Nasıl bir E-posta güvenliği?

Albert Levi

Sabancı Üniversitesi
Mühendislik ve Doğa Bilimleri Fakültesi
levi@sabanciuniv.edu

Giriş

Bilgisayar bağımlısı yaşayan ve çalışan çoğu insanın güne başlarken yaptığı ilk iş muhtemelen e-postalarını okumak ve cevaplamaktır. İnternet'i İnternet yapan Amerikalıların tabiriyle "*killer application*" da kuşkusuz e-posta'dır. Bu kadar popüler olan bir sistemin, atakların merkezinde olmasını yadırgamamak lazım. Milyonlarca dolarlık zararlar yaratan virüs ataklarının yayılmak için e-posta sistemini kullanması, e-postanın popülerliğinin bir başka göstergesidir.

E-posta, gerek akademik gerek de ticari çevrelerde iş süreçlerinin de içine girmiştir. Resmi yazışmalardan duyurulara kadar haberleşme gerektiren birçok kurum-içi uygulamada e-postayı sistemin herhangi bir yerinde görmek mümkündür. Hal böyleyken gönderdiğimiz ve aldığımız bir e-postanın güvenliği de sorgulanır hale gelmiştir.

Peki e-posta güvenliği deyince ne anlıyoruz? Öncelikle e-postanın adresine ulaşıncaya kadar geçtiği güzergahta yetkisiz kişilerce okunup okunmadığı önemlidir. İkinci ve bazı durumlarda ilkinden daha önemli olan nokta ise gönderenin gerçekten gönderen olduğunu iddia ettiği kişi olup olmadığıdır; yani e-postanın başlık (header) kısmında ismi ve e-posta adresi yazan kişi, gerçekten söz konusu e-postayı gönderen kişi midir? Yoksa ortada bir tür kimlik hırsızlığı mı vardır?

Her gün kullandığımız yazılımlar ne kadar güvenlik sağlıyor?

Yukarıda sözü edilen güvenlik gereksinimlerinin her ikisi de, yaygın olarak kullanılan e-posta istemci yazılımlarının varsayılan kurulum ve kullanımlarıyla karşılanamamaktadır. Basit bir e-posta, yol üzerinde her yerde okunabilir. Herhangi biri sizin adınıza e-postalar gönderebilir. Her ne kadar bu durum e-postanın başlık kısmının incelenmesi ile anlaşılabilir ise de bunun garantisi yoktur. Ayrıca çoğu zaman sahtekarı yakalamak mümkün değildir. İşin en kötü yanı, gönderen kişi sonradan gönderdiği mesajı inkar edebilir. Özellikle finanssal işlemlerde bu çok önemlidir. Örneğin bir banka müşterisinin e-posta ile bir havale emri verdiğini ve sonradan bu emri vermediğini iddia ettiğini düşünün. Bankanın elinde bulunan tek kanıt olan e-posta aslında, doğru bile olsa, geçersiz bir kanıttır, çünkü herkes o e-postayı rahatlıkla gönderebilir.

Var olan çözümler ve sorunları

Bahsettiğimiz sorunlar çözümsüz değildir. Genel kabul görmüş iki çözüm olarak PGP (Pretty Good Privacy) ve S/MIME (Secure / Multipurpose Internet Mail Extensions) sayılabilir. Şimdi bu çözümleri daha yakından inceleyeceğiz.

PGP

Kullandığı kripto algoritmalarının kuvvetliliği ile dikkati çeken PGP, kendini dijital mahremiyetin korunmasına adamış bir aktivist olan Phil Zimmermann tarafından geliştirilen ve gayrı ticari kullanımı ücretsiz bir e-posta güvenlik yazılımıdır. Diğer bir özelliği ise içerdiği güven mekanizmalarının karmaşıklığıdır. Güvenli otorite kavramına karşı çıkan bir yaklaşımın ürünü olduğu için, isteyen herkes açık anahtarları onaylayan bir otorite olabilir. Ancak kullanıcılar güvendiği kişileri kendileri seçerler. Güvenilir olmak da değişik kategorilerde incelenmiştir. Sonuçta ortaya sadece güvenlik konusunda uzman kullanıcıların anlayıp layıkıyla uygulayabildiği karmaşık bir güven mekanizması çıkmıştır.

