ÇEVRİMİÇİ SERTİFİKA DURUM PROTOKOLÜ (OCSP)

BİLEN ÖĞRETMEN

Yazar Adresi, ogretmen@ueake.tubitak.gov.tr

ÖZET : Bu bildiride bir sayısal sertifikaya ait geçerlilik durumunun sertifika iptal listelerine (SİL) gerek duyulmadan çevrimiçi olarak sorgulanabilmesini sağlayan Çevrimiçi Sertifika Durum Protokolü (OCSP) incelenmiştir. OCSP, SİL'nin sayısal sertifikalar hakkında sağladığı durum bilgisiyle karşılaştırıldığında sadece daha güncel durum bilgisi sağlamakla kalmaz aynı zamanda sertifika durumu hakkında ek bilgilerin de elde edilebilmesini sağlar. OCSP protokolüne göre OCSP istemcisi, OCSP sunucusuna bir sertifikaya ilişkin durum istek bilgisi gönderir, OCSP sunucusu ise istemciye söz konusu sertifikayla ilgili durum bilgisini cevap olarak gönderir.

ANAHTAR KELİMELER: Sayısal sertifika, OCSP, SİL, Sertifika geçerlilik durumu

ONLINE CERTIFICATE STATUS PROTOKOL

ABSTRACT :In this paper a protocol (OCSP) used for querying the current status of a digital certificate with no need to CRL is studied. In addition to its timely operation, OCSP provides detailed revocation status information about digital certificates. In OCSP, OCSP client sends a certificate revocation status request to OCSP Server and waits for the receipt of the certificate revocation status response produced by OCSP Server.

KEYWORDS : OCSP, CRL, Revocation Status

Giriş

Günümüzde bilgi sitemlerindeki güvenliği arttırmak üzere büyük güvenlik altyapıları kurulmaktadır. Bilgisayar dünyasında güvenliğin tanımı yapılırken genellikle güvenlik ihtiyaçları göz önüne alınmaktadır. Bu ihtiyaçlar, gizlilik, bütünlük, doğruluk ve inkar edememezlik olarak sıralanabilir. Söz konusu ihtiyaçlar karşılanırken de şifreler, sayısal imzalar gibi kriptolojik teknikler kullanılmaktadır. Güvenlik hizmetlerinin sağlanmasında varlıklara ait anahtarların (genellikle açık anahtar) ve kimlik bilgilerinin bu hizmeti alacak varlıklar arasında paylaşılması gerekmektedir. Sayısal sertifikalar, bahsedilen türden bir paylaşımı sağlayabilecek en ideal araçlar olarak görülmektedir. Çok sayıda varlık barındıran birbirine bağlı açık sistemlerde, varlıklar arasındaki güven ilişkisinin kurulmasında sertifikalar büyük önem taşımaktadır[3].

Sertifikalar, sertifika makamı (SM) olarak adlandırılan güvenilir otoriteler tarafında üretilir ve dağıtılır. Sertifikalara ait geçerlilik periyodu SM'nin güvenlik politikasıyla belirlenir ve bu periyot boyunca sertifikanın geçerliliği garanti edilebilir.

SM bazı durumlarda bir sertifikayı geçerlilik süresi içinde iptal edebilir. Sistemdeki tüm varlıkların bu iptal durumundan haberdar olabilmesi için SM'nin bunu bir güvenlik politikasıyla belirlemesi gerekir. Sertifika durum yönetimi için günümüzde birçok model önerilmiştir. Bu bildiride, sertifika durum yönetiminde ilk olarak kullanılan SİL yönteminden kısaca söz edilecek daha sonra da SİL'e göre bir çok avantaj sağlayan OCSP ayrıntılı olarak incelenecektir. Bildirinin bundan sonraki kısmında öncelikle sertifika durum yönetimi metotlarından söz edilecek, daha sonra OCSP protokolü hakkında bilgi verilecektir. SİL ve OCSP yöntemlerinin karşılaştırılması ve sonuç bölümleriyle bildiri sonlandırılacaktır.

