Taktik Sahada Özel Bir Sertifika Doğrulama Problemine Alternatif Yaklaşım

A. Betül Şaşıoğlu, Çağdaş Cirit, Zerrin Çakmakkaya, *Tübitak UEKAE*
Bülent Örencik, *Tübitak MAM-BTE*

***Özet*—Günümüzde kişiler ve kurumlar arasında bilgi paylaşma aracı olarak elektronik posta (e-posta), yaygın olarak kullanılmaktadır. Her türlü kritik bilginin taşındığı bu ortamın olası pasif veya aktif ataklara karşı güvenliği önem arzetmektedir. Bu bildiride öncelikle güvenliğin vazgeçilmez olduğu askeri ortamlar için kullanılan mesajlaşma mimarisi ele alınmaktadır. Daha sonra düşük bant genişliği ve veri kayıplarının fazla olduğu taktik sahada güvenli mesajlaşma problemleri ortaya konulmakta ve en son olarak da mesaj iletmede imzalı/şifreli bir mesajın imza doğrulama hatasından kaynaklanan özel bir probleme çözüm önerilmektedir.**

***Anahtar Kelimeler*—Açık Anahtar Altyapısı, Güvenli Elektronik Mesajlaşma, Taktik Saha, Sertifika Doğrulama.**

***Abstract*—E-mail is widely used for sharing of information among people and organizations. The security of this platform data transferring against active and passive attacks is very important. In this paper, first of all, the military messaging architecture in which the security is mandatory is discussed. Then the tactical secure messaging environment, in which the problems such as low bandwidth and data losses in the network are valid, is evaluated. And lastly, a solution to a specific messaging problem caused by signature verification is proposed.**

***Index Terms*—Certificate Validation, Public Key Infrastructure (PKI), Secure Messaging, Tactical Domain.**

I. GİRİŞ

KİŞİLER ve kurumlar arasında bilgi alışverişini elektronik ortamda, bilgisayarlar aracılığıyla sağlayan elektronik posta (e-posta), gün geçtikçe her alanda hayatımızın içine girmektedir. E-posta, başlangıçta sadece düz yazı göndermek amacıyla geliştirilmişken, teknolojinin gelişmesiyle birlikte e-posta içinde resim, ses, video, html dokümanları da göndermek mümkün hale gelmiştir.

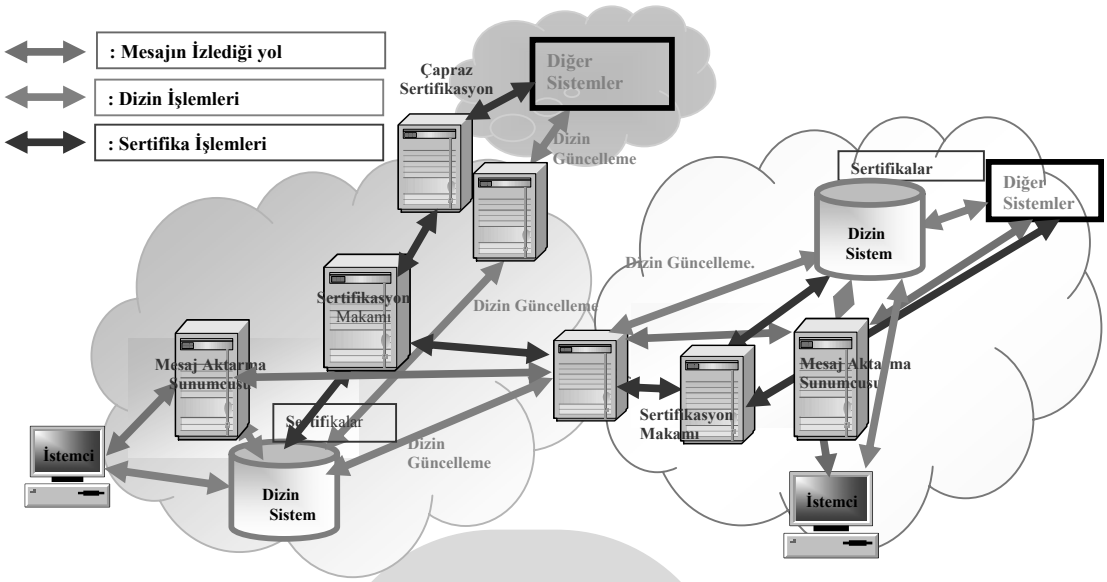
E-posta, her türlü bilginin yüksek hızlı ve düşük maliyetli olarak iletimini sağlamış ancak beraberinde bazı yeni sorunların ortaya çıkmasına aracı olmuştur: Elektronik haberleşme ortamlarında, bilginin yetkisiz kişilerin eline geçmesi ya da ilgili kişiye/kuruma ulaşamaması gibi güvenlik problemlerine rastlanabilmektedir. Bu durum, kurumların ticari kayıplara uğramasına neden olabilmekte, özellikle de askeri uygulamalar gibi bilginin gizli ve hızlı bir şekilde iletiminin büyük önem taşıdığı durumlarda çok ciddi sonuçlara neden olabilmektedir. [[23]] Bunun için güvenli iletişimi sağlayan çözümlere ihtiyaç vardır. Askeri ve ticari uygulamada güvenlik ve güvenilirlik yaygın olarak Açık Anahtar Altyapısı (PKI: Public Key Infrastructure) ile sağlanmaktadır.

