Elektronik Posta Güvenliği ve Açık Anahtar Sunucuları

Electronic Mail Security and Public Key Servers

ÖZET

Internet'in yaygın olarak kullanılmaya başlanması ile birlikte ağ güvenliği ilgili çeşitli sorunlar ortaya çıkmıştır [1,2]. En önemli Internet servislerinden olan Elektronik posta (E-posta) da güvenlik tehditleri altındadır. Bu bildiride öncelikle E-posta uygulamalarının genel güvenlik sorunlarından ve çözümü için yaygın olarak kullanılan PGP (Prety Good Privacy) yazılımından bahsedilecektir. Daha sonra anahtar dağıtım sorunları ve PGP'nin anahtar dağıtım aracı olarak kullandığı açık anahtar sunucuları anlatılacaktır. Bildirinin sonunda ise Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü, Bilgisayar Ağları Araştırma Laboratuvarı'nda bu konuda yapılan ve yapılması düşünülen çalışmalardan bahsedilecektir.

ÖZGEÇMİŞ

Albert Levi
1969 yılında İstanbul'da doğdu. Boğaziçi Üniversitesi Bilgisayar Mühendisliği bölümünden 1991'de lisans, 1993'da yüksek lisans derecelerini aldı. Şu anda Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü'nde doktora çalışmalarına devam etmekte ve araştırma görevlisi olarak çalışmaktadır. E-posta: levi@boun.edu.tr

M. Ufuk Çağlayan
1951'de Ankara'da doğdu. 1973'te ODTÜ Elektrik Mühendisliği bölümünden lisans, 1975'te ODTÜ Bilgisayar Mühendisliği bölümünden yüksek lisans derecelerini aldı. 1981'de Northwestern Üniversitesi'nde doktorasını tamamladı. Yurt içi ve dışında çeşitli üniversitelerde öğretim üyeliği yaptıktan sonra şu anda Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü'nde doçent olarak görevini sürdürmektedir. E-posta: caglayan@boun.edu.tr

Nazik Kurtuldu
1974 yılında doğdu. 1997 yılında Boğaziçi Üniversitesi Bilgisayar Mühendisliği Bölümü'nden mezun oldu. E-posta: kurtuldu@hamlin.cc.boun.edu.tr

ABSTRACT

Starting with the widespread usage of the Internet, network security became an important issue. Electronic mail (E-mail), which is one of the most important Internet services, has also some security problems. In this paper, first general E-mail security problems and the use of PGP (Pretty Good Privacy) software for the solution of those problems will be discussed. Then, the key distribution problem and the public key servers as the key distribution medium of PGP will be told. At the end of the paper, the studies that are being done and are thought to be done on this subject in Boğaziçi University, Department of Computer Engineering, Computer Networks Research Lab will be given.

Elektronik Posta Güvenliği ve Açık Anahtar Sunucuları

1. GİRİŞ

Internet kullanımının geniş kitlelere açılıp ticari anlamda önem kazanması ile birlikte "ağ güvenliği" önemli bir sorun olmaya başlamıştır [1,2]. Ağlarda güvenlik sorunu olarak yetkisiz erişim sorunları ön plana çıkmaktadır. Bu sorunların bir bölümünün kaynağı uygulamaların tasarım ve kodlama hatalarından doğan gedikleri kullanan bazı kişilerin kendilerine ait olmayan bilgilere izinsiz ve yetkisiz erişimleridir.

En önemli Internet servislerinden olan E-posta, bir tür iki taraflı elektronik veri iletişimi olarak nitelendirilebilir. Bu veri ileşiminin güvenlik gerekleri diğer Internet uygulamalarından farklı değildir. E-postada ön plana çıkan en önemli gereksinim iletilen bilginin kişiselliğidir. Nasıl normal bir postanın alıcısına, başka hiç bir kimsenin postanın içeriğini görmeden ulaşmasını istiyorsak, E-postanın da alıcısına aynı şekilde ulaşmasını istemek en doğal hakkımızdır. E-posta kullanıcısının bir başka gereksinimi ise iletilen bilginin alıcısına değişmeden ulaşmasıdır. Normal postada iletinin zarfa konulması ile çözülen bu iki sorun, E-posta uygulamalarında şifreleme yöntemleriyle çözülmektedir.

