MUH442 Bilişimde Güvenlik – 2

Prof. Dr. Hasan Hüseyin BALIK

(11. Hafta)

İçerik

- 4.Ağ güvenliği
  - 4.1. İnternet Güvenlik Protokolleri ve Standartları
  - 4.2.İnternet Kimlik Doğrulama Uygulamaları
  - 4.3 Kablosuz Ağ Güvenliği

4.1 İnternet Güvenlik Protokolleri ve Standartları

4.1.İçerik

- Güvenli E-posta ve S/MIME
- DomainKeys Tanımlı Posta
- Güvenli Soket Katmanı (SSL) ve Aktarım Katmanı Güvenliği (TLS)
- HTTPS
- IPv4 ve IPv6 Güvenliği

MIME ve S/MIME

MIME

- Bir İnternet posta biçiminin eski RFC 822 belirtiminin uzantısı
  - RFC 822, Kime, Kimden, Konu ile basit bir başlık tanımlar
  - ASCII metin formatını varsayar
- Mesajın gövdesi hakkındaki bilgileri tanımlayan bir dizi yeni başlık alanı sağlar.

S/MIME

- Güvenli/Çok Amaçlı İnternet Posta Uzantısı
- MIME İnternet e-posta biçiminde güvenlik geliştirmesidir
  - RSA veri güvenliği teknolojisine dayalıdır
- E-posta mesajlarını imzalama ve/veya şifreleme yeteneği sağlar

MIME İçerik Türleri

Tip	Alt tip	Açıklama
Metin	Sade	Biçimlendirilmemiş metin; ASCII veya ISO 8859 olabilir.
	zenginleştirilmiş	Daha fazla format esnekliği sağlar.
Çok parçalı	Karma	Farklı parçalar bağımsızdır ancak birlikte iletilmelidir. Posta mesajında göründükleri sırayla alıcıya sunulmalıdırlar.
	Paralel	Parçaların alıcıya teslimi için herhangi bir sıra tanımlanmadığı için Karma'dan farklıdır.
	Alternatif	Farklı kısımlar, aynı bilginin alternatif versiyonlarıdır. Orijinaline artan bağlılıkla sıralanırlar ve alıcının posta sistemi, kullanıcıya "en iyi" sürümü göstermelidir.
	Digest (özet)	Karma'ya benzer, ancak her bölümün varsayılan türü/alt türü mesaj/rfc822'dir.
İleti	rfc822	Gövdenin kendisi, RFC 822'ye uyan kapsüllenmiş bir mesajdır.
	Kısmi	Alıcı için şeffaf olacak şekilde büyük posta öğelerinin parçalanmasına izin vermek için kullanılır.
	Harici gövde	Başka bir yerde var olan bir nesneye işaretçi içerir.
Resim	jpeg	Resim JPEG formatında, JFIF kodlamalıdır.
	gif	Resim GIF formatındadır.
Video	mpeg	MPEG biçimi.
Ses	Temel	8 kHz örnekleme hızında tek kanallı 8 bitlik ISDN mu-law kodlaması.
Uygulama	PostScript	Adobe Postscript'i
	sekizli (oklet) akış	8 bit bayttan oluşan genel ikili veriler.

S/MIME İçerik Türleri

Tip	Alt tip	S/MINE parametresi	Açıklama
çok parçalı	Signed		İki bölümden oluşan açık imzalı bir mesaj: biri mesaj, diğeri imza.
Uygulama	pkcs7-mime	signedData	İmzalı bir S/MIME varlığı.
	pkcs7-mime	envelopedData	Şifreli bir S/MIME varlığı.
	pkcs7-mime	degenerate signedData	Yalnızca ortak anahtar sertifikaları içeren bir varlık.
	pkcs7-mime	CompressedData	Sıkıştırılmış bir S/MIME varlığı.
	pkcs7-signature	signedData	Çok parçalı/imzalı bir mesajın imza alt bölümünün içerik türü.

S/MIME İşlevleri

Zarflanmış veri	İmzalanmış veri	Açık (Clear) imzalı veri	İmzalanmış ve zarflanmış veri
Şifrelenmiş içerik ve ilişkili anahtarlar	Kodlanmış mesaj + imzalı özet	Düz metin mesajı + kodlanmış imzalı özet	İmzalı ve şifrelenmiş varlıkların iç içe yerleştirilmesi

