Bilgi Güvenliği ve Kriptografi

(SPK'da Geçen Ay Dergisi, Ocak 2006 sayısı)

Teknolojinin baş döndürücü gelişimi, elektronik ortamda bilgi ve haber iletimini dünyanın en ücra köşelerine dek yaymayı başarmıştır. Doğal olarak bu gelişmeler, sorunlarını da beraberinde getirmiştir. Sosyal, psikolojik vb. sorunlar bir tarafa, teknik olarak en önemli sorun bilgi ve haber güvenliği sorunu olmuştur.

Haberleşme ve bilişimde temel sorun bilgi güvenliğidir. İnternet gibi dünyanın hemen her noktasına açık erişimin sağlandığı bir ortamda bilgi güvenliği can alıcı bir öneme sahiptir. Teknoloji geliştikçe bilgi çoğalmakta, bilgiye erişim, paylaşma, koruma, eleme, vb. önem kazanmaktadır. Tüm bunların güvenli bir ortamda ve güvenli bir biçimde gerçeklenmesi için parola sorma, şifreleme gibi teknikler kullanılmaktadır.

Bilgi teknolojilerine giderek artan bağımlılık, yönetimleri değişik güvenlik önlemleri almaya yöneltmektedir. İnternet üzerinden banka fon transferleri, bireysel bankacılık işlemleri, uçak rezervasyonları, sanal ortamda alış-veriş gibi ekonomik ve toplumsal yaşamın her alanında olduğu kadar, ulusal savunma ve ulusal güvenlik konularında da güvenlik bir numaralı sorun haline gelmiştir. Şu unutulmamalıdır ki; köprünün başını tutan, kimin geçeceğine de karar verir. Yani internet alt yapısında ve haberleşme araç gereçlerinde teknolojiyi belirleyenler, haberleşme ve güvenlik konusunda da en avantajlı ülkelerdir. İnternet üzerinde tam güvenliğin sağlanması olanaksızdır. O halde sorun, bilgi ve haberleşme güvenliğinin yüksek oranda sağlanmasının nasıl gerçekleneceğinde düğümlenmektedir.

İnternet üzerinde bilgi ve haber gizliliğini sağlamanın başlıca yolları şunlardır:

- Kriptografi: Bilginin/haberin gönderen tarafında özel bir program ile şifrelenmesi ve alıcının da aynı programı kullanarak şifreyi çözmesi
- Stenografi: Gönderilecek bilginin/haberin bir ses ya da görüntü kaydının içine şifrelenerek yerleştirilmesi ve alıcı tarafında şifrenin çözülerek bilgiye/habere ulaşılması

Bunların yanında, bilginin/haberin aktarmalı olarak birden fazla e-posta adresinden gönderilmesi ya da pek duyulmamış, kullanılmayan siteler aracılığı ile iletişimin sağlanması gibi yöntemler de kullanılmaktadır.

Bilgi ve haberleşme güvenliğine karşı tehditler kabaca üç başlık altında toplanabilir [1]:

- Sisteme yetkisiz giriş, gizlice dinleme, bilgi çalma, casusluk ve TEMPEST (yayılan elektromanyetik dalgalardan bilgiyi oluşturma) gibi kasıtlı eylemler,
- Bilgi ağı ve haberleşme sisteminin doğal afetler sonucu kısmen ya da tamamen çökmesi,
- Teknolojinin ve malzemenin kötü kullanımı ya da işletme hataları.

Bu ve benzeri tehditlere karşı alınacak önlemler de değişik başlıklar altında toplanabilir:

- Haberleşme güvenliği (COMSEC: Communication Security)
- Bilgisayar güvenliği (COMPUSEC: Computer Security)
- Bilgi Güvenliği (INFOSEC: Information Security)

Bilgi güvenliğinin sağlanması için; donanım, yazılım, kripto, emisyon (TEMPEST), ağ, iletişim, personel, doküman ve yöntem güvenliği gibi unsurların da göz önünde tutulması gerekmektedir. Örneğin, pahalı yatırımlarla, yazılım ve donanım güvenliğini sağlamanıza karşın personel, gizlilik konusunda yeterli eğitim ve bilinçle donatılamazsa bilgi ve haberleşme güvenliğinin sağlanması hayalden öte gidemez. Keza, her türlü önlemi almanıza ve hatta kripto kullanmanıza karşın, örneğin gönderilen kriptolu mesajların sonuna klasik "arz/rica ederim", "emirlerinizi beklerim" gibi klasik tümceler koymak tüm güvenliği bir anda sıfırlamak anlamına gelebilir.

