Mikromimari yan kanal saldırıları

ÇETİN KAYA KOÇ

"Simple branch prediction" denilen saldırı yönteminde, birkaç ölçme ile RSA anahtarının bütün bitlerini bulmak söz konusu.

Geçen hafta kısaca giriş yaptığımız bu konuya devam edelim. Daha önce sadece akıllı kartlara yapılan yan kanal saldırıları, şimdi artık özelleşmiş bir şekilde sunucuların işlemcilerine de yapılabiliyor. Prensip olarak 2 türlü saldırı söz konusu: "Cache" ve "Branch Prediction" saldırıları. Bu saldırılar işlemcinin "microarchitecture" özellikleri ile alakalı olduğu için, bunları mikromimari yan kanal saldırıları diye isimlendirmek de fayda var.

İki saldırı türünü de uzaktan (remote) veya sunucu üzerinden (intraprocessor) yapmak mümkün olabiliyor. Uzaktan yapılan saldırıları yapma ihtimali daha fazla (çünkü saldırganın bütün yaptığı sunucuya mesaj parçacıkları göndermek ve sunucunun cevap verme zamanlarını ölçerek kaydetmek) ancak başarı ihtimali daha az (çünkü istatiksel başarı için çok mesaj göndermek gerekiyor). Diğer taraftan, sunucu üzerinden bir saldırıyı başlatmak çok güç (çünkü sunucuya casus program yerleştirmek gerekli), ancak saldırı bir kere başlatılabilirse, başarılı olma ihtimali çok yüksek (çünkü çok az ölçme yeterli olabiliyor). Özellikle "simple branch prediction" denilen saldırı yönteminde, birkaç ölçme ile RSA anahtarının bütün bitlerini bulmak söz konusu.

"Branch prediction" saldırısı, şimdilik sadece HT (hyperthreading) özelliğine sahip modern ve hızlı işlemciler üzerinde çalışıyor. Ancak biz, kısa bir zaman içinde diğer işlemciler üzerinde de başarılı olacağını düşünüyoruz. Önemli olan şey, işlemcinin üzerinde bir "branch prediction" ünitesi olması. Peki saldırı nasıl gerçekleşiyor? Özet olarak, işlemcinin "branch" olacak veya olmayacak diye iki varsayımdan birini seçmesi ve yanıldığı durumda ise ödenen zaman penaltısının çok yüksek olması bize bu zamanı doğru bir şekilde ölçme imkanı tanıyor. RSA algoritmasının (aynı şekilde AES) anahtarının bitleri ile ölçülen bu zaman dilimleri arasında direkt bir ilişki var. Detayları http://eprint.iacr.org/2006/351 adresinde bulabilirsiniz.

koc@krip.to