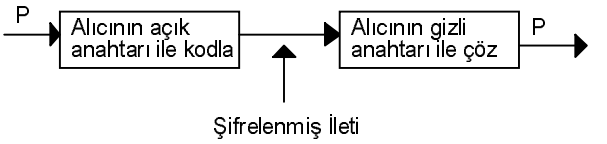
Normal postada bir iletinin göndericisi, kendi kimliğini iletiyi imzalayarak ispatlayabilir. Böylelikle, alıcı hem gönderenin kimliğinden emin olur, hem de bir anlaşmazlık durumunda gönderenin sözkonusu iletiyi gönderdiğini üçüncü bir şahsa ispatlayabilir. E-posta uygulamasında ise bu gereksinim sayısal imzalar ile sağlanmaktadır.

Bu bildiride önce E-posta güvenliği için yaygın olarak kullanılan Pretty Good Privacy (PGP) [2,3,4] yazılımı kısaca tanıtılacaktır. Daha sonra, anahtar dağıtım sorunları ve açık anahtar sunucuları anlatılacaktır. PGP kullanımını yaygınlaştırmak amacı ile Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü'nde yapılmakta olan araştırma-geliştirme faaliyetleri ve ileride yapılması düşünülen çalışmalar bildirinin son kısmını oluşturacaktır.

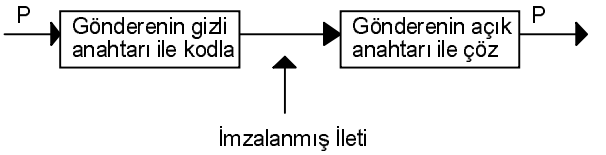
2. PGP

PGP (Pretty Good Privacy) temel olarak insanların E-posta haberleşmesindeki kişisellik (privacy) ihtiyacından doğmuştur. Phillip Zimmermann'ın çabaları ile oluşturulan PGP, şu an dünyada en yaygın kullanılan E-posta şifreleme ve sayısal imzalama yazılımıdır. Açık anahtar tabanlı kodlama algoritmaları kullanan PGP'de herkesin bir gizli, bir de açık anahtarı vardır. Gizli anahtarı sadece sahibi bilir, açık anahtar ise herkese açıktır ve gizli kalmasına gerek yoktur.

PGP kullanarak şifreleme yapmak için alıcının açık anahtarı gereklidir, alıcı şifrelenmiş iletiyi aldığında kendi gizli anahtarını kullanarak şifreyi çözebilir. Bir iletiyi imzalamak için ise gönderenin gizli anahtarı gerekir. Alıcı ise imzanın doğruluğunu kontrol etmek için gönderenin açık anahtarına gereksinim duyar. Şekil 1a ve Şekil 1b, PGP'de şifreleme ve sayısal imzalamanın nasıl yapıldığını göstermektedir.



Şekil 1a İleti Şifreleme



Şekil 1b Sayısal İmzalama

3. ANAHTAR DAĞITIM SORUNLARI

Kökeni Roma İmparatorluğu'na kadar uzanan şifreleme tabanlı iletişim sistemlerinin en köklü ve önemli sorunu anahtar dağıtım sorunu olmuştur. Anahtar dağıtım sorunu iletişimde bulunan iki tarafın ortak bir şifreleme anahtarı üzerinde anlaşmaları sorunudur. Şifreleme anahtarı ile şifreyi çözme anahtarının aynı olduğu klasik şifreleme algoritmaları kullanan sistemlerde, anahtar dağıtım sorunu ya önceden elden ele anahtarı vererek, ya özel ve güvenli bir kanal vasıtasıyla, ya da güvenli anahtar dağıtım sunucuları kullanarak çözülmektedir. Ancak, bu dağıtım mekanizmaları her zaman sorun olmuştur. 1976'da Diffie ve Hellman'ın [5] temellerini attığı açık anahtar (public key) tabanlı şifreleme algoritmaları ve bu algoritmaları kullanan güvenlik sistemleri ile anahtar dağıtım sorununun sona ereceği düşünülmüştür. Açık anahtar tabanlı sistemlerde, şifreleme için kullanılan açık anahtar ve şifreyi çözmek için kullanılan gizli anahtar farklı anahtarlardır ve birinden diğerini elde etmek imkansızdır. Bu yüzden, açık anahtarların herkesçe bilinmesinde bir sakınca yoktur. Bundan başka, açık anahtar tabanlı sistemlerde bir kişi kendi gizli ve açık anahtarını kendisi yaratır ve açık anahtarını yayınlar, gizli anahtarını ise saklar. Açık anahtarın gizli olması gerekmediği için bu dağıtım işleminin gizli ve özel kanallardan olmasına gerek yoktur.

