Internet'te Veri Güvenliği

Giriş

İnsanoğlu varlığının ilk dönemlerinden itibaren güvenliğe gereksinim duymuştur. İnsanlar güvenlik açısından herhangi bir sorun ile karşılaşmak istememektedir. Gereksinim üzerine çalışan araştırmacıların listesinde her zaman güvenlik gereksinimi yerini almıştır. Elektronik ortamın, yaşamın vazgeçilmez bir parçası haline gelmesine paralel olarak, günümüzde fiziksel güvenlik kadar elektronik ortamdaki güvenliğin de önem kazandığı bilinmektedir. Özellikle Internet gibi açık iletişim ağlarındaki kullanıcılar amaçları farklı kişiler tarafından tehdit edilmektedir. Söz konusu tehdit kimi zaman ciddi boyutlarda zaman, para ve emek kaybına neden olabilmektedir.

İnsanlar verilerini kaybetmemek için farklı önlemler almaktadır. Değişik önlem alma teknikleri kullanılmakla birlikte; ağ ortamında güvenliği yüzde yüz sağlanmış bir bilgi yığını bulmak hemen hemen imkânsızdır. Çünkü her geçen gün, konuyla ilgili yeni teknolojiler üretilmektedir (Al, 2002:39). Sürekli olarak iki grup (güvenliği artırmaya çalışanlar ve güvenlik açıklarını ortaya çıkaranlar) karşı karşıya gelmekte ve ürettikleri teknolojilerle adeta birbirlerine meydan okumaktadır. Kimi zaman güvenliği artırmaya çalışanlar ile güvenlik açıklarını ortaya çıkaranlar aynı kişi ya da gruplar olabilmektedir.

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) tarafındaki işletim sisteminin tasarım hatalarıdır. Bu tür güvenlik sorunları "uzaktan erişim" sorunları olarak adlandırılmaktadır. Günümüzde bu sorunların çözümü olarak ateş duvarları (firewall) yaygın olarak 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, 1997:3-4)

TUENA tarafından üretilen "*Açık iletişim ağlarında bilgi güvenliği*" başlıklı dokümanda, iletişimin güvenli olarak yapılabildiği elektronik bir ortamın kullanıcıya sağlaması gereken üç niteliğin bulunduğu ifade edilmektedir (Yücel, 1997:2). Söz konusu üç nitelik: Kimlik, bütünlük ve gizliliktir. Aşağıda bu niteliklere ilişkin açıklamalar yer almaktadır.

- Kimlik: Alıcı, bilgiyi gönderenin kimliğinden emin olabilmelidir. Bir başka ifadeyle, kimlik bilgisini içeren elektronik imza taklit edilemez olmalıdır.
- Bütünlük: Bilgiyi gönderen ve alan taraflar, üçüncü bir kişi tarafından en ufak bir değişikliğe uğratılmamış olduğuna güvenebilmelidirler.
- Gizlilik: İstendiği takdirde, gönderilen bilgi, yalnız bilgiyi alan kişi tarafından çözülecek ve üçüncü kişilerden gizlenecek şekilde şifrelenebilmelidir.

Kurumların Internet veya özel iletişim hatları üzerinden akan verilerinin güvenliğinin sağlanması amacıyla kullanılabilecek teknolojiler "*E-devlet dönüşüm sürecinde bilişim güvenliği: e-devlet çalışma grubu*" 2004 yılında yayımlanan ön raporunda aşağıdaki şekilde özetlenmektedir (Türkiye Bilişim Derneği, 2004).

- Fiziksel Güvenlik: Bilgisayarların fiziksel güvenliğinin gerek şifre gibi unsurlarla gerekse akıllı kart 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.
- Şifreleme: Güvensiz ağlar üzerinden geçen verilerin güvenliği için Virtual Private Network veya şifreleme yapan donanımların kullanılması. Ayrıca Web tabanlı güvenli veri transferi için SSL (Secure Socket Layer) ve Public Key şifrelemenin kullanılması. Donanım tabanlı şifreleme çözümleri de mümkündür.
- İnkâr edilemezlik ve mesaj bütünlüğü: Sayısal imza teknolojisi kullanarak mesajı bütünlüğü sağlanabilir.

Kriptoloji ve Kriptografi

Kriptolojinin Türkçe karşılığı şifrebilim iken, kriptografi şifre yazım anlamına gelmektedir. Kriptografi, gizlilik, kimlik denetimi, bütünlük gibi bilgi güvenliği kavramlarını sağlamak için çalışan matematiksel yöntemler bütünü olarak düşünülmektedir (Vikipedi, 2010). Güven (2004:61) kriptolojinin matematiğin iki dalını kapsadığını ifade etmekte ve bu dalların kriptografi ve kriptanaliz olduğunu belirtmektedir. Kriptografinin amacı ileti güvenliğini sağlamakken; kriptanalizin amacı var olan şifreleri çözmektir.

