

E-Ticaret Protokolleri

Dr. Fatih KALEMKUŞ

Kafkas Üniversitesi

00. İerikler

- 01. E-Ticaret Sularının Durdurulması
- 02. Bilgi Gvencesi
- 03. Kurumsal Genel Elektronik Ticaret Gvenlik Modeli
- 04. Tehditler ve Saldırılar
- 05. E-Ticaret İletiřiminin Gvenliđi
- 06. E-Ticaret Ađlarının Gvenliđi
- 07. Dolandırıcı Tketiciler & Satıcı Koruma

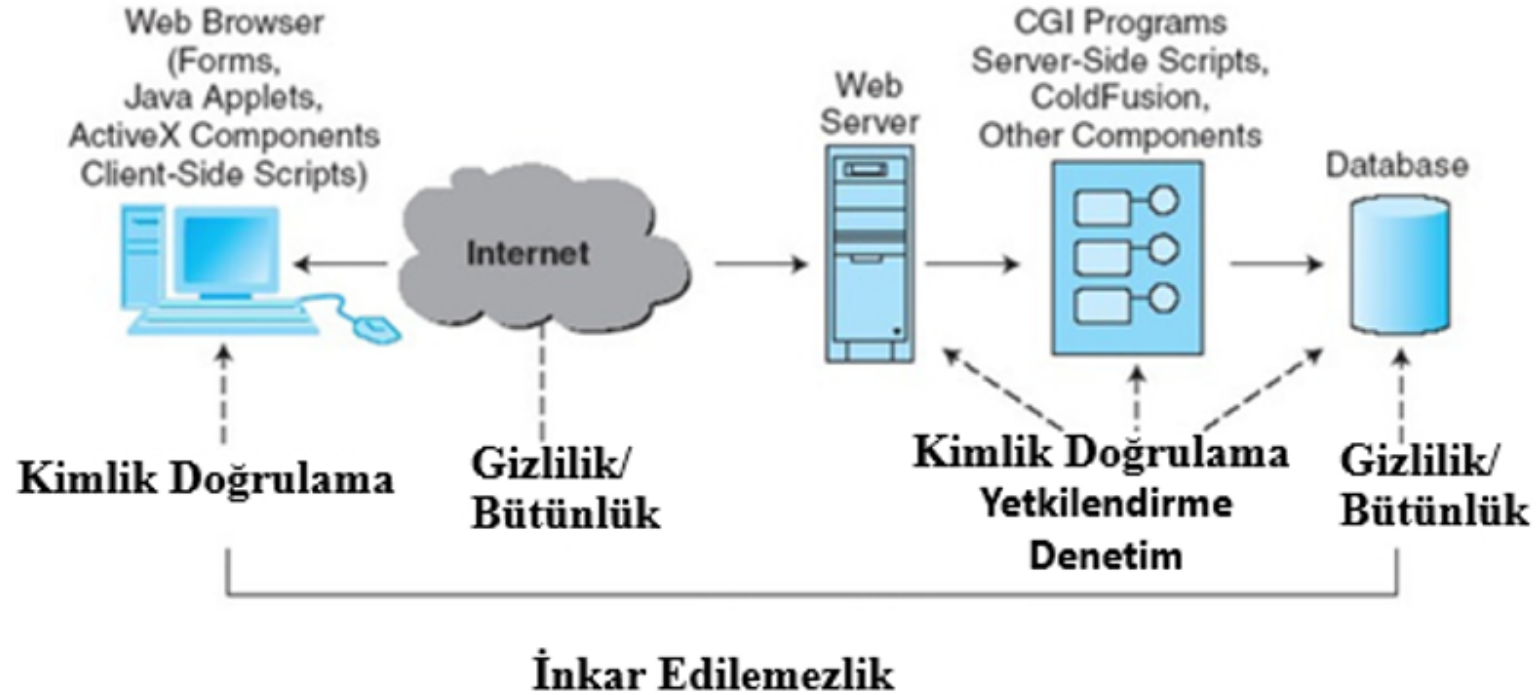
01. E-Ticaret Suçlarının Durdurulması

- E-perakendeciler için siber suçluları ve dolandırıcıları durdurmanın zor olmasının altı ana nedeni:
 - Güçlü e-ticaret güvenliği online alışverişi müşteriler için zahmetli hale getiriyor.
 - Kredi kartı sağlayıcıları ve yabancı ISP'lerin işbirliği yapmaması
 - İnternet üzerinden alışveriş yapanlar mağdur olmamak için gerekli önlemleri almıyor.
 - BT tasarımı ve güvenlik mimarisi saldırılara karşı savunmasızdır.
 - Yazılım açıkları (bugs-hatalar) büyük bir güvenlik sorunudur.
 - Yöneticiler bazen gerekli bakım standartlarını göz ardı etmektedir.



01. E-Ticaret Suçlarının Durdurulması

- e-Ticaret Sitelerinde Genel Güvenlik Sorunları



01. E-Ticaret Suçlarının Durdurulması

- Gerekli Bakım

- Bir şirketin e-ticaret işlerini ve çevrimici işlemlerini etkileyen riskler temelinde makul olarak göstermesi beklenen özen.



01. E-Ticaret Suçlarının Durdurulması

- E-Ticaret Güvenlik Stratejisi ve Yaşam Döngüsü Yaklaşımı
 - İnternetin savunmasız tasarımı
 - Kâr amaçlı suçlara geçiş
 - e-Ticaret güvenliği için en iyi uygulamaların göz ardı edilmesi
 - CompTIA (Bilgisayar Teknolojisi Endüstrisi Birliği)
 - Bilgi güvenliği araştırmaları ve en iyi uygulamaları sağlayan kar amacı gütmeyen ticaret grubu

<http://www.comptia.org>



Dr. Fatih KALEMKUŞ

02. Bilgi Gvencesi

- Bilgi Gvenliđi
 - Bilgi sistemlerinin, depolama, iřleme veya aktarım sırasında bilgilere yetkisiz eriřime veya deđiřikliklere karřı korunması ve bu tr tehditleri tespit etmek, belgelemek ve bunlara karřı koymak iin gerekli nlemler de dahil olmak zere, yetkili kullanıcılara hizmet reddine karřı koruma.



02. Bilgi Güvencesi

- Güvenliğin Ana Bileşenleri
 - Gizlilik (= Gizlilik)
 - Veri gizliliği ve doğruluğu güvencesi
 - Özel veya hassas bilgilerin yetkisiz kişilere, kuruluşlara veya süreçlere ifşa edilmesini engellemek
 - Bütünlük
 - Saklanan verilerin izinsiz olarak değiştirilmediğine dair güvence; gönderilen mesajın alınan mesajla aynı olması.
 - Kullanılabilirlik (= kimlik doğrulama)
 - Verilere, Web sitesine veya diğer e-ticaret veri hizmetlerine erişimin zamanında, kullanılabilir, güvenilir ve yetkili kullanıcılarla sınırlı olduğuna dair güvence.

02. Bilgi Güvencesi

- Güvenliğin Ana Bileşenleri
 - Gizlilik (= gizlilik)
 - Bütünlük
 - Kullanılabilirlik (= akimlik doğrulama)



Gizlilik:

Bilgilerin ifşası



Bütünlük:

Bilgilerin değiştirilmesi



Kullanılabilirlik:

Hizmetlere erişimin engellenmesi

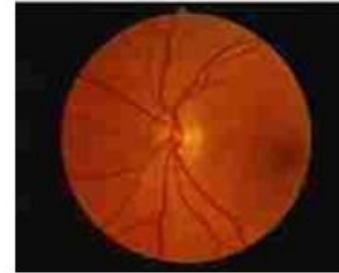
02. Bilgi Gvencesi

- Gvenliđin Eriřim Kontrolleri
 - Bir ađ kaynađını kimin yasal olarak kullanabileceđini belirleyen mekanizma
- Eriřim kontrollerinin trleri
 - Zorunlu eriřim
 - İsteđe bađlı eriřim