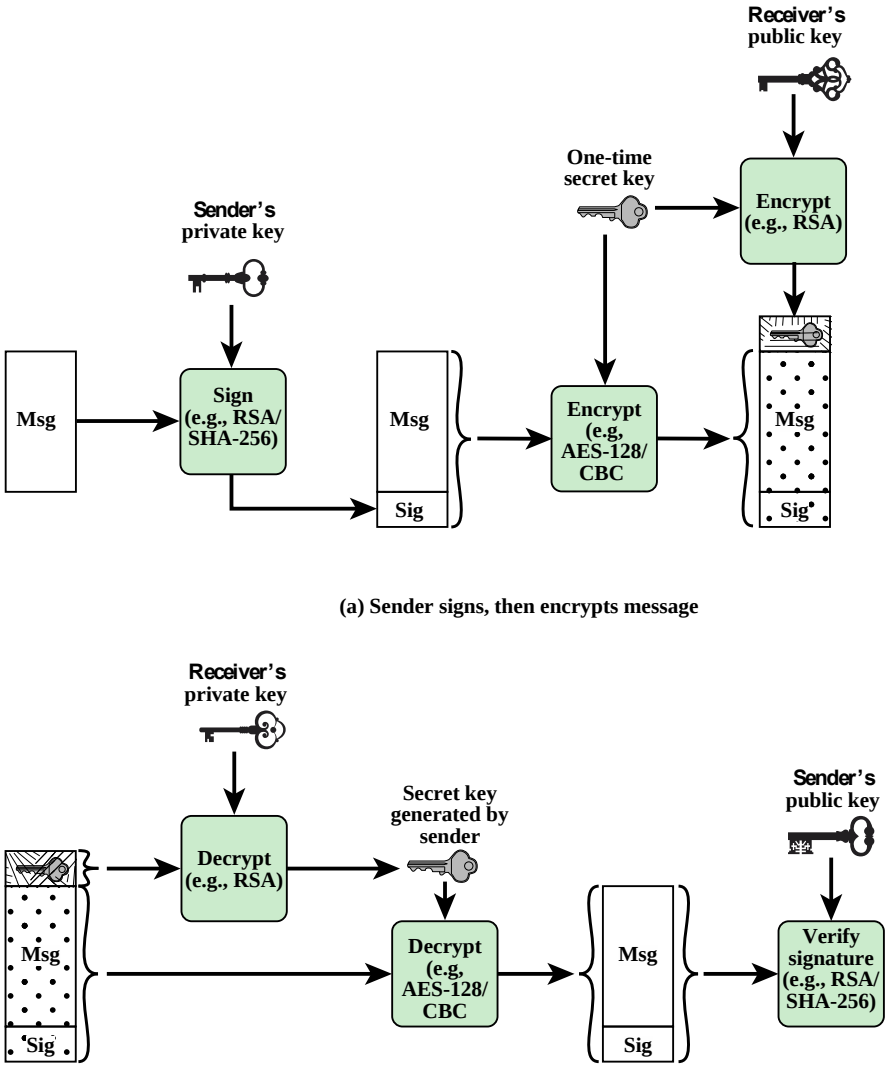


Figure 22.1 Simplified S/MIME Functional Flow

İmzalı ve Açık İmzalı Veriler

- S/MIME mesajlarını imzalamak için kullanılan tercih edilen algoritmalar, ya RSA veya DSA imzasını ya da SHA-256 mesaj özetini kullanır .
- Süreç şu şekilde işler:
  - Göndermek istediğiniz mesajı alın ve SHA-256 kullanarak 256 bitlik sabit uzunlukta bir koda eşleyin
  - 256-bitlik mesaj özeti bu mesaja özeldir ve birisinin bu mesajı değiştirmesini veya başka bir mesajla değiştirmesini ve yine de aynı özeti bulmasını neredeyse imkansız hale getirir.
  - S/MIME, özeti RSA'yı ve gönderenin özel RSA anahtarını kullanarak şifreler
  - Sonuç, mesaja eklenen dijital imzadır.
  - Artık mesajı alan herkes mesaj özetini yeniden hesaplayabilir, ardından RSA ve gönderenin genel RSA anahtarını kullanarak imzanın şifresini çözebilir.
  - Bu işlem yalnızca 256 bitlik bir bloğu şifrelemeyi ve şifresini çözmeyi içerdiğinden, çok az zaman alır.

Zarflanmış Veri

- S/MIME mesajlarını şifrelemek için kullanılan varsayılan algoritmalar AES ve RSA'dır.
  - S/MIME, mesajı AES veya başka bir geleneksel şifreleme şeması kullanarak şifrelemek için kullanılan sözde rasgele bir gizli anahtar üretir.
  - Her yeni mesaj şifrelemesi için yeni bir sözde rasgele anahtar oluşturulur.
  - Bu oturum anahtarı mesaja bağlıdır ve onunla birlikte iletilir.
  - Gizli anahtar, anahtarı alıcının genel RSA anahtarıyla şifreleyen genel anahtar şifreleme algoritması RSA'ya girdi olarak kullanılır.
  - Alıcı tarafta S/MIME, gizli anahtarı kurtarmak için alıcının özel RSA anahtarını kullanır, ardından düz metin mesajını kurtarmak için gizli anahtarı ve AES'yi kullanır.
  - Şifreleme tek başına kullanılıyorsa, şifreli metni ASCII formatına dönüştürmek için radix-64 kullanılır.

DomainKeys Tanımlı Posta (DKIM)

- İmzalayan bir etki alanının posta akışındaki bir iletinin sorumluluğunu üstlenmesine izin veren kriptografik olarak imzalanan e-posta iletilerinin belirtimi
- Önerilen İnternet Standardı (RFC 4871:*DomainKeys Tanımlı Posta (DKIM) İmzaları)*
- Çeşitli e-posta sağlayıcıları tarafından geniş çapta benimsenmiştir

