AKILLI KART MOBİL ORTAM DESTEKLİ ASİMETRİK ŞİFRELEME SİSTEMİ İLE İSTEMCİ SUNUCU MİMARİSİNDE GÜVENLİ BİR İLETİŞİM PLATFORMU TASARIMI

Ebru Çelikel, Geylani Kardaş
{celikel, kardas}@ube.ege.edu.tr
Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü, 35100 Bornova/İzmir

Özet: Bu çalışmada sistem yetkilendirmesinin ve güvenliğinin akıllı kart mobil medyaları sayesinde yerine getirildiği bir bilgisayar ağında, kullanıcıların asimetrik anahtarlama kullanarak bilgi alışverişinde bulunabildiği bir protokol tasarımı tanıtılmaktadır. Tasarlanan sistemde, ağ kapsamındaki her bir bilgisayar üzerinde akıllı kartlar ile haberleşecek ve kullanıcılarının belirlenmiş bir elektronik posta sistemine uygun olarak mesaj alışverişi gerçekleştirebilecekleri akıllı kart ve bilgisayar yazılımı bileşenleri yer almaktadır. Sistemde güvenli iletişimi sağlamak amacıyla bir asimetrik şifreleme yöntemi olan *PGP* (*Pretty Good Privacy*) algoritması kullanılmıştır. Adı geçen sistem, bütünleşik sistem testlerinin yapılması ve elde edilen sonuçların teorideki senaryo sonuçları ile karşılaştırılması amacı ile kullanılacaktır.

1. GİRİŞ

Günümüz bilgisayar ve ağ teknolojilerindeki gelişmeler sayesinde bilgisayar iletişimi, gün geçtikçe daha hızlı ve nispeten ucuz hale gelmektedir. Bunun sonucu olarak her geçen gün daha çok sayıda bilgisayar ağ üzerinden birbirine bağlanmakta ve Internet trafiği artmaktadır. Bu sayede coğrafi koşullara bağlı olmaksızın bilginin bir noktadan diğerine transferi kolaylıkla gerçekleştirilebilmektedir.

Ağ altyapısına bağlı çok sayıda bilgisayarın oluşu, ağ üzerinde iletilen bilginin içerik ve önem derecesi bakımından çeşitlilik taşıması anlamına gelmektedir. Bu sebeple iletilen bilginin güvenliğini sağlamak, çoğu zaman iletiyi başarıyla gerçekleştirmek kadar büyük önem taşır. Burada sözü edilen güvenlik:

- Gizlilik (*Confidentiality*): İletinin sadece yetki verilmiş (*authorized*) kişi(ler) tarafından erişilebilir olması, üçüncü kişilerin eline geçmesinin engellenmesi,
- Yetki (*Authentication*): İletinin kaynağının belirlenmesi,

- Bütünlük (*Integrity*): İletinin sadece yetki verilmiş kişiler tarafından değiştirilebilir olması ve kayıpsız olarak göndericiden alıcıya transferinin sağlanması,

- Reddedememe (*Non-repudiation*): Gönderici veya alıcının iletinin varlığını reddedememesi

konularını kapsamaktadır (Stallings, 1995).

Günümüzde ağ üzerinden gerçekleştirilecek bilgi iletimi için, çeşitli veri iletim yöntemleri mevcuttur. Bunlardan en yaygın kullanılanı, elektronik posta yoluyla iletimdir. Bu yöntemde bir ana bilgisayar elektronik posta sunucusu olarak hizmet verirken, buna bağlı istemci bilgisayarlar kendi aralarında elektronik posta yolu ile iletişim kurarlar. Bu tür bir iletişimde güvenlik, çeşitli şekillerde sağlanabilir.

Elektronik posta iletiminde güvenliği sağlamak üzere farklı teknikler kullanılmaktadır. Mesaj iletiminde, yetkilendirme için sayısal imza (*digital signature*) algoritmalarının kullanılması, elektronik postaların trojan virüsü taşıma riskine karşılık virüs kontrollerinin yapılması bunlara birer örnektir.