4. AÇIK ANAHTAR SUNUCULARI

Internet gibi milyonlarca insanın birbirleriyle elektronik anlamda konuştuğu bir ortamda herkesin açık anahtarını bilmek nerdeyse imkansızdır. E-posta kullanan çoğu insan belirli bir arkadaş grubu ile iletişimde bulunmaktadır. Bu yüzden, sadece o insanların açık anahtarlarını bilmek E-posta güvenliğinde PGP kullanmak için yeterli olabilir. Ancak, küreselleşen dünyada birbirlerini hiç tanımayan insanların da birbirlerine E-posta atmaları veya haber grupları aracılığıyla haberleşmeleri hiç de ender durumlar değildir. Böyle bir durumda iletişimde kişisellik hedefleniyorsa, hiç tanımadığımız insanların da açık anahtarlarına ulaşmamız gerekebilir.

Açık anahtar sunucuları bu gereksinimi karşılamak amacıyla oluşturulmuşlardır. Şu anda dünyada yaklaşık 25 tane açık anahtar sunucusu vardır. Bir kullanıcı kendi açık anahtarını başkalarının bilgisine sunmak için bu açık anahtar sunucularının herhangi birine kaydettirir. Açık anahtar sunucuları kendi aralarında da haberleşirler. Böylelikle, birine kaydettirilen açık anahtarları diğerleri de öğrenmiş olur. Bu şekilde, birinin açık anahtarını öğrenmek isteyen biri bütün açık anahtar sunucularını dolaşmak zorunda kalmaz. Açık anahtarını kaydettirmek isteyenler de bütün sunuculara kaydettirmekten kurtulmuş olurlar.

Açık anahtar sunucuları aslında birer veritabanından başka bir şey değillerdir. Bu veritabanında açık anahtarlar ve bu anahtarlar üzerindeki anahtar imzaları saklanır. Anahtar imzaları daha sonra özetlenecektir. Bir kişinin açık anahtarını öğrenmek isteyen bir kullanıcı açık anahtar sunucusunu sorgular. Kullanıcı, bu sorgulama sonucu sunucunun gönderdiği açık anahtarlardan kendi aradığını seçer ve bilgisayarına yükler. Açık anahtar sunucularının sorgulanmaları kelime eşleştirme tabanlıdır. Kullanıcı, bir kelime vererek sunucunun veritabanında isim ve/veya E-posta adreslerinde o kelimenin geçtiği anahtarları arattırır. Sunucunun veritabanında her anahtarın sahibinin kimliği ve E-posta adresi de saklanır.

Açık anahtar sunucularının çoğu E-posta arayüzüyle çalışır. Başka bir deyişle, kullanıcı sorgulama amaçlı anahtar kelimesini E-posta ile gönderir ve cevabı E-posta olarak alır. Bunun dışında, WWW arayüzüyle çalışan, daha kullanışlı ve hızlı anahtar sunucular da mevcuttur.

Anahtar sunucularının yapabildiği işlemler temel olarak ikiye ayrılır: sunucuya erişimi olan tüm kullanıcıların yapabildiği işlemler ve sadece sunucu operatörlerinin yapabildiği işlemler.

Tüm kullanıcılar sunucuya açık anahtarlarını kaydettirebilir ve sunucuda kaydı bulunan anahtarları veritabanını sorgulayarak öğrenebilirler. Açık anahtar sunucularının operatörleri ise bu işlemlere ek olarak sunucuda kaydı bulunan anahtarları geçersiz kılma, daha sonra geçerli duruma getirme ve herhangi bir anahtarı sunucudan silme haklarına da sahiptirler. Bu işlemler kullanıcının anahtarına erişimini kaybettiği veya açık anahtarını değiştirdiği durumlarda gereklidir.

