RSA anahtarını üretirken kaybetme tehlikesi

ÇETİN KAYA KOÇ

Herşeyden önce birçok elektronik imza uygulaması saldırılara karşı güvenli.

RSA algoritması elektronik imza ve güvenli haberleşme için gizli anahtar alışverişi (örneğin, SSL protokolu içinde) kullanılan açık anahtarlı bir şifreleme algoritması. Yakın zamanda geliştirilen mikromimarı yan kanal saldırı teknikleri, RSA anahtarını üretirken başkası tarafından öğrenilme tehlikesini ortaya çıkardı. Peki bu tehlike hangi sistemler ve uygulamalar için geçerli? Şimdi bunu biraz irdeleyelim.

Herşeyden önce birçok elektronik imza uygulaması bu saldırıya karşı güvenli. Özellikle, RSA anahtarının magnetik olarak yalıtılmış bir güvenlik merkezinde veya akıllıkart içinde üretilmesi durumunda, anahtarın başkaları tarafından öğrenilme olasılığı yok gibi. En azından şimdiye kadar böyle bir saldırı gerçeklenmiş veya rapor edilmiş değil. Mikromimari yan kanal saldırıları, akıllıkartlar üzerinde uygulanamıyor, çünkü bu saldırılar ancak Pentium gibi çok karmaşık işlemciler için geçerli (işlemcinin cache veya branch-prediction birimi olması gerekiyor). Diğer yan kanal (zaman, basit ve diferansiyel güç) saldırıları ise kart RSA anahtarını üretirken fiziksel erişim gerektirdiği için uygulanabilir değiller. Elektromagnetik yan kanal saldırısının akıllıkarta uygulanabilirliği ancak antenlerin karta birkaç santimetre (hatta milimetre) yaklaşması ile mümkün. Özet olarak, elektronik imza için kullandığınız RSA anahtarlarınız güvenlik merkezinde veya akıllıkart içinde üretilmişlerse, gayet güvendeler.

Güvende olmayan RSA anahtarları, bir sunucu üzerindeki karmaşık bir işlemci tarafından üretilen anahtarlar. Bu özellikle SSL gibi uygulamalarda geçerli olan bir durum. Uzaktan veya bir casus program yardımı ile zamanlaması gözlenen bir işlemciden, mikromimarı yan kanal saldırı metotlarını kullanıp anahtarı öğrenmek mümkün. 2 hafta önce CERT tarafından yayınlanan bir uyarı (http://www.kb.cert.org/vuls/id/724968) bize OpenSSL uygulamasının bu tip bir saldırıya karşı güvensiz olduğu ifade ediyor. Bu zayıflığı kaldırmak için, OpenSSL 0.9.8 sürümünü edinmek gerekiyor.

koc@krip.to