Güvenli ağ iletimi için kullanılan yöntemlerden biri de Kerberos tekniğidir (Security: Secure Internet Data Transmission URL, 2004). Bu yöntemde bir kullanıcı bir iş istasyonuna (workstation) login olduğunda bu iş istasyonu bu kullanıcıyı yetkilendirir ve böylece kullanıcının şifresinin ağ üzerinden iletimi engellenir. Daha sonra bu iş istasyonu, kullanıcıya sisteme dahil olan diğer ağ kullanıcılarını yetkilendirmeye yarayan şifrelenmiş bilgiyi içeren bir bilet sağlamak üzere, Kerberos sunucusuna bağlanır. Bu sistemin dezavantajlarından biri, sistemde bağlanılmak istenen her bir bilgisayarın Kerberos tekniği ile çalışıyor olmasının gerekliliğidir. Bu yöntemin bir diğer dezavantajı, Kerberos sunucusunun üçüncü kişilerce ele geçirilmesi durumunda, sistem güvenliğinin tamamıyla ortadan kalkacak olmasıdır. Kerberos sisteminde bilgisayarlar arasındaki iletişim değil, sadece yetkilendirme süreci şifrelenmektedir.

Güvenli iletişim için bir başka yöntem, güvenli uzaktan yordam çağırma (*Secure RPC – Remote Procedure Call*) tekniğidir. Bu yöntemde bilgisayarlar arası iletişim de dahil tüm süreç, şifrelenmektedir.

Mesaj iletiminde güvenliği sağlamak amacıyla kullanılmakta olan bir başka yöntem de SSL (*Secure Socket Layer*) yöntemidir. Bu yöntemde bir Web sunucusu ile Web tarayıcısı

arasındaki iletişimin tamamı, RSA (Rivest, Shamir, Adelman) açık anahtar şifreleme algoritması kullanılarak şifrelenir.

Bizim sistemimizde, geleneksel elektronik posta güvenlik tedbirlerine ek olarak, sistemde taşınabilirlik (*mobility*) ve ekstra güvenlik sağlayan akıllı kart (*smart card*) bileşeni de yer almaktadır. Akıllı kart ile gerçekleştirilen bir hasta takip sisteminde, yetkilendirmenin DSA sayısal imza algoritması ile sağlandığı bir uygulama bulunmaktadır (Kardaş, 2003).

Takip eden bölümde, tasarlanan sistemin altyapı ve bileşenleri anlatılmakta, üçüncü bölümde sistemin gerçekleştirimine ilişkin detaylar verilmekte, son bölümde ise sonuç ve ileriye yönelik çalışmalara dair öngörüler sunulmaktadır.

2. ALTYAPI

Bir sonraki bölümde detayları verilecek olan sistem mimarisinin daha somut bir biçimde anlaşılabilmesi için bu bölümde sistem gerçekleştirilirken kullanılması düşünülen teknolojiler hakkında bilgiler yer almaktadır. Önerilen sistem güvenli posta oturumları sırasında akıllı kartlar ve posta istemcisi yazılımlarının etkileşimini gerektirdiğinden, söz konusu bu teknolojiler hakkında genel bir bilgi sahibi olmak yaralı olacaktır.

2.1. Akıllı Kart ve JavaCard:

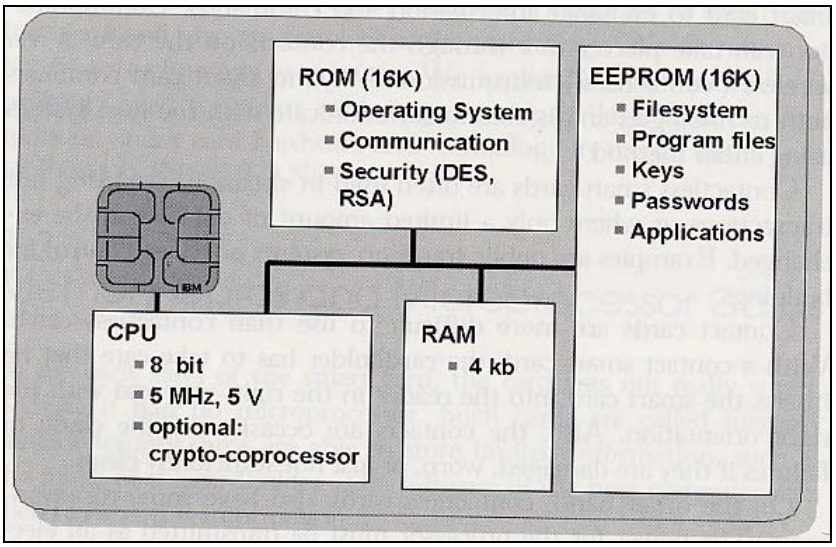
Akıllı kart, içinde bilgi saklayan ve bu bilgiyi işleyen, taşınabilir bir entegre olup standart hafıza-yonga kartlarının gelişmiş bir versiyonudur. Mikroişlemci içeren bu kartlar yerleşik hesaplama güçleri, taşınabilir güvenlik sağlamaları ve kolay kullanımları sayesinde başta telekomünikasyon (cep telefonlarında SIM kart olarak) ve ulaşım olmak üzere birçok sektörde geniş kullanım alanına sahiptir.

