ÖZET FONKSİYONLARINDAKİ ZAYIFLIKLAR VE ELEKTRONİK İMZALARA ETKİSİ

CEVAT MANAP
TÜBİTAK UEKAE, P.K.74, 41470 Gebze Kocaeli, cmanap@uekae.tubitak.gov.tr
A.MURAT APOHAN
TÜBİTAK UEKAE, P.K.74, 41470, Gebze Kocaeli, murat@uekae.tubitak.gov.tr

ÖZET: Elektronik İmza şemalarının önemli bir kısmını oluşturan özet fonksiyonları (hash functions) son dönemde akademik çevrenin yoğun ilgisiyle karşılaşmıştır. Bunun en büyük nedeni son zamanlarda özet fonksiyonlarına düzenlenen ataklarla beraber özet fonksiyonlarının sanıldığı kadar güçlü olmadıklarının anlaşılmasıdır. Standart olarak kullanılan özet fonksiyonlarının benzer yapıda olmaları, özet fonksiyonlarından birine uygulanabilen bir saldırının, bir diğer özet fonksiyonuna da uygulanabilmesini mümkün kılmıştır. Bu çalışmalar sonucunda Elektronik İmza şemalarının da güvenliğini gözden geçirme gereği doğmuştur. Bu nedenle özet fonksiyonlarının güvenlik ve tasarım kriterleri belirlenmeli ve yeni özet fonksiyonlarının tasarımına başlanmalıdır.

ANAHTAR KELİMELER: Elektronik İmza, Özet Fonksiyonu, Kriptografi.

WEAKNESSES IN HASH FUNCTIONS AND DIGITAL SIGNATURES

ABSTRACT : Hash functions are a vital part of Digital Signature schemes which met with interest form the academic community. Main reason of this interest is the recent cryptographic attacks that showed that hash functions are not strong as they are supposed to be. Hash functions used as standards have similar structure which made it possible to use an attack devised for one hash function to attack another hash function. Recent research made it obligatory to review the security of Digital Signature schemes. Hence, security and design criteria for hash functions must be established and new hash functions must be designed with these criteria.

KEYWORDS : Digital Signature, Hash Function, Cryptography

Giriş

Elektronik imzalamada, her kullanıcının bir açık anahtarı bir de gizli anahtarının bulunduğu asimetrik sistemler kullanılır. Açık anahtardan gizli anahtara ulaşmanın hesapsal karmaşıklığı pratik bir atak düzenlenemeyecek derecede yüksektir. Açık anahtarla doğrulama işlemi ve gizli anahtarla imza atma işlemi yapılır. Dolayısıyla bu tür kripto sistemler sayısal imza uygulamalarını mümkün kılmaktadır. Diğer taraftan asimetrik sistemler simetrik sistemlere göre son derece yavaştırlar. Bu nedenle asimetrik sistemler ile bir veriye imza atılmadan önce, simetrik bir yapı ile imzalanacak verinin boyutu küçültülerek özeti elde edilir. Sayısal imza da verinin bu özetine atılır. Günümüzde kullanılmakta olan Elektronik İmza şemalarının temel olarak iki kısımdan oluştuğunu düşünebiliriz. Bu kısımlardan ilki imzalanacak verinin boyunu küçülterek özetini çıkaran "özet fonksiyonu", ikincisi ise oluşturulan özeti kriptografik olarak imzalayan "imzalama algoritması" dır.

Özet fonksiyonları genellikle simetrik algoritma tabanlı ve hızlı algoritmalardır. Ayrıca özetin uzunluğu, verinin uzunluğundan bağımsız ve sabittir. Özet uzunluğu mesajın uzunluğu ne olursa olsun oldukça kısadır (160 bit, 256 veya 512 bit gibi). Dolayısıyla özet kullanımı imzalamanın pratik olarak gerçeklenebilmesini sağlamaktadır.

Özet kullanımının sağladığı hız ve imzalı verinin uzunluğundaki verimlilik imzalama sisteminin güvenliğini olumsuz yönde etkileyebilir. Örneğin aynı özeti veren iki farklı metnin imzaları da aynı olacaktır. Bu sayısal imzaların sağlaması gereken "her veriye tekil imza" özelliğinin sağlanmaması anlamına gelir. Bu da bir güvenlik açığıdır. Çünkü bu durumda bir sayısal imza birbirinden farklı metinler için de geçerli olacaktır. Dolayısıyla, özet fonksiyonları birebir fonksiyonlar olmasalar da, bir verinin özeti sadece o veriyle ilişkilendirilebilen bir

tür parmak izi gibi davranmalıdır. Bu özellik "zayıf çakışmaya dayanıklılık" (weak collision resistance) olarak adlandırılır.

