Gündelik Hayatta Kriptoloji

Teknolojik ürünlerin gündelik hayatımızın bir parçası haline geldiği günümüzde, pek çok değerli varlığımız sayısal bir bilgi bulutu halinde etrafımızı çevreliyor. Yolda yürürken cep telefonumuzdan bankamıza erişebiliyor, yol haritalarını takip edebiliyor, ihtiyacımız olan anlık bilgilere talep ettiğimiz anda ulaşabiliyoruz. Sağlık verileri gibi şahsi bilgilerin yanı sıra, kurumların önemli bilgileri de bu bulutta yerlerini çoktan aldılar. Bu bilgilerin gelişen teknoloji ile herkes tarafından ulaşılabilir hale gelmesiyle bilgilerin güvenliği konu oldu. Uzmanlar uzun zamandan beri bu bilgilerin korunması için kriptoloji kullanıyorlar. Peki, nerede bu kriptoloji?

A. Murat Apohan, doktora derecesini İstanbul Teknik Üniversitesi'nden almıştır. NATO kripto ve bilgi güvenliği çalışma gruplarında yer almıştır. TÜBİTAK UEKAE Kriptoloji Bölümü sorumlusu olarak görev yapmaktadır. 2007-2008 yıllarında Uluslararası Kriptoloji Organizasyonu'nun (www.iacr.org) yönetim kurulunda yer almıştır.

Anahtar Kavramlar

Gündelik hayatta kullandığımız cep telefonları kriptolu haberleşme yapmaktadır.

Güvenli olduğu zannedilen bazı uzaktan kumandalı araç alarm ve çalıştırma anahtarlarında kullanılan kriptografik yapılar kırılarak bu anahtarların kopyalarının üretilebildiği 2008 yılında bir grup araştırıcı tarafından gösterildi.

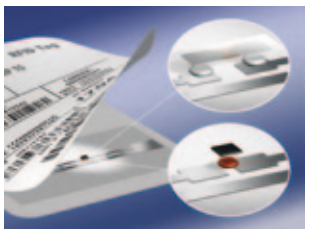
Yaygınlaşan RFID teknolojisinin yarattığı mahremiyet endişesine kriptoloji çözüm vaat etmektedir.

Güçlü kriptoya sahip bir cep telefonu

Sıradan teknoloji kullanıcısı kriptoloji ile karşı karşıya olduğunu ancak bazı ipuçlarından anlayabilir. Size kullanıcı şifresi soran bir internet sitesi, evde kurmaya çalıştığınız kablosuz ağ bağlantısı için istenen şifre veya kredi kartınızı kullanırken sorulan şifre, sahnenin arkasında oluşturulması yüzyıllara yayılmış güncel matematiğin en derin konularını kullanan kriptolojinin varlığına dair ilk işaretlerdir. Kriptoloji aslında gündelik hayatımızın her yerinde: cebimizdeki çipli banka kartında, otomobil anahtarında, internet üzerinden yaptığımız bankacılık işlemlerinde, kablosuz ağlarda, cep telefonlarımızda, DVD'lerin kopya korumasında, kısaca değerli bilginin olduğu her yerde.

Kriptoloji günümüzde askeri haberleşme, komuta kontrol ve karmaşık silah sistemlerinin de vazgeçilmez bir parçası haline gelmiştir. Savaş uçakları dostu düşmanı yüzlerce kilometre uzaktan kriptoloji sayesinde ayırt ederken, pilotun silah kullanmaya yetkisi olup olmadığını kriptografik metotlarla denetlemektedir. Zaman içinde diğer askeri teknolojilerde olduğu gibi kriptoloji de sıradan vatandaşın gündelik hayatına girmiş ve bu konuda öncü teknoloji internet olmuştur. İnternetin yaygınlaşması ile banka şubeleri bilgisayarlarımıza taşınmış ve bankadaki paralarımızın sanal karşılığı olan sayıların korunması gerekmiştir. Bu amaçla kullanılan ilk kripto protokolü NETSCAPE firması tarafından geliştirilen SSL olmuştur. Ancak o dönemde ABD'nin uyguladığı güçlü kriptonun yayılmasını engelleyen kurallar gereği, SSL kripto protokolündeki şifreleme algoritması düşük anahtar boyu ile kullanılmıştır. Bunun sonucunda Andrew Twyman isimli bir öğrenci 1996 yılında, bağlantı başına 584 dolar maliyet ile bu sistemin kırılabileceğini göstermiştir. Kriptologların çalışmaları ile bu protokol oldukça güvenilir bir hale gelmiş ve TLS ismi ile bankacılık işlemlerinde temel güvenlik bileşenlerinden biri olmuştur.