Standart hafıza-yonga kart sistemlerinde (örneğin manyetik kart), veri işleme donanım ve yazılımı karttaki bilgiyi okumakta, hesaplamaları yapmakta ve veriyi tekrar

karta yazmaktadır. Akıllı kart sistemlerinde ise kartın içinde hafızaya ilave olarak bir mikroişlemci bulunmakta ve gerekli hesaplamalar onun vasıtası ile yapılabilmektedir. Diğer bir deyişle akıllı kartlar, kart üzerine monte edilmiş bilgisayarlardır. (Kardaş, 2003)

Akıllı kartlara yönelik ilgi, sunmuş olduğu faydaların bir sonucudur. Yerleşik bilgi işleme gücü yanında güvenlik, taşınabilirlik ve kolay kullanım akıllı kartların temel avantajlarıdır.

Şekil 2.1'de görüldüğü gibi bir akıllı kart entegresi; bir mikroişlemci, ROM (*Read Only Memory*), EEPROM (*Electrical Erasable Programmable Read Only Memory*) ve RAM (*Random Access Memory*) bileşenlerini içermektedir. Kart üretilirken bellek mimarisinde yer alan ROM bölgesine, kart işletim sistemi, kalıcı uygulamalar ve kullanıcı bilgileri yazılmaktadır. Kart üretildikten sonra bu bölgeye bilgi yazılamaz. Bu alanda bilgilerin tutulması için elektriksel güce ihtiyaç yoktur. EEPROM bölgesinde de tıpkı ROM'da olduğu gibi kalıcı bilgiler tutulmaktadır. ROM'dan farkı ise bu alana kart üretildikten sonra bile bilgiler ve uygulamalar yazılabilir. Bu bellek alanı kişisel bilgisayarlardaki sabit disklere benzetilebilir. Bilgiler bu alanda yaklaşık olarak 10 yıl süre ile saklanabilmektedir. EEPROM'dan bilgi okuma RAM'den bilgi okuma kadar hızlı olmasına rağmen bilgi yazılması 1000 kat daha yavaştır.



Şekil 2.1: Bir akıllı kart entegresi ve bileşenleri (Hansmann et al., 2000)

RAM bölgesi bilgi modifikasyonu ve depolamada geçici çalışma alanı olarak kullanılmaktadır. Bu bellekte bilgiler, kart bir güç kaynağına bağlı kaldığı sürece tutulmaktadır. Karttan elektrik kesildiğinde bu bilgiler kaybedilmektedir. Bu bellek alanı kişisel bilgisayarlardaki ana bellek ile aynı işleve sahiptir.

2.1.1. Akıllı Kart İletişim Modeli:

Uygulamalarda akıllı kartların kullanılması için kartların CAD (Card Acceptance Device) adı verilen aygıtlara yerleştirilmesi gerekir.

Kart ile ev sahibi (host) arasındaki iletişim kanalı yarı çift yönlüdür (half-duplex). Bilgisayar ağlarında nasıl veriler bir protokole (örneğin TCP/IP) dayanan paketler halinde transfer ediliyorsa aynı durum akıllı kart ile iletişimde bulunduğu bilgisayar arasında da geçerlidir. APDU (Application Protocol Data Unit) adı verilen veri paketleri ya emir ya da cevap mesajları içerirler.

Kullanılan model master / slave (efendi / köle) modeli olup akıllı kart köle, iletişimde bulunduğu terminal ise efendi durumundadır. Akıllı kart her zaman ana bilgisayardan emir APDU'ları beklemekte; gelen APDU içindeki komutları işlemekte ve ana bilgisayara cevap APDU ile yanıt vermektedir (Rankl & Effing, 2000).