E-posta iletişiminde karşılaşılan diğer bir sorun da farklı formatlarda bilgi taşınmasıyla transfer edilen bilginin veri uzunluğunun artmasıdır. Bu durum, düşük bant genişlikli, veri kaybı ve hataları yüksek bağlantısız taşıyıcı katmanı üzerinden yapılan ve "Taktik Saha" olarak adlandırılan ortamlarda veri transferini güçleştirmektedir.

Bu bildiride, kullanıcılar arasında bilgi teatisinin güvenilir, süratli ve emniyetli bir iletişim altyapısıyla sağlanmasının vazgeçilemez olduğu resmi mesajlaşma altyapısı ele alınmaktadır. Sırasıyla bildiride; güvenli resmi mesajlaşma sistem bileşenleri tanıtılmakta, taktik sahada mevcut mesajlaşma sistemlerinin kullanılmasında ortaya çıkan problemler ve çözümlere değinilmektedir. En son olarak da tespit edilen imza doğrulamasından kaynaklanan bir mesajlaşma problemine çözüm yöntemi önerilmektedir.

Bu metin 21 Eylül 2007 tarihinde kabul edilmiştir.

A. Betül Şaşıoğlu, Tübitak UEKAE, 41470, Gebze/Kocaeli, Türkiye (betul.sasioglu@uekae.tubitak.gov.tr).
Çağdaş Cirit, Tübitak UEKAE, 41470, Gebze/Kocaeli, Türkiye (cirit@uekae.tubitak.gov.tr).
Zerrin Çakmakkaya, Tübitak UEKAE, 41470, Gebze/Kocaeli, Türkiye (zerrin@uekae.tubitak.gov.tr).
Bülent Örencik, Tübitak MAM-BTE, 41470, Gebze/Kocaeli, Türkiye (bulent.orencik@bte.mam.gov.tr).



Şekil 1: Mesajlaşma Sistemi Genel Yapısı

II. GÜVENLİ RESMİ MESAJLAŞMA ALTYAPISI

Güvenli mesajlaşmanın sağlanabilmesi için yerine getirilmesi gerekli olan başlıca unsurlar; veri kaynağının doğrulanması, gizlilik, bütünlük, inkar edememedir. Bu unsurlar imzalama ve şifreleme yöntemleriyle sağlanmaya çalışılır. Buna ilave olarak S/MIME v3 [[7],[8],[9]] standardı kullanılmak suretiyle hazırlanan mesajlarda imzalı alındı notu, güvenlik etiketleri, güvenli mesaj listesi gibi ilave güvenlik unsurları tanımlanabilmektedir.

En genel anlamda e-posta iletiminde kullanılmakta olan mesajlaşma alt yapısının temeli, istemci olarak çalışan "Kullanıcı Arayüzü" bilgisayarları ile mesajların dağıtımını sağlayan "Mesaj Aktarma Sunumcusu"ndan oluşmaktadır. Buna ilave olarak mesajlaşma sistemlerinde kullanıcılara özel bilgilerinin tutulduğu "Dizin Sistemleri" ve "Sertifika Makamı", "Akıllı Kart Okuyucuları", "Akıllı Kartlar" gibi mesajların uçtan uca güvenliğini ve güvenilirliğini sağlamak maksadıyla imzalama ve şifreleme için kullanılan bileşenler yer almaktadır.

Mesajlaşma Sistemi Genel Yapısı

Şekil 1'de verilmektedir. Mesajlaşma Sistemi Uygulama katmanı olarak değerlendirildiğinde yukarıda da bahsedilen başlıca üç önemli alt yapı karşımıza çıkar:

- Dizin Sistemi (DS): Tüm e-posta kullanıcı bilgileri, sertifikalar ve iptal edilen sertifikalara ait CRL (SİL-Serifika İptal Listesi) [[15]], dizin adı verilen özel amaçlı veri tabanında saklanmaktadır. Dizin Sistemi, gerek "Güvenlik Alt Yapısı" ile gerekse "İstemci/Sunumcu Altyapısı" ile direkt bağlantılı olarak görev yapmaktadır. "Güvenlik Alt Yapısı" tarafından oluşturulan Kullanıcı Sertifikaları ve iptal edilen sertifikaların listesinin tutulduğu SIL'ler DS'lerde tutulmaktadır. "İstemci/Sunumcu Altyapısı" ise DS'e mesaj göndermek istediği alıcıların e-posta kullanıcı bilgilerine ve geçerli sertifikalarına ulaşmak için bağlanmaktadır. Genelde mimariye göre DS'ler çok sayıda olup herbir dizindeki bilgilerin güncelliğini koruması gerekmektedir. DS'lerin bilgilerinin güncellenmesi özellikle taktik sahada önemli bir sorun olarak karşımıza çıkar.
- Güvenlik Alt Yapısı: Bu örnekte mesajlaşma sistemlerinde sıklıkla kullanılan Açık Anahtar Alt Yapısı gösterilmektedir. Sertifikasyon Yöneticisi, kullanıcı sertifikalarının oluşturulması ve yönetiminden sorumludur. Şekli sade tutabilmek için Şekil 1'de özel anahtar ve kullanıcı sertifikalarının saklanma mekanizması gösterilmemiştir.
- İstemci/Sunumcu Altyapısı: Son kullanıcıların bulunduğu İstemci makinalarıyla E-posta (SMTP) [[11],[25]] veya X400[[21],[22]] Sunumcuları arasındaki ilişkiyi tanımlamaktadır.