Sertifika Durum Yönetimi Metodları

Sertifika durum yönetimi çevrimiçi veya çevrim dışı olarak yapılabilir. Bazen her iki metodun birlikte kullanıldığı durumlarla da karşılaşılabilir. Çevrimiçi durumda, sertifikalara ait geçerlilik bilgisi SM tarafından önceden oluşturulur ve sistemde yer alan kullanıcıların erişebileceği ortak bir alana yerleştirilir. Çevrimiçi durumda ise, geçerlilik durumu sorgulanan sertifikaya ait durum bilgisi çevrimiçi olarak çalışan güvenilir bir otorite tarafından güncellenir. SİL yöntemi çevrimdışı, OCSP ise çevrimiçi sertifika durum yönetimi metodlarına örnek verilebilir.

Sertifikalar birçok farklı nedenden ötürü iptal edilebilir. Bu nedenlerden başlıcalarına bakılacak olursa,

- Kullanıcının veya Sertifika makamının özel anahtarı çalınmış olabilir.
- Sertifikanın verdiği bilgilerden bir veya bir kısmının değişmesi
- Sertifikanın imzalanmasında kullanılan imzalama algoritmasının kırılmış olabileceği
- Sertifikanın yer aldığı sertifika zincirindeki başka bir sertifikanın iptal edilmesi

Sertifika İptal Listesi (SİL)

Sertifika İptal Listeleri, X.509 tipindeki sertifikalarla birlikte ilk olarak 1988'de ITU-T tarafından ortaya atılmıştır. 1993 yılında ise ikinci sürümüne erişmiştir [3]. SİL'ler, iptal edilmiş sertifikaların listesini taşır ve çevrimdışı olarak belirli periyodlarla üretilir. Bir SİL iptal edilmiş sertifikalara ait seri numaralarını, iptal tarihlerini, ve kendi oluşturulma ve bir sonraki güncelleme tarihlerini içerir. İsteğe bağlı olarak, sertifikaların iptal nedenlerini de içerebilir. SİL yayınlayıcısı tarafından sayısal olarak imzalanır, böylece SİL listesinin geçerliliği de kontrol edilebilir. Herhangi bir sertifikanın geçerliliği kontrol edilirken, söz konusu sertifikayı yayınlayan SM'nin yayınladığı SİL'in imzası kontrol edilir, eğer imza doğruysa sorgulanan sertifikanın SİL'de yer alıp almadığı kontrol edilir. Eğer sertifikaya ait seri numarası SİL içinde bulunamazsa söz konusu sertifika geçerli kabul edilir, aksi durumda sertifika geçersizdir.

Çevrimiçi Sertifika Durum Protokolü (OCSP)

Bu bildiride ayrıntılı olarak incelenecek olan metod IETF tarafında önerilen OCSP'dir. OCSP, bir sertifikaya ait güncel iptal bilgisinin çevrimiçi elde edilmesini sağlayan bir protokoldür. X.509 sertifikaları için tasarlanmış olmasına rağmen farklı tipteki sertifikalarla da çalışabilir. OCSP, SİL yönteminin yerine veya bu yöntemle birlikte kullanılabilir, böylece sorgulanan sertifikaya ait en güncel durum bilgisi elde edilebilir.

OCSP istemcisi bir sayısal sertifikanın kontrolü sırasında, OCSP sunucusuna bir geçerlilik durum isteği gönderir ve söz konusu sertifikayla herhangi bir işlem yapmadan önce OCSP sunucusundan gelecek olan geçerlilik durum bilgisini bekler. OCSP isteği içinde bulunan alanlar

- Protokol sürüm bilgisi
- Hizmet isteği (Hizmeti almak isteyen)
- Sorgulan sertifikaya ait ayırt edici bir özellik (Yayıncı-Seri No, veya Açık Anahtarın Özeti vb...)
- OCSP Sunucusu tarafından işlenebilecek eklentiler

İstek mesajının sunucuya ulaşmasından sonra OCSP sunucusu,

- Mesaj biçiminin düzgün olup olmadığını kontrol eder
- İstenilen hizmetin sağlar (Sorgulanan sertifika(lar) hakkında geçerlilik durum bilgisi oluşturur)
- OCSP istemcisine sertifika durum bilgisini içeren bir cevap gönderir. Aksi durumda hata mesajı üretir.