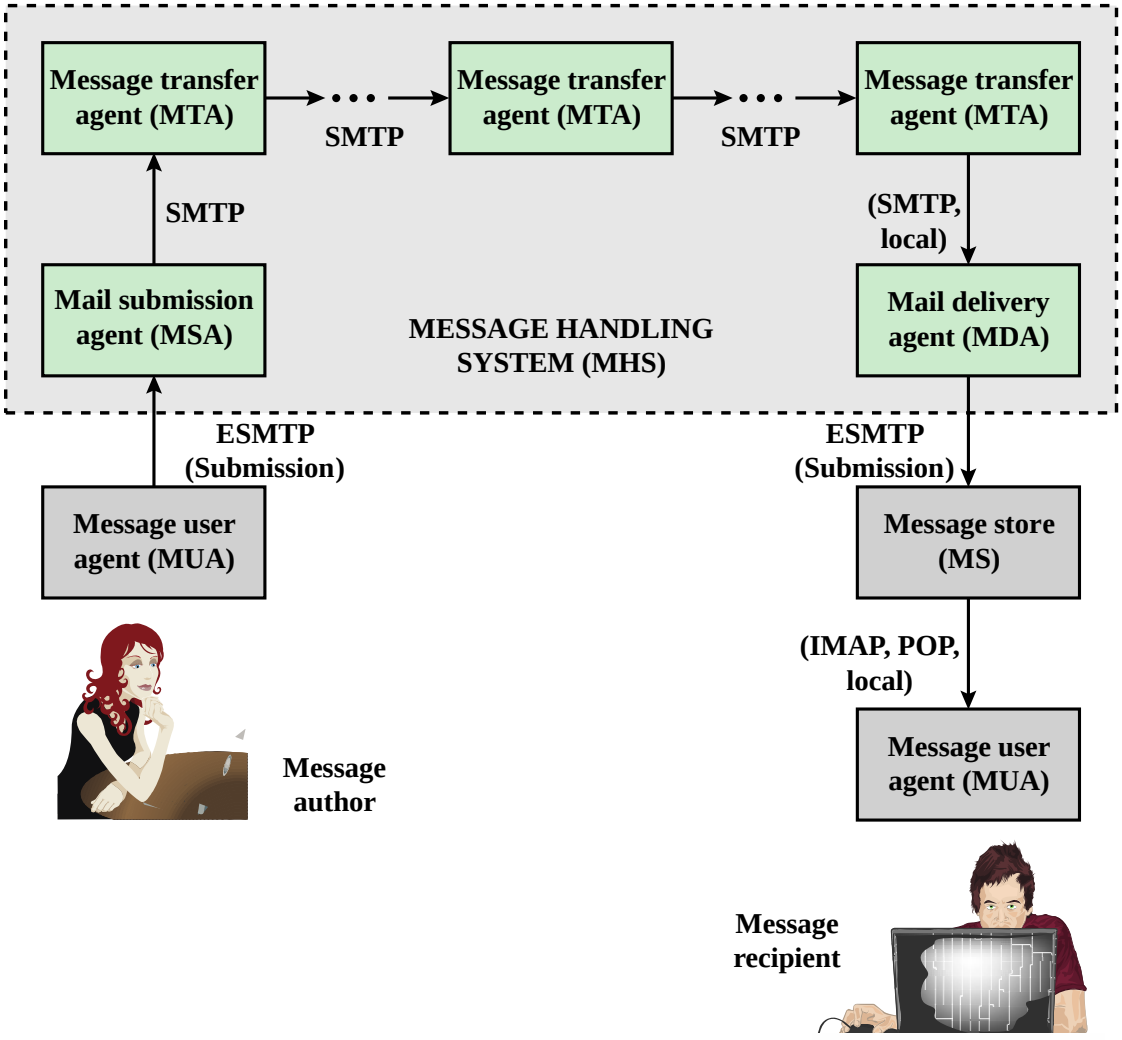
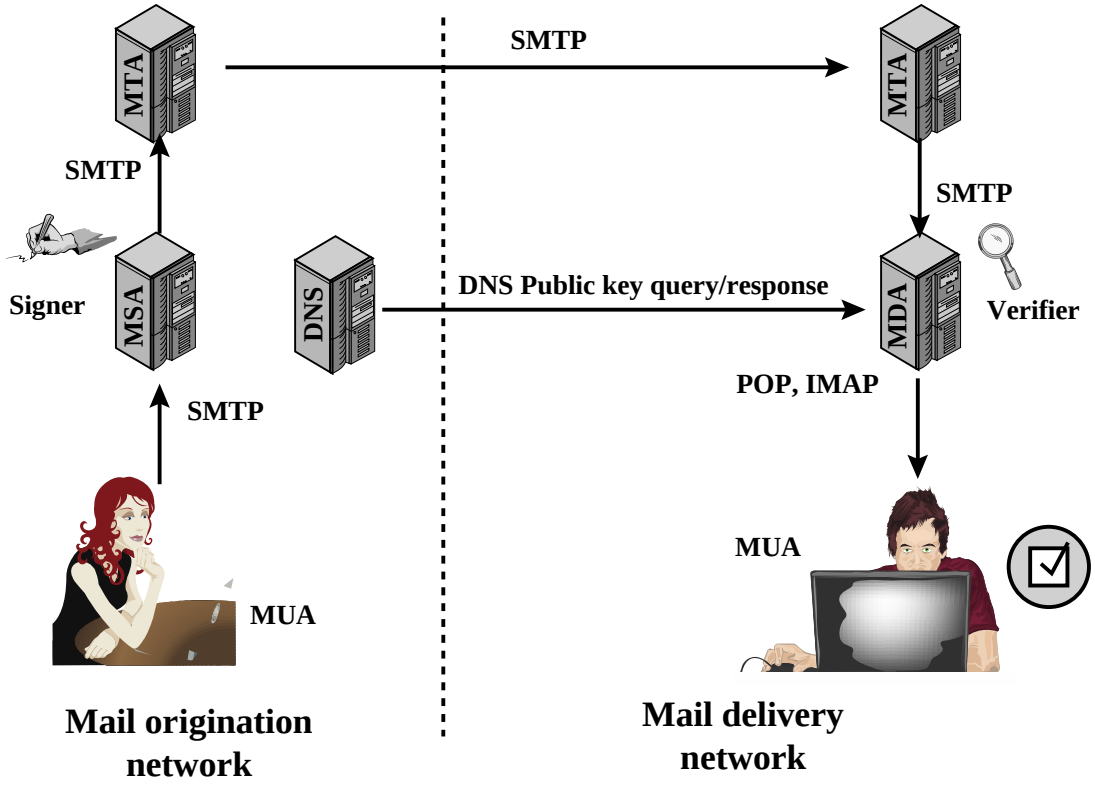


Figure 22.2 Function Modules and Standardized Protocols Used Between Them in the Internet Mail Architecture



DNS = domain name system
MDA = mail delivery agent
MSA = mail submission agent
MTA = message transfer agent
MUA = message user agent