III. TAKTİK SAHADA MESAJLAŞMA SİSTEMLERİNDE KARŞILAŞILAN SORUNLAR

Günümüzde bağlantısız haberleşmenin yaygınlaşmasıyla esnek ofis ortamlarına geçiş sağlanmıştır. Bağlantısız taşıyıcı ortamların kapasiteleri gün geçtikçe artmakta ancak bu hatların saldırılara fazlasıyla açık olması güvenlik çözüm arayışlarını da beraberinde getirmektedir. Ayrıca askeri uygulamalarda taktik saha olarak adlandırılan düşük bant genişlikli, yüksek veri kayıpları olan bağlantısız ortamlarda da "Güvenli Resmi Mesajlaşma" kesintiye uğramaksızın

kullanılmak istenmektedir. Bu durum, güvenli mesajlaşmanın uygulanmasında genel yapısı tanıtılan "Güvenli Resmi Mesajlaşma Altyapısı" bileşenlerinin taktik saha için de geçerli olması anlamına gelmektedir.

Taktik sahada bahsi geçen yöntemlerin kullanılmasında şu şekilde sorunlar yaşanmaktadır: [[30]]

- Yüksek bant genişlikli bağlantılı taşıyıcı ortamlar için geliştirilen güvenli mesajlaşma yöntemleri taktik sahada çoğu zaman performans problemleri yaratmaktadır.
- Taktik sahadaki bant genişliği, veri kaybı v.s. gibi ortam özelliklerden kaynaklanan kısıtlar nedeniyle mesajlaşma kapasitelerinden ve/veya uçtan uca güvenlikten ödün verme durumu ortaya çıkmaktadır.
- Taktik Sahada yaygın kullanımı bulunan kablosuz iletişim ortamının topolojisi nedeniyle her türlü saldırılara açıktır. Güvenli haberleşmeyi sağlamak bağlantılı ortamlara göre daha büyük bir sorun olarak karşımıza çıkmaktadır.

Standart protokolleri her seviyede kullanmak sistemlerin birlikte çalışmasını ve esnekliği sağlamakta ancak yukarıda özetlenen sorunlar ortaya çıkmaktadır. Bu sorunların üstesinden gelmek için kablosuz iletişim ortamlarında protokollerin basitleştirilmesi yöntemi benimsenir. Burada ana prensip taşınan verinin mümkün olduğunca azaltılması ve bu şekilde bant genişliğinden tasarruf sağlanmasıdır.[[29]] Ayrıca kablolu ortamlarda kullanılan "Ulaşım Katmanı" protokolleri kablosuz ortamlara uygun olmadığından bu katmanda protokol değişikliğine gidilir.[[30]] Son olarak "Uygulama Katmanı"nda kullanılan standart protokollerin taktik sahada geçerli olabilmesi için bu katman protokolleri ile farklı olan "Ulaşım Katmanı" protokolleri arasında "Taktik Saha Adaptasyon Katmanı" oluşturulur.

IV. SERTİFİKA DOĞRULAMA PROBLEMİ VE ÇÖZÜM ÖNERİSİ

Dizin sistemlerinde içerisinde bulunan farklı dizinlerin içeriklerininin güncel bilgileri taşıyabilmeleri için belli koşullarda verilerin kopyalanması gerekmektedir. Bu güncelleme işlemi için büyük miktarlarda veri transferine ihtiyaç duyulmaktadır. Özellikle Taktik sahada, ortam koşulları gereği zaman zaman veri transferi kesintiye uğrayabilmektedir. Burada ele alınan senaryoda dizinde tutulan ve güncellenmesi gereken bir İmzalama sertifikasının ve/veya SİL'in güncellenememesi durumudur. (Şekil 2)

