Kara Kutu mu, Şeffaf Kutu mu?

Geleneksel olarak kriptografik bir cihaz iç işleyişi bilinmeyen, girdiler, çıktılar ve transfer algoritmasından oluşan bir karakutu olarak görülür. Kötü niyetli bir kişinin elinde girdiler, çıktılar veya girdi-çıktı ikilileri hakkında birtakım bilgiler olsa bile, gizli anahtarı bilmeden saklanan bilgiyi deşifre etmesinin mümkün olmadığı düşünülür. Kriptografik algoritmaya karşı bilinen tüm saldırıları olanaksız hale getirecek büyüklükte bir anahtar seçtikten sonra kuramsal olarak güvenli bir şifreleme sistemi oluşturmuş oluruz. Bu güvenlik tanımı, kötü niyetli kişilerin kriptografik cihazlara sadece karakutu olarak erişebileceği varsayımı üzerine kuruludur. Bu nedenle karakutu yaklaşımı ile tasarlanan bir sistemin sadece kuramsal olarak güvenli olduğunu söyleyebiliriz. Oysa gerçek hayatta kriptografik cihazlar, fiziksel yan kanallar yoluyla iç işleyişleri hakkında bilgi edinilebilen, kara değil şeffaf kutulardır.

Anahtar Kavramlar

Yan kanal: Kriptografik bir cihazın, iç işleyişi hakkında bilgi sızdırılmasına yol açan fiziksel özellikleri

Yan kanal analizi: Kriptografik cihazların fiziksel özellikleri yolu ile gizli tutulması gereken iç işleyişleri hakkında bilgi edinilmesi

Kriptoanaliz: Şifreleri ve kriptogramları analiz etme ve çözme bilimi

Deniz Karakoyunlu, 1999 yılında İzmir Fen Lisesi'nden mezun oldu. Lisans eğitimini 2004 yılında Sabancı Üniversitesi'nin Mikroelektronik Mühendisliği Bölümü'nde tamamladıktan sonra, ABD'nin Massachusetts eyaletinde bulunan Worcester Politeknik Enstitüsü'nün Elektronik ve Bilgisayar Mühendisliği Bölümü'nde yüksek lisans eğitimine devam etti. 2007 yılında yüksek lisans diplomasını almaya hak kazanan Karakoyunlu, halen Worcester Politeknik Enstitüsü bünyesindeki Kriptografi ve Enformasyon Güvenliği Laboratuvarı'nda doktora çalışmalarına devam ediyor. İlgi alanları kriptografik donanım tasarımı, yan kanal analizi, yüksek verimli kriptografik mimariler ve aritmetik algoritmalardır.

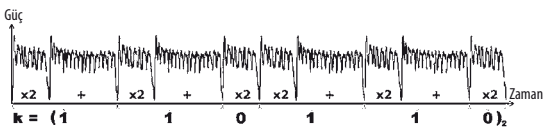
Matematiksel olarak tam güvenlik sağlamak, bir cihazın fiziksel işleyişinin de güvenli olduğu anlamına gelmeyebilir. Yani güvenli olduğu düşünülen karakutu, iç işleyişi hakkında bilgi sızdırıyor olabilir. Yan kanallar yolu ile edinilen bilgi kriptografik cihazın güvenlik tanımını tamamıyla geçersiz kılabileceği gibi, kısmi bilgi sağlayarak imkân dahilinde olmayan saldırıları da olası hale getirebilir. Yan kanal yolu ile elde edilen bilgiler, sistem güvenliğini sadece % 1 oranında azaltsa bile, bu sistemin kullanılamaz hale gelmesi demektir. Bir elektronik cihazın % 99 oranında çalışması performans değerlendirmesi açısından kabul edilebilir olabilir. Oysa bir kriptografik cihazın % 99 oranında güvenli olması güvensiz olduğu anlamına gelir. Bu nedenle, kriptografik cihazların her koşulda % 100 güvenlik sağladığından emin olabilmek için fiziksel işleyiş sırasında sızdırılan bilgileri de dikkate almak gerekir.