Figure 22.3 Simple Example of DKIM Deployment

Güvenli Soket Katmanı (SSL) ve Aktarım Katmanı Güvenliği (TLS)

- En yaygın kullanılan güvenlik hizmetlerinden biridir
- TCP'ye dayanan bir dizi protokol olarak uygulanan genel amaçlı hizmettir
- Daha sonra İnternet standardı RFC4346: Aktarım Katmanı Güvenliği (TLS) oldu

İki uygulama seçeneği:

- Altta yatan protokol paketinin bir parçası olarak sunulur
- Belirli paketlere gömülüdür

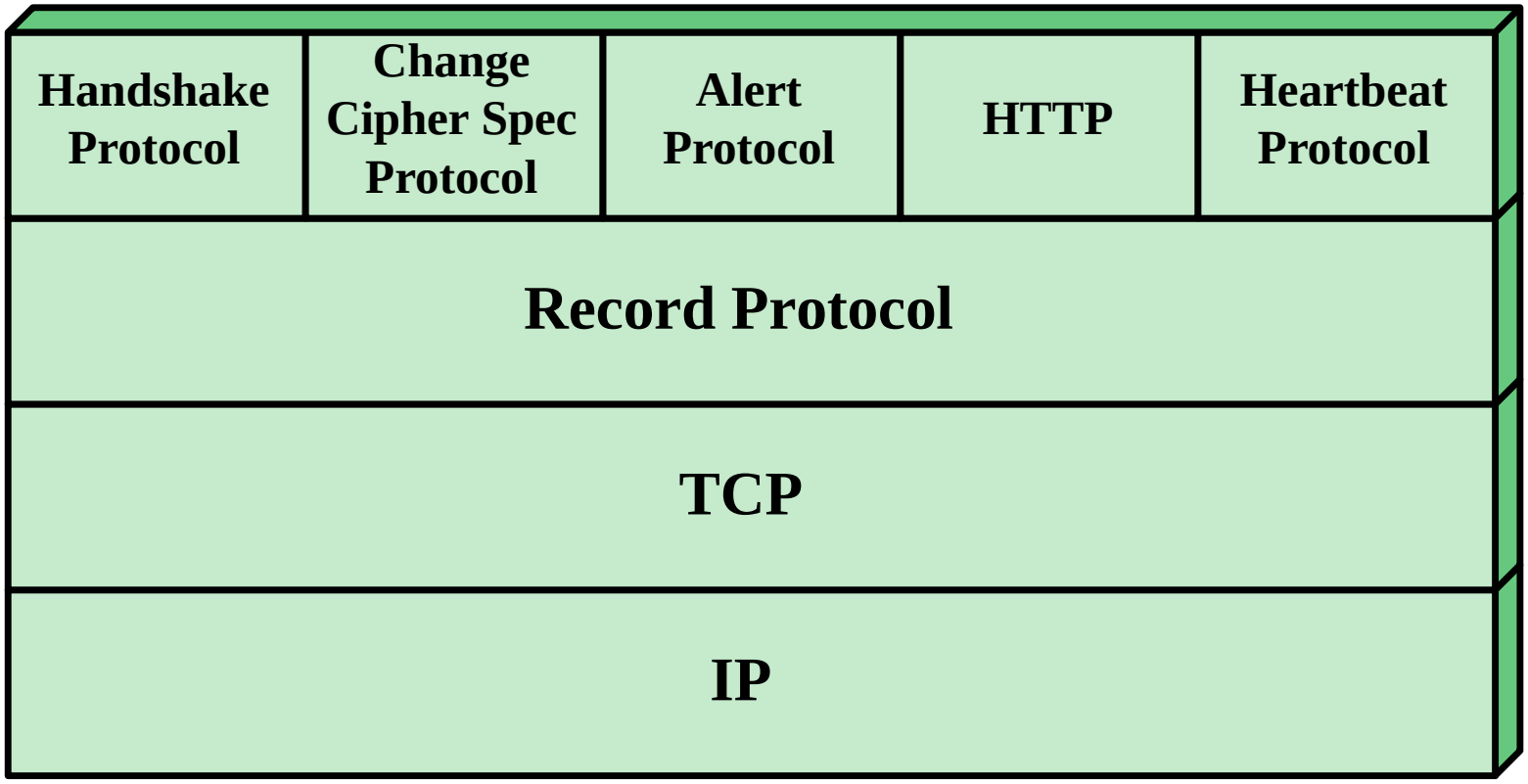


Figure 22.4 SSL/TLS Protocol Stack

TLS Kavramları

TLS Oturumu

- İstemci ve sunucu arasındaki ilişki
- El Sıkışma Protokolü tarafından oluşturulur
- Bir dizi kriptografik güvenlik parametresi tanımlar
- Her bağlantı için yeni güvenlik parametrelerinin maliyetli müzakeresinden kaçınmak için kullanılır

TLS Bağlantısı

- Uygun bir hizmet türü sağlayan bir taşıma (OSI katman modeli tanımında)'dır
- Eşler arası ilişkilerdir
- Geçici
- Her bağlantı bir oturumla ilişkilendirilir