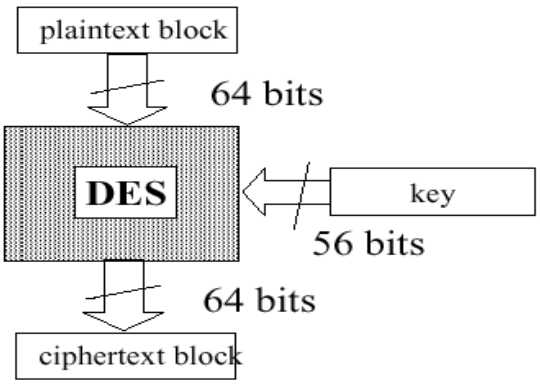
PGP (Pretty Good Privacy)

PGP günümüzde oldukça yaygın olarak kullanılan bir elektronik posta şifreleme programıdır. PGP ile ilgili enteresan bir dizi gelişme yaşanmış ve PGP'yi yaratan Phil Zimmermann'ın  başı oldukça ağrımıştır. Güçlü bir şifreleme algoritması içermesinden ötürü PGP'nin Amerika Birleşik Devletleri dışına çıkartılması ABD gümrük kurallarına göre yasaktır. Fakat bilinmeyen bir şekilde ABD dışına çıkmıştır. Günümüzde PGP'nin uluslararası sürümü ABD ve Kanada dışındaki ülkelerde WWW ve FTP sitelerinden dağıtılmaktadır. PGP'nin uluslararası sürümü ile Amerikan sürümü arasında işlevsel hiçbir fark bulunmamaktadır. Amerikan hükümeti, PGP'nin ABD dışına çıkartılmasından Zimmermann'ı sorumlu tutmuş ve hakkında soruşturma başlatmıştır. Ancak, Zimmermann bu olay hakkında dava açılmasını gerektirecek deliller bulunmadığından temize çıkmıştır. PGP'nin uluslararası sürümünün ABD ve Kanada dışında kullanımı kanunidir (Güven, 2004:77).

Şifreleme Yöntemleri

Veri güvenliğini sağlayabilmek için farklı şekillerde şifreleme yapılmaktadır. Birçok şifreleme yöntemi olmasına karşın bu ders notunda sadece üç tanesi (DES, RSA, DSA) hakkında ısa bilgiler verilmektedir.

Data Encryption Standard (DES): Açık anahtarlı bir kriptografik algoritma olan DES, 1970 yılında IBM tarafından geliştirilen Lucifer algoritmasının geliştirilmiş halidir. En çok bilinen algoritmalar arasında yer alan DES, 64 bit blok boyutu olan bir blok şifrelemedir. 64 bitlik düzyazı bloklarını 56 bitlik anahtarlar kullanarak 64 bitlik şifreli yazı bloklarına çevirmektedir. Düzyazı, bazı permutasyon ve yedeklemelerle işleme tabi tutulmaktadır. Daha sonra güvenli bir şifreli yazı bloğu oluşturmak için çıktılar orijinal düzyazı ile birleştirilmektedir. Söz konusu kriptolama serisi 16 kez tekrarlanmakta ve her seferinde farklı anahtar ve bit grupları kullanılmaktadır (Güven, 2004:63). Aşağıda düzyazı bloklarının şifreli yazıya dönüşümü şekil üzerinde gösterilmektedir.



Şekil 1. DES algoritması

DES, 56 bitlik kısa anahtar boyutuyla, özellikle teknoloji ve işlem gücündeki gelişmeler karşısında sınırlı bir koruma sağlamaktadır. Bu yüzden daha güçlü kriptolama yöntemlerinin geliştirildiği görülmektedir.

RSA: Adını geliştiricilerinin soyadlarının baş harflerinden (**R**ivest, **S**hamir, **A**dleman) alan RSA 1977 yılında yaratılmış açık anahtarlı bir kriptografik yapıdır. Şekil 2'de de gösterildiği üzere sistem ilk olarak iki tane asal sayı (p ve q) üretmektedir. Daha sonra bunlar birbirleri ile çarpılarak n elde edilir. n sayısı elde edildikten sonra n sayısından küçük ve (p-1) . (q-1) sayısıyla 1 dışında herhangi bir ortak böleni bulunmayan bir e sayısı seçilir. Daha sonra (e.d-1) sayısının (p-1) . (q-1) çarpımına tama olarak bölünmesini sağlayan bir d sayısı bulunur. e ve d değerleri sırasıyla açık ve gizli üs olarak adlandırılmaktadır. Açık anahtarı (n,e) çifti, gizli anahtarı ise (n,d) çifti oluşturur. p ve q sayıları ya yok edilmeli ya da gizli anahtar ile birlikte saklanmalıdır. Gizli anahtar olan d sayısının (n,e) sayılarından elde edilmesi zor bir işlemdir. Eğer bir kişi n sayısının çarpanlarına ayırarak p ve q sayılarını elde edebilirse gizli anahtarı da kolaylıkla bulabilir. Bu sebeple RSA sisteminin güvenliği çarpanlara ayırma probleminin zorluğu temeline dayanmaktadır (Güven, 2004:64).

