilirlerdi.

Kriptografinin Uygulama Şekilleri

Kriptografi güvenli haberleşme, elektronik ticaret, tarama ve doğrulama gibi farklı alanlarda kullanılmaktadır (Erdun, 2000, s. 210-212).

Güvenli haberleşme: Kriptografinin en belirgin kullanım biçimlerinden biridir. İki kişi, birbirlerine gönderdikleri mesajları şifreleyerek güvenli bir şekilde haberleşebilirler. Bu işlem, üçüncü kişinin mesaja kulak misafiri olması durumunda, mesajın asla deşifre edilemeyeceği şekilde yapılabilir. Güvenli haberleşme, yüzyıllardır mevcutken, şifrelemenin anahtar yönetim sorunu, onun sıradan bir şey olmasını ortadan kaldırmıştır.

Tanıma (Identification) ve doğrulama ***(Authentication):*** Tanıma ve doğrulama, kriptografinin geniş bir alanında kullanılan iki uygulamadır. Tanıma, birisinin veya bir şeyin kimliğini belirleme işlemidir. Örneğin, bir bankadan para çekeceğiniz zaman veznedar, hesabın sahibi olup olmadığınızından emin olmak için sizden bir kimlik sorar. Bu işlemin aynısı, elektronik ortamda kriptografi kullanarak yapılmaktadır. Kriptografinin diğer önemli uygulaması doğrulamadır. Hem doğrulama, hem de tanıma kaynaklara erişime izin verme bakımından, birbirlerine benzemektedir; fakat bir kişinin kimliğini belirleme zorunluluğu olmadığından dolayı, doğrulama uygulaması daha yüzeyseldir. Doğrulama, yalnızca kişi veya varlığa, sorudaki her neyse onun için yetki verilip verilmediğini belirler.

Elektronik Ticaret: Son yıllarda, internet üzerinden idare edilen iş miktarında da büyük bir artış olmuştur. İşin bu şekilde yürütülmesi elektronik ticaret olarak isimlendirilir. Elektronik ticaretin uygulamalarından bazdan, çevrimiçi bankacılık, çevrimiçi komisyon-devir hesaplan ve internet alışverişidir.

Şifreleme

Şifreleme, veri güvenliğini sağlamada en güçlü araç olarak görülmektedir. Şifreleme veriler için gizlililiğin yanında, doğruluğu da sağlamayı amaçlamaktadır. Çünkü veriler genellikle okunamadığı gibi, anlamlı yöntemlerle de değiştirilememektedir. Şifreleme bilgisayar güvenliğinde önemli bir araçtır, ancak kullanıcılar şifrelemenin veri güvenliği ile ilgili bütün problemleri çözemeyeceğini bilmelidirler (Pfleeger, 1997, s.13).

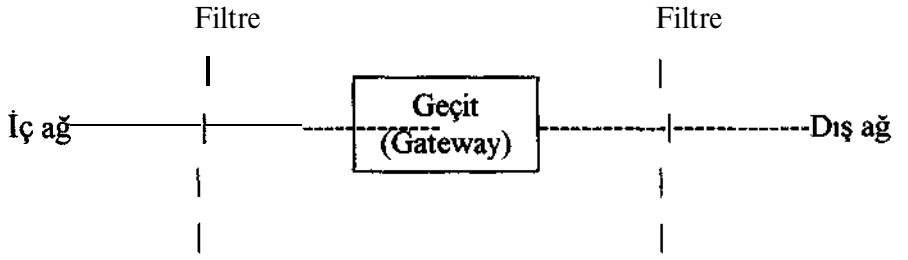
Şifreleme konusunda karar verilmesi gereken bazı konular bulunmaktadır. Bu konuların başında, şifrelemenin nerede yapılacağı gelmektedir. Bu konuda iki alternatif mevcuttur. Bunlardan biri IP (Internet Protokol) yığınında, diğeri ise uygulama yazılımı seviyesinde şifreleme yapmaktır. Şu anda piyasada var olan ürünlerin % 70'ten fazlası, IP yığınında şifreleme yapmaktadır. Bu yöntemdeki yaklaşım, kurulmuş olan bir bağlantı üzerindeki bütün verilerin şifrelenmesine dayanmaktadır. Bankalar gibi, güvenlik konusunda titiz davranan kurumlar için bu oldukça iyi bir yaklaşım olarak kabul edilmektedir. Yerel ağdan dışarı giden her şey şifrelenmekte, böylece mümkün olan en üst düzeyde güvenlik sağlanmaya çalışılmaktadır. Bu yaklaşımın dezavantajı, fazla merkezi işlem ünitesi (CPU-Central Processing Unit) zamanı almasıdır. Şifrelemeyle ilgili