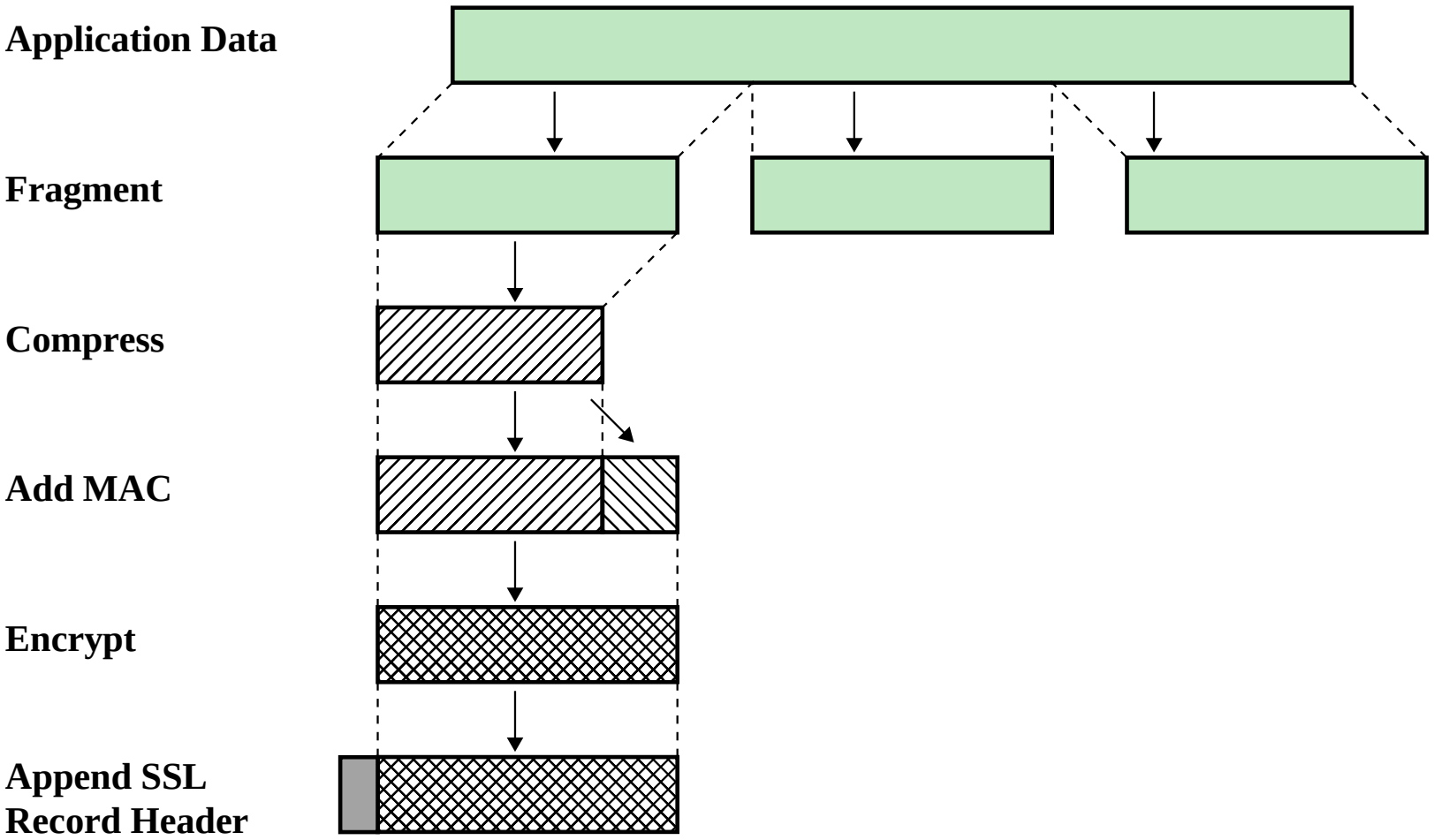


Figure 22.5 TLS Record Protocol Operation

Cipher Spec Protokolü

- TLS Kayıt Protokolünü kullanan TLS'ye özgü dört protokolden biridir
- En basiti
- 1 değerine sahip tek bir bayttan oluşan tek bir mesajdan oluşur
- Bu mesajın tek amacı, bekleyen durumun mevcut duruma kopyalanmasını sağlamaktır.
- Bu nedenle kullanımda olan şifre paketini günceller

Uyarı Protokolü

TLS ile ilgili uyarıları eş varlığa iletir

Uyarı mesajları sıkıştırılır ve şifrelenir

Her mesaj iki bayttan oluşur:

İlk bayt, mesajın ciddiyetini iletmek için warning (1) veya fatal (2) değerini alır

ikinci bayt, belirli uyarıyı gösteren bir kod içerir

Seviye fatal ise, TSL bağlantıyı hemen sonlandırır

Aynı oturumdaki diğer bağlantılar devam edebilir ancak bu oturumda yeni bağlantı kurulamaz

El Sıkışma Protokolü

- TLS'nin en karmaşık kısmıdır
- Herhangi bir uygulama verisi iletilmeden önce kullanılır
- Sunucu ve istemcinin şunları yapmasına izin verir:

Birbirinin kimliğini doğrular → **Şifreleme ve MAC algoritmaları üzerinde uzlaşılır** → **Kullanılacak kriptografik anahtarlarda uzlaşılır**

- İstemci ve sunucu tarafından değiş tokuş edilen bir dizi mesajdan oluşur
- Değişimin dört aşaması vardır