Kriptolojinin yer aldığı ve gündelik hayatta karşılaştığımız bir başka uygulamaysa cep telefonlarıdır. Neredeyse bir parçamız haline gelen cep telefonumuzun aslında kriptolu bir telefon olduğunu pek azımız biliriz. Cep telefonu ile baz istasyonu arasındaki haberleşme, yapılan görüşmelerin yetkisiz kişilerce dinlenmesini engellemek amacıyla GSM standartları doğrultusunda A5/1 (ABD ve Avrupa kullanımına özel), A5/2 (ABD ihraç izinleri çerçevesinde kullanılmak üzere zayıflatılmış algoritma) veya A5/3 (3G standardı için özel algoritma) isimli algoritmalardan birisi kullanılarak şifrelenir. Kriptologların çalışmaları ile A5/1 ve A5/2'nin yetersiz olduğu gösterilmiştir. A5/3 ise sıradan bir kişiyi meraklı kulaklardan uzak tutacak kadar güce sahiptir. Ancak bu sistemlerin hiçbiri güçlü bir kripto analiz grubuna karşı bir cep telefonundan diğerine kadar güvenli bir kanal oluşturmak için yeterli değildir. Bu nedenle aktarılan bilgilerin gizliliğinin yüksek olduğu yerlerde çok güçlü kripto algoritmalarına ve anahtar yönetimine sahip özel tasarlanmış haberleşme sistemleri kullanılır.



RFID etiket

Kriptoloji eğlence hayatımıza da girmiştir. DVD'lerde kullanılan kopya koruma sistemi de kriptografik tekniklere dayanmakta olup burada da kripto tasarımcıları ile kripto analizciler arasında bir rekabet süregitmektedir. DVD'lerde kullanılan içerik koruma sistemleri hedeflenen başarıyı gösterememiştir. Bunun temel sebeplerinden biri kriptolojide bulunan karmaşık yapıların yarattığı güven zincirinin son halkası olan kripto anahtarını koruyacak yapıların uygun bir biçimde oluşturulmamış olmasıdır. Bu sistemlerde tersine mühendislik yöntemleri ile kriptografik anahtarlar ele geçirilebilmiş ve kopya koruma özelliği kaldırılabilmiştir.

Peki kriptolojide güvenin temel dayanağı olan kripto anahtarlarını nasıl koruyacağız? Gündelik hayatta kripto anahtarlarını korumayı başarabilen en gelişkin sistem çipli banka kartlarıdır. Banka kartı, bizim hesap sahibi olduğumuzu bankaya ispatlamada kullandığımız araçtır. Kartın görevi ise yeterince uzun bir kriptografik anahtarın güvenli olarak saklanmasını sağlamaktır. Bir işlem sırasında kart bu anahtara sahip olduğunu bankaya ispatlar, bu da kart sahibi olan bizim yetkili kişi olduğumuzu gösterir. Burada önemli olan karttaki anahtarın üçüncü şahısların eline geçmesinin engellenmesidir. Geçmiş dönemlerde kullanılan manyetik kartlarda saklanan bu bilgiler basit bir kopyalayıcı ile ele geçirilebiliyorken, günümüz çipli kartlarının sahip oldukları güvenlik mekanizmaları içeriklerini kopyalamayı imkânsız hale getiremese de, iyi tasarlanmış bir kart için oldukça güç ve yüksek maliyetli bir işlem olur. Akıllı kartlar banka kartlarının yanı sıra kimlik, pasaport, ehliyet gibi kimlik sistemlerinde de yer almaya başlamıştır. Kripto tasarımı ile analizi arasındaki mücadele biz farkında olmasak bile cebimizde devam etmektedir.

Kriptografi bize güvenlik desteğinin yanı sıra beklemediğimiz bazı kolaylıklar da sağlamıştır. Örneğin tükenmez kalemle attığımız imzalar, bilgilerin kâğıttan dijital ortama kayması ile yerini dijital imzaya bırakmıştır. Mürekkepsiz imza! Sayısal imza asimetrik kriptonun bize sunduğu bir imkânı kullanır. Çok basitçe sayısal imzayı açıklamak istersek: şifreleme ve şifre çözme anahtarlarının birbirinden farklı olması bir mesajı sadece bizim sahip olduğumuz bir anahtarla (imza anahtarı) şifrelememizi sağlar. Herkesin kolayca erişebildiği ikinci anahtar (imza kontrol anahtarı) ise bu mesajın açılabilmesini ve imzanın bizim tarafımızdan atıldığının teyit edilmesini sağlar. Günümüzde gerekli yasal düzenlemelerin yapılması ile elektronik imza kullanılmaya başlanmıştır. Bu sayede elektronik yolla aldığımız belgeler ıslak imzalı kâğıt belgeler gibi hukuki geçerliliğe sahip olur ve kâğıt tasarrufu sağlanabilir.