Açık anahtar sunucularındaki açık anahtarların tümüne veya indeksine ulaşmak için FTP adresleri de mevcuttur.

5. YANLIŞ AÇIK ANAHTAR SORUNU

Açık anahtarların dağıtımındaki en önemli sorun, insanların yanlış açık anahtar kullanmaları yönünde kandırılmalarıdır. Açık anahtar tabanlı bir yazılım olduğu için PGP'de de sorun olan bu durumu, hem şifrelemede hem de sayısal imzalarda ayrı ayrı incelemek gerekir.

Bir iletinin şifrelenmesi sırasında alıcıya ait olduğu sanılan fakat ona ait olmayan bir açık anahtarın kullanılması, alıcının o iletinin üzerindeki şifreyi çözememesine neden olacaktır. Bunun dışında, anahtarın gerçek sahibi şifreyi çözüp kendisine gönderilmeyen mesajı okuyabilecektir. Bu durum da kişisellik ve bilgi gizliliği açısından son derece sakıncalıdır.

Sayısal olarak imzalanan bir iletinin üzerindeki imzanın doğrulanması sırasında yanlış bir açık anahtar kullanılıyorsa, imza doğru olsa bile doğrulanamayacaktır.

Bu sorunları aşıp doğru açık anahtar kullanmak, küçük bir grup içinde kolay olabilir. Böyle bir durumda, herkes birbirine açık anahtarını ya elden ya da güvenli bir kanaldan dağıtabilir. Ancak, insanların kişiselleşme ihtiyacı geniş kitlelere yayılınca bu dağıtım işlemini daha hızlı ve özdevimli şekilde yapmak gereği ortaya çıkmıştır. Açık anahtar sunucuları bunun için hizmet vermektedirler. Ancak, yanlış açık anahtar sorunu açık anahtar sunucuları ile de çözülememiştir. Çünkü, açık anahtar sunucuları sakladıkları anahtarların doğruluğu konusunda garanti veremezler. Herhangi bir kişi kendi ismini, E-posta adresini ve açık anahtarını deklare ederek sunucuya kaydolabilir. Günümüzün açık anahtar sunucuları, kaydolmak isteyen insanın gerçekten o kişi olup olmadığını ve sözkonusu E-posta adresinin ona ait olup olmadığını kontrol edemezler. Böylelikle, bir kişi bir başkasının adını ve/veya E-posta adresini kullanarak sunucuya kaydolabilir. Açık anahtar sunucularının bu duruma karşı aldığı tek önlem, kayıt işleminden sonra bahsi geçen E-posta adresine bir teyid mesajı göndermekten ibarettir. Böylelikle, eğer sözkonusu E-posta adresi o insana ait değilse, adresin gerçek sahibi kayıt işleminden haberdar olabilecektir. Bu durum bir şekilde E-posta adresi sahteciliğinin önüne geçebilir ama isim sahteciliğini bu şekilde önlemek imkansızdır.

Açık anahtar tabanlı sistemlerde, isim ve E-posta sahteciliğinin önüne geçmek için kullanılan en yaygın yöntem kefalet (certification) yöntemidir. Kefalet, bir açık anahtar, açık anahtarın sahibinin kimliği ve E-posta adresinden oluşan bir veriye herhangi birinin koyduğu sayısal imzadır. Eğer bir başkası kefaleti imzalayan insana güveniyorsa, kefaletin içindeki açık anahtara ve açık anahtarın sahibininin kimliği ile E-posta adresinin doğruluğuna da güvenecektir. Kefalet yöntemleri açık anahtar imzalama yöntemleri olarak da adlandırılmaktadır. Bu sistemde kefaletleri üreten makama Kefalet Otoritesi (KO) denir. PGP'nin kullandığı kefalet sisteminde herkes KO olabilir, başka bir deyişle herkes bir başkasına kefil olabilir. Bu durum, geniş bir açıdan değerlendirildiğinde oldukça dağıtık ve kaotik bir yapı sergilemektedir. Birbirlerini hiç tanımayan insanların ortak güvendikleri KO'lar bulmak hiç de kolay değildir. Ancak, birbirlerini tanıyan küçük grupların haberleşmesinde PGP'nin bu özelliği yararlı olmaktadır.