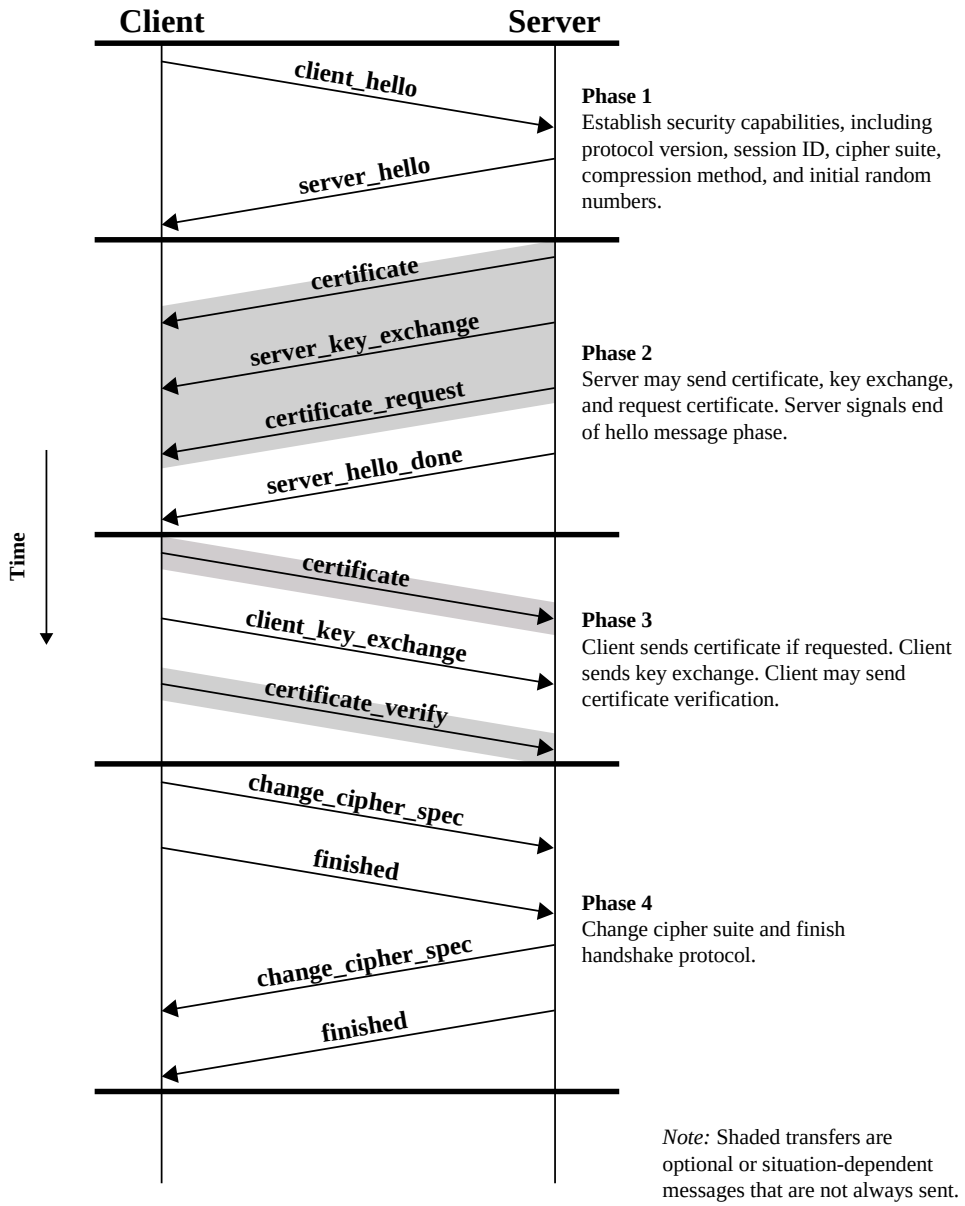
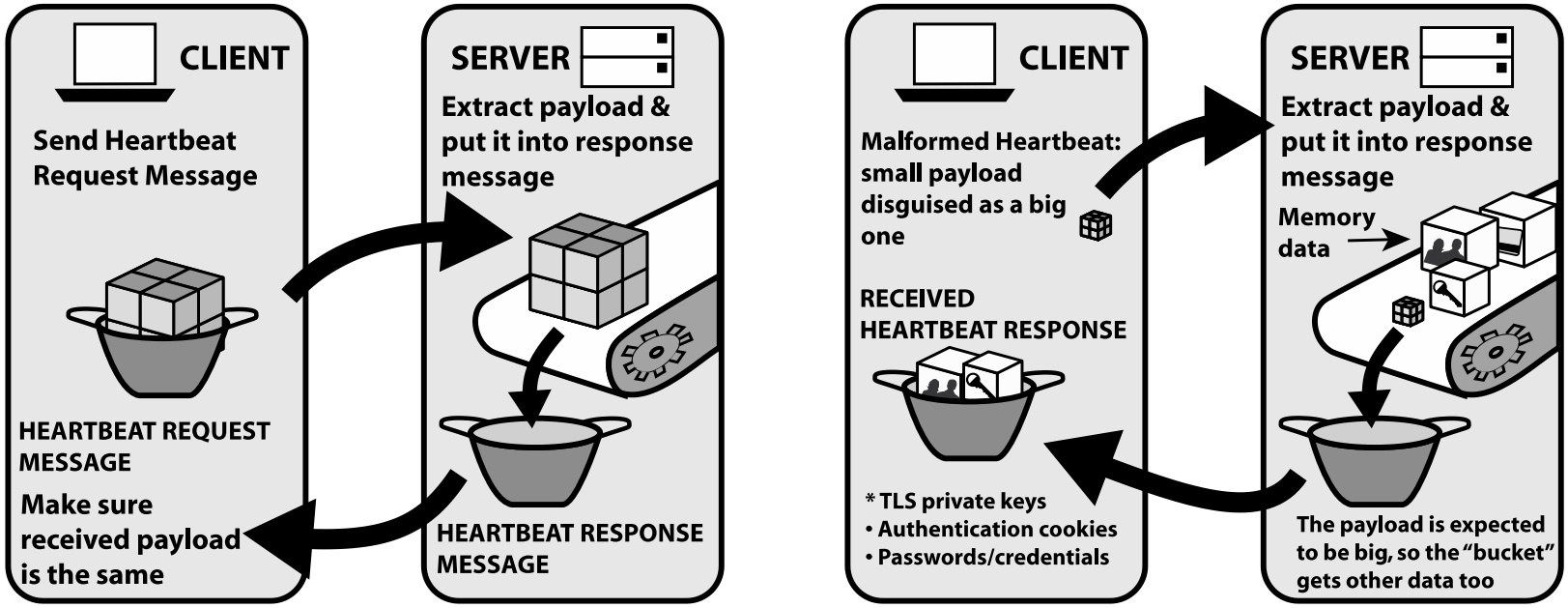


