ASAL FAKTÖRLER

Klonlanamayan donanım (1)

ÇETİN KAYA KOÇ koc@sehir.edu.tr

Basit donanımlar, örneğin manyetik şeritli bir kredi kartı, kolaylıkla klonlanabilir. Sahteciliğe karşı başarılı bir savunma yapmak istiyorsak, fiziksel ve algoritmik olarak çok daha iyi çözümlere ihtiyacımız olduğu kesin. Sahteciliği önlemenin etkili yollarından biri klonlamayacak (veya klonlanması zor ve pahalı) donanımlar üretmek ve bunlarla çalışmak. Bu konu kriptografinin ilginç ve önemli bir çalışma alanı haline geldi. Konuya katkıda bulunan birkaç araştırmacı var. Örneğin Naccache, Pappu, Devadas, ve Tuyls. Kısaca fiziksel olarak klonlanayamayan fonksiyonlar (PUF: physically unclonable functions) dediğimiz metotlarla, aynı seri içinde ürettiğimiz donanım birimlerinde farklılıklar oluşturup, bunları ölçerek algılamaya çalışıyoruz. Bu farklılıklar donanımlar üzerinde farklı kimlik doğrulama metotları haline dönüştürülürse, iyi çözümler elde ederiz.

Aranılan en önemli özellik, böyle bir farklılaşmış donanımın kolay üretimi ancak aynı zamanda kopyasının kolaylıkla yapılamaması. Bunu başarmanın birkaç yöntemi keşfedildi. Herhalde zamanla daha yeni yöntemler de bulunur. Biz fiziksel cihaza PUF ilave etmenin maliyeti de çok düşük olmalı. Pahalı çözümler ancak çok özel durumlarda kullanılabilir ve yaygınlaşamazlar.

Eşdeğer cihazların birbirlerinden farklılığı, bir anlamda onların randomize olması demek. Bu randomizasyon iki türlü elde edilebiliyor: Ya dışardan bir metotla ilave edilir (explicitli introduced randomness) veya zaten cihazın doğasında var olan (intrinsic randomness) bir randomizasyon ölçülebilir bir hale getirilebilir.

Birinci metot, ilk olarak Pappu isimli araştırmacının tezinde, kredi kartları için önerilmişti. Kartın bir bölümü cam veya plastik gibi saydam bir malzemeden yapılır ve üretim sırasında bu bölgede (her kart için) birtakım kabarcıklar oluşturulur. Rastgele kabarcıklar oluşturmak kolay, ancak aynı büyüklük, pozisyon ve sayıda kabarcık kümesini tekrar oluşturmak çok zordur (imkansızdır). Kredi kartını her okurken bu kabarcıklar lazer ışığıyla yeniden algılanır ve elde edilen geometrik görünüm teyid edilir. İşte alın size klonlamayan bir donanım ve dolayısıyla etkin bir kimlik doğrulama metodu.