PGP dışındaki diğer açık anahtar tabanlı güvenlik ve sayısal imzalar sistemlerinde KO'luk görevi belli bir takım makamlara verilmiştir. İnsanlar gerektiğinde kendi açık anahtarlarını bu KO'lara imzalatmak zorundadırlar. Bir bakıma noter görevi gören bu KO'lar hiyerarşik bir ağaç yapısındadır. International Telecommunications Union (ITU) tarafından geliştirilen X.509 [6] standart önerisi, kefalet yöntemlerine, kefalet yapılarına ve KO hiyerarşisine bir standart getirmeyi hedeflemiştir. PGP dışındaki diğer tüm (SSL, PEM, vb.) açık anahtar tabanlı sistemler bu standart önerisine uygun sistemlerdir.

PGP açık anahtar sunucuları, açık anahtarlarla beraber o anahtarlar üzerindeki kefaletleri de saklayabilmektedir. Ancak, üzerinde imza bile olsa, eğer imza sahipleri tanınan ve güvenilen insanlar değillerse, bir açık anahtar sunucusunun döndürdüğü açık anahtara sadece açık anahtar sunucusundan dolayı güvenmek büyük bir yanılgıdır.

6. BOĞAZİÇİ ÜNİVERSİTESİNDE YAPILMAKTA OLAN VE YAPILMASI DÜŞÜNÜLEN ÇALIŞMALAR

PGP hem ilk, hem de ücretsiz oluşu nedeniyle dünyada en yaygın kullanılan E-posta şifreleme ve sayısal imzalar yazılımıdır. Standart dışı yaklaşımlarına rağmen, özellikle kişisel kullanım için tasarlanmış olması, gizliliğe ve kişiselliğe önem veren insanların dikkatini çekmiş ve şu anda dünyada 100 binden fazla kişinin kullandığı bir yazılım haline gelmiştir. Ancak, Türkiye'de PGP kullanımı son derece azdır, yazarların bilgisine göre bu makalenin yazıldığı sırada Türkiye'de sadece 5 kişi PGP kullanmaktadır. PGP'nin yararı ancak geniş kitlelerce kullanıldığı zaman belirginleşecektir. O yüzden, Internet gibi herkesin üzerinden geçen paketleri okuma hakkının olduğu bir ortamda, her zaman bir yerlerde bir meraklı insanın başkalarının E-postalarını okuyabileceği gerçeğini gözardı etmemek gerekir. PGP kullanımı, insanların E-posta güvenliği ve kişisellik konularında bilinçlenmeleri ile birlikte yaygınlaşacaktır.

Boğaziçi Üniversitesi, Bilgisayar Mühendisliği Bölümü'nde E-posta güvenliği ve kişisellik için PGP kullanımını Türkiye çapında yaygınlaştırmak amacıyla çalışmalar yapılmaktadır. Bu çalışmaların en önemlisi bir açık anahtar sunucusu kurulmasıdır. WWW arayüzlü olan bu sunucu, işlev ve içerik olarak diğer sunuculardan farklı değildir. Ancak, sunucunun Türkiye'de olması, kullanıcının bilgiye daha hızlı ulaşmasını sağlayacaktır.

PGP açık anahtar sunucusu şu anda deneysel olarak çalışmaktadır. WWW arayüzlü olan bu sunucuya "http://fangri.cmpe.boun.edu.tr/KEYSERVER.html" adresinden ulaşılabilir. PGP açık anahtar sunucusu halen dünyadaki bütün anahtar sunucularının kullandığı orijinal İngilizce arayüzü kullanmaktadır. Bu arayüzde açık anahtar kaydetme ve açık anahtar öğrenme işlemleri yapılabilmektedir. PGP açık anahtar sunucusu için bir Türkçe arayüz de yazılmaktadır. İşlevsel olarak bir değişiklik olmamakla beraber, arayüzün Türkçe olması kullanımı kolaylaştıracaktır.