Figure 22.6 Handshake Protocol Action

Kalp Atışı Protokolü

- Normal çalışmayı belirtmek veya bir sistemin diğer parçalarını senkronize etmek için donanım veya yazılım tarafından üretilen periyodik bir sinyaldir
- Genellikle bir protokol varlığının kullanılabilirliğini izlemek için kullanılır
- 2012'de RFC 6250'de tanımlanmıştır
- TLS Kayıt Protokolünün üstünde çalışır
- Kullanım, El Sıkışma Protokolünün 1. Aşaması sırasında kurulur
- Her eş, kalp atışlarını destekleyip desteklemediğini ifade eder
- İki amaca hizmet eder:
  - Gönderene, alıcının hala hayatta olduğunu garanti eder
  - Boşta kalma sürelerinde bağlantı genelinde etkinlik oluşturur

SSL/TLS Saldırıları



(a) How TLS Heartbeat Protocol works

(b) How TLS Heartbleed exploit works

Figure 22.7 The Heartbleed Exploit

Source: BAE Systems

HTTPS (SSL üzerinden HTTP)

- Bir Web tarayıcısı ve bir Web sunucusu arasında güvenli iletişim uygulamak için HTTP ve SSL kombinasyonudur
- Tüm modern Web tarayıcılarında yerleşiktir.
  - Arama motorları HTTPS'yi desteklemez
  - URL adresleri https:// ile başlar
- TLS Üzerinden HTTP RFC 2818'de yayınlanmıştır
- HTTP istemcisi olarak görev yapan aracı, aynı zamanda TLS istemcisi olarak da işlev görür
- Bir HTTPS bağlantısının kapatılması, TLS'nin uzak taraftaki eş TLS varlığıyla bağlantıyı kapatmasını gerektirir; bu, temeldeki TCP bağlantısının kapatılmasını içerecektir.

IP Güvenliği (IPsec)

- Çeşitli uygulama güvenlik mekanizmalarıdır
  - S/MIME, Kerberos, SSL/HTTPS
- Güvenlik, çapraz protokol katmanlarıyla ilgilidir
- Tüm uygulamalar için ağ tarafından uygulanan güvenlik ister misiniz?
- Yeni nesil IPv6'da bulunan kimlik doğrulama ve şifreleme güvenlik özellikleri
- Mevcut IPv4'te de kullanılabilir

IPsec'in Avantajları

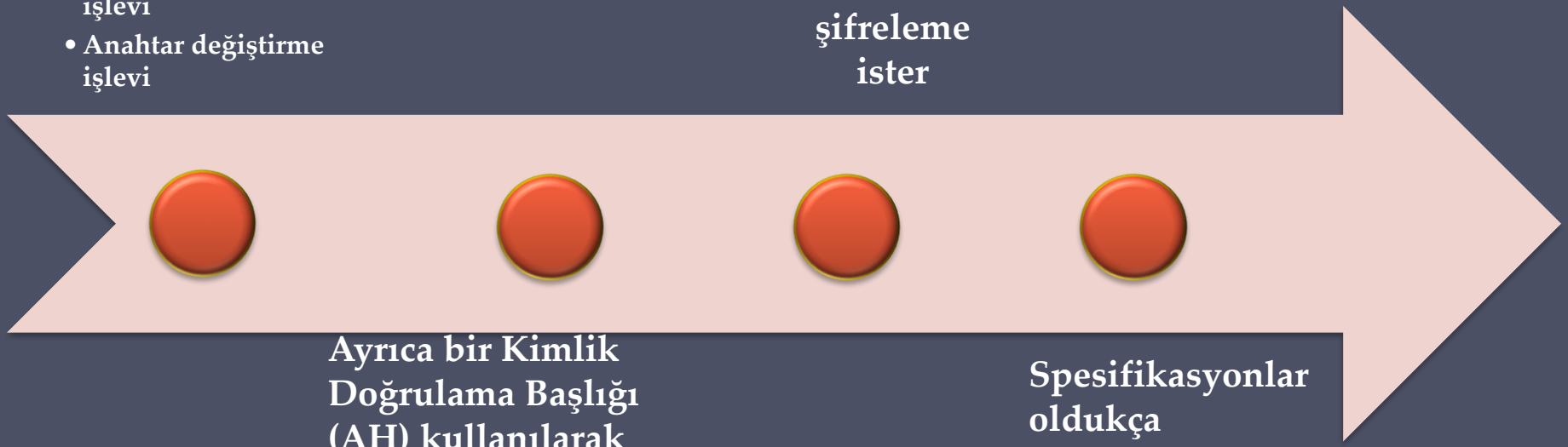
- Bir güvenlik duvarına veya yönlendiriciye uygulandığında, alandan geçen tüm trafiğe güçlü güvenlik sağlar.
- Bir güvenlik duvarında bypass'a karşı dirençlidir
- Taşıma katmanının altındadır, bu nedenle uygulamalar için transparandır
- Son kullanıcılara karşı transparan olabilir
- Bireysel kullanıcılar için güvenlik sağlar
- Yönlendirme mimarisini korur

IPsec Kapsamı

İki ana işlev sağlar:

- Kapsüllenen Güvenlik Yükü (ESP) adı verilen birleşik bir kimlik doğrulama/şifreleme işlevi
- Anahtar değiştirme işlevi

VPN'ler hem kimlik doğrulama hem de şifreleme ister



Ayrıca bir Kimlik Doğrulama Başlığı (AH) kullanılarak uygulanan yalnızca kimlik doğrulama işlevi

- Mesaj kimlik doğrulaması ESP tarafından sağlandığından, geriye dönük uyumluluk için AH kullanımı IPsecv3'e dahil edilmiştir ancak yeni uygulamalarda kullanılmamalıdır.