Zayıf çakışmaya dayanıklılığı sağlamak oldukça zor bir problemdir. Bir çok özet fonksiyonunun bu özelliğe sahip olduğu tasarımcıları tarafından iddia edilmiş ancak yıllar sonra bu iddiaların doğru olmadığı yapılan kripto analiz çalışmalarıyla ortaya çıkmıştır.

Günümüzde güvenli özet fonksiyonları tasarımı konusunda birçok açık problem vardır ve bu konudaki çalışmalar blok şifreleme ya da dizi şifreleme algoritmaları üzerine yapılan çalışmalarla karşılaştırılamayacak kadar azdır. Bu nedenle akademik çevrelerde özet fonksiyonlarının güvenlik analizleri ve tasarım ölçütleri konusunda yoğun çalışmalar başlatılmıştır.

Bu bildiri günümüzde kullanılan ve zayıflıkları olan bazı özet fonksiyonlarının güvenlik durumları hakkında bir değerlendirme niteliğinde olup, olası önlem ve faaliyetleri de irdelemektedir.

Özet Çakışmalarının Muhtemel Etkileri

Tüm dünyada standart olarak kullanılmakta olan Elektronik İmza şemaları, genelde "MD ailesi"ne mensup özet fonksiyonlarını kullanmaktadır. MD ailesinin en önemli temsilcileri olan MD4, MD5, RIPEMD, RIPEMD-160, SHA-0, SHA-1, SHA-256 ve SHA-512 özet fonksiyonları aynı yapıtaşlarını kullanmakta ve küçük farklarla birbirlerinden ayrılmaktadır. Son yıllarda yoğunlaşan akademik çalışmalarla bu özet fonksiyonlarının bir kısmının kriptografik olarak güvenli olmadığı ortaya çıkmıştır [1], [2], [3], [4]. SHA-1 özet fonksiyonunun Elektronik İmza şemalarında en yaygın olarak kullanılan özet fonksiyonu olması nedeniyle Wang'ın [2] çalışması büyük önem taşımaktadır. Bu çalışmada SHA-1'e düzenlenen saldırının karmaşıklığı 2^{63} olmasına karşın yakın zamanda SHA-1 için gerçek bir özet çakışmasının (hash collision) tespit edilip, açık literatürde yayınlanması beklenmektedir.

SHA-1'de bulunacak bir özet çakışmasının elektronik imzalar üzerinde çok büyük etkileri olacaktır. Örneğin, Avustralya'da aşırı hız kameraları kaydettikleri görüntünün bütünlüğünü MD5 özet fonksiyonu ile sağlamaktadır. Avustralya mahkemesine yapılan bir itiraz sonucu, mahkeme MD5 özet fonksiyonunun kriptografik olarak kırılmış olması nedeniyle, kaydedilen görüntünün üzerinde oynama yapılmadığı ispatlanamayacağı için, verilen trafik cezasını iptal etmiştir [5]. Bu nedenle, Nitelikli Elektronik İmza'nın en önemli özelliği olan inkar edilememe (non-repudiation) gerektiren elektronik imzalarda SHA-1 kullanımından vazgeçilmesi tavsiye edilmektedir.