işlemler, karmaşık hesaplamaya dayalı işlemlerdir. Dolayısıyla, gelen ve giden her şeyin şifrelenmesi, çok fazla CPU zamanı alacaktır. Bu, ağın transfer hızına da yansıyacak, birim zamanda aktarılan veri miktarını düşürecektir. Şifrelemenin yapılacağı yer konusundaki diğer bir alternatif, uygulama seviyesinde şifrelemedir. Bu yaklaşımın avantajı, ağ yöneticisinin, neyin şifrelenip neyin şifrelenmeyeceğine karar verebilmesidir. Böylece ağ yöneticisi, şifrelenmesine ihtiyaç olmadığını düşündüğü verilerle ilgili zaman kaybının önüne geçebilecek, bu da CPU zamanından kazanılmasını sağlayacaktır. Ancak böyle bir çalışma düzeninde, veriyi alacak olan tarafın, nelerin şifrelenip nelerin şifrelenmediğini bilmesi gerekmektedir (İTÜ, 2000).

Ağ yöneticisi, şifrelemenin nerede yapılacağına karar verdikten sonra, düşünmesi gereken ikinci şey, şifrelemenin nasıl yapılacağı, hangi tekniğin kullanılacağıdır. Şu an için en iyi bilinen ve en çok kullanılan yöntem Veri Şifreleme Standardı (Data Encryption Standard - DES)'dır. İlk olarak 1970'lerin başında geliştirilen ve Amerika Birleşik Devletleri tarafından 1977'de son hali verilen DES, çözülmesi en zor algoritma olarak kabul edilmektedir (İTÜ, 2000).

Ateş Duvarları

Kişisel kullanıcıların Internet'te, verilerini en düşük maliyetle korumasını sağlayan en önemli araçlardan birisi ateş duvarlarıdır. Ateş duvarı, iç ağ ile dış ağ arasındaki tüm veri trafiğini filtrelemektedir (Pfleeger, 1997). Ateş duvarları sayesinde sisteme istenmeyen girişler engellenmektedir. Aşağıda bir ateş duvarı şematik olarak gösterilmektedir.



Şekil: (Cheswick ve Bellovin, 1995, s. 52)

Ateş duvarlarının belli bir maliyeti vardır. Bu maliyet şunları içermektedir:

- Donanımın satın alınması
- Donanım oluşturma
- Yazılım geliştirme veya satın alma
- Yazılımın güncelleme
- Yönetimsel kurulum ve eğitim
- Sorunları gidermek İçin harcanacak zaman ve para (Cheswick ve Bellovin, 1995, s. 51-52)

Geleneksel olarak ateş duvarları, kurum ile dış dünya arasına yerleştirilir. Fakat büyük bir organizasyon, iç (internal) ateş duvarlarına da ihtiyaç duyabilir. İç ateş duvarları kurmak için birçok neden vardır. Bunlardan en önemlisi, bir şirkette çalışanların tamamının, şirket içindeki tüm bilgilere erişiminin istenmemesidir. Bu gibi durumlarda, iç ateş duvarları, farklı yetkilerdeki kişilerin, erişmesi gereken verilerin de farklı olacağı düşüncesinden hareketle kullanılmaktadır (Cheswick ve Bellovin,

1995, s. 53).

Ateş duvarlarının da yetersiz kaldığı durumlar bulunmaktadır. Bir ateş duvarının, verileri kontrol eden ve sistemi çeşitli virüs veya trojanlardan koruyan bir virüs programının yerini alamayacağı ifade edilmektedir. Ateş duvarları, belirli bazı sunucuları tanımlayıp, indirdiklerinizi kontrol edebilir, fakat her sunucuyu da tanımlayabilmesi oldukça zordur (Bıktım, 2000, s. 240).

Ateş duvarları kolay uygulanabilirliği yüzünden yaygın olarak kullanılmaktadır. Ancak "ya hep ya hiç" mantığındaki bu çözümün, kesin çözüm olmadığı da açıktır. Birçok kuruluş sadece izin verdiği kişilerin kendilerine ulaşmasına olanak tanıyan sistemler kurmak istemektedir. Bu da ancak, kimlik kanıtlama (authentication) özelliği olan sistemlerle mümkün olabilmektedir. Kimlik kanıtlama sistemleri, şifrelemeye dayalı sistemlerdir. İstemci ile sunucu bir protokolle aralarında haberleşerek ortak bir sırrı paylaşırlar. Böylelikle, birbirlerinin kimliklerinden emin olurlar. Açık kanallardan giden bilginin, yetkisiz insanlar tarafından öğrenilmesini engellemek için şifreleme yöntemleri kullanılır. Bu şekilde, insanların birbirlerinin kimliklerini kullanması önlenir. Bunun dışında, iletişimde bulunan taraflar ortak bir oturum anahtarı üzerinde anlaşarak, aralarında ilettikleri veriyi şifrelerler. MIT (Massachusetts Institute of Technology) tarafından geliştirilen Kerberos[1], yaygın olarak kullanılan özel anahtar (private key) tabanlı bir kimlik kanıtlama sistemidir. Bunun dışında açık anahtar (public key) tabanlı kimlik kanıtlama sistemleri de vardır (SecurelD, SSL, SET, vb.). Açık anahtar şifreleme algoritmaları,