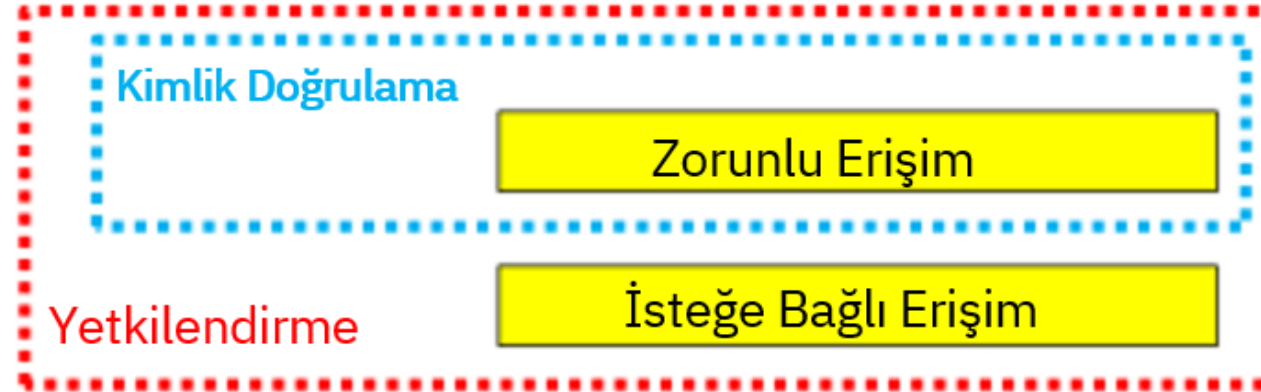
02. Bilgi Güvencesi

- Güvenliğin Erişim Kontrolleri
 - Biyometrik sistemler
 - Bir kişiyi parmak izleri, iris (göz) desenleri, yüz özellikleri veya ses gibi biyolojik bir özelliğin ölçümü yoluyla tanımlayan kimlik doğrulama sistemleri.
 - Örneğin;
 - Parmak izi
 - El Geometrisi
 - Retina
 - İris
 - İmza dinamikleri
 - Klavye dinamikleri
 - Ses baskısı
 - Yüz tarama



02. Bilgi Güvencesi

- Güvenliğin Seviyeleri
 - (Basit seviye) Kimlik Doğrulama
 - Bir bireyin, bilgisayarın, bilgisayar programının veya e-ticaret web sitesinin gerçek kimliğini doğrulamaya (güvenceye almaya) yönelik süreç.
 - (Çoklu seviye) Yetkilendirme
 - Kimliği doğrulanmış varlığın neye erişebileceğini ve hangi işlemleri gerçekleştirebileceğini belirleme süreci.



02. Bilgi Güvencesi

E-Ticaret Güvenliđinin Ana Bileşenleri

- Gizlilik
- Bütünlük
- Kullanılabilirlik
- İnkâr Edilemezlik
 - Çevrimiçi bir müşterinin veya ticari ortađın, satın alma veya işlemlerini yanlışlıkla inkâr edemeyeceđine (reddedemeyeceđine) dair güvence



Gizlilik:

Bilgilerin ifşâ edilmesi



Bütünlük:

*Bilgilerin
deđiştirilmesi*



Kullanılabilirlik:

*Hizmetlere erişimin
engellenmesi*



İnkâr Edilemezlik:

*Mesajın alındıđının
reddedilmesi*

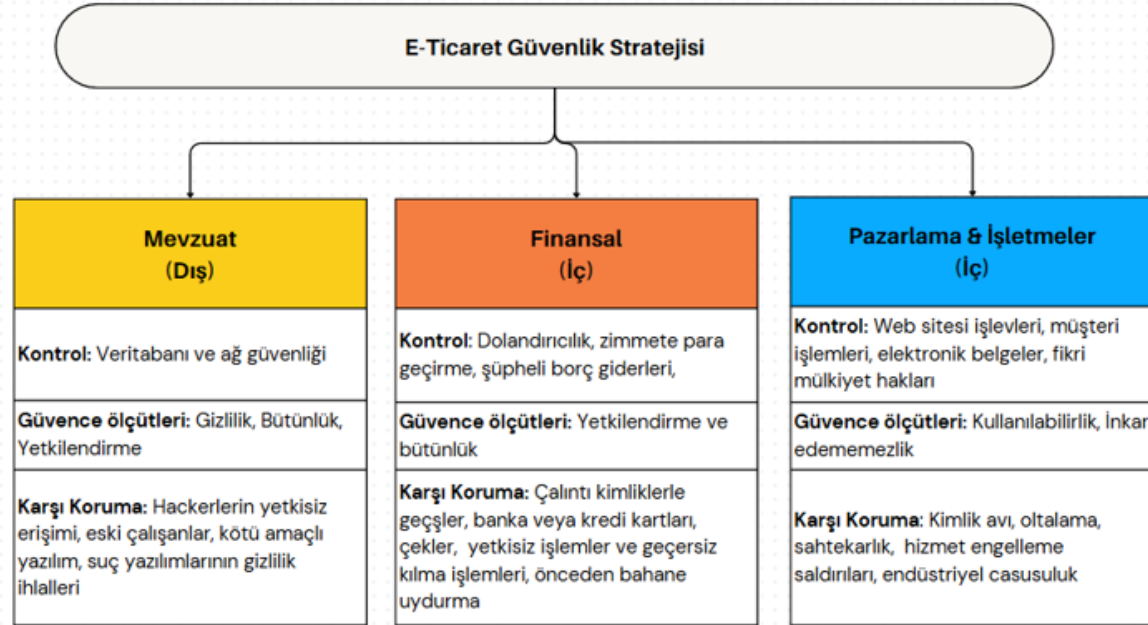
02. Bilgi Güvencesi

- Güvenlik Sınıflandırması
 - Dış güvenlik (= fiziksel güvenlik)
 - Arayüz güvenliği
 - İç güvenlik
 - İşletim sistemleri güvenliği
 - Veritabanı güvenliği
 - Ağ güvenliği



02. Bilgi Güvencesi

- E-Ticaret Güvenlik Sınıflandırması
 - Dış güvenlik
 - Mevzuat güvenliği
 - İç Güvenlik
 - Finansal güvenlik
 - Pazarlama ve işletme güvenliği



03. Kurumsal Çapta E-Ticaret Güvenlik Modeli

- E-Ticaret Güvenlik Programı
 - Kurumsal varlıkları korumak için güvenlik süreçleri üzerinde bir dizi kontrol.
 - Bilgileri, iş yapma yeteneğini ve diğer varlıkları korumak için birlikte çalışan tüm politikalar, prosedürler, belgeler, standartlar, donanım, yazılım, eğitim ve personel.



03. Kurumsal apta E-Ticaret Gvenlik Modeli

- Kurumsal apta E-Ticaret Gvenlik ve Gizlilik Modeli



03. Kurumsal Çapta E-Ticaret Güvenlik Modeli

- Temel E-Ticaret Güvenliği Sorunları ve Bakış Açıları
 - Kullanıcıların bakış açısından:
 - Kullanıcı, Web sunucusunun yasal bir şirkete ait olup olmadığını ve onun tarafından işletilip işletilmediğini nasıl bilebilir?
 - Kullanıcı, Web sayfasının ve formun casus yazılım veya diğer kötü amaçlı kodlar tarafından ele geçirilmediğini nasıl bilebilir?
 - Kullanıcı, bir çalışanın bilgileri ele geçirip kötüye kullanmayacağını nasıl bilebilir?



03. Kurumsal apta E-Ticaret Gvenlik Modeli

- Temel E-Ticaret Gvenliđi Sorunları ve Bakıř Aıları
 - řirketlerin bakıř aısından:
 - řirket, kullanıcının web sunucusuna sızmaya veya sitedeki sayfaları ve ieriđi deđiřtirmeye alıřmayacađını nereden bilebilir?