RSA Public Key Sistemi	*Örnek*
Hem p'nin hem de q'nun asal olduğu p ve q seçilir.	*P = 11; q = 13*
Mod alınacak değer hesaplanır n = pq.	*N = 11*13 = 143.*
Euler's totient fonksiyonu uygulanır t = (p-1)(q-1).	*t = (11-1)*(13-1) = 120.*
T değeri ile en büyük ortak böleni 1 olan bir e değeri hesaplanır.	*e = 7. (7<120 ve 7 ve 120 nin en büyük ortak böleni 1 dir*
*e*d = 1 mod t olacak şekilde d değeri hesaplanır*	*7*d = 1 mod 120 => d = 103 çünkü 7*103 = 721 = 1 mod 120.*
public key (e, n).	*public key (7, 143).*
Private key (d, n).	*private key (103, 143).*
Plaintext M olsun.	*M = 5 kabul edelim*
ciphertext C = M^e mod n.	*Ciphertext: C = 5^7 mod 143= 47*
Şifre çözme işlemi => plaintext = C^d mod n = (M^e)^d mod n = M	*Plaintext: 47^103 mod 143 = 5 47^103 = (5^7)^103 = 5^721 = 5*[5^720] =5*[(5^120)^6] = 5*[1^6] = 5. 5^120 = 5^t = 1 mod 143 (Euler teoremi)veya, daha basitçe, x^(e*d) = x; bu sebepten, 5^721 = 5'tir.*

Şekil 2. RSA algoritmasının çalışma şekli

DSA (Digital Signature Algorithm): Oldukça yaygın kullanımı olmasına karşın sadece sayısal imzalamada kullanılabilmektedir. DSA'nın çalışma mantığına bakacak olursak:

p, bit uzunluğu 512-1024 arasında olan bir asal sayı

q, bit uzunluğu 160 olan ve p-1 sayısını bölen bir asal sayı

g, (p-1)'den küçük herhangi bir h sayısı için g=h(p-1)/q(mod p) eşitliğini sağlayan ve 1'den farklı herhangi bir sayı olmak üzere p,q ve g sayıları uygun yöntemler kullanılarak bulunur (NIST, 2000).

DSA, NIST (National Institute of Standards and Technology) tarafından sayısal imza standardı (Digital Signature Standard) olarak yayımlanmıştır.

Ateş Duvarları (Firewalls)

Kişisel kullanıcıların Internet ortamında verilerini düşük maliyetle korumalarını sağlayan önemli araçlardan bir tanesi ateş duvarlarıdır. Ateş duvarı, iç ağ ile dış ağ arasındaki tüm veri trafiğini filtrelemektedir (Pfleeger, 1997). Ateş duvarları sayesinde sisteme istenmeyen girişler engellenmektedir. Günümüzde farklı gereksinimleri karşılamaya yönelik farklı ateş duvarı türleri bulunmaktadır. Ateş duvarı türüne verilecek örnekler arasında; paket filtrelemeli ateş duvarı (packet filtering firewall), çift taraflı geçit (dual-homed gateway), perdelenmiş kullanıcı tipindeki ateş duvarı (screened host firewall), uygulama katmanlı ateş duvarı (application level firewall) ve durum denetlemeli ateş duvarı (stateful firewall) sayılabilir (Güven, 2004:104-106; Notarus, 1999; Price, 1996).

Sayısal İmza (Digital Signature)

Elektronik ortamdaki yazışmalara eklenen, yazıyı gönderenin kimliğini ve gönderilen yazının iletim sırasında bozulmadığını kanıtlamaya yarayan bölüme verilen isimdir. Sayısal imza, yazının içeriğine ve imzalayanın gizli anahtarına bağlı bir kriptografik yöntemle atıldığı için, sayısal imzanın doğrulanmasında, imzayı atanın açık anahtarı kullanılır (Hermes, 2006).

Konuyla İlgili Bazı Kavramlar

Aşağıda konuyla ilgili bazı kavramlar ve açıklamaları verilmektedir.