Bu durumda, B kullanıcısının bağlı olduğu dizinde A kullanıcı ucuna ait İmzalama sertifikası güncellenememekte ve bu esnada acil ve gizli bir mesaj A kullanıcısından B kullanıcısına gönderilmek istenmektedir. Bu durumda mesajın direkt olarak (aracısı olmaksızın) ya da Güvenilir Mesaj Aktarım Birimi (GMAB) aracılığıyla ulaştırılması şeklinde iki çözüm değerlendirilmektedir. Burada GMAB güvenilir makam rolünü üstlenmekte ve kendisine ulaştırılan mesajların alıcılarına mesajları güvenli bir biçimde iletmekle sorumludur. Bu birimin kimliğine her zaman güvenilmesi gerektiği için bazı özel koşulları sağladığı varsayılmaktadır. GMAB kendi imzalama ve şifreleme özel anahtarlarını güvenli bir ortamda saklar, çalınması veya iptal edilmesi gibi durumlar söz konusu değildir. Açık anahtarları ise sahadaki kullanıcı makinelerinde gömülü olarak bulunur ve güvenilen sertifikalar arasında yer alır. GMAB'nin sertifikalarının değişmesi gerekiyorsa, yeni açık anahtarların bulunduğu sertifikaların uç kullanıcılara güvenilir yollarla ulaştırılması sağlanır. GMAB'nin güncel dizin sistemine kesintisiz erişimi vardır; imza doğrulama ve şifreleme işlemlerini her zaman güncel sertifika ve SİL'leri ile yaptığı için sahadaki kullanıcılar GMAB'den gelen mesajların gerçekten mesajın göndericisi tarafından gönderildiğini bilir.

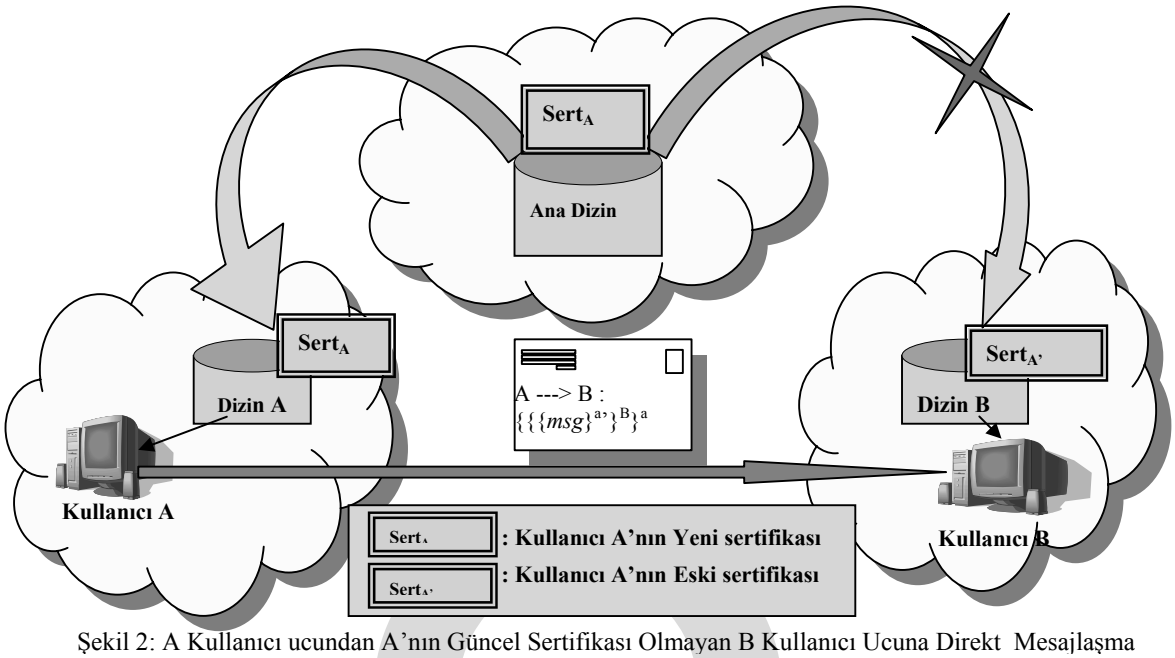
Öncelikle direkt mesajın ulaşmasını inceleyelim: Olası senaryolar;

1) SİL güncel değildir ve göndericinin sertifikasına erişilebilmektedir.

Bu durumda göndericinin imzalama sertifikası dizinden çekilebilmiş ya da göndericinin sertifikası yenilenmiş ve gönderici S/MIME v3 standardında [[7]] tanımlanan seçenekli olarak bırakılmış olan sertifikanın mesaj içerisinde gönderilebilmesi özelliğini kullanarak yeni sertifikasını mesaj ile birlikte alıcıya ulaştırmıştır. Her iki durumda da alıcı gönderenin sertifikasının zincir kontrolünü yapmalı ve bu sertifikanın SİL'de olup olmadığını kontrol etmelidir. Böylece mesajın gerçekten göndericiden geldiğini ve bütünlüğünün korunduğunu anlayabilecektir.

