RSA anahtarınız ne kadar güvende?

ÇETİN KAYA KOÇ

Bu yazıda, çok özel bir probleme değinmek istiyorum: Gizli anahtarların üretilirken yetkili olmayan bir gözlemci tarafından yan kanal bilgilerine bakılarak öğrenilmesi ihtimali.

Elektronik imza veya güvenli haberleşme için kullanılan endüstriyel standart RSA algoritması, anahtarları üretme ve iletme süreçlerinin karmaşıklığı yüzünden bazen beklenilmeyen güvenlik açıklarına maruz kalabiliyor. Bir taraftan, açık anahtarın üretilip, sertifika içine yerleştirilmesi ve bu sertifikaların güvenli dağıtımında ortaya çıkabilecek sorunlar, diğer taraftan ise gizli anahtarın üretilmesi, güvenli donanım içine yerleştirilmesi veya şifrelenerek sunucuda tutulması, uygun zamanlarda ve belirli prosedürler izlenerek kullanılmasında ortaya çıkabilecek sorunlar var. Bu yazıda, çok özel bir probleme değinmek istiyorum: Gizli anahtarların üretilirken yetkili olmayan bir gözlemci tarafından yan kanal bilgilerine bakılarak öğrenilmesi ihtimali.

Hatırlarsanız, daha önceki yazılarımda sunucunun işlemcisi ile alakalı (mikromimari) yan kanal saldırılarından kısaca bahsetmiştim. Bu yan kanal saldırıları, sunucu işlemcisine yerleştirilen bir casus program yardımı ile, işlemcinin bir komutu koştururken izlediği yolda harcadığı zamanın her seferinde farklı olmasından ve bu farklılıkların ise gizli anahtarın bitleri hakkında fikir vermesinden faydalanıyorlardı. Bu saldırılar, Oregon State University'deki doktora öğrencim Onur Acıiçmez tarafından geliştirildi ve mükemmelleştirildi. Onur, Aralık 2006'da mezun oldu ve şimdi bir Ar-Ge kurumunda çalışmalarına devam ediyor. Son çalışmasında, mikromimari saldırılarının, RSA anahtarı üretilirken de etkili olabileceğini ve gizli anahtarın öğrenilebileceğini gösterdi. Makalenin detaylarını burada bulabilirsiniz: http://eprint.iacr.org/2007/336.pdf.

Ancak en önemli detay CERT'in bu saldırıyı çok ciddiye alıp ve bir zayıflık notu yayınlaması: http://www.kb.cert.org/vuls/id/724968. Bunun anlamı, bu saldırının çalışan endüstriyel sistemler için tehlike oluşturabileceği. Bu zayıflığın etkileyebileceği sektör veya sistemler hakkındaki görüşlerimi bir sonraki yazıda anlatacağım.

koc@krip.to