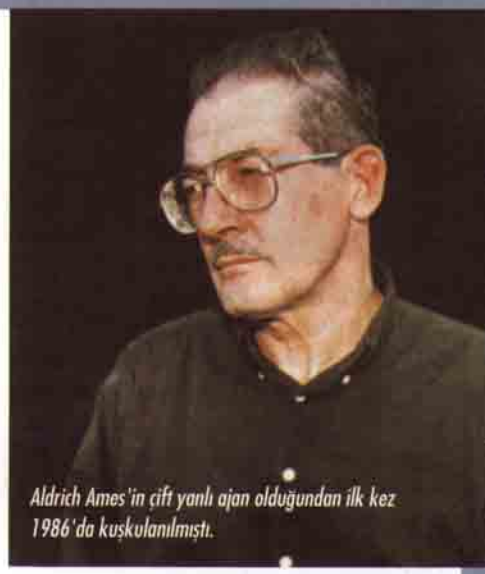
Bilgisayarınızda Bir Casus

Yakın zamana kadar, kriptografi - şifreleme ve deşifre etme bilimi - sır perdesinin ardına gizlenmişti. ABD'de bu alandan sorumlu Amerikan Ulusal Güvenlik Örgütü'nün (NSA) çalışmaları o kadar gizli tutuluyordu ki, Amerika yıllarca bu örgütün varlığını bile inkar etti. NSA, hiç kimsenin örgütçe çözülemeyecek bir şifresi olamayacağı iddiasındaydı. Bunu da, şifreli metni düz metne tercüme eden "anahtarlar"ı sıkıca denetleyerek ve Dijital Kripto standardı olarak adlandırılan şifre cetvellerini NSA'nın istediği an çözebileceği kadar zayıf bir yapıda tutarak yapmaktaydı.Ancak son yıllarda NSA'nın şifreleme teknolojisi üzerinde kurduğu tekel yıkılmıştır. Bunun önemli bir sebebi de bilgisayarların gelişmesine paralel olarak şifrelemenin de gelişmesidir. Son olarak Ocak ayında bilgisayar üreticileri NSA'nın bile kırmayı başaramayacağı yeni bir şifreleme standardı geliştirdiklerini açıklamışlardır.

Böylece şimdiye kadar gerçekleşen en şiddetli teknoloji politikası savaşının ilk aşaması da başlamıştır: Kıskaç Chip'i Savaşı!.. Savaşan taraflardan biri FBI, NSA ve CIA ile Clinton'unekibinden oluşurken, öbür taraf ise bilgisayar firmaları, insan hakları savunucuları, tutucu gazete yazarları, gibi değişik gruplardan oluşmaktadır.

Savaşın nedeni ise, NSA'nın ürettiği ve her telefona, bilgisayar modemine ve faks'a konmasını istediği yarıiletken Kıskaç Chip'idir. Bu Chip'in özelliği bir "arka kapısı" olan güçlü bir şifreleme sistemini gerçekleştirmiş olmasıdır. "Arka kapı" kriptografide yedek anahtar denebilecek bir işleve sahiptir. Bu Chip'in içine yerleştirildiği bir telefon, yedek anahtarı elinde tutan hükümetçe kolaylıkla dinlenebilecektir.Savaş , 1993 Nisan'ında bu projenin açıklanmasıyla başlamıştır. Dokuz ay boyunca firmaların chip aleyhine sürdürdüğü kampanya sonuçsuz kalmış ve 1994 Şubatı başında bilgisayar endüstrisinin liderlerinin kendi şifreleme standartlarını uygulamak istediklerini açık bir şekilde belirtmelerine karşın, hükümet NSA planını uygulamaya koyacağını açıklamıştır. Chip'in ticari kullanımı ise şimdilik kaydıyla kullanıcının isteğine bırakılmıştır. Sadece Amerikan vatandaşının sorunu gibi görünen bu savaş, aslında telekomünikasyon firmalarının ihracatı gözönüne alındığında çok daha geniş bir tüketici kitlesini ilgilendirmektedir. Yabancı müşteriler ABD casuslarının kolayca sızabilecekleri ürünleri almak istememektedirler.



Aldrich Ames'in çift yanlı ajan olduğundan ilk kez 1986'da kuşkulanılmıştı.