Sunucunun yanısıra, PGP kullanımını yaygınlaştırmak ve E-posta kullanıcılarını kişisellik konusunda bilinçlendirmek için konuyu aydınlatan Türkçe WWW sayfaları oluşturulmustur ve yeni sayfaların oluşturulmasına devam edilmektedir. PGP Türk Web Sitesinden PGP ile ilgili diğer sayfalara ulaşılabilir, yazılımın kendisi elde edilebilir ve PGP'yi Türkçe anlatan dokümanlar okunabilir. PGP Türk Web Sitesinin adresi "http://fangri.cmpe.boun.edu.tr"dir.

Orjinal PGP istemci yazılımı, İngilizce arayüzü olan bir yazılımdır. Daha uzun vadeli bir çalışma olarak, arayüzü daha kullanışlı ve Türkçe uç kullanıcı PGP yazılımları üretilmesi de düşünülmektedir. PGP'nin kaynak kodlarının da dağıtılması bu çalışmayı mümkün kılacaktır.

Yine uzun vadede yapılması düşünülen diğer bir araştırma-geliştirme faaliyeti de daha güvenilir bir sunucu yazılımı oluşturmaktadır. Böylelikle, kullanıcılar açık anahtar sunucularından öğrendikleri anahtarların doğruluğuna güvenebilecektir. Açık anahtar sunucusu ile kullanıcı arasındaki protokole bir kaç mesaj transferi ekleyerek açık anahtarı sunucuya kaydeden kişinin gerçekten o kişi olup olmadığı anlaşılablir. Diğer bir yaklaşım da açık anahtar sunucusunun aynı zamanda KO'luk görevi de yüklenmesidir. Sadece kendi güvendiği açık anahtarları tutacak olan bu sunucuya güvenen diğer kullanıcılar, sunucunun tuttuğu açık anahtarların doğruluğuna da güvenecektir. Türkiye geneli için düşünüldüğünde bu yapı hiyerarşik bir yapıya dönüştürülebilir. Ana KO'nun Boğaziçi Üniversitesi'nde geliştirilen açık anahtar sunucusunun olduğu ve altında yerel KO'lar olarak da üniversitelerin, büyük şirketlerin ve devlet kuruluşlarının olduğu bu hiyerarşik yapıda en fazla 2-3 güven zincirinden sonra doğruluğuna güvenilir bir açık anahtara ulaşmak mümkün olabilecektir. X.509 standardı da benzer bir hiyerarşi önermektedir. PGP açık anahtar sunucusunun sadece doğruluğuna güvendiği anahtarları saklaması, sunucunun evrensel özelliğini yitirmesi anlamına da gelmektedir, çünkü diğer açık anahtar sunucularında doğruluğuna güvenilmeyen birçok açık anahtar da vardır. Normal bir PGP açık anahtar sunucusu, diğer açık anahtar sunucuları ile haberleşerek kendi aralarında senkronizasyon sağlarlar. Ancak, önerilen sistemde, doğruluklarına güvenilmedikleri için birçok açık anahtar tutulamayacaktır.

7. TEŞEKKÜR

Türkiye'de PGP anahtar sunucusu kurulmasını 97A0102 numaralı proje ile destekleyen Boğaziçi Üniversitesi Araştırma Fonu'na, 96K120490 numaralı proje ile destekleyen Devlet Planlama Teşkilatı'na ve Albert Levi'nin doktora çalışmalarını verdiği burs ile destekleyen TÜBİTAK'a teşekkür ederiz.

8. KAYNAKÇA

1. Tanenbaum A. S., Computer Networks, 3rd Edition, Prentice-Hall, New Jersey, 1996.

2. Stallings, W., Network and Internetwork Security, Prentice-Hall, New Jersey, 1995.

3. PGP User's Guide Volume I: Essential Topics, Philip Zimmermann, http://www.pegasus.esprit.ec.org/people/arne /pgpdoc1/pgpdoc1.html

4. PGP User's Guide Volume II: Special Topics, Philip Zimmermann, http://www.pegasus.esprit.ec.org/people/arne /pgpdoc2/pgpdoc2.html

5. Diffie, W., and M. E. Hellman, "New Directions in Cryptography," IEEE Trans. Inform. Theory, vol. IT-22, no. 6, sayfa. 644 - 654, Kasım 1976.

6. ITU-T Recommendation X.509, ISO/IEC 9594-8, Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 1993.