OCSP yanıtları farklı tiplerde olabilir. Bir OCSP yanıtı, yanıt tipi ve yanıt sekizlilerinden oluşur. Tüm OCSP istemci ve sunucularının desteklemesi beklenen bir OCSP yanıtı bulunmaktadır. Bu bildiride tüm OCSP istemci ve sunucuların desteklemesi beklenen bu yanıt üzerinde durulacaktır. Tüm "anlamlı" OCSP yanıtları elektronik olarak imzalanmalıdır. Yanıtın imzalanmasında kullanılan anahtar,

- Geçerliliği sorgulanan sertifikayı veren Sertifika Makamı
- İstemci tarafından açık anahtarına güvenilen bir OCSP sunucu
- Sertifika Makamı tarafından verilen ve söz konusu Sertifika Makamına ait sertifikaların geçerliliği hakkında sorgulama yapılabilmesini sağlayan özel işaretli bir sertifikaya sahip olan Yetkili Sunucu

Anlamlı bir yanıt mesajı aşağıdaki bileşenleri içerir.

- Yanıtın sürümü
- Yanıt verenin adı
- İstek içinde yer alan tüm sertifikalar için ayrı ayrı yanıt bilgileri
- Seçime bağlı eklentiler
- İmzalama algoritması OID'i
- Yanıtın özetinden hesaplanan imza değeri

İstek içinde yer alan tüm sertifikaların yanıtlarının her birinde ise,

- Sorgulan sertifikaya ait ayırt edici bir özellik (Yayıncı-Seri No, veya Açık Anahtarın Özeti vb...)
- Sertifika durum bilgisi
- Yanıtın geçerli olduğu zaman dilimi
- Seçime bağlı eklentiler

yer alır.

"Anlamlı" sertifika durum bilgisi aşağıdakilerden biri olabilir,

- İyi
- İptal edilmiş
- Bilinmeyen

"İyi" durumu, sertifika geçerlilik sorgulamasına verilen olumlu bir yanıttır. En azından, sertifikanın iptal edilmiş sertifikalar arasında yer almadığını belirtir. Fakat "iyi" durumu, sertifikanın daha önce yayınlandığı veya cevabın söz konusu sertifikanın geçerlilik süresi içinde üretildiği anlamına gelmez. "İptal edilmiş" durumu, sertifikanın iptal edilmiş (sürekli veya geçici) olduğunu belirtir. "Bilinmeyen" durumu ise, OCSP sunucusunun geçerliliği sorgulanan sertifika hakkında bilgiye sahip olmadığını gösterir. OCSP yanıtı, OCSP sunucusu tarafından sayısal olarak imzalanır. Herhangi bir hata durumunda OCSP yanıtı bir hata mesajı içerir. Hata içeren OCSP yanıt mesajları sayısal olarak imzalanmaz. Hata mesajları aşağıdakilerden biri olabilir.

- İstek biçimi doğru değil
- İç hata
- Daha sonra yeniden dene
- İmza gerekli
- Yetkisiz sorgu

OCSP sunucusu, istemciden gelen istek mesajı OCSP sentaksına uymuyorsa "istek biçimi doğru değil" yanıtını üretir.

"İç hata" yanıtı OCSP sunucusunun tutarsız bir duruma geldiğini belirtir. İstek başka bir OCSP sunucusuna gönderilebilir.

"Daha sonra yeniden dene" yanıtı OCSP sunucusunun, gelen isteğe şu an için yanıt vermediğini gösterir.

"İmza gerekli" yanıtı OCSP sunucusu tarafından üretilir ve istemciye isteği imzalayarak göndermesini belirtmek amacıyla oluşturulur.

OCSP sunucusu tarafından gönderilen "Yetkisiz sorgu" yanıtı ise, istemcinin söz konusu sorgulamayı yapma yetkisinin olmadığı durumları ifade eder.

OCSP kullanıcıya daha güvenli ve kapsamlı bilgi sunabilmek için istek ve yanıt yapılarında eklentiler (extensions) kullanılmasını desteklemektedir[2].

