SHA-1 Güvenlik Problemi ve Öneriler

ÇETİN KAYA KOÇ

Sürpriz algoritmik gelişmelerin bu durumu hızlı bir şekilde SHA-1 aleyhine döndürme ihtimali de artmıştır.

Bir önceki yazının ana fikrini özetlersek: SHA-1 özet algoritmasının güvenliği 63 bitten daha iyi değil ve üzerinde çakışma saldırıları düzenlenebilir. Böyle bir saldırı, dağınık bilgisayarlar ve özel donanım araçları gerektirmektedir ve büyük bir ihtimalle maliyeti bir kaç yüz bin dolar mertebesindedir. Bu durum 2005 Ağustos ayından beri bilinmektedir, ancak geçen 9 ay süresinde saldırı maliyetleri düşmüş ve risk artmıştır. Üstelik sürpriz algoritmik gelişmelerin bu durumu hızlı bir şekilde SHA-1 aleyhine döndürme ihtimali de artmıştır.

Durumun farkında olan ABD Standartlar Enstitüsü (NIST), 15 Mart 2006'da bir genelge yayınlayarak federal birimlerin SHA-1 özet algoritmasını, e-imza ve zaman damgası uygulamalarında mümkün olan en kısa zamanda kullanmayı durdurmalarını ve 2010 yılından itibaren ise mutlaka SHA-2 ailesi algoritmalarını kullanmalarını istemiştir. İkinci Kriptografik Özet Fonksiyonlar Konferansı 24 Ağustos 2006 tarihinde Santa Barbara'da yapılacak. Ben bu konferansta yeni saldırıların gündeme geleceğini ve *durumun çok daha hızlı* değişeceğini düşünüyorum.

Telekomünikasyon Kurumu ve Elektronik Sertifika Hizmet Sağlayıcıları mümkün olan en kısa zamanda SHA-1 algoritmasını emekli etmeli ve SHA-2 ailesine geçişi sağlamalıdır.

Peki bu değişiklik olursa eski sertifikalar ve eskiden imzalanmış dokümanlar ne olacak? Herşeyden once eski sertifikalar iptal edilir ve yeni sertifikalar üretilir. SHA-1 algoritmasını bekleyerek daha sonra kaldırmanın maliyeti bence çok daha yüksek olacaktır. Yeni sertifikalar üretilince, eski sertifikalar artık geçersiz olur ve onlarla yapılan yeni imzalar da kabul edilmez. Eskiden imzalı dokümanlar hala imzalı olarak geçerliklerini korurlar; bunlar üzerinde çakışma nedeni ile birtakım saldırılar veya iddialar olursa, mahkemeler böyle bir dokümanın diğer özelliklerine ve alakalı delillere bakarak karar verirler.

Kriptografi sürekli değişim içinde olan bir bilim dalıdır; aslında klişe gibi görünen bu söz bütün bilim dalları için geçerli olmalı diye düşünebiliriz, ancak kriptografik algoritmalar ile ilgili güvenlik ölçütlerimiz, bunlara düzenlenen saldırılar yüzünden zamanla değişir. Daha once bu tip değişikler birkaç on yıl alırken, kriptografik algoritmaları kırmak için bulunan matematiksel yöntemlerin özellikleri ve bunları koşturduğumuz bilgisayar sistemlerinin hız, kapasite ve maliyet faktörleri artık bu değişimlerin sıklığını artırdı. Yapılması gereken şey bu gerçeği kabul edip, konu üzerinde ciddi yatırımlar yapmadan önce konuyu bilen uzmanlara danışmak veya doğru kararları vermektir.

koc@cryptocode.net