2.1.2. JavaCard Teknolojisi:

Java Card teknolojisi, akıllı kart uygulamalarının daha etkin, kolay ve hızlı bir biçimde tasarlanıp hayata geçirilmesini sağlamaktadır. Akıllı kartların ve diğer bellek-sınırlı cihazların Java programlama dilinde yazılmış uygulamaları – ki bu uygulamalara "applet" adı verilir – çalıştırmalarına olanak sunar. Temelde Java Card teknolojisi, Java programlama dilinin birçok avantajını barındıran, güvenli, taşınabilir ve bünyesinde birden fazla uygulama (multiapplication) barındırabilen bir akıllı kart platformu tanımlamaktadır.

Java Card teknolojisinde, Java sistem yazılımının uygulamalara yeterince çalışacak alan bırakacak şekilde akıllı karta yerleştirilmesi hedeflendiğinden Java dilinin özelliklerinin belli bir alt kümesi desteklenmiş ve iki parçadan oluşan bir Java sanal makine mimarisi uygulanmıştır.

Java Card sanal makinesinin biri kart üzerinde biri de kart dışında çalışan iki parçası mevcuttur (Chen, 2000). Uygulama çalışma zamanında yer almayan sınıf yükleme, baytkodu (bytecode) doğrulama, bağlama ve optimizasyon gibi sistem kaynak kapasitesinin önemli olmadığı bir çok işlem kart dışında çalışan sanal makine üzerinde gerçekleştirilmektedir. Bu ayrık sanal makine mimarisinden dolayı platform akıllı kart ve masaüstü bilgisayar üzerinde dağıtık yapıda olup üç parçadan oluşur:

- JCVM (Java Card Virtual Machine), Akıllı kart uygulamalarına uygun Java programlama dili alt kümesi ve sanal makine tanımlamalarını içerir.
- JCRE (Java Card Runtime Enviroment), bellek yönetimi, *"applet"* yönetimi ve diğer çalışma zamanı özellikleri içeren kart çalıştırma işlemlerini tanımlar.
- Java Card API (Application Programming Interface), akıllı kart uygulamalarını programlamada kullanılacak olan çekirdek ve uzantı Java paketlerini ve sınıflarını tanımlar. Bu paketler ve sınıflar *JCF* (*Java Card Framework)*'yi oluştururlar.

2.2. OpenCard Çatısı (Framework):

OpenCard Framework (OCF), Java programlama dili kullanılarak hazırlanmış bir akıllı kart özel yazılımıdır (middleware). *OpenCard Konsorsiyumu* tarafından geliştirilen OCF mimaride, bir akıllı kart ev sahibi uygulaması ile kart okuyucu (CAD) aygıtı arasında yer almaktadır. Çok esnek bir altyapısının olması ve Java dilinde hazırlanmasından kaynaklanan platform bağımsızlığı, akıllı kart uygulama geliştiricilerinin yüksek seviyeli programlama ara yüzlerini kullanabilmelerine ve farklı

kart üreticilerine ait kart okuyucular ile uğraşmaya gerek kalmadan uygulama hazırlamalarına imkan sağlar.

OCF, farklı tipteki akıllı kartlar ile iletişime geçmek ve uygulamalarda kullanabilmek amacıyla iki katmanlı bir yapıdan oluşmaktadır. Bu katmanlar *CardTerminal* katmanı ve *CardService* katmanıdır (OpenCard Consortium, 1999).

2.3. JavaMail API:

JavaMail API'si mesaj okuma, yazma, alma ve gönderme amaçlı seçimlik bir Java paketidir. Bu kütüphane aracılığı ile Microsoft Outlook, Eudora ve Pine benzeri posta istemci yazılımları hazırlamak mümkündür. Akıllı kart etkileşimli posta istemci bileşenlerini hazırlamada bu kütüphane ve sağladığı çatıdan yararlanılması düşünülmektedir. Sistemin prototip kurulumunda bağlantıya geçilecek mail sunucularının desteklediği protokole bağlı olarak değişse de, ilk etapta SMTP (Simple Mail Transfer Protocol) ve POP3 (Post Office Protocol version 3) protokollerinin gerçekleştiriminin bu kütüphane aracılığı ile yerine getirilmesi hedeflenmektedir (jGuru URL, 2001).