OCSP, günümüzde birçok ticari örneklerini görebileceğimiz bir protokoldür. Bu örnekler genellikle HTTP protokolü üzerinde gerçeklenmiştir ve Internet üzerinden sorgulanabilmektedirler. Internet gibi dışarıya açık bir sistem içerisinde ticari bir OCSP gerçeklemesine sahip olmak beraberinde dikkat edilmesi gereken güvenlik sorunları getirmektedir. "İyi" durumu barındıran ve imzalı bir OCSP yanıtı, istemci ile sunucu arasında başka bir bilgisayar tarafından yakalanır ve saklanırsa, geçerliliği sorgulanan sertifikanın herhangi bir sebepten iptal edilmesinden sonra istemci söz konusu sertifikayı tekrar sorguladığında bu ara bilgisayar tarafından istemciye daha önceden saklanmış olan "iyi" yanıtının döndürülmesi bu duruma örnek olarak verilebilir. OCSP, nonce kullanarak bu güvenlik açığının üstesinden gelebilir. Nonce, bir istek ve yanıtı kriptografik olarak örtüştüren rastgele üretilen büyük bir sayıdır. OCSP istemcisi, oluşturduğu istek içerisine kendi oluşturduğu bir nonce değerini yerleştirir ve OCSP sunucusuna gönderir. Sunucu ise cevap oluştururken istemciden gelen nonce değerini alıp OCSP yanıtının içine yerleştirir. Böylece istemci-sunucu arasına üçüncü bir varlığın girip istemciye yanıltıcı yanıtlar göndermesi engellenmiş olur. Bunun yanı sıra TLS/SSL veya başka alt düzeyli protokoller kullanılarak HTTP üzerindeki OCSP gerçeklemelerinin güvenliği sağlanabilir [4].

SİL ve OCSP Karşılaştırması

Sertifikaların doğrulanmasında SİL yöntemi yerine OCSP kullanılması aşağıdaki nedenlerden dolayı tercih edilebilir.

- OCSP sertifikaların iptal durumları hakkında daha güncel bilgi sağlar.
- İstemcilerin SİL'leri kendi lokal depolarına çekmelerine gerek kalmaz. Bu durum daha düşük ağ trafiğine neden olarak bant genişliği kullanımı azaltır
- OCSP kullanıldığında istemciler, SİL'leri incelemek zorunda kalmaz, istemci tarafındaki işlem yükü azalır.
- SİL'ler iptal edilmiş sertifikaları gereksiz şekilde afişe ederler. (Bu durum bir kredi kartı şirketinin yayınladığı kötü müşteri listesine benzetilebilir)

Öte yandan OCSP'nin SİL'e göre dezavantajı olarak, OCSP sunucusunun kimlik kanıtlamak için ürettiği tüm OCSP yanıtlarını imzalaması örnek verilebilir. Bu da OCSP sunucusundaki işlem yükünü arttıran ve OCSP'nin ölçeklenebilirliğini sınırlayan bir durum olarak ortaya çıkmaktadır[5].

Sonuç

Sertifika iptal durumlarının sorgulanmasında farklı metodlar ortaya atılmıştır. Çevrimdışı yöntemler kullanıldığında, sertifika durum bilgilerine ait iki güncelleme arasında uzun bir zaman aralığı bulunduğundan, sertifikaların durumu tam anlamıyla garanti edilemez. Fakat bu durum bazı uygulamalar için yeterlidir. Çevrimiçi yöntemler ise, çevrimdışı yöntemlerle elde edilenden daha güncel sertifika durum bilgisine ihtiyaç duyulduğunda kullanılır. Genellikle, yüksek güvenlik gerektiren durumlarda çevrimiçi yöntemlerin kullanılması tercih edilir.

Kaynaklar

[1] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. IETF, June. 1999. http://www.rfc-editor.org/rfc/rfc2560.txt

[2] P. Hallam-Baker: OCSP Extensions. Internet Draft draft-ietf-pkix-ocspx-00.txt, Sep 03, 1999.

[3] International Telecommunication Union: ITU-T Recommendation X.509 (1997 E): Information technology - Open Systems Interconnection - The Directory: Authentication Framework, 6-1997

[4] M. Myers, R. Ankney, C Adams, S Farrel, C Covey: Online Certificate Status Protocol, version 2, March, 2001

[5] Peifang Zheng. Tradeofs in certificate revocation schemes. SIGCOMM Comput. Commun. Rev., Volume 33, Issue 2, pages 103 – 112, April 2003