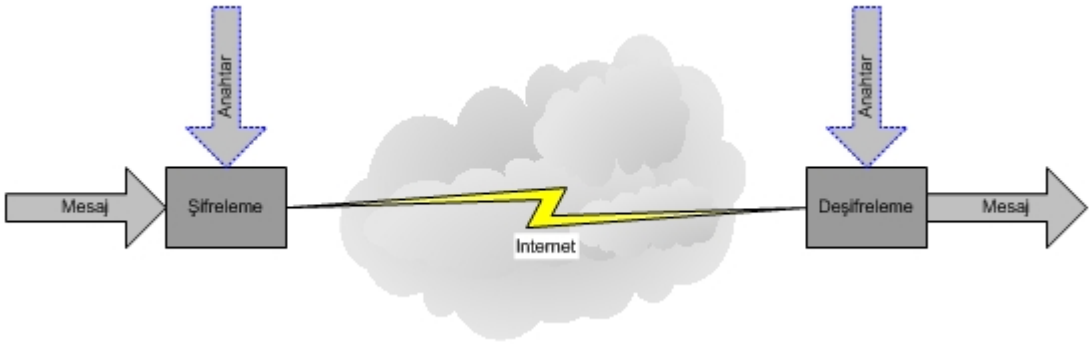
Peki nedir bu kripto ?

Kripto, daha bilimsel adıyla kriptografi, bilgi güvenliğini inceleyen ve anlaşılabileni anlaşılamaz hale getiren bir çalışma alanıdır. Diğer bir deyişle belli matematiksel yöntemleri içeren *şifreleme* ve *şifre çözme* bilimidir.

Kriptografi genel olarak şu dört ana konuyla ilgilenir:

- *Gizlilik (confidentiality):* Bilgi istenmeyen kişiler tarafından anlaşılamamalı.
- *Bütünlük (integrity):* Bir iletinin alıcısı bu iletinin iletim sırasında değişikliğe uğrayıp uğramadığını öğrenmek isteyebilir; davetsiz bir misafir doğru iletinin yerine başka bir yanlış ileti koyma şansına erişmemelidir. Saklanan veya iletilmek istenen bilgi farkına varılmadan değiştirilememeli.
- *Reddedilemezlik (non-repudiation):* Bilgiyi oluşturan ya da gönderen, daha sonra bilgiyi kendisinin oluşturduğunu veya gönderdiğini inkar edememeli. Bir gönderici daha sonrasında bir ileti göndermiş olduğunu yanlışlıkla reddetmemelidir.
- *Kimlik belirleme (authentication):* Gönderen ve alıcı, birbirlerinin kimliklerini doğrulayabilirler. Davetsiz bir misafir, başkasının kimliğine bürünme şansına erişmemelidir.

İletişim kurmak isteyen iki kişi bunu, bir ortamın fiziksel değişkenlerini belli kurallara göre değiştirerek yaparlar. Çoğu zaman, iletişim ortamına uyguladığımız değişikliklerin hangi alıcılar tarafından dinlendiğini bilemeyiz.[1] Birisinden mektup aldığımızda, mektubun açılıp başkaları tarafından okunup okunmadığından emin olamayız. Elektronik mektuplar ise hedeflerine ulaşmak için onlarca bilgisayardan geçtiğine göre, mektuplarımızın gizliliği bu bilgisayardan sorumlu kişilerin insafına kalmıştır.[2] Doğal olarak bilgisayar ortamındaki verilerin okunup okunmadığına dair hiç bir şey bilmemiz mümkün değildir. Daha da önemlisi, aldığımız bir elektronik mektubun gerçekte kimden geldiğini ve yolda değiştirilip değiştirilmediğini öğrenmemiz de son derece zordur. Dolayısıyla iletişimin gizliliğini ve güvenliğini sağlamak için tek çare, bu işlerini ciddiye alan bütün kurum ve kuruluşlar gibi şifreleme kullanmaktır.



Şifreleme Nasıl Yapılmaktadır?

Şifreleme (*encryption*), bir iletinin (düz metin - *plaintext*) içeriğini, uygun bilgi (anahtar bilgisi - *key*) elde olmadan okunamayacak hale (şifrelenmiş metin - *ciphertext*) getirme işlemidir. Şifrelemenin amacı, iletinin istenmeyen şahıslar tarafından okunmasını engellemektir. Şifre çözümü (deşifre - *decryption*) ise şifrelemenin tam tersi, yani şifreli metnin düz metine çevrilmesi işlemidir.

Şifreleme metotları (algoritmalar da denilebilir), anahtar kullanma yöntemlerine göre genel olarak ikiye ayrılmaktadır:

- Gizli-Anahtar (Simetrik) Yöntemleri (Geleneksel kriptolama sistemleri)
- Açık-Anahtar (Asimetrik) Yöntemleri (Açık anahtar kriptolama sistemleri)

---

[1] Quantum kriptografisiyle iletişimin dinlenip dinlenmediği anlaşılabilir.

[2] Veri trafiğinin yoğun olduğu kavşaklara yerleştirilen dinleyici programlarla, bir ülkenin (özellikle o ülkenin internet ağı merkezileşmiş bir yapıya sahipse) internet iletişimi gayet güzel gözetlenebilir.