Kullanıcıların açık anahtarları PGP açık anahtar sunucularında tutulur ve istem bazında bu sunucular tarafından dağıtılır. Bu sunucular aslında birer veritabanı sunucularıdır ve hiçbir şekilde güvenlik imasında bulunamazlar. Yani bir açık anahtarın bu sunucularda bulunması, söz konusu açık anahtarın bahsi geçen kişiye ait olduğunun kanıtı değildir. Ancak çoğu kullanıcı bu gerçeğin farkında olmadan sunucudan indirdiği açık anahtarları doğruymuş gibi kullanmaktadır.

S/MIME

S/MIME aslında bir ürün değildir. IETF (Internet Engineering Task Force) tarafından geliştirilen MIME standardının devamı niteliğinde olan ve ona güvenli e-posta eklentileri getiren bir standarttır. Bu standart, Netscape Messenger, MS Outlook gibi popüler e-posta istemci yazılımları tarafından desteklenmektedir.

S/MIME, açık anahtarların sahiplerinin doğruluğunu garantileme mekanizması olarak güvenli sertifika otoritelerini (Certification Authority – CA) kullanmaktadır. Aslında birer şirket olan bu otoriteler, kişilere ve kurumlara ücret karşılığı dijital kimlik olarak da adlandırılan sertifikalar pazarlamaktadırlar. Bu sertifikalar içinde, kullanıcı bilgileri ile beraber sertifika sahibinin açık anahtarı da bulunmaktadır. Sertifikayı dijital olarak imzalayan CA, sertifika içinde var olan bilgilerin doğruluğuna garanti vermektedir. Bu sertifikayı doğrulayanlar, sertifika sahibinin açık anahtarını güvenli bir şekilde öğrenmiş olmaktadır. Oldukça basit olan bu mekanizmanın çalışması için, CA'lara ait kök sertifika tabir edilen ana sertifikaların e-posta istemci yazılımlarıyla beraber gelmesi veya sonradan kullanıcılar tarafından kurulması gerekmektedir. Sadece gönderenin değil, tüm alıcıların kök sertifikayı kurması gerektiği için, kök sertifikaları yazılımlarla beraber gelmeyen CA'ların varlıklarını sürdürmesi daha zordur.

Sertifika üretilirken değişik seviyelerde kimlik kontrolü yapılabilir. Class-1 tabir edilen sertifikalarda sadece e-posta adres erişim doğrulaması yapılmakta, kullanıcının gerçek kimliği ile ilgili herhangi bir kontrol yapılmamaktadır. Bu işlem çevrim-içi yapılabilmektedir. Class-2 ve Class-3 sertifikalarda artan oranlarda kimlik doğrulamaları yapılmaktadır. Class-3 sertifikalar, kişisel başvuru ve kimlik tespiti gerektirdiğinden ancak çevrim-dışı verilebilmektedir.

Class-1 sertifikalar kimlik kontrollü dağıtılmadığı için, bir class-1 sertifikayı başka birinin adına almak ve kullanmak olasıdır. S/MIME'da sertifikalarla ilgili diğer bir sorun da, hangi class olursa olsun, sertifika içindeki isim dışında başka bir isimle imzalı e-posta gönderdiğinizde, istemcilerin imzayı başarıyla doğrulamasıdır. Çünkü istemciler sadece e-posta adres kontrolü yaparlar. İsim kontrolü standartlarca yapılması istenen bir kontrol olmadığı için yapılmaz. Her iki sorun da yazılım hatası olarak değerlendirilmemelidir. Bunlar standartlarda var olan sorunlardır.