Göndericinin sertifikasının SİL'de yer alıp almadığını kontrol etmek için dizinden liste çekilmiş fakat listenin güncelliğini kaybettiği görülmüştür. Dizin sistemi imkansızlıklar yüzünden güncelliğini kaybetmiştir. Bu durumda alıcının SİL kontrolünü yapabilmesi için sertifika içerisinde belirtilen Online Certificate Status Protocol (OCSP) veya CRL Distribution Point (CRLDP) adreslerini çevrimiçi kullanması gerekecektir [[4]]. Burada belirtilen OCSP, bir sertifikanın iptal edilip edilmediğine dair güncel bilginin çevrim içi alınabilmesini sağlayan bir protokoldür. İstemci, durumunu sorgulamak istediği sertifikaya ait ayırt edici bir özellik (yayıncı & seri numarası, veya açık anahtarın özeti gibi) ve diğer eklentilerden oluşan hizmet isteğini OCSP sunucusuna gönderir. Sunucu, sertifikanın durumu ve geçerli olduğu zaman aralığı gibi bilgileri içeren bir yanıt oluşturarak imzalar. Yanıtın imzalanmasında kullanılan özel anahtar, geçerliliği sorgulanan sertifikayı veren makama ya da istemci tarafından açık anahtarına güvenilen bir OCSP sunucusuna ait olabilir. CRLDP adres noktalarında ise ilgili sertifikayı veren yayıncı kuruluşun güncel SİL'leri bulunmaktadır.

OCSP kullanılması durumunda alıcının çevrimiçi bir adrese bağlanarak istekte bulunması ve dönen cevabı doğrulayarak işleme devam etmesi gerekmektedir. Dönen cevabın imzalı olması boyutunu artırarak kısıtlı olan bant genişliğinde alınması sorun yaratabilecektir. Ayrıca güvenlik hat safhada olduğu için tekrar saldırılarından korunmak amaçlı büyük bir rastgele sayının üretilip istekle beraber gönderilmesi ve dönen cevapta aynı sayının geri döndürülmesi beklenmektedir. Bu büyük sayı da trafikteki verinin boyutunu arttırabilecektir.



Şekil 2: A Kullanıcı ucundan A'nın Güncel Sertifikası Olmayan B Kullanıcı Ucuna Direkt Mesajlaşma

CRLDP kullanılması durumunda alıcının SİL'in tamamını yereline indirmesi gerekecektir. 10.000 sertifika barındıran bir Sertifika Makamının yayınladığı SİL'in ortamalama olarak 1 MB olduğu düşünüldüğünde kısıtlı bant genişliğinde bu verinin de indirilip kullanılması sorun teşkil edebilmektedir.

Sertifika içerisinde OCSP ve CRLDP adreslerinin verilmediği, bu servislerin çalışmadığı ya da alıcının bu servislere bağlanma imkanı olmadığı durumda (taktik sahada bağlantı kurulmasının sakıncalı olduğu pasif olarak sadece dinleme yapılabildiği durumlar olabilir) alıcı güncel SİL'e ulaşamayarak sertifikanın güncelliğini kontrol edemeyecek ve mesajın gerçekten göndericisinin tarafından gönderilip gönderilmediğini anlayamayacaktır.

2.) SİL güncel değildir ve göndericinin sertifikasına erişilememektedir.

Gönderici SMIME standardında gönderdiği mesajda imza sertifikasını ekleyebileceği seçeneği boş geçerek sadece sertifikanın sağlayıcısının bilgisini ve sertifikanın No'sunu mesaja eklemiştir. Alıcı mesaj bilgisinden sertifikayı bulabilmesi için gereken bu iki bilgiyi çıkarmış ve bu bilgileri kullanarak dizin sisteminden sertifika bilgisini talep etmiştir. Göndericinin sertifikası yenilenmişse ve dizin sistemi kendini güncelleyemiyorsa bu yeni sertifikaya erişilemeyecektir (veya alıcının dizin sistemine ulaşamadığı bir durum oluşarak göndericinin sertifikası elde edilemeyebilir), dolayısıyla alınan mesajdaki imza doğrulanamayacaktır.

Gönderici tarafının bu gibi sorunlar olabileceğini göz önünde bulundurarak her gönderdiği imzalı mesaja sertifikasını eklemesi ise mesaj boyutunu artıracak ve bant genişliğinin verimli kullanılamamasına sebiyet verebilecektir.