Teknolojinin gelişimi ile ürünlerde kâğıt etiketler yerine elektronik etiketler kullanılmasıyla kriptografi mağaza raflarında da görülmeye başlandı. Bu etiketlerle, üründen çıkarılması unutulduğunda çalan alarmlar sebebiyle belki tanışmışızdır. Bu etiketler ürünle ilgili bilgileri kablosuz haberleşme kullanarak sorgu cihazına iletir. Bu sayede ürünle ilgili bilgilere uzaktan erişilebilir. RFID teknolojisi sayesinde çamaşır makinesi, içindeki giysinin etiketini okuyup doğru programı seçebilir, buzdolabı sakladığı ürünlerin son kullanma tarihlerini denetleyip uyarı verebilir, pasaportlar uzaktan okutularak sınır kapılarından geçilebilir, uzaktan ödeme ve binlerce ürünün bulunduğu bir ambarda hızlı stok sayımı yapılabilir. Ancak bu sistem, etiketleri taşıyan ürünlerin uzaktan izlenebilmesi nedeniyle önemli bir mahremiyet endişesi de yaratmıştır. Bir okuyucu ile bir kişinin üzerinde taşıdığı bu yolla etiketlenmiş bütün ürünleri izlemek mümkün olabilir. Bu noktada da kriptoloji devreye girerek bu etiketlerin sadece yetkili okuyucular tarafından sorgulanabilmesini sağlamaktadır.

Özetle biz farkında olmasak bile, bizi çevreleyen ve etrafımızla iletişim halinde kalmamızı sağlayan elektronik dünyanın güvenli ve güvenilir kalmasını kriptoloji sağlamaktadır.

Mini Bilgisayarlar: Akıllı Kartlar

Bellek, işlemci, dış dünya ile bağlantıyı sağlayan arayüz ve bir işletim sistemine sahip olan akıllı kartlar her gün karşılaştığımız bilgisayarların ölçek ve kapasite olarak küçük bir modelidir. Peki bu hesaplama gücüne neden ihtiyaç duyuluyor? Sonuçta bu kartlardan beklenen, kripto anahtarı denilen ortalama birkaç yüz bit uzunluğundaki bir veriyi saklaması ve ihtiyaç duyulduğunda doğru anahtara sahip olduğunu ispatlamasıdır. Bu basit işlem neden böylesine karmaşık bir yapı gerektiriyor? Zorluk özel kripto anahtarının kimseye verilmemesi gereğinden doğar. Eğer bir kez bu karttan çıkarılıp kopyalanabilirse, bu anahtarı kopyalayan kişi artık bu anahtarın asıl sahibinin kimliğine sahip olmuş olur. Bu nedenle akıllı kartlar, bu anahtar yerine, kriptografik olarak kendisine yöneltilen sorgu bit dizisine karşılık bu anahtarı ve bu sorguyu kriptografik bazı algoritmalara girdi yaparak hesapladığı bir sayı dizisini verir. Böylece anahtarı korumuş olur. Bu işlemler belirli bir hesaplama gücü gerektirir. Bu nedenle bu kartlar bir mini bilgisayara dönüşmüştür. Günümüzün çipli kartları sahip oldukları yüksek güvenlik önlemlerine rağmen eğer gerekli tedbirler alınmamış ise yan kanal saldırıları denilen saldırılara maruz kalabilirler. Bu saldırılar kartların kriptografik işlem yaparken harcadıkları güç, zaman vb bilgileri kullanarak sakladıkları anahtarları hesaplamayı hedefler. Ancak kart tasarımcıları bu saldırılara karşı da önlem alır.

Milli işletim sistemli ve çipli akıllı vatandaşlık kartı

Kaynaklar
Menezes, A., *Handbook of Applied Cryptography*, CRC Press, 1996.
Indesteege, S., Keller N., Dunkelman O., Biham E., Preneel, B., "A Practical Attack on KeeLoq", www.iacr.org/conferences/eurocrypt2008/.
Garfinkel, S. ve Rosenberg, B. (ed.) *RFID: Applications, Security, and Privacy*, ISBD-ISSN 032190968.
Barkan, E., Biham E., Keller, N., "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Technion - Computer Science Department, Technical Report CS-2006-07 – 2006.
http://www.akiskart.com.tr