SHA-1 özet (hash) fonksiyonu hakkında

ÇETİN KAYA KOÇ

Sayısal imza uygulamasına ek olarak, birçok veri ve kimlik doğrulama protokollerinde SHA-1 kullanılmaktadır.

SHA-1 özet algoritmasının tarihçesi eski sayılır. ABD ulusal standartlar organizasyonu NIST, 1993 ve ardından da 1995 yıllarında SHA-1 algoritmasını standart bir özet fonksiyonu olarak ilan etti. O tarihten beri SHA-1 algoritması, bir özet fonksiyonu olarak, devletlerin ve endüstriyel organizasyonların standartlarında yer aldı. Sayısal imza uygulamasına ilave olarak, birçok veri ve kimlik doğrulama protokollerinde SHA-1 kullanılmaktadır. SHA-1 algoritması 160 bit (20 byte) uzunluklu özet değerler üretir ve dolayısı ile güvenliği 80 bittir. Ortaya çıktığı günden beri üzerinde herhangi bir zayıflık bulunamamış olması, onu tasarlayan kişiler için gerçekten de bir övünç kaynağı olmalıdır.

Ancak bu durum 16 Ağustos 2005'te değişti. Üç kriptografi uzmanı (Wang, Yao ve Yao), SHA-1 algoritmasının güvenliğinin aslında 63 bitden daha iyi olmadığını ve üzerinde teorik bir çakışma (collision) saldırısı düzenlenebileceğini gösterdiler. Bu çalışma, bundan kısa bir süre önce yapılan benzeri bir çalışmanın devamı olarak, SHA-1 güvenliğine vurulan önemli bir darbe olarak karşımıza çıkmıştır. Bu durumda biz, SHA-1 algoritması artık MD5 kadar bile güvenli değil diye düşünmek zorundayız. Ancak bu yapılan saldırı çalışması o kadar da pratik bir çalışma sayılmaz; yazarlar aslında bu kadar çok sayıda deneme yapıp gerçek çakışma vektörleri üretmiş değiller. Bu denemeleri yapmak için dağınık bilgisayarlar kullanmak ve önemli miktarlarda kaynak ve zaman ayırmak gerekli.

Eğer bir çakışma bulunursa, yani özet değeri aynı olan iki farklı veri bulunabilirse, bunların sayısal imzaları da birbirinin aynısı olur. Bu durum SHA-1 kullanan sayısal imza sahiplerinin önemli bir risk altında olduğu anlamına gelir: İmzalamadığımız dokümanlar imzalanmış gibi karşımıza çıkarlar. Bu riskin kabul edilemez olduğu haller vardır. Eğer koruduğunuz değerler binlerce YTL ile ölçülüyorsa, SHA-1 veya MD5 güvenliği sizin için yeterli olabilir. Ancak milyonlarca YTL ile ölçülen değerlerin sayısal imza sahiplerinin SHA-1 kullanması doğru değildir.

E-imza uygulama çalışmalarının hız kazandığı ve kısmen eleştirildiği bu dönemde, "bu SHA-1 baş ağrısı nereden çıktı" diyebilirsiniz. Görevim, bir bilgi güvenliği uzmanı olarak, aydınlatmak ve çözümler üretmek. Bu yazıyla sizi aydınlatmış ve uyarmış bulunuyorum, bir sonraki yazımda ise çözümlerden bahsedeceğim.

koc@cryptocode.net

Düzeltme: Köşe yazarımızın bir önceki yazısında (BThaber Sayı: 567, 24-30 Nisan) iki tane yazım hatası oluşmuştur. 3. paragraf, 5. cümledeki 264 sayısını 2^{64} olarak, 4. paragraf, 1. cümledeki 280 sayısını 2^{80} olarak düzeltir, özür dileriz.