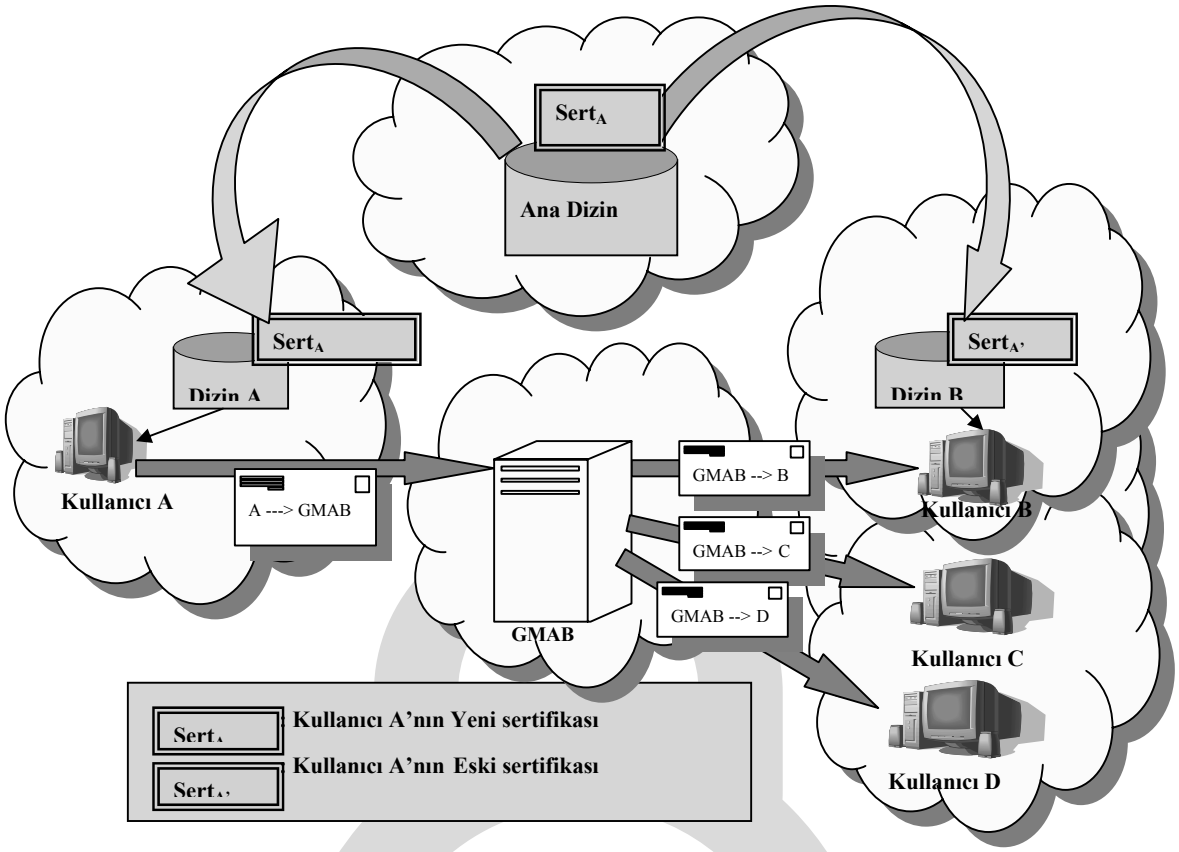
Bu sorunlar göz önüne alındığında göndericinin sertifikasını yenilemek zorunda kaldığı durumda yani B'nin güncel sertifikaya sahip olmadığı durum için bir yöntem önerelim; Bu yöntemde "triple wrapping [[7],[8],[9]]" adı verilen S/MIME v3'de yer alan özelliğin değiştirilerek kullanılması söz konusu olacaktır. Bu yöntemde standartta seçenekli olarak bırakılmış olan imza sertifikasının mesaj içerisinde taşınması sağlanacaktır. Mesaj (Denklem 1)'de verildiği şekilde ilk önce A kullanıcısının eski özel anahtarıyla ($\{msg\}^{a'}$) imzalanacakır. Bu şekilde iç imza oluşturulmaktadır. "Triple Wrapping" standart uygulamasında A kullanıcısı geçerli özel anahtarıyla imzalama yapmaktadır. Bundan sonraki işlemler standart "Triple Wrapping" uygulamasında olduğu gibidir: Eski özel anahtarıyla imzalanmış mesaj ($\{msg\}^{a'}$), B'nin açık anahtarı kullanılmak suretiyle ($\{\{\{msg\}^{a'}\}^B\}$ şifrelenir. En son olarak da A'nın geçerli özel anahtarıyla imzalanmak ($\{\{\{msg\}^{a'}\}^B\}^a$) suretiyle mesaj hazırlanır.

$$A \text{ ---> } B \quad : \{\{\{msg\}^{a'}\}^B\}^a \qquad \textbf{(Denklem 1)}$$

B kullanıcısı, A'nın geçerli "Açık Anahtarı"na sahip olmadığı için kendisine gelen mesajdaki dış imzayı doğrulayamadığında, kendisi için şifrelenmiş mesajı açarak iç imzaya bakacaktır. İç imzanın doğrulanması durumunda öncelikle mesajı yürürlüğe sokabilecek ve aynı zamanda mesaj içerisinde bulunan A'nın Açık İmzalama sertifikasına ulaşacaktır.

Bu öneri iki uç arasında direkt mesajlaşmaya dayanmaktadır ve birçok sakınca barındırmaktadır. İlk olarak "man in the middle attack"[[19]] olarak bilinen saldırıya kolaylıkla maruz kalabilir. Bir kişinin imzalama özel anahtarını ele geçiren kötü niyetli kişi kendine ait imzalama özel anahtarını da kullanarak bu yöntemle kendi imzalama sertifikasını başkasının sertifikası yerine koydurtabilmektedir.