>>>

JUPITERIMAGES

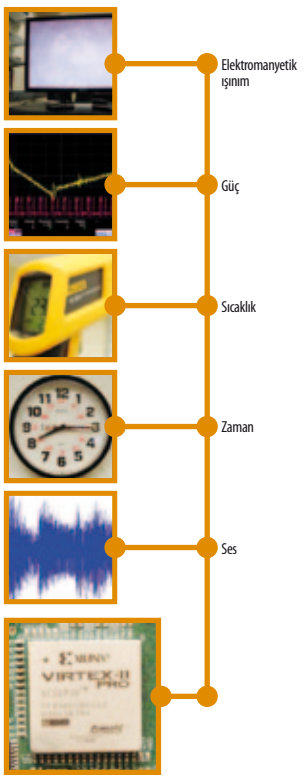
Peki, nedir bu bilgi kaçağına yol açan yan kanallar? İsminden de anlaşılacağı gibi, bir sistem hakkında bilgi sızdıran ve tasarım aşamasında öngörülemeyen kanallardır. İlk olarak 1996 yılında Paul Kocher tarafından öne sürülen yan kanal analizini, günümüzde polisin sıklıkla kullandığı, ilk kullanımı yine aynı yıllara rastlayan, kaçak esrar yetiştiriciliğini tespit etme yöntemi ile benzeştirebiliriz. 9 Aralık 1997'de ABD'nin Kolorado eyaletinde tarihin en büyük kaçak esrar yetiştiriciliği baskınlarından biri gerçekleştirildi. Polisin bu başarılı operasyonuna katkı sağlayan bilgiler, gizli olarak esrar yetiştirilen evin çatısının havadan termal sensör ile yapılan tarama sonucunda kırmızı görünmesi ve evin elektrik faturalarının çevresindekilere göre 10 kat fazla olmasıydı. Yani esrar yetiştiriciler yakalanmamak için gereken tüm güvenlik önlemlerini aldıkları halde, polisin yan kanallar yolu ile kendilerine ulaşmasına engel olamadılar. Her ne kadar bu örnekte yan kanal kullanımı iyi bir amaca hizmet etse de, kriptografik cihazların fiziksel işleyişleri farkında olunmadan kötü niyetli kişilerin gizli bilgilere ulaşmasına yol açabilir.

Yan kanal analizi, elektronik cihazların fiziksel özellikleri yoluyla, gizli tutulması gereken iç işleyişleri hakkında bilgi edinilmesidir. Mesela aşağıdaki grafik bir çarpma işlemine ait güç profilini gösteriyor. Çarpma işlemi süresince çarpılmakta olan anahtar sayı bit bit taranıyor ve bit değerlerine göre toplama ve ikiye katlama işlemleri yapılıyor. Anahtar sayının şu anki bit değeri 0 olduğunda sadece ikiye katlama işlemi yapılıyor, ama bu değer 1 olduğunda ikiye katlama ve toplama işlemleri art arda yapılıyor. Grafik üzerinde gösterildiği gibi, ikiye katlama işleminin toplama işlemine göre daha basit olması gerçeğinden yola çıkarak, tek başına ikiye katlama işlemi yapılan kesimleri ve ikiye katlama işlemini takiben toplama işlemi yapılan kesimleri ayırt edebiliriz. Bu da gizli tutulması gereken anahtar sayının kolaylıkla deşifre edilmesi demektir. Yan kanal güvenliği hiç göz önünde bulundurulmadan gerçekleştirilmiş bu algoritmanın güvenliği teoride ne kadar iyi olursa olsun, görüldüğü gibi pratikte algoritmanın işleyişi dışında hiçbir bilgiye ve uğraşa gerek duyulmadan kolaylıkla alt edilebilir. Aynı prensip günümüzde dünyada en yaygın olarak kullanılan açık anahtar kriptosunu kırmakta da kullanılabiliyor. Siz farkında olmasanız da, internette bir web tarayıcı ile alışveriş sitelerine girdiğiniz hemen hemen her sefer, güvenlik için bu algoritma kullanılıyor!