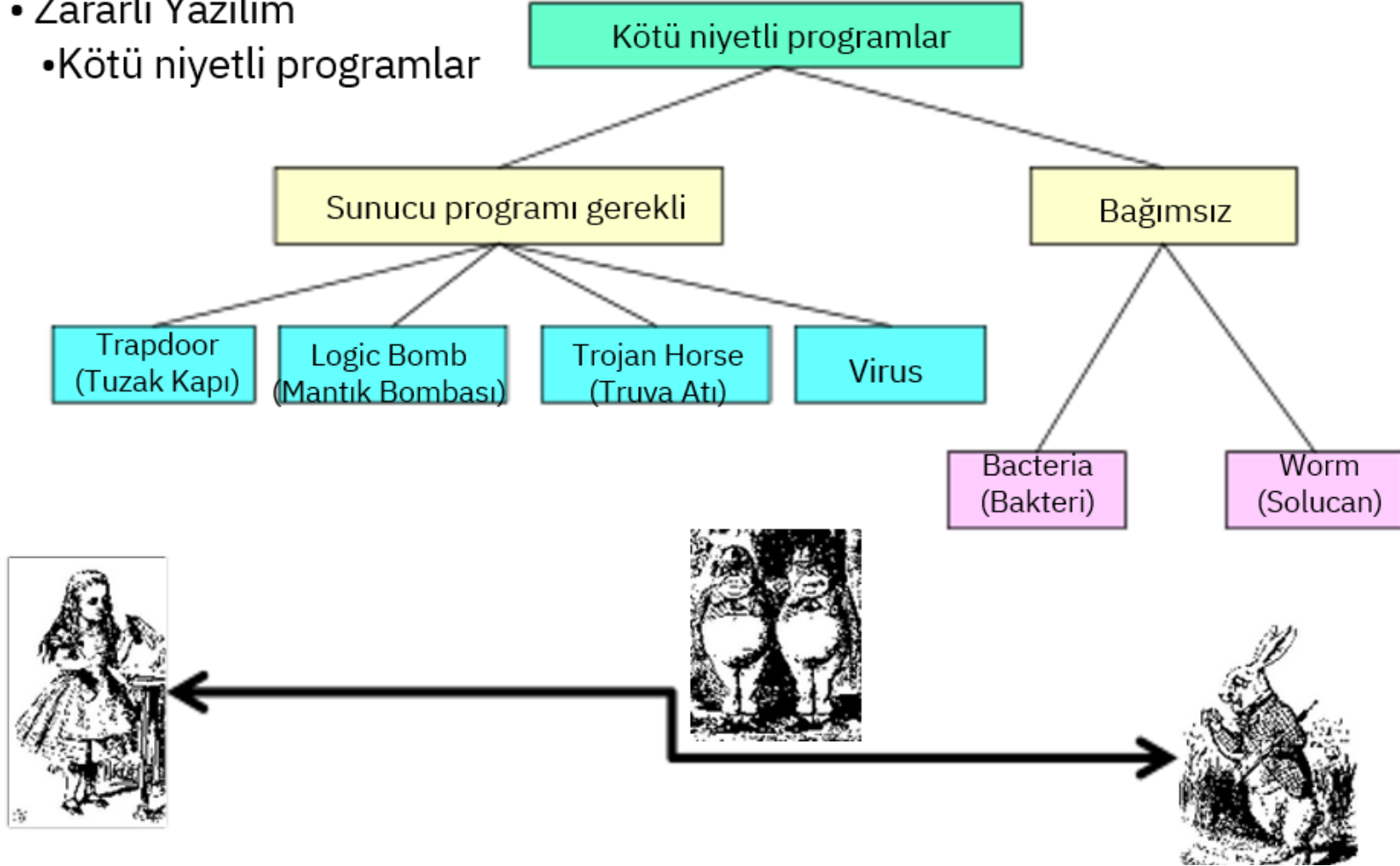
03. Kurumsal Çapta E-Ticaret Güvenlik Modeli

- Temel E-Ticaret Güvenliği Sorunları ve Bakış Açıları
 - Her iki tarafın bakış açısından:
 - Her iki taraf da ağ bağlantısının, hattı "dinleyen" bir üçüncü taraf tarafından dinlenemeyeceğini nasıl bilebilir?
 - Sunucu ile kullanıcının tarayıcıları arasında gidip gelen bilgilerin değiştirilmediğini nasıl biliyorlar?



04. Tehditler ve Saldırılar

- Zararlı Yazılım
- Kötü niyetli programlar



04. Tehditler ve Saldırılar

- Saldırı Türleri
 - Teknik olmayan saldırı (Nontechnical attack)
 - İnsanları hassas bilgileri ifşa etmeleri veya bir ağın güvenliğini tehlikeye atacak eylemler gerçekleştirmeleri için kandırmak amacıyla hile kullanan bir saldırı.



04. Tehditler ve Saldırılar

- Saldırı Türleri
 - Sosyal mühendislik (Social engineering)
 - Kullanıcıları bilgileri açığa vurmaları veya bir bilgisayarı veya ağı tehlikeye atan bir eylemi gerçekleştirmeleri için kandırmak amacıyla bazı hileleri kullanan, teknik olmayan bir saldırı türüdür.



04. Tehditler ve Saldırılar

- Saldırı Türleri
 - Kimlik Avı (Phishing)
 - Müşterilerinin kimliklerini elde etmek amacıyla hedef şirketin kimliğini çalmak için kullanılan bir suç yazılımı tekniği



04. Tehditler ve Saldırılar

- Saldırı Türleri
 - Sömürme zamanı (Time-to-exploitation)
 - Bir güvenlik açığının keşfedilmesi ile bu güvenlik açığının kullanılması arasında geçen süre.



04. Tehditler ve Saldırılar

- Saldırı Türleri
 - Casus yazılım rehberi (SpywareGuide)
 - Casus yazılımlar için herkese açık bir referans sitesi.



<http://www.askdeb.com>

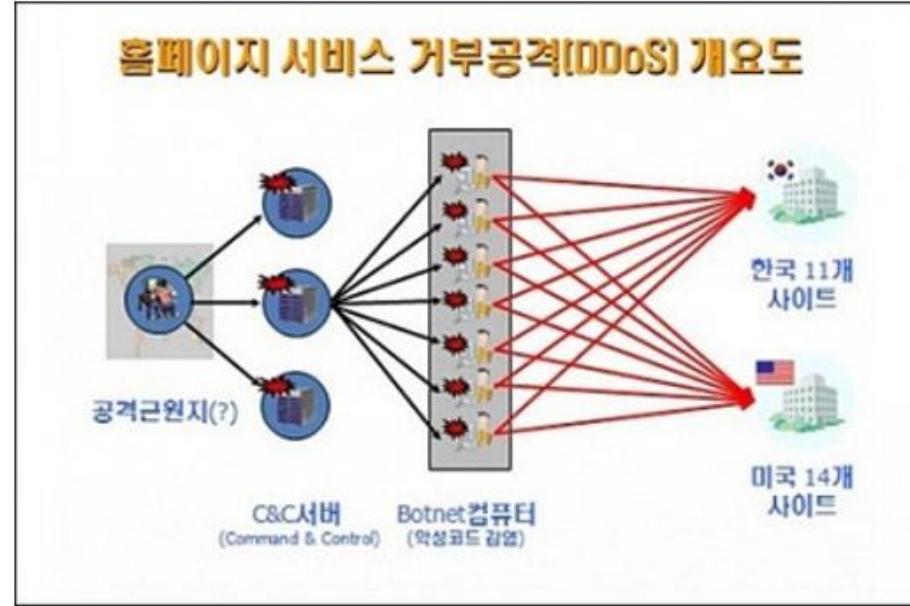
04. Tehditler ve Saldırıları

- Saldırı Türleri
 - Hizmet engelleme saldırısı (DoS(Denial of Service) attack)
 - Bir saldırganın, hedef bilgisayarın kaynaklarını aşırı yüklemek amacıyla bir dizi veri paketi göndermek için özel bir yazılım kullandığı, bir Web sitesine yapılan saldırı.



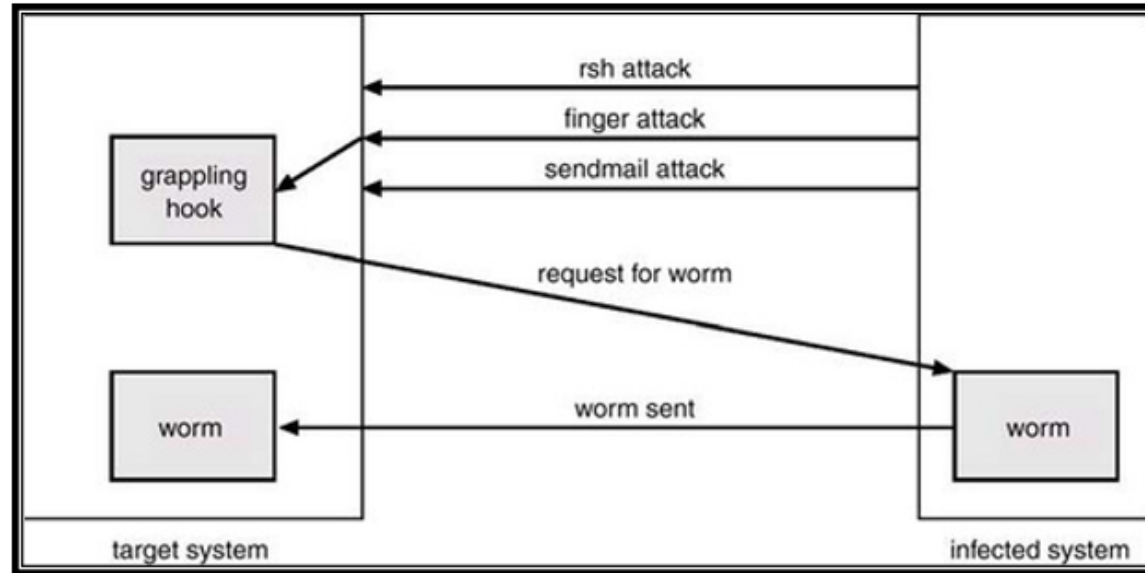
04. Tehditler ve Saldırılar

- Saldırı Türleri
 - Botnet
 - Spam ve virüsler de dahil olmak üzere trafiği İnternet'teki diğer bilgisayarlara iletmek üzere ayarlanmış çok sayıda (örneğin yüz binlerce) ele geçirilmiş İnternet bilgisayarı.