2.4. PGP:

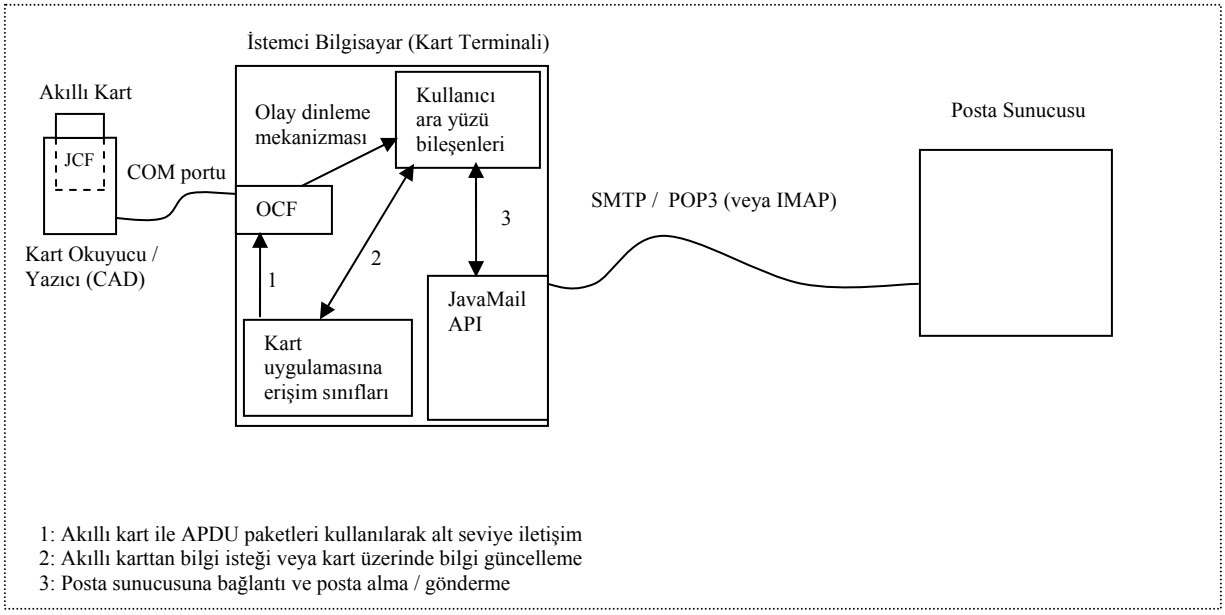
PGP (Pretty Good Privacy) bir halka açık anahtarla şifreleme (public key encryption) sistemi olup en büyük avantajı, anahtarların alıcı ve verici arasında alışverişi için güvenli bir kanala ihtiyaç duymamasıdır (Erkan H. O., 2002). Bir kişiye ait PGP anahtar çiftinden halka açık olan adından da anlaşılacağı gibi herkes tarafından bilinir ve ilgili kişiye gönderilecek iletiler bu anahtar ile şifrelenir. Kişiye özel anahtara ise sadece ilgili kişinin kendisi sahiptir ve kendisine gelen şifreli mesajları bu anahtar ile deşifre eder. Bu iki anahtar üretilirken, halka açık anahtardan yararlanılarak kişiye özel anahtarın belirlenmesine olanak vermemek esas alınmıştır.

3. SİSTEM MİMARİSİ

Bu çalışmada önerilen akıllı kart etkileşimli güvenli posta istemci sistemine ait genel mimari Şekil 3.1'de görülmektedir.

İstemci bilgisayar aynı zamanda bir akıllı kart terminali olup COM portu üzerinden kendisine bir kart okuyucu/yazıcı ünitesi bağlıdır. Elektronik posta istemci yazılımı kart olaylarını kontrol etmek için OCF kütüphanesinden yaralanmaktadır. Akıllı kartlar içerisindeki sistem yazılımları ile haberleşebilmek için sisteme özel tasarlanan erişim sınıfları da yine OCF üzerinden APDU alışverişinde bulunmaktadırlar.

Kullanıcı ara yüzü bileşenleri ise posta istemci yazılımını kullanacak olan kişilere grafiksel kullanıcı dostu bir ortam sağlamaktadırlar. Şifreli mail gönderiminde ve alımında sırası ile SMTP ve POP3 (eğer posta sunucusu IMAP kullanıyorsa bu durumda IMAP) kullanımı gerçekleştirilmektedir.