Bu örnekten de anlaşılacağı gibi bir kullanıcının yeni sertifikasına güvenilebilmesi için sadece o kullanıcıdan alınan



Şekil 3: A Kullanıcı ucundan A'nın Güncel Sertifikası Olmayan B Kullanıcı Ucuna GMAB Üzerinden Mesajlaşma

bilgiler yeterli olmamaktadır. Muhakkak güvenilir bir makamın yardımına ihtiyaç duyulmaktadır.

Mesajın GMAB üzerinden iletilmesi durumu (Şekil 3);

A kullanıcısı alıcının dizin sistemindeki sorunlardan haberdardır ya da pasif modda çalışması gerektiğini bilmektedir. Bu durumda gönderdiği mesajın doğrulanmasının riskli olduğunu düşünerek mesajı GMAB üzerinden gönderir. Gönderim ayrıntılarına bakacak olursak;

GMAB güvenilir bir bileşen olduğu için şifreleme ve imzalama sertifikaları/açık anahtarları tüm uç birimlerde mevcut olmalıdır. A göndericisi kendi imza özel anahtarını kullanarak mesajı imzalar $\{msg\}^a$ daha sonra GMAB'nin şifreleme sertifikasını kullanarak GMAB için mesajı şifreler $\{\{msg\}^a\}^{GMAB}$ **(Denklem** 2). Gönderim için hazırladığı mesaja kendi imza sertifikasını koymaz çünkü GMAB dizin sistemine bağlıdır ve dizinini güncel tutmakla sorumludur. Böylece mesaj imza barındırmadığı için gönderimi daha kolay olabilecektir. GMAB kendisine ulaşan bu imzalı ve şifreli mesajın önce kendi şifreleme özel anahtarını kullanarak çözer daha sonra mesajın imzalayanlar kısmından gerekli bilgileri çekerek dizin sisteminden ya da yerel deposundan göndericinin imzalama sertifikasına erişir. Bu sertifikanın geçerliliğinini teyit ettikten sonra sertifikayı kullanarak mesajın imzasını doğrular. Böylece mesajın A kişisinden geldiğini ve mesajın bütünlüğünün bozulmadığından emin olur. Mesajın başlık bilgilerindeki alıcılar kısımını kullanarak mesajı ileteceği adres yada adreslerin bilgilerine ulaşır. Senaryo gereği mesajın B kişisine gideceği bilgisine ulaşır öncelikle mesajı imza özel anahtarıyla imzalar $\{msg\}^{gmab}$ daha sonra alıcı taraf yani B için mesajı B'nin şifreleme sertifikasını kullanarak şifreler $\{\{msg\}^{gmab}\}^B$ **(Denklem** 2) ve mesajı B'ye iletir. B alıcısı kendisi için şifrelenmiş mesajı kendi şifreleme özel anahtarıyla çözer daha sonra mesajın imzalayanlar kısmındaki bilgileri kullanarak imzalayanın GMAB olduğunu anlar (GMAB imza sertifikasını mesaja eklememiştir). Yerel deposunda gömülü bulunan GMAB imzalama sertifikasını kullanarak mesajın gerçekten GMAB tarafından gönderildiğini teyit eder. Böylece mesajın güvenilen makama gerçekten gönderici tarafından iletildiğini ve kendisine bütünlüğü bozulmamış şekilde ulaştırıldığını anlar.

A ---> GMAB	: $\{\{msg\}^a\}^{GMAB}$	
GMAB---> B	: $\{\{msg\}^{gmab}\}^B$	**(**Denklem 2**)**

Bu bildiride önerilen GMAB kullanılanan yöntemin birçok avantajı vardır; mesaj içerisinde imza sertifikası gönderilmesi zorunluluğu ortadan kalkmaktadır, pasif olarak çalışmak zorunda kalan uç birimler OCSP/CRLDP gibi bir dış birime

bağlanmak zorunda kalmamakta ve dolayısıyla fazladan bant genişliği kullanmamaktadır.

V. SONUÇ VE DEĞERLENDIRME

Günümüzde güvenli mesajlaşmanın farklı altyapılara sahip ortamlarda kesintiye uğramaksızın gerçekleştirilmesi büyük önem taşımaktadır. Geniş bant genişliğine sahip kablolu ortamlarda kullanılan mesajlaşma yöntemleri, düşük bant genişliği ve yüksek veri kaybı/hatası içeren kablosuz ortamlarda sorunlar yaratmaktadır. Bu bildiride bu sorunlardan bir tanesi olan SİL'lere ve güncel sertifikalara erişim problemi irdelenmiş ve GMAB kullanan bir yöntem önerilmiştir. Bu yöntemde bant genişliği optimum seviyede kullanılmakta ve OCSP/CRLDP gibi dışbirimlere olan ihtiyacı belli koşullarda ortadan kaldırmaktadır. Taktik sahada pasif çalışması gereken, dizin sistemine erişimlerin sorunlu olduğu veya dizin bilgilerinin güncelliğini yitirdiği birimlere mesaj iletmek isteyen göndericiler GMAB üzerinden mesajlarını hızlı ve güvenli bir biçimde alıcılarına iletebilirler.