Spesifikasyonlar oldukça karmaşıktır

- Çok sayıda RFC 2401/4302/ 4303/4306

Güvenlik Kuruluşları

- Trafik akışı için güvenlik sağlayan gönderici ve alıcı arasında tek yönlü bir ilişkidir
  - İki yönlü güvenli değiş tokuş için bir akran ilişkisi gerekiyorsa, iki güvenlik ilişkilendirmesi gerekir
- IPv4 veya IPv6 başlığındaki Hedef Adres ve ekteki uzantı başlığındaki (AH veya ESP) SPI tarafından benzersiz bir şekilde tanımlanır

3 parametre ile tanımlanır:

- Güvenlik Parametre İndexi (SPI)
- IP Hedef Adresi
- Protokol Tanımlayıcı

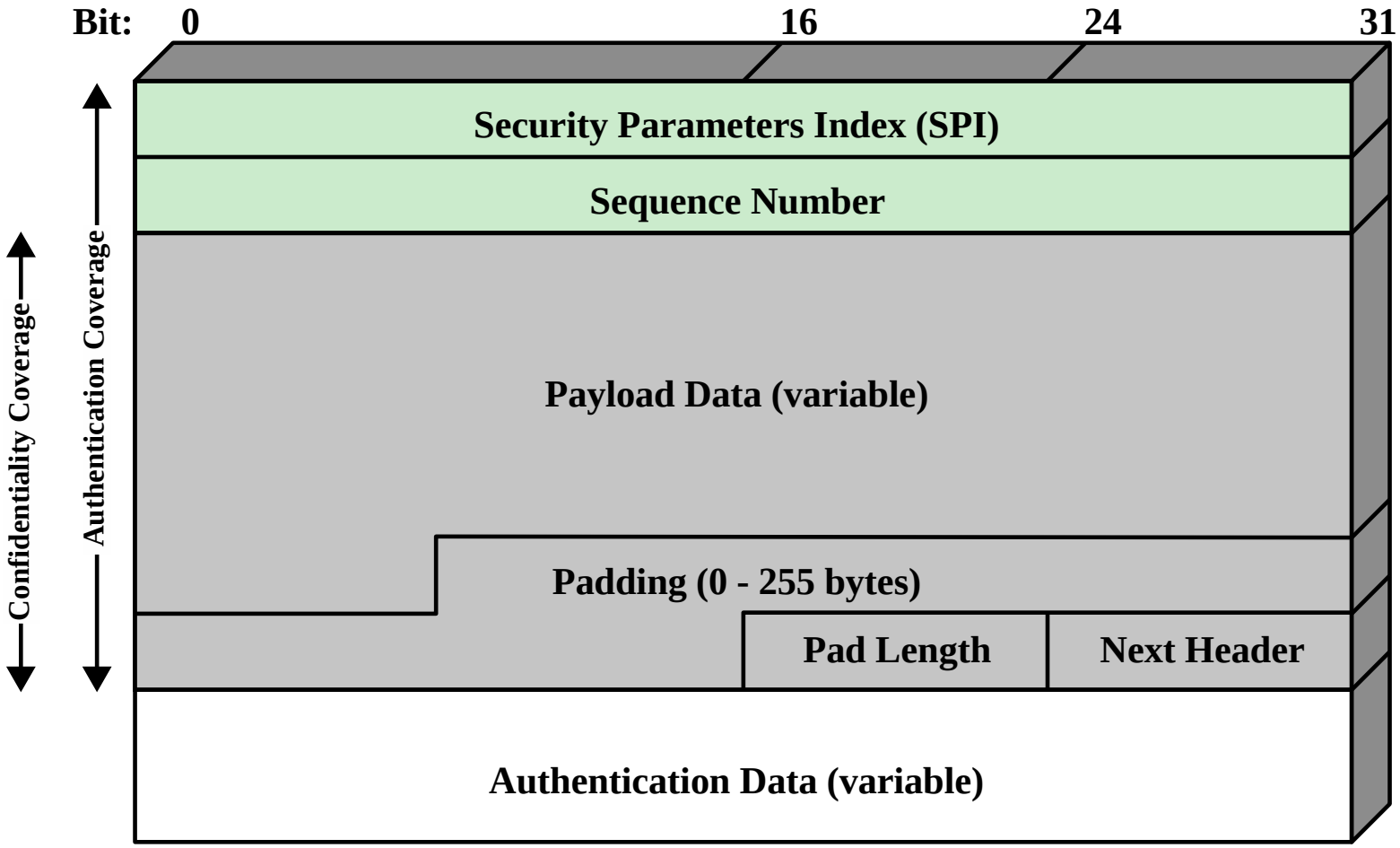


Figure 22.8 IPSec ESP Format

Taşıma ve Tünel Modları

Taşıma modu

- Bir IP paketinin yüküne kadar uzanır
- Genellikle iki ana bilgisayar arasında uçtan uca iletişim için kullanılır
- ESP, IP başlığını değil, IP yükünü şifreler ve isteğe bağlı olarak doğrular

Tünel Modu

- IP paketinin tamamına koruma sağlar
- Tüm orijinal paket, bir IP ağının bir noktasından diğerine bir tünelden geçer.
- Bir güvenlik ilişkisinin uçlarından biri veya her ikisi de bir güvenlik ağ geçidi olduğunda kullanılır
- Güvenlik duvarlarının arkasındaki ağlardaki bazı ana bilgisayarlar, IPsec uygulamadan güvenli iletişim kurabilir