MD Ailesi ve Zayıf Noktaları

Saldırıların üzerinde yoğunlaştığı MD ailesi yapısal olarak benzerlikler taşıması nedeniyle risk altındadır. MD ailesindeki özet fonksiyonları "mesaj genişletme fonksiyonu" ve "çevrim fonksiyonu" şeklinde adlandırılan iki kısımdan oluşmaktadır. "mesaj genişletme fonksiyonu" özetlenecek mesaj bloklarını alıp bu bloklardan daha uzun bir bit dizisi üretmekte yani mesaj bloğunu genişletmektedir. "çevrim fonksiyonu" ise genişletilmiş mesaj bloğunu kullanıp yinelemeli olarak özet değerini hesaplamaktadır. MD ailesindeki özet fonksiyonlarının zaman içindeki gelişimleri göz önüne alındığında en büyük gelişmenin "mesaj genişletme fonksiyonu"nda yaşandığı görülür. Bu gelişim sırasıyla şu şekilde olmuştur: MD5 algoritmasında genişletme fonksiyonu sadece mesaj bloklarının kopyalarını çıkarırken, SHA-0 algoritmasının genişletme fonksiyonu mesaj bloklarını birbiriyle XOR'lamakta, SHA-1 algoritmasının mesaj genişletme fonksiyonu mesaj bloklarını hem birbiriyle XOR'lamakta hem de dairesel olarak kaydırmakta, SHA-256 ve SHA-512 algoritmalarının mesaj genişletme fonksiyonu ise hem mesaj bloklarını modülo 2^{32}'de toplamakta hem XOR'lamakta hem de dairesel olarak kaydırmaktadır. MD ailesinin gelişimi izlendiğinde mesaj genişletme fonksiyonunun giderek daha karmaşık hale geldiği görülmektedir. Buna rağmen mesaj genişletme fonksiyonunun sağlaması gereken özellikler ve bu özelliklerin nasıl sağlanabileceği konusunda literatürde önemli bir bilgi bulunmamaktadır. Özet fonksiyonlarına düzenlenen kriptografik saldırılar incelendiğinde bu saldırıların genellikle mesaj genişletme fonksiyonunda bulunan zayıflıkları kullandığı görülür. Hem Wang'ın SHA-1'e [2], hem de Biham ve Chen'in SHA-0'a düzenlediği kriptografik saldırılar [6,7], mesaj genişletme fonksiyonunun yayılım özelliğinin düşük olmasını kullanmaktadır. Bu saldırılarda özetlenecek mesaj bloğunda küçük değişiklikler yapılmakta ve bu değişikliklerin genişletilmiş mesajda oluşturduğu değişiklikler kontrol altına alınarak, genişletilmiş mesajdaki değişikliklerin çevrim fonksiyonu içinde kaybolması sağlanmakta, sonuç olarak farklı mesaj bloklarının aynı özet değerini oluşturması sağlanmaktadır.

Alınabilecek Önlemler

SHA-1 özet fonksiyonunun halihazırda hangi kullanımlarının güvenli hangilerinin güvensiz olduğunu tespit etmek çok fazla insan gücü, zaman ve uzmanlık gerektirmektedir. Örneğin, çakışmaya bağımlılık (collision-resistance) gerektirmeyen kullanımlar güvenli görünmektedir. Firma ve kurumlar, uluslararası entegrasyon gerektiren uygulamalar için geliştirdikleri ürünlerde uluslararası kripto standartlarına göre üretim yapmaktadır. Bu alanda en önemli standart belirleyici kurum ise ABD'de bulunan National Institute of Standarts and Technology (NIST)'dır. NIST bu alandaki çalışmalarda liderliği üstlenmiş durumdadır. NIST'in SHA-1 özet fonksiyonunun yeni projelerde

kullanımını artık onaylamadığı, yeni özet fonksiyonu standardı geliştirilene kadar SHA-2 ailesindeki özet fonksiyonlarının (SHA-224, SHA-256, SHA-384, SHA-512) kullanımını tavsiye ettiği bilinmektedir. Bu nedenle, yeni üretilen sistemlerin, en azından daha uzun özet boyuna sahip SHA–256, SHA–384, SHA–512 gibi özet fonksiyonlarını kullanması gerekmektedir. Yeni bir özet fonksiyonunun tasarlanıp kullanıma geçmesi NIST'in tahmini ile yaklaşık 5 yıl süreceğinden, standart olarak kullanılacak yeni bir özet fonksiyonunun en kısa sürede tasarımına başlanması gerekmektedir. NIST'in bu konuda harekete geçtiği ve çalıştaylar düzenlemek yoluyla akademik çevrelerle işbirliği yaparak yeni bir özet fonksiyonunun tasarlanmasına önayak olduğu bilinmektedir. Bu süreçteki en büyük problem, tasarlanacak yeni özet fonksiyonunun ne kadar güvenli olduğunu belirleyecek hiç bir kriterin bulunmamasıdır. Bu nedenle öncelikle bu kriterlerin oluşturulması için bir çalışma gereklidir. Bu çalışma iki farklı yöntemle yürütülebilir. Birinci yöntem olarak, önce AES standardının oluşturulma aşamasındakine benzer bir özet fonksiyonu tasarlama yarışması düzenlemesi ve bu yarışma sırasında gerçekleştirilecek araştırma faaliyetleri ile özet fonksiyonu tasarımı üzerine bilgi ve deneyim elde edilmesi. İkinci yöntem ise önce akademik araştırma faaliyetlerinin yeterince olgun bir seviyeye gelmesini beklenmesi ve yarışmanın daha sonra düzenlenmesidir. Bu sayede akademik araştırma faaliyetleri ile elde edilen bilgi birikiminin, yarışmaya katılan özet fonksiyonlarının analizini kolaylaştırması hedeflenmektedir. Yeni özet fonksiyonu standardına duyulan ihtiyaç nedeniyle NIST'in en kısa sürede yeni standardı oluşturmak amacıyla birinci yöntemi uygulayacağı tahmin edilmektedir. Bunun yanı sıra NIST yeni özet fonksiyonu standardı oluşturma çalışmalarının 5 yıl süreceğini öngörmekte ve 2013 yılından önce yeni bir standardın yayınlanması beklenmemektedir. Akademik çevrelerde yapılan çalışmalar göz önüne alındığında, akademik araştırmaların SHA-256 ve SHA-512'nin güvenliğini ölçmeye çalışmaktan çok, SHA-1 özet fonksiyonundaki zayıflığı anlamaya veya yeni özet fonksiyonları tasarlamaya yöneldiği söylenebilir. Bu çalışmalar çerçevesinde NIST tarafından birkaç çalıştay daha düzenlenmesi beklenmektedir.