Sertifikaların ücret karşılığı satıldığından bahsetmiştik. Ücretsiz dağıtılan sertifikalar da vardır. Ancak bu sertifikalar ya tanınmayan CA'lar tarafından dağıtılmakta, ki bu doğrulamada sorunlar çıkarmaktadır, ya da tanınmış CA'lar tarafından ama kısa süreli (en fazla birkaç ay) verilmektedir.

S/MIME ile ilgili belki de en önemli sorun, halen bir düzene sokulamamış üçlü sacayağı olarak tabir edilen sertifikalar, e-posta istemci sistemleri ve SMTP sunucuları arasındaki birlikte işlerlik (interoperability) sorunlarıdır. Sistemin sorunsuz işleyebilmesi için, herhangi bir CA'dan alınmış bir sertifika kullanılarak, herhangi bir e-posta istemci programı ile gönderilmiş imzalı ve/veya şifreli bir mesajın, alıcı ve gönderen taraflarda hangi SMTP sunucu ürünleri kullanılıyor olursa olsun, sorunsuz bir şekilde iletilebilmesi olmazsa olmaz bir koşuldur. Ancak kişisel tecrübelerimiz, bu üçlü sacayağının o kadar da başarılı bir şekilde birlikte çalışamadığını göstermiştir. Buradaki en önemli sorun, sadece belli başlı e-posta istemci yazılımlarının (Netscape Messenger, MS Outlook gibi) S/MIME'i desteklemesi, ancak çok yaygın olarak kullanılan Hotmail, Yahoo gibi ağ tabanlı e-posta servislerinin bu desteği vermemesidir. Bunların dışında, yukarıda bahsi geçen üçlü sacayağının herhangi bir yerindeki yazılım hatalarından dolayı ortaya çıktığı tahmin edilen performans düşüklüğü, alıcının mesajı düzgün bir şekilde görememesi ve doğru olduğu halde imzaların doğrulanamaması gibi sorunlar da gözlemlenmiştir.

Dağıtık çözüm merkeziyetçi çözüme karşı

Gerek PGP, gerekse de S/MIME doğal olarak dağıtık çözümlerdir. Doğal tabirini kullanmamızın sebebi, e-posta sisteminin yapı itibarıyla dağıtık olmasından kaynaklanmaktadır. Dolayısıyla güvenlik çözümü olarak da dağıtık yapılar kullanılmıştır. Madalyonun diğer yüzüne baktığımızda ise, başta son paragrafta sözü edilen birlikte işlerlik sorunları olmak üzere, yukarıda bahsi geçen birçok sorunun özünde dağıtık yapı olduğunu görürüz. Eğer S/MIME dağıtık olmasaydı, birlikte işlerlik sorunları en aza inerdi; sertifikalar ile e-posta istemci yazılımları birbirlerini daha iyi anlarlardı ve isim sahteciliği yapılamazdı.

Dağıtık yapıda imzalı e-posta gönderen biri, alıcının S/MIME veya PGP desteği olup olmadığını bilmeden göndermektedir. Eğer alıcının bu desteği yoksa, imzalar anlamsız eklentiler olarak görünmekte, hatta bazen - alıcı sistemin, tanımadığı S/MIME formatını yorumlamasına bağlı olarak - mesajın tümü anlamsız bir şekilde gözükebilmektedir. Ayrıca PGP ve S/MIME gibi dağıtık çözümler herkes tarafından kullanılmadığı için birinin tek başına kullanması o kişiyi güvenli kılamamaktadır. S/MIME'ın kritik bir kütleye ulaşamamasının ardındaki nedenlerden biri de budur. Eğer çözüm merkeziyetçi olsaydı, kullanıcıları gruplar halinde güvenli e-posta sistemlerine adapte etmek daha kolay olurdu. Ayrıca hangi kullanıcıların güvenli e-posta desteği ile çalıştığını bilen merkeziyetçi bir sistemde, alıcıların kapasitelerine göre göndericileri yönlendirmek mümkün olabilir ve böylelikle alıcıların işleyemeyecekleri e-postalar alması engellenebilirdi.