04. Tehditler ve Saldırılar

- Saldırı Türleri
 - Virus
 - Solucan (Worm)



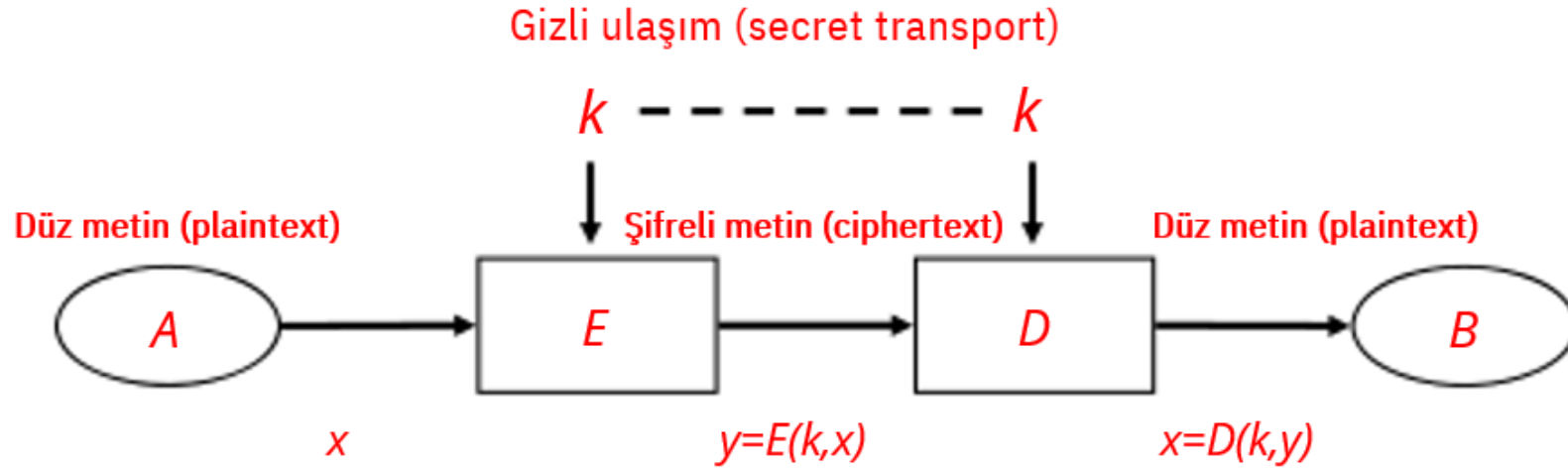
04. Tehditler ve Saldırılar

- Saldırı Türleri
 - Truva atı (Trojan horse)
 - Trojan-Phisher-Rebery (Kimlik avcısı)
 - Banking trojan (Bankacılık)



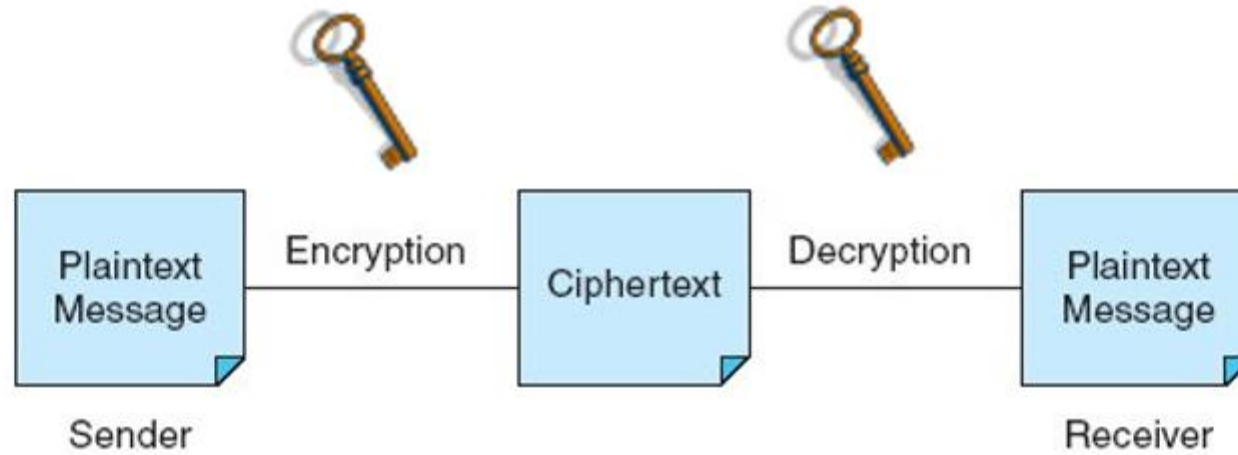
05. E-Ticaret İletişimlerinin Güvenliği

- Şifre Sistemleri
 - Şifreleme (Encryption)
 - Şifre çözme (Decryption)
 - Anahtar (Key)



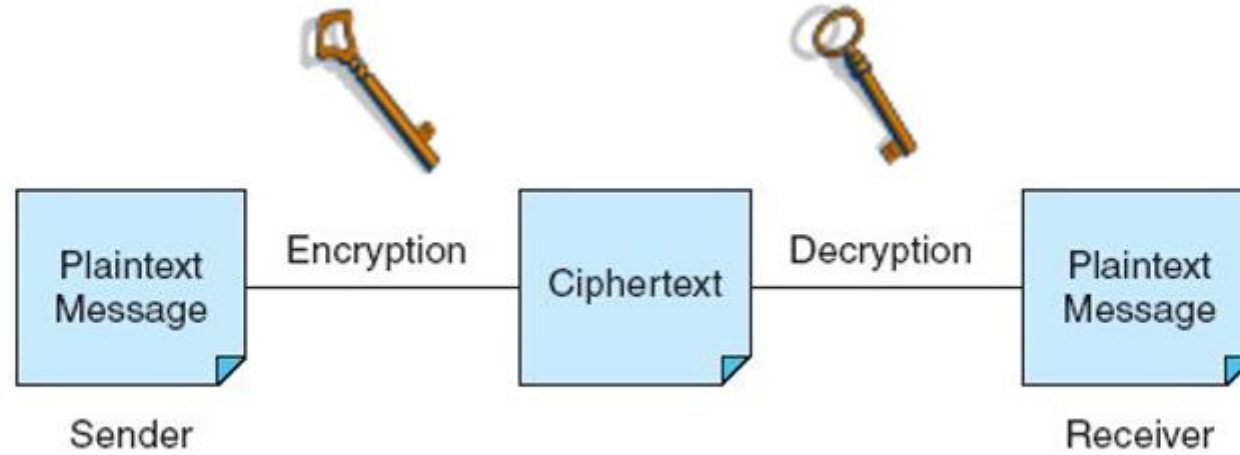
05. E-Ticaret İletişimlerinin Güvenliği

- Simetrik (özel) anahtar sistemi (Symmetric (Private) Key System)
 - Mesajı şifrelemek ve şifresini çözmek için aynı anahtarı kullanan bir şifreleme sistemi.
 - Örneğin; DES