Özet fonksiyonları ile ilgili bir diğer problem de bilgisayar dünyasında bu fonksiyonların gerekli olmadıkları yerlerde de yaygın olarak kullanılmasıdır. Bu durumun sonucu olarak standart kabul edilmiş bir özet fonksiyonundaki problemlerin gerçek dünyadaki yansımalarının önceden kestirilmesi ya da tahmin edilmesi mümkün değildir. Bu nedenle, özet fonksiyonlarının kullanım yerleri ve kullanım amaçları belirlenmeli ve bu amaçlar dışında kullanılmaları engellenmelidir. Özellikle güvenli MAC algoritmalarının varlığı bilinirken özet fonksiyonları MAC algoritmaları yerine kullanılmamalıdır. Endüstri çevrelerinin (Microsoft, Sun, vb.) yaptığı önemli bir tespit de şudur: Akademik çevreler SHA-1'in güvenliği konusunda endişeye kapılmışken, dünyanın büyük kısmı hala SHA-1'e göre çok daha güvensiz olan MD5 özet fonksiyonunu kullanmaktadır. Dünyadaki tüm sayısal haberleşme altyapısında, özellikle elektronik ticaret ve elektronik devlet altyapılarında MD5 ve SHA-1'den daha kuvvetli bir özet fonksiyonuna geçilmesi gerekmektedir. Kısa vadede uygulanabilecek çözüm SHA-1'den SHA-256, SHA-384, SHA-512 gibi daha uzun özet boyuna sahip özet fonksiyonlarına geçilmesidir. Böylece, yeni ve güven veren bir özet fonksiyonu tasarlayabilecek alt yapının oluşturulması için zaman kazanılacaktır. Burada dikkat edilmesi gereken bir diğer husus da SHA-256'nın SHA-1'e göre daha güçlü görünmesine karşın kripto çevrelerine tam olarak güven vermemesidir. Dolayısıyla, tasarlanacak her kripto sisteminde özet fonksiyonlarının kullanım yerleri ve kullanım amaçları ayrı ayrı değerlendirilmeli, bu değerlendirme sonucunda uygun özet fonksiyonu belirlenmeli ve imkan olan durumlarda MAC algoritmaları kullanılmalıdır.

Sonuç

Hem akademik çevrelerin özet fonksiyonları konusunda çalışmaları hem de bilgisayar teknolojisindeki hızlı gelişim göz önüne alındığında en geç 10 yıl içinde SHA-1 için bir özet çakışmasının yayınlanması beklenmektedir. En kısa sürede özet boyu daha uzun özet fonksiyonlarının kullanımına geçilmeli ve NIST'in başlattığı yeni özet fonksiyonu tasarlama girişimi yakından takip edilmelidir.

Kaynaklar

[1] Wang, Lai, Guo, Chen, Yu. Cryptanalysis for Hash Functions MD4 and RIPEMD. Advances in Cryptology-Eurocrypt'05. Springer-Verlag.

[2] Wang, Lin, Yu. Finding Collisions in the Full SHA-1. Advances in Cryptology-Crypto'05. Springer-Verlag.

[3] Wang, Yu. How to Break MD5 and Other Hash Functions. Advances in Cryptology-Eurocrypt'05. Springer-Verlag.

[4] Wang, Lin, Yu. Efficient Collision Search Attacks on SHA-0. Advances in Cryptology-Crypto'05. Springer-Verlag.

[5] www.schneier.com/crypto-gram-0508.html

[6] Biham, Chen. Near Collisions of SHA-0. Advances in Cryptology-Crypto'04 , Springer-Verlag.

[7] Biham, Chen, Joux, Carribault, Jalby, Lemuet. Collisions in SHA-0 and Reduced SHA-1. Advances in Cryptology-Eurocrypt'05 , Springer-Verlag.