[1] Kerberos, Yunan Mitolojisi'ndeki, ölüler dünyasının kapısını bekleyen üç başlı köpeğin ismidir.

yapılarından dolayı yavaştırlar, fakat kırılmaları güçtür ve anahtar dağıtım sorunu da özel anahtar tabanlı sistemlere göre daha azdır. Açık anahtar tabanlı sistemler bankacılık, elektronik alışveriş ve elektronik ödeme gibi paraya dayalı Internet uygulamalarında daha güvenli olduğu için tercih edilmektedir. Ancak performans düşüklüğü, bu açık anahtar tabanlı sistemlerin gerçek zamanlı uygulamalardaki şansını azaltmaktadır (Levi ve Çağlayan, 1997).

Sonuç

Günümüzdeki teknolojilerle yapılması gereken şey, elimizdeki verilerin istenmeyen şekilde kullanılması, zarara uğratılması veya yok edilmesini önlemek için çalışma yapmaktan ibarettir. Internet'teki verilerin önem derecesi ile korunma yöntemleri arasında doğru bir orantı bulunmaktadır. Örneğin; bir ülkenin merkez bankasındaki koruma ile, küçük bir iş yeri sahibinin koruma yöntemleri birbirinden farklıdır. Merkez bankası üst düzey güvenlik önlemleri (şifreler, güvenlik görevlileri, bilgisayar sistemleri, kameralar vb.) uygularken, küçük iş yerlerinin kapısının kilitlenme yoluna gidilerek güvenliğinin sağlanması çok sık görebileceğimiz bir uygulamadır. İşte gerçek hayatta var olan bu örneği, sanal ortama taşıdığımız zaman ortaya çıkan en çarpıcı sonuç, önemli verilerin korunması için ekstra güvenlik önlemleri almak gerektiğidir. Internet'te, ateş duvarları gibi araçlar kullanılarak güvenlik sağlanmaya çalışılsa da, ağ ortamının kendine has özellikleri bu çabaların karşısında yeni teknolojiler üretmekte ve veri güvenliğini tehdit etmektedir. Bu nedenle Internet'te veri güvenliği konusundaki gelişmeleri takip etmek yararlı olacaktır.

KAYNAKÇA

Bıktım, E. (2000). Saldırılardan korunun. *CHIP*, 4: 238-240.

Cheswick, W. R. ve Bellovin, S. M. (1995). *Firewalls and Internet security: repelling the willy hacker.* Massachusetts: Addison-Wesley.

Erdun, H. (2000). Kodlama teorisi. *PC LIFE2:* 206-214.

İTÜ. (2000). Internet güvenliğine bir bakış [Çevrimiçi]. Elektronik adres: http://www.itu.edu.tr/bid/bilgi/guvenlik2.htm [24 Mart 2002].

Kurbanoğlu, S. (1995). Elektronik uzayda suç ve ceza. *Hacettepe Üniversitesi Edebiyat Fakültesi Dergisi,* 12(1/2): 167-186.

Levi, A. ve Çağlayan, M. U. (1997). Elektronik posta güvenliği için PGP kullanımı. [Çevrimiçi]. Elektronik adres: http:// mercan.cmpe.boun.edu.tr/~levi/AS97.HTM [29 Mart 2002].

Pfleeger, C. P. (1997). *Security in computing.* Upper Saddle River. NJ: Prentice-Hall.

Tonta, Y. (1996). Internet, elektronik kütüphaneler ve bilgi erişim. *Türk Kütüphaneciliği,* 10(3): 215-230.

Türkiye Kriptografi Sayfaları (1997). Kriptografiye küçük bir giriş [Çevrimiçi]. Elektronik adres: http://gsu.linux.org.tr/kripto-tr/kripto-giris.html [24 Mart 2002].

Yücel, Melek D. (1997) Açık iletişim ağlarında bilgi güvenliği [Çevrimiçi]. Elektronik adres: http://www.tuena.tubitak.gov.tr/rapor/pdf/2103-M-T-A-02.pdf [21 Mart 2002].