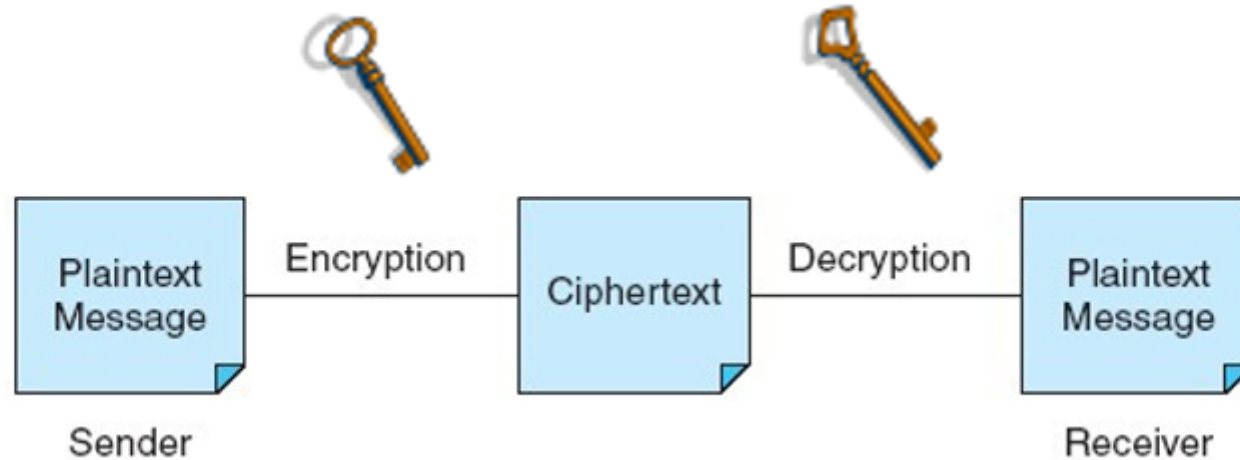
05. E-Ticaret İletişimlerinin Güvenliđi

- Açık anahtar altyapısı (Public Key Infrastructure (PKI))
 - Açık anahtar şifrelemesi ve çeşitli teknik bileşenler kullanılarak e-ödemelerin güvenliđini sağlamaya yönelik bir plan
 - Örneđin; RSA



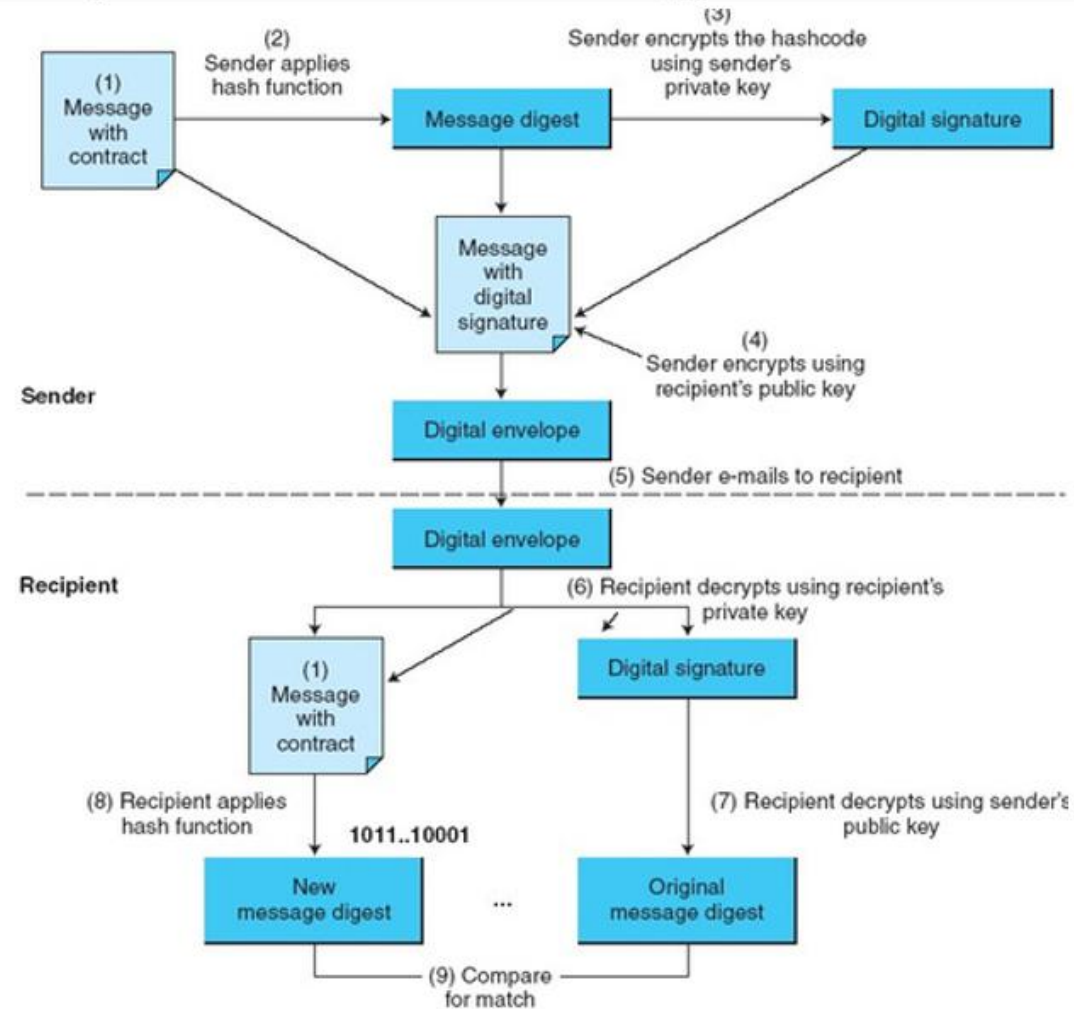
05. E-Ticaret İletişimlerinin Güvenliđi

- Dijital imza ya da dijital sertifika (Digital signature or Digital certificate)
 - Bir işlemin göndericisini ve zaman damgasını doğrular, böylece daha sonra işlemin yetkisiz veya geçersiz olduđu iddia edilemez.
 - Örneđin; Anlamsız veri (Hash), mesaj özeti (message digest (MD)), dijital zarf (digital envelope), sertifika yetkilileri (certificate authorities (Cas))



05. E-Ticaret İletişimlerinin Güvenliği

- Digital signature or Digital certificate



05. E-Ticaret İletişimlerinin Güvenliği

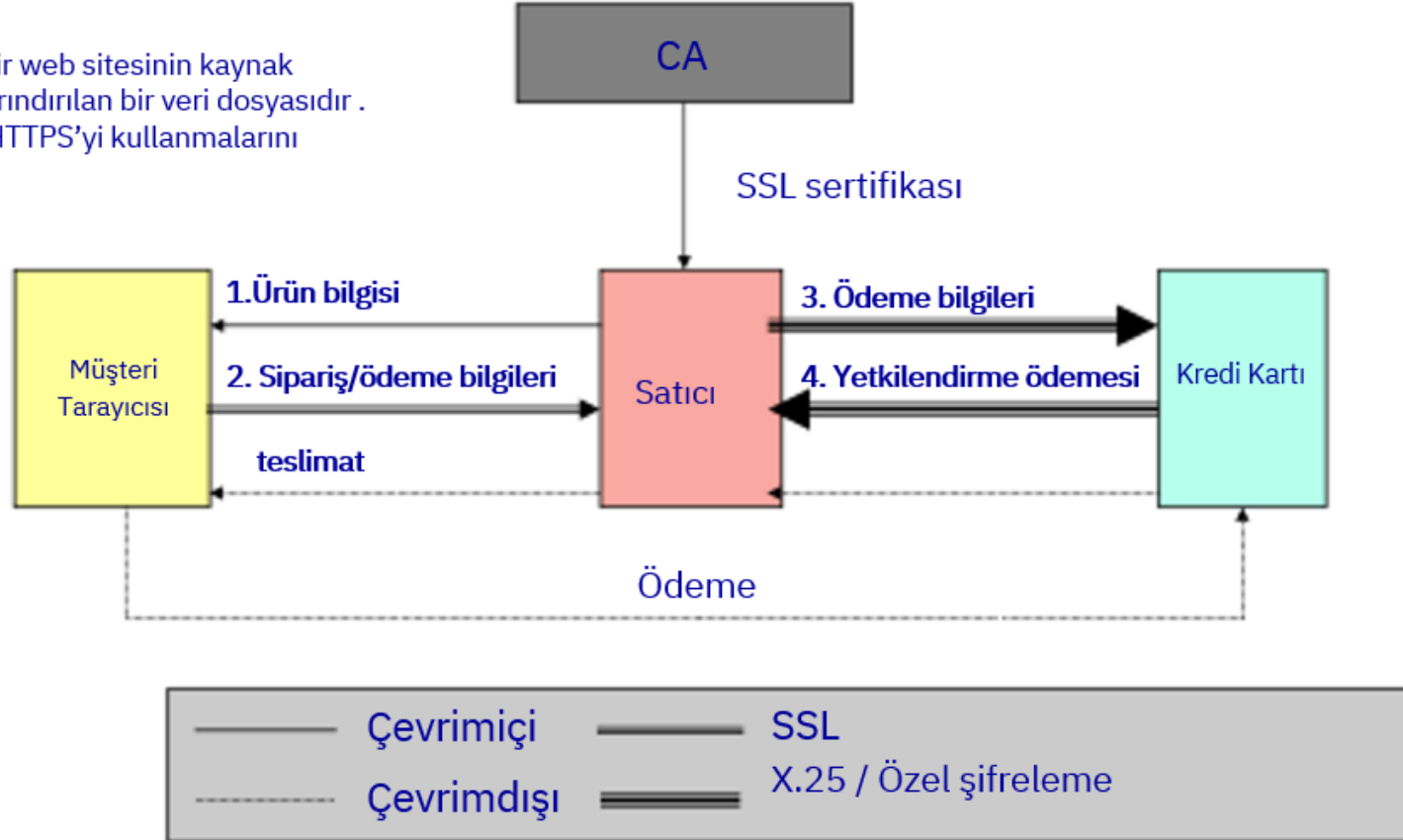
- e-Ödeme protokolleri (ePayment Protocols)
 - 1) Güvenli soket katmanı (Secure socket layer (SSL))
 - Gizliliği veya mahremiyeti sağlamak amacıyla kimlik doğrulama ve veri şifreleme için standart sertifikaları kullanan protokol
 - Web tabanlı ve genel amaçlı
 - 2) Güvenli elektronik işlem (Secure electronic transaction (SET))
 - Kredi kartı bazlı ödeme prosedürüne özel
 - 3) Güvenli borç/havale işlemi (Secure debit transaction (SDT))
 - KAIST tarafından geliştirildi