Güç ve zaman dışında başka fiziksel özellikler de, örneğin ses, elektromanyetik ışınım ve sıcaklık da yan kanal olarak kullanılabilir. Yan kanaldan pasif olarak yani sadece çalışmakta olan cihazı dinleyerek bilgi elde edilebileceği gibi, aktif olarak cihazı istenilen bir koşula yönlendirmek de mümkündür. Ayrıca yan kanal analiz teknikleri, bilginin işleniş yöntemi açısından da iki temel kola ayrılır. Yukarıdaki örnekte olduğu gibi bir veya birkaç ölçüm sonucu elde edilen bilgileri doğrudan yorumlayarak yapılan analizlere "basit yan kanal analizi" denir. Birbirleriyle korelasyon içeren birçok yan kanal ölçümünü istatistiksel olarak inceleyerek yapılan analizlere ise "diferansiyel yan kanal analizi" denir.

Günümüzde kriptografik cihazların algoritmik güvenliğinin yanı sıra yan kanal güvenliğine de büyük önem verilmektedir. Yan kanalları öngörmek ve yan kanaldan sızdırılan bilgi miktarını belirlemek kolay olmadığı için, yan kanal güvenliğini ölçmek veya mutlak güvenlikten bahsetmek de mümkün değildir. Yan kanal güvenliğinin öncelikli koşulu, yapılan farklı işlemlerin farklı fiziksel özellikler göstermesini engellemektir. Bu amaçla, cihaz-



Yan Kanallar

lar öncelikle basit yan kanal analizine karşı güvenli hale getirilmeye çalışılır. Yapılan çalışmalar, bilgiye bağlı olarak işlem seçimini engelleyerek yan kanaldan bilgi sızdırılmasını en aza indirmeye yöneliktir. Bu süreç, bilgiye bağlı olmaları durumunda performans artırmak amacıyla kullanılan hızlı algoritmalardan vazgeçilmesi ve daha yavaş olan ama bilgi sızdırmayan algoritmaların tercih edilmesi anlamına gelir. Örneğin bahsettiğimiz çarpma işlemini yan kanal açısından güvenli hale getirmek için öncelikle, anahtar sayının bit değerine bağlı olarak toplama işlemi yapılıp yapılmamasına karar verilmesini engellemeliyiz. Bu amaçla akla ilk gelen yöntem, anahtar sayının mevcut bit değeri 0 dahi olsa toplama yapmak ve sonucu göz ardı etmektir. Fakat, yalancı toplamalar diye adlandırılan bu yöntem de yeterince güvenli değildir. Aktif bir yan kanal analizcisi, sürmekte olan işleme yer yer hata iliştirip sonucun da hatalı olup olmadığını kontrol edebilir. Eğer sonuç da hatalıysa, yapılan toplama gerçek toplamadır ve anahtarın şu anki bit değeri gerçekten 1'dir. Eğer sonuç iliştirilen hataya rağmen doğruysa, yapılan toplama yalancı toplamadır ve anahtarın şu anki bit değeri 0'dır. Görüldüğü gibi yan kanallardan sızdırılan bilgiyi engellemek çok kolay bir iş değil. Öngörülen bir saldırıya karşı bilgi sızdırmayı engellemek için kullandığımız bir yöntem, sistemi öngöremediğimiz başka bir saldırıya karşı zayıf hale getirebilir. Örneğimizde verilen çarpma metodunu, yalancı işlemler içermeyen fakat yine de anahtar bitlerinden bağımsız olarak toplama ve ikiye katlama işlemi yapan algoritmalarla güvenli hale getirmemiz gerekir.

Basit oldukları için, koruyucu yüzeylerin ve devreye gömülü algılayıcıların kullanılması aktif yan kanal ataklarına karşı çekici bir çözüm alternatifi oluşturuyor. Fakat maalesef bu çözümler üretimde ciddi maliyet artışlarına sebep oluyor ve pratikte de çok rağbet görmüyor.

Yan kanal denildiğinde öncelikle akla ölçümü ve değerlendirmesi daha kolay olan "güç" ve "zaman" gelmektedir. Yukarıda verilen çarpma işlemi örneği, bu iki yan kanalın yapılmakta olan ara işlemleri nasıl ayırt edilebilir hale getirdiğini gösteriyor. Genellikle ihmal edilen fakat oldukça kuvvetli yan kanallardan biri de akustik kanalı, yani ses kanalıdır. Bir hesaplama esnasında işleme bağlı ses dalgaları da üretilir. Ses kanalı analizinin çok güzel bir örneğini Tromer vermiştir. Bu çalışmada önce standart bir bilgisayardaki işlemcinin çıkardığı ses, kriptografik bir algoritma çalıştırırken sıradan bir mikrofon ile kaydedilmiştir. Sonra bu ses, işlemcinin çalışma hızına göre parçalanıp işlemcinin komutları önceden teşhis edilen parmak izleri ile karşılaştırılarak, tek tek işletilen komutlar ortaya çıkarılabilmiştir.