REFERANSLAR

[1] [RFC1801]: MHS use of the X.500 Directory to support MHS Routing.
[2] [RFC1802]: Introducing Project Long Bud: Internet Pilot Project for the Deployment of X.500 Directory Information in Support of X.400 Routing
[3] [RFC2527] Chokhani, S., and Ford, W., "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,", 1999.
[4] [RFC2560] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "X.509 Internet Public Key Infrastructure":Online Certificate Status Protocol–OCSP", Mayıs, 1999 http://www.ietf. org/rfc/rfc2560.txt
[5] [RFC2630] R. Housley, ``Cryptographic Message Syntax," Haziran 1999. ftp://ftp.isi.edu/in-notes/rfc2630.txt
[6] [RFC2631] E. Rescorla, RTFM Inc. "Diffie-Hellman Key Agreement Method", http://www.ietf.org/rfc/ rfc2631.txt , Haziran 1999
[7] [RFC2632] Ramsdell, B., Editor, "S/MIME Version 3 Certificate Handling", http://rfc.net/rfc2632.html, Haziran 1999.
[8] [RFC2633] Ramsdell,B., Editor, S/MIME Version3 Message Specification, Network Working Group, Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/ rfc2633.txt Haziran 1999
[9] [RFC2634] Hoffman, P., Editor, Enhanced Security Services for S/MIME, Network Working Group, Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc2634.txt Haziran 1999
[10] [RFC2797] M. Myers · X. Liu · J. Schaad · J. Weinstein, "Certificate Management Messages over CMS" , 2000
[11] [RFC2821], SMTP (Single Mail Transfer Protocol), A.B.D. , 2001
[12] [RFC2828] R. Shirey, GTE / BBN Technologies, "Internet Security Glossary", http://www.ietf.org/rfc/rfc2828.txt, Mayıs 2000
[13] Defective Sign & Encrypt in S/MIME, PKCS#7, MOSS, PEM, PGP, and XML, Don Davis, http://world.std.com/~dtd/sign_encrypt/sign_encrypt7.html#tthFrefAAB
[14] [RFC3580] "S/MIME (Secure/Multipurpose Internet Mail Extensions) Certificate Handling", http://www.ietf.org/rfc/rfc3850.txt
[15] [RFC3280] Housley, R., Polk, W., Ford, W., Solo, D., Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Ağ Çalışma Grubu. http://www.ietf.org/rfc/rfc3280.txt , Nisan 2002.
[16] [RFC3851] S/MIME (Secure/Multipurpose Internet Mail Extensions) Message Specification, http://www.ietf.org/rfc/rfc3851.txt
[17] [RFC3852] Housley, R., Cryptographic Message Syntax (CMS), Ağ Çalışma Grubu. http://www.ietf.org/rfc/rfc3852.txt , Temmuz 2004
[18] W. Stallings, Cryptography and Network Security: Principles and Practice (2nd Ed.), Prentice Hall PTR, Upper Saddle River, NJ, 1997
[19] W. Stallings, Network Security Essentials: Applications and Standards, Prentice Hall PTR, Upper Saddle River, NJ, 2000
[20] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C (2nd Ed.), John Wiley & Sons, 1996
[21] CCITT X.400: Data Communication Networks – Message Handling Systems – Message Handling Services – Message Handling System and Service Overview, 1984
[22] MMHS Extensions to [ITU-T X.400 | ISO/IEC 10021-1]
[23] Şaşıoğlu, B., Acar, D., Güneş, İ., Bahadır, Ö., Çakmakkaya, Z. "Güvenli Kurumsal Mesajlaşma Uygulaması", Ulusal Elektronik İmza Sempozyumu, Ankara, Aralık 2006
[24] Akkurt, D., "Email Güvenliği" Security Letters, Cilt 141, No 21, 41-155, 2005
[25] [RFC2487]: SMTP Service Extension for Secure SMTP over TLS http://www.ietf.org/rfc/
[26] [RFC2830]: Lightweight Directory Access Protocol (v3): Extension for Transport Layer Security.,
[27] [RFC3207]: SMTP Service Extension for Secure SMTP over Transport Layer Security.,
[28] [RFC3546]: Transport Layer Security (TLS) Extensions.,
[29] [RFC3749]: Transport Layer Security Protocol Compression Methods
[30] STANAG 4406 Annex E: Tactical MMHS Protocol and Profile Solution, Version 2, Haziran 2004
[31] "Tactical MMHS Protocol Solutions", NATO MMHS Çalışma Grubu, Ekim 2000
[32] "Transport Layer and Security Protocols for Ad Hoc Wireless Networks", B.S. Manoj, C. Siva Ram Murthy, Prentice Hall PTR
[33] "Computer Networks", Andrew S. Tenenbaum, Prentice Hall