Kullanıcı, bir mesajı (**M**) göndermeden önce bir anahtar (k1) kullanarak şifreler. Şifreli metin (**C**) tüm herkese açık olan bir kanaldan gönderilir (örneğin internetten). Mesajı okumak için alıcı bir anahtar (k2) kullanarak şifreyi çözer ve **M** mesajını elde eder. Aktif düşmanlar araya girip iletişimi dinleyebilir. Eğer k1 ve k2 eşitse, sistem simetriktir. Aksi takdirde bu sistem asimetrik olarak adlandırılır. Güvenliğin garantilenmesi için k2 her zaman gizli olmalıdır, ancak k1'i kullanarak k2'yi elde etmek mümkün olmadığı sürece k1 açıklanabilir. Bu durumda sisteme açık anahtarlı sistem (public key system) adı verilir. Açık anahtarlı sistemler pek çok ilginç olanaklar sunar; örneğin herkes online bir mağazaya, mağazanın açık k1 anahtarını kullanarak şifrelenmiş bir kredi kartı numarası gönderebilir. k2 anahtarını sadece mağaza bildiği için, kartın numarasını sadece mağaza öğrenebilir. Eğer simetrik sistem kullanılsaydı, mağaza potansiyel müşterilerinin her biriyle önceden ve gizlice ayrı ayrı anahtarlar belirlemek zorunda kalırdı. Açık anahtarlı sistemlerin güvenliği her zaman belirli matematiksel problemleri çözmenin zorluğuna dayanır, simetrik sistemler daha çok tek kullanımlık, geçici yapıdadırlar. Açık anahtarlı sistemlerin en büyük dezavantajı matematiksel yapıları nedeniyle simetrik sistemlerden daha yavaş olmalarıdır; özellikle açık anahtarlı sistemlerdeki anahtarların boyutları simetrik sistemlerin anahtarlarının boyutlarından çok daha büyüktür. Kısaca, kullanılacak şifreleme yöntemi gerçekleştirilecek uygulamaya bağlı olarak seçilir.

Algoritmalardaki bütün güvenlik anahtara (veya anahtarlara) dayalıdır, hiçbiri algoritmanın ayrıntılarında yer almaz. Bu, algoritmanın yayınlanabildiği ve incelenebildiği anlamına gelir. Bu algoritmayı kullanan ürünler seri üretilebilir. Bir davetsiz misafirin sizin algoritmanızı bilmesi önemli değildir; sizin özel anahtarınızı bilmedikçe, o şahıs iletilerinizi okuyamaz.

Özet

Bilgi güvenliği, günümüzde kişisel bazdaki öneminden çok, bazı toplumların geleceklerinin teminatı olan özel iş ve görev yapan birimlerde/kurumlarda önem arz etmektedir. Silahlı kuvvetler buna en iyi örneklerden birisi olabilir. II. Dünya Savaşı'ndan 35 yıl sonra açıklanan bir raporda, İngiltere ile Almanya arasında olan savaşın seyrinin, savaş taktiklerini içeren mesajların çözülmesiyle (deşifre) değiştiği bildirilmiştir. Bir şifre çözme olayı, savaşın müttefikler tarafından kazanılmasında büyük rol oynamıştır. Boston Globe gazetesi, bu olayın II. Dünya Savaşı hakkında daha önce yazılmış tarih kitaplarında birçok değişiklikler yapılmasını gerektirecek kadar önemli olduğunu vurgulamıştır. Tarihi değiştirecek kadar önemli olan şifre çözme olayı bu konunun önemini vurgulamada verilebilecek en iyi örneklerden birisidir. Günümüzde insanı gerçekten hayrete düşürecek milyonlarca örnek bulunabilir. Bilişim dünyasında dijitalleşmenin hızla yaygınlaşması gerek kişisel gerekse kurumsal veri güvenliği için şifreleme metotlarının veya kriptolama sistemlerinin kullanımını bir zorunluluk haline getirmiştir.

Referanslar

[1] O. Salcan, "Bilgi Güvenliği", Silahlı Kuvvetler Dergisi, Sayı 370, sf: 5467, Ekim 2001.

[2] L. Sevgi, "11 Eylül - Değişen Dünyada Elektronik Savaşlar, Bilgi Güvencesi ve Ulusal Savunma", EMO Merkez Özel Sayısı, Aralık 2001.

[3] H. Kodaz, "RSA Şifreleme Algoritmasının Uygulaması", Selçuk Üniv., 2003.

[4] M. Tunçkanat, Ş. Sağıroğlu, "Güvenli Internet Haberleşmesi İçin Bir Yazılım: TurkSteg", 2002.

[5] http://www.olympos.org/

Atilla BEKTAŞ (Matematikçi)

Ocak 2006