Bir diğer yan kanal ise cihazların çalışırken yaydıkları elektromanyetik ışınımdır. Elektromanyetik ışınım tıpkı güç gibi yapılan işlemin ne kadar karmaşık olduğuna dair bilgi verebileceği gibi, daha detaylı bilgilere, örneğin bir hat boyunca akımın hangi yönde aktığı gibi bilgilere de ulaşmamızı sağlayabilir. 2001 yılında Karine Gandolfi ve çalışma arkadaşları farklı algoritmalar kullanan üç ayrı kriptografik cihaz üzerinde elektromanyetik analiz uygulamış ve her üç cihazın da gizli anahtarlarının tümünü elde etmeyi başarmışlardır. Çalışmakta olan bir kriptografik cihazın sıcaklığı da bize yapılmakta olan işlemin ne kadar güç harcadığı ve ne kadar

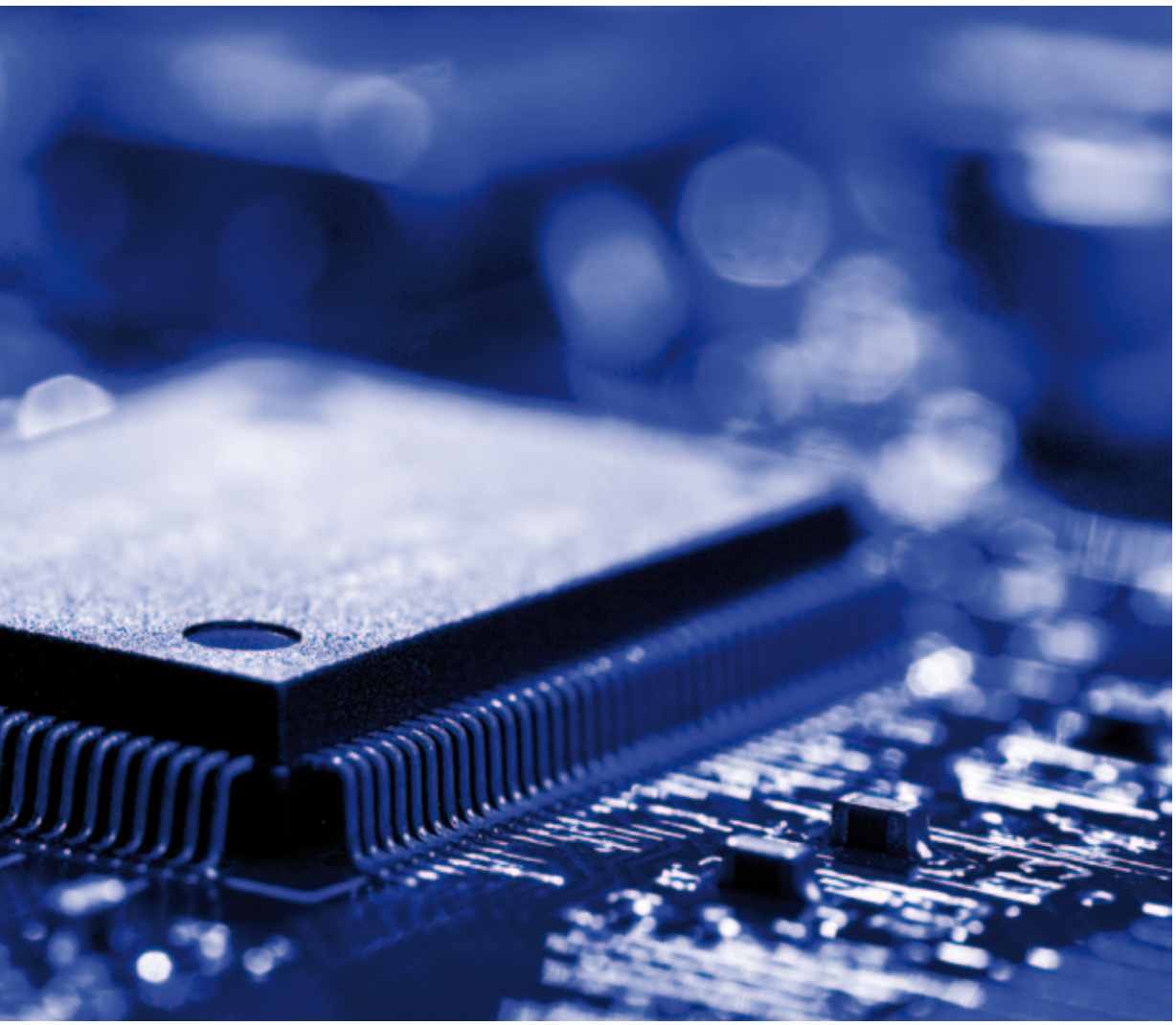
ısınmaya yol açtığı hakkında bilgi verir. Lokal sıcaklık değerlerinin çevreden izole edilerek ölçülmesi, diğer yan kanallarla karşılaştırıldığında daha çok emek isteyen bir iştir. Yine de ileri teknoloji ile üretilmiş termometreler sayesinde bu yan kanaldan da önemli bilgiler elde edilebilir.