Şekil 3.1: Sistemin genel mimarisi

Bir posta sunucusundan postalarını indirip okumak isteyen veya posta göndermek isteyen bir kullanıcı kart terminaline içerisinde kendisine ait PGP özel anahtarının

saklandığı akıllı kartını yerleştirir. Olay dinleme mekanizması sayesinde posta istemci programı tetiklenerek kart ile APDU iletişimine başlar. Güvenli kart oturumunun başlatılması için kullanıcıdan PIN girişi istenmektedir. Başarılı PIN girişi sonucunda akıllı kart üzerinde yetkilendirme sağlanır ve posta sunucusuna bağlantı bilgileri akıllı karttan transfer edilir.

Kullanıcıya ait elektronik postalar sunucudan transfer edilir. Transfer edilen postalar ilgili kullanıcının genel (public) PGP anahtarı ile şifrelendiğinden okunabilmeleri için öncelikle deşifre edilmeleri gerekmektedir. Tabi bunun için kullanıcının PGP özel (private) anahtarına ihtiyaç duyulmaktadır. Bu noktada posta istemcisi kullanıcı akıllı kartı ile yeni bir iletişim dizisi başlatarak karttan kullanıcıya ait PGP özel anahtarını ister. Kart üzerinde yetkilendirme tamamlandığı için kart APDU paketleri içerisinde istemci yazılıma anahtarı transfer eder. PGP özel anahtarı elde edildiği için gelen postalar deşifre edilir ve kullanıcıya görüntülenir.

Elektronik posta gönderimi de yine bu kart oturumu içerisinde gerçekleştirilebilir. Kullanıcı postayı göndermek istediği kişi veya kişilerin genel PGP anahtarları ile iletisini şifreler ve ilgili protokol aracılığı ile spota sunucusuna gönderir. Posta sunucusu da kullanıcı adına şifreli postaları alıcılarına gönderecektir.

4. SONUÇ VE İLERİYE YÖNELİK ÇALIŞMALAR

Bu çalışmada, bir asimetrik şifreleme sistemi olan PGP kullanarak, akıllı kart mobil ortam destekli istemci sunucu mimarisinde güvenli bir iletişim platformunun tasarımı anlatılmıştır. Geliştirilecek bu sistem, güvenli elektronik posta iletimi amacıyla kullanılacaktır.

Tasarlanan bu sistemde kullanılan akıllı kart bileşeni, güvenliği sağlamak amacıyla kullanılan asimetrik şifrelemede hem gizli anahtarın saklanmasında, hem de mobil olarak taşınmasında kullanılmaktadır.

Tanıtılan sistemin hayata geçirilmesinin ardından hedeflenen sonuçlar elde edildikten sonra, modüler ve platform bağımsız hale getirilmesi ve güvenli dosya transferi gibi ek özellikleri de içerecek şekilde modifikasyonunun gerçekleştirilmesi düşünülmektedir.

5. KAYNAKLAR

Chen Z. (2000); JavaCard™ Technology for Smart Cards Architecture and Programmer's Guide, Addison - Wesley, MA - USA, 368p.

Erkan H. O. (2002); PGP, http://www.mutasyon.net/makaleoku.asp?id=23

Hansmann U., Nicklous M. S., Schack T., Seliger F. (2000); Smart Card Application Development Using Java, Springer, Berlin - Germany, 293p.

jGuru: Fundamentals of the JavaMail API (2001); http://java.sun.com/developer/onlineTraining/JavaMail/contents.html

Kardaş, G. (2003); Sağlık Kayıtlarının İzlenmesinde Akıllı Kart Kullanımı, Yüksek Lisans Tezi, Ege Üniversitesi, Uluslararası Bilgisayar Enstitüsü, Bornova/İzmir.

OpenCard Consortium (1999); OpenCard Framework 1.2 Programmer's Guide, IBM Deutschland Entwicklung GmbH, Boeblingen - Germany, 82p.

Rankl W., Effing W. (2000); Smart Card Handbook Second Edition, John Wiley & Sons, West Sussex - England, 746p.

Stallings, W. (1995); Network and Internetwork Security Principles and Practice, p. 5, IEEE Press, NY, USA.

Security: Secure Internet Data Transmission URL, 2004: http://secinf.net/misc/Security_Secure_Internet_Data_Transmission.html#HowMuchIsTooMuch.