FBI ajanları, Ames'in sırlarını "satan" bilgisayara 1993 Kasım'ında sızmayı başarmışlardı.
1 3 Ekim 1993'te Ames bu posta kutusunu tebeşirle işaretleyerek sırları alacak olana Bogota'da randevu vermişti.
Ames çifti Virginia'daki bu evi 540 bin $'a almışlardı.

Olmadığına Emin misiniz?

Bir zamanların parlak öğrencisi, başarılı öğretmeni ve etkin kültür ataşesi Rosario Ames, şimdi Amerikan sırlarını 1.5 milyon $'a Moskova'ya satmakla suçlanıyor.

Şimdiki çatışmanın tohumları ise bundan yaklaşık yirmi yıl önce Whitfield Diffie isimli genç bir öğrencinin tüm geleneksel şifreleme projelerine "gözetleme deliği " ilave edilmesi projesini geliştirmesiyle başlamıştır. Bu gözetleme delikleri esas olarak mesajları kodlamak ya da kodunu çözmek için basıt bir parola ya da anahtara dayandırılmaktadır.

Kodlanmış mesajların gizliliği ise gizli kod çözücü anahtarların nasıl saklandığına bağlıdır. Esas sorun ise şifrelemenin geniş çaplı yapıldığı ve anahtar listelerinin merkezi olarak kaydedildiği durumlarda çıkmaktadır.Diffie'nin bu sorun için bulduğu çözüm herkese iki anahtar vermek olmuştur; bir anahtar genel, birisi de özel olacak ve genel olan anahtarı herhangi birinin bilmesinde bir sakınca olmayacaktır. Matematiksel nedenlerden ötürü, bir anahtarın mesajını bir diğeri ile çözmek olasıdır. Eğer birine ait genel anahtarı kullanarak bir mesaj gönderirseniz,bunun düz bir metin haline getirilebilmesi ancak özel anahtarın kullanılması ile mümkün olabilecektir. Ancak bu uygulama, zamanla NSA için oldukça başağrıtıcı bir sorun haline gelmiştir. Kullanıcıların kodlanmış mesajları aralarında değiştirmeleri NSA'nın devreye girmesini çok zorlaştırmıştır.

Amerikan hükümetinin elindeki önemli bir koz 'kıskaç' teknolojisinin maliyetini düşürerek diğer teknolojilerin karşısındaki rekabet gücünü artırmaktır. Bu politika alternatif bir uygulamanın yaygınlaşmasını çok zorlaştırmıştır. Eğer bu sistem bir pazar standardı haline gelirse o zaman insanların bu standarda uymayan bir sistemle işleyen araçlarını kullanamamaları gibi bir sonuç kaçınılmaz olacaktır.

Son günlerde Amerika'da çift taraflı bir casusluk olayının ortaya çıkarılabilmesi casusun kişisel bilgisayarına FBI'ın sızabilmesi ile mümkün olmuştur. FBI konunun önemini gündeme getiren bu operasyonun nasıl gerçekleştirildiğini açıklamasa da elektronik uzmanları bunun nasıl yapılmış olabileceğini tahmin etmektedirler.Şüpheli kişinin bilgisayarına ulaşmanın yollarından biri, uzaktan gözetlemedir: Binanın altına parkedilen bir araçtaki ajanlar şüphelinin bilgisayar ekranından çıkan elektromanyetik dalgaları çekip bunları tekrar karakterize ederek monitöre kelimeler şeklinde yansıtırlar. Zanlının yazdığı herşey bu yolla okunabilmektedir. FBI ajanlarının Aldrich Ames'in evine girerek, bilgisayarına yerleştirdikleri cihazla tuşa vuruşlarını kaydetmek gibi eski bir yöntem kullanmış olmaları olasılığı da vardır. Daha etkili bir yöntem ise bilgisayara yerleştirilen dinleme cihazı ile bilgisayardaki tüm eski dosyaları ya radyo ya da telefon modemi ile FBI'ın cihazlarına aktarmaktır. Bu durumda bilgisayarın ve modemin uzaktan sinyalle kapatılabilecek şekilde programlanması gerekmektedir. Disketlerin kopyalanması da başka bir yoldur.

Uzmanlar bu yolların hepsinin de kullanılmış olabileceğini söylemektedirler. Çift taraflı casusluk yapan Aldrich Ames, bu yöntemlerden birini kullanarak bilgisayarına giren casus sayesinde yakalanmıştır!...

Füsun Oralalp
Time, 7 Mart 1994.
Time, 14 Mart 1994.