Tahmin edileceği üzere, daha gelişmiş donanım ile çok daha hassas yan kanal atakları gerçekleştirilebilir. Henüz birkaç yıl önce Skorobogatov'un gösterdiği gibi, bir çipin belleğinde kayıtlı bitleri tek tek okumak ve hatta değiştirmek mümkündür. Bu atağı gerçekleştirmek için yüksek çözünürlükte bir mikroskop, ucuz bir lazer ve biraz da el emeği yeterli olmaktadır.

Peki kripto cihazlarımızı bu kadar kuvvetli bir tehlikeye karşı nasıl koruyacağız? Bunun için önerilen çözümler kısaca şöyle özetlenebilir: Güç yan kanalını ortadan kaldırmak için, güç kullanımı dengelenmiş mantıksal kapılar kullanılabilir. Bu tür dijital devrelerde mantıksal kapılar işlenilen bit değerlerinden bağımsız ve hemen hemen sabit bir güç kullanır. Bu tür dijital tümleşik devre teknolojileri mükemmel olmasalar da kötü niyetli kişilerin işini hayli güçleştirir. Ayrıca dengeli bir güç dağılımı diğer yan kanalların da dengeli dağılmasını sağlayacaktır.

Basit oldukları için, koruyucu yüzeylerin ve devreye gömülü algılayıcıların kullanılması aktif yan kanal ataklarına karşı çekici bir çözüm alternatifi oluşturuyor. Fakat maalesef bu çözümler üretimde ciddi maliyet artışlarına sebep oluyor ve pratikte de çok rağbet görmüyor.

Yeni geliştirilen bir diğer çözüm de fiziksel olarak kopyalanması mümkün olmayan özelliklerin gizli bilgi saklamak için kullanılması. Bu tür devreler herhangi bir dış etki karşılığında sakladıkları bilgileri "kaybederler". Böylece bilgi sızması engellenmiş olur.



JUPITERIMAGES

Kaynaklar

Kocher, P., "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems", *Uluslararası Kriptoloji Konferansı: Kriptolojide Gelişmeler (CRYPTO 1996),* Santa Barbara, Kaliforniya, ABD, Cilt 1109, s.104-113, 1996.

"Glowing Roof Leads Police to Marijuana: 263 Plants Confiscated from Area Warehouse", *The Gazette* gazetesi, Kolorado, ABD, 9 Aralık 1997.

http://people.csail.mit.edu/tromer/acoustic/

Gandolfi, K., Mourtel, C. ve Olivier F., "Electromagnetic Analysis: Concrete Results", *Kriptografik Donanım ve Tümleşik Sistemler Çalıştayı, (CHES 2001),* Paris, Fransa, Cilt 2162, s. 251-261, 2001.

Skorobogatov, S.P. ve Anderson, R.J., "Optical Fault Induction Attacks", *Kriptografik Donanım ve Tümleşik Sistemler Çalıştayı, (CHES 2002),* Redwood Shores, Kaliforniya, ABD, Cilt 2523, s. 2-12, 2002.