Cracker: Sistemlere girerek sisteme zarar veren kişilerdir. Buradaki zarar kelimesi sadece sistemi çökertmek anlamında değildir. Kimi zaman sisteme girebildiklerini göstermek amacıyla not bırakırlarken, kimi zaman buldukları kaynaktan daha sonra faydalanmak amacıyla kendi çıkarları doğrultusunda söz konusu kaynakları kullanmaktadırlar. Bu kişilerin Internet hakkındaki bilgi düzeyi oldukça yüksektir.

Hacker: Kültür ve bilgi düzeyi oldukça yüksek olan, en az bir işletim sisteminin yapısını tam olarak bilen, programcılık deneyimleri yüksek ve konusunda ileri eğitimler alarak uzun yıllarını bu işe adamış kişilerdir. İşletim sistemleri bu kişilerin uzmanlık alanına girdiği için, esas amaçları bu sistemleri daha güvenli hale getirebilmek ve açıklarını keşfetmeye çalışmaktır.

Lamer: Hacker'lara özenti, basit taktiklerle kendini olduğundan iyiymiş gibi gösteren, "filanca sitede şöyle bir "bug" buldum, sonrada bir trojan gönderdim" türünde ifadeler kullanarak aslında çok fazla anlamlı işler yapmayan, genellikle çok küçük yaştaki kişilerdir.

Newbie: Scrip Kiddy'lerden bir adım daha yukarıda olan kişilerdir.

Phreaker: Telefon hatları ve santralleri üzerindeki açıklardan yararlanan kişilerdir. Söz konusu kişiler telefonun çalışma prensibini çok iyi bilmekte ve bundan yararlanıp telefonla bedava konuşabilmektedir.

SET (Secure Electronic Transactions): Banka kartları ve ödemeler ile ilgili bilgilerin güvenliğini sağlamak amacıyla Visa, Mastercard**,** Microsoft, Netscape gibi kuruluşların katılımıyla oluşan bir konsorsiyum tarafından geliştirilen protokol.

SSL (Secure Socket Layer): Ağ üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla Netscape tarafından geliştirilmiş bir güvenlik protokolüdür.

Script Kiddy: Güvenlik, ağ ve protokollerle ilgili bilgisi son derece sınırla ya da hiç olmayan sadece çeşitli script'ler kullanan, bununla birlikte lamer'dan bir adım yukarıda olan ve kullandıkları script'lerin ne anlama geldiğini tam olarak bilmeyen kişilerdir.

Yukarıda geçen kavramlar ve açıklamaları *Internet'te Güvenlik ve Hacker Cracker Meselesi* (Güven, 2004) ve *How to Become a Hacker* (Raymond, 2006) adlı kaynaklardan yararlanılarak derlenmiştir.

Kaynakça

Al, U. (2002). Internet'te veri güvenliği. *Oluşum*, 10(38): 37-50.

Güven, M. (2004). *Internet'te güvenlik ve hacker cracker meselesi.* Ankara: Grafiker Yayıncılık.

Hermes. (2006). 25 Aralık 2006 tarihinde http://www.dijital-imza.com/sozluk.htm adresinden erişildi.

Levi, A. ve Çağlayan, M.U. (1997). Elektronik posta güvenliği için PGP kullanımı. 23 Mayıs 2011 tarihinde http://people.sabanciuniv.edu/levi/as97.htm adresinden erişildi.

NIST. (2000). Digital Signature Standard (DSS). 12 Aralık 2007 tarihinde http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf adresinden erişildi.

Notarus, M. (1999). Firewalls and security. 12 Aralık 2007 tarihinde http://www.cites.uiuc.edu/firewall/presentation/ adresinden erişildi.

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

Price, D.H. (1996). Firewalls. 23 Mayıs 2011 tarihinde http://www.uniforum.chi.il.us/slides/price/index.htm adresinden erişildi.

Raymond, E.S. (2006). How to become a hacker. 23 Mayıs 2011 tarihinde http://www.catb.org/~esr/faqs/hacker-howto.html adresinden erişidi.

Türkiye Bilişim Derneği. (2004). *E-devlet dönüşüm sürecinde bilişim güvenliği: e-devlet çalışma grubu*. 12 Aralık 2007 tarihinde http://www.bilisimsurasi.org.tr/e-turkiye/docs/guvenlik07042004.doc adresinden erişildi.

Vikipedi. (2010). Kriptografi. 23 Mayıs 2011 tarihinde http://tr.wikipedia.org/wiki/Kriptografi adresinden erişildi.

Yücel, M.D. (1997). *Açık iletişim ağlarında bilgi güvenliği*. 12 Aralık 2007 http://www.tuena.tubitak.gov.tr/Pdf/2103-M-T-A-02.pdf tarihinde adresinden erişildi.