E-posta, ağ mimarisi açısından dağıtık olmakla beraber kullanım açısından bakıldığında merkeziyetçi bir yapıya sahiptir. Çünkü insanlar genelde kapalı gruplar içinde haberleşirler. Sabancı Üniversitesi içinde yaptığımız küçük bir araştırma, idari personelin % 80'inin, akademik personelin de %65'inin e-posta trafiğinin kurum-içi olduğunu göstermiştir. Elektronik iş süreçlerinin yaygınlaşmasıyla kurum-içi haberleşme oranı daha da artacaktır.

Bu incelemeler ışığında başlıkta sorduğumuz soruya geri dönecek olursak, nasıl bir e-posta güvenliği hedeflenmelidir?

- Sorunun büyük bir kısmını çözecek merkeziyetçi bir yaklaşım yerinde olacaktır.
- Sertifika kullanmaktansa, açık anahtarların istem bazında merkezi bir sunucu tarafından dağıtımı birçok yönden sorun gidericidir. Ortada sertifika diye bir kavram olmayacağı için
  - sertifika ücreti diye de bir şey olmayacaktır,
  - uyumsuzluk sorunları ortadan kalkacaktır,
  - sertifika iptal kontrolü yapmak gerekmeyecektir,
  - sertifika ile birlikte etrafta kontrolsüz bir şekilde e-posta adresleri dolaşmayacaktır.
- Sisteme ilk kayıt da dahil olmak üzere tüm işlemler çevrim-içi ve kullanıcıya saydam gerçekleştirilmelidir.
- Kullanıcıların güvenlik ve kriptolama konularında uzman oldukları ve kendi güven mekanizmalarını oluşturacak bilgi birikimine sahip oldukları varsayılmamalıdır.
- Şifreleme, orijin kimlik doğrulaması, inkar edememe gibi güvenlik isterleri, ataklara imkan vermeyecek bir şekilde yerine getirilebilmelidir.

Sabancı Üniversitesi'ndeki çalışmalar

Sabancı Üniversitesi'nde yukarıda özetlenen ana prensipler çerçevesinde bir e-posta güvenliği sistemi tasarımı ve gerçeklenmesi tamamlanmak üzeredir. PractiSES (Practical and Secure E-mail System - Pratik ve Güvenli E-posta Sistemi) adı verilen bu sistemde, merkezi bir sunucuda tutulan açık anahtarlar diğer sistem kullanıcılarına sunucunun dijital imzası ile istem bazında dağıtılmaktadır. Potansiyel kullanıcılar (grup üyeleri) hakkındaki kişisel bilgiler ve e-posta adresleri önceden sunucuya kaydedilmektedir. Açık anahtarları sisteme kaydetme aşamasında ise kişisel bilgiler sorgulanarak ve sisteme kayıtlı e-posta adreslerine erişim kontrol edilerek kimlik kontrolü sağlanmaktadır. Sertifika tabanlı olmayan bu sistem, merkezi sunucuya mutlak güven prensibi ile çalışmakta ve böylelikle güvenlik konularında çok da fazla bilgili olmayan kullanıcılara kolaylık sağlamaktadır. Sistemin istemci ara yüzü sunucu ile ortak çalışmaktadır. Böylelikle istemci, sisteme kayıtlı ve güvenli e-posta alabilecek kişilere güvenlik opsiyonları açık, diğerlerine ise normal e-posta gönderebilmekte ve bu işlemi gönderen ve alana saydam bir şekilde gerçekleştirebilmektedir. PractiSES beta versiyonu çok kısa bir süre içinde ücretsiz olarak dağıtılacaktır.