05. E-Ticaret İletişimlerinin Güvenliği

- e-Ödeme protokolleri (ePayment Protocols)
 - 1) Güvenli soket katmanı (Secure socket layer (SSL))

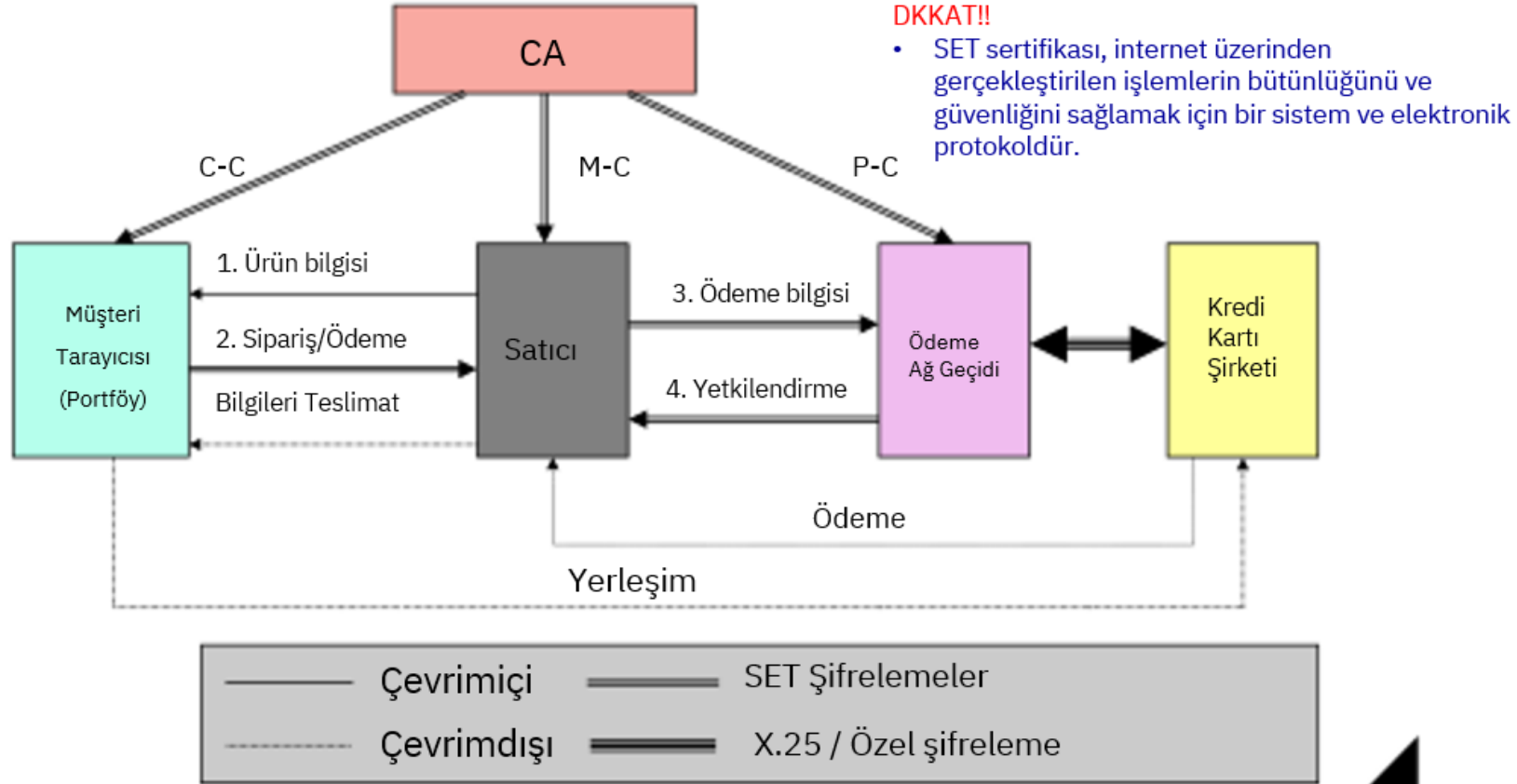
DKKAT!!

- SSL sertifikası, bir web sitesinin kaynak sunucusunda barındırılan bir veri dosyasıdır .
- Web sitelerinin HTTPS'yi kullanmalarını sağlar.



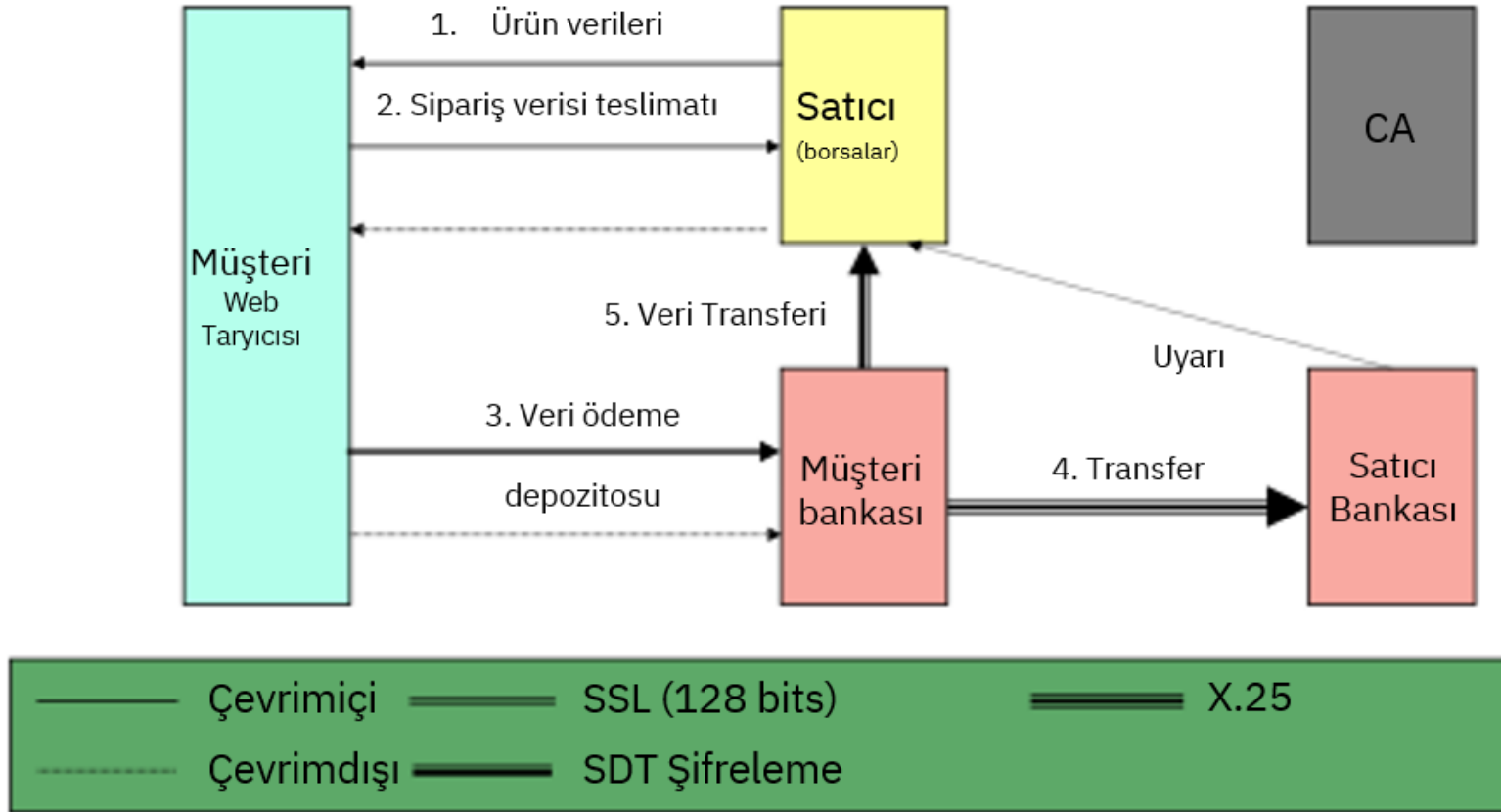
05. E-Ticaret İletişimlerinin Güvenliği

- e-Ödeme protokolleri (ePayment Protocols)
 - 2) Güvenli elektronik işlem (Secure electronic transaction (SET))



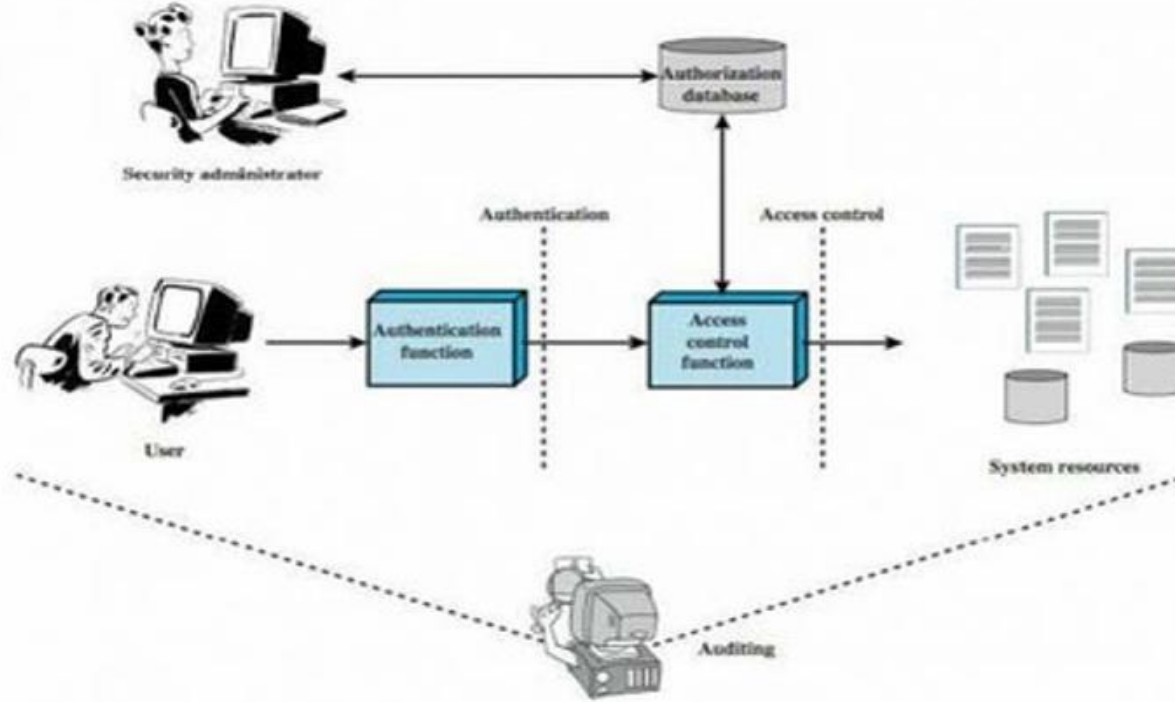
05. E-Ticaret İletişimlerinin Güvenliği

- e-Ödeme protokolleri (ePayment Protocols)
 - 3) Güvenli ödeme işlemi (Secure debit transaction (SDT))



06. E-Ticaret Ağlarının Güvenliđi

- En az imtiyaz politikası (Policy of Least Privilege (POLP))
 - İŖi yrtmek iin eriŖim gerekmedike ađ kaynaklarına eriŖimi engelleme politikası



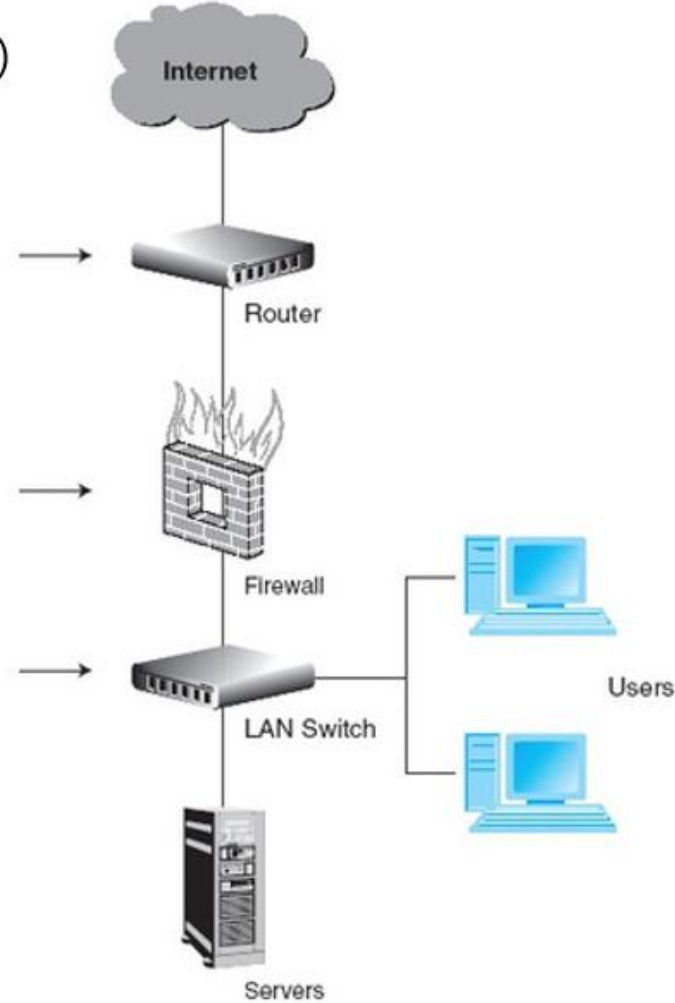
<http://zulcap.wordpress.com>

06. E-Ticaret Ağlarının Güvenliđi

- Katmanlı güvenlik (Layered Security)

Her katmanda
güvenliđi uygulayın

Implement
Security
at Every
Layer



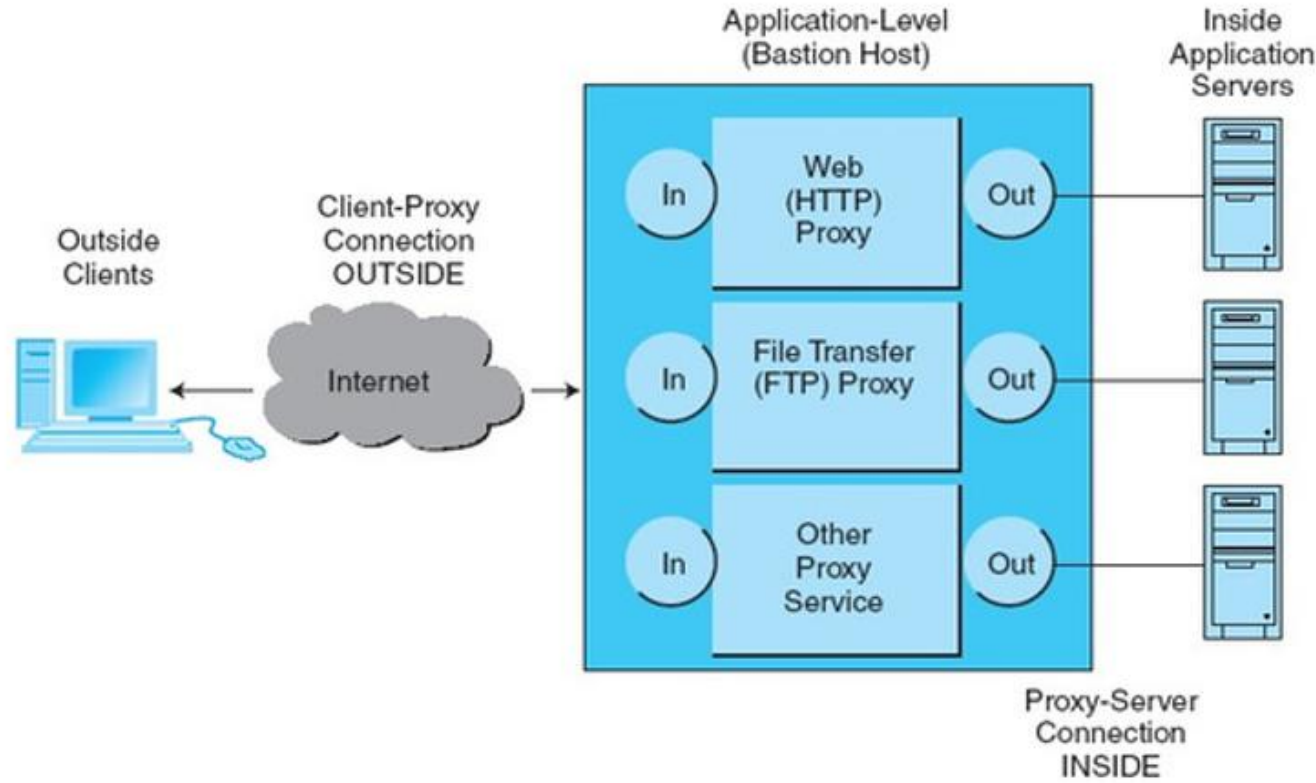
06. E-Ticaret Ağlarının Güvenliği

- Güvenlik duvarı (Firewall)
 - İki veya daha fazla ağ arasında tüm trafiğin geçmesi gereken tek bir nokta (dar geçit); cihaz tüm trafiği doğrular, kontrol eder ve günlüğe kaydeder.
 - İlgili teknolojiler
 - Packet
 - Paket filtreleme yönlendiricileri
 - Paket filtreleri
 - Uygulama düzeyinde proxy
 - Kale ağ geçidi
 - Proxy'ler (ara/vekil sunucu)



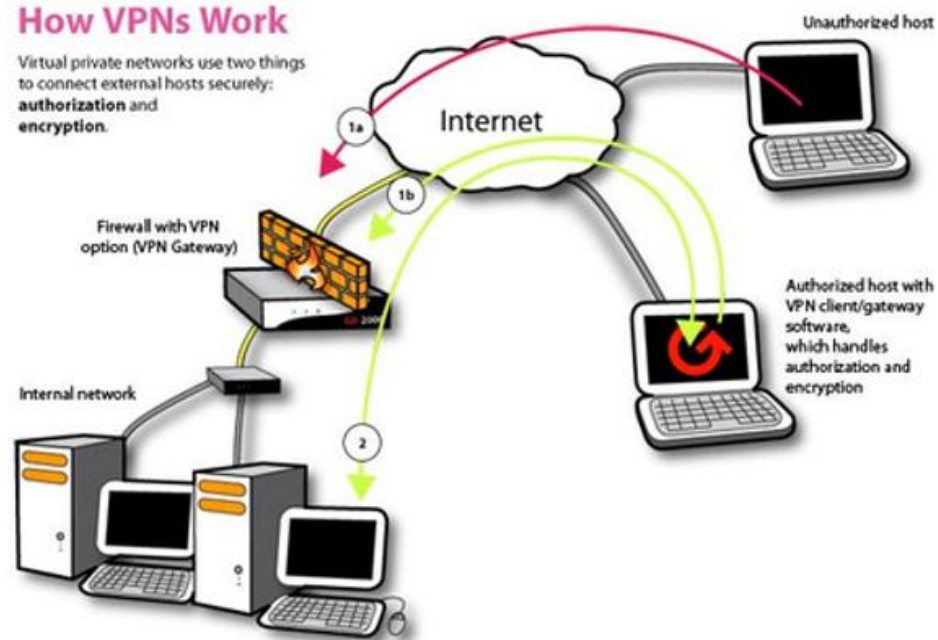
06. E-Ticaret Ağlarının Güvenliđi

- Uygulama düzeyinde Proxy (Application-Level Proxy)
 - Kale ađ geçidi (Bastion gateway host)



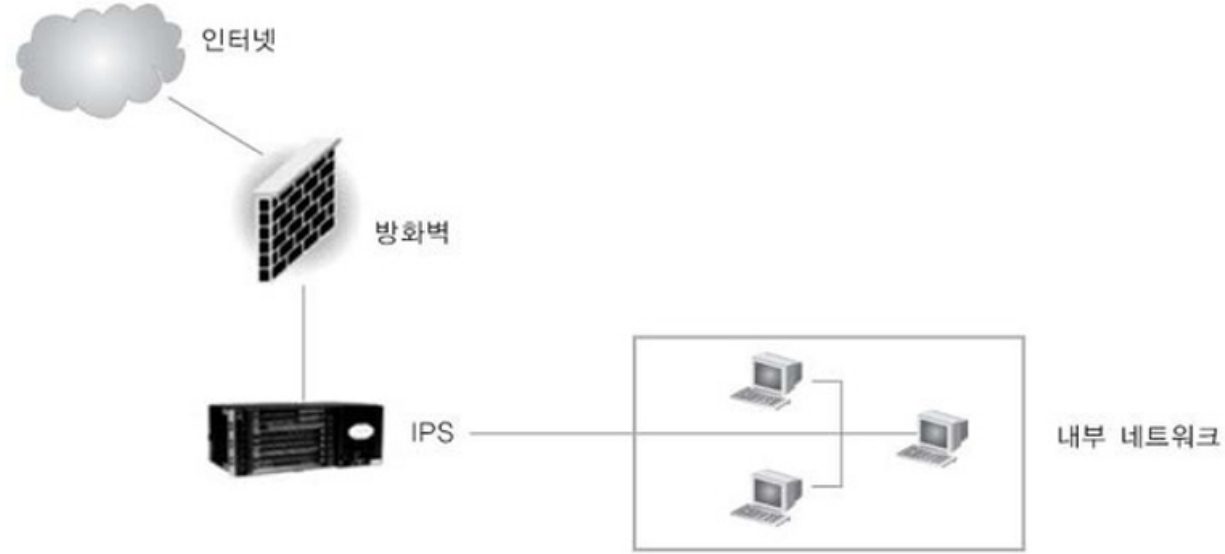
06. E-Ticaret Ağlarının Güvenliđi

- Sanal özel ađ (Virtual Private Network (VPN))
 - Bilgi tařımak iin genel interneti kullanan ancak iletiřimi karıřtırmak iin řifreleme, bilginin tahrif edilmediđinden emin olmak iin kimlik dođrulama ve ađı kullanan herkesin kimliđini dođrulamak iin eriřim kontrol kullananak gizli kalan bir ađ.



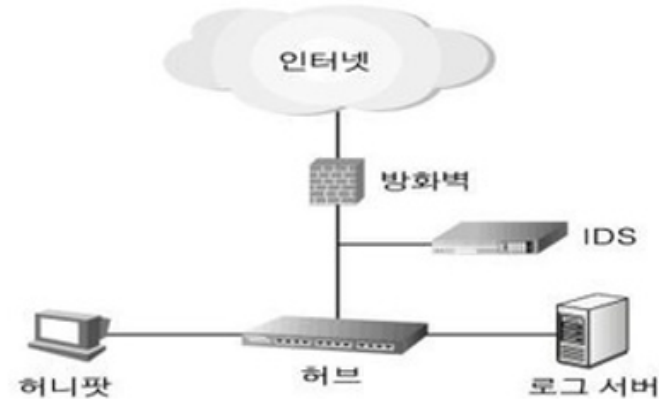
06. E-Ticaret Ağlarının Güvenliđi

- İzinsiz giriş tespit sistemleri (Intrusion Detection Systems (IDSs))
- Saldırı önleme sistemleri (Intrusion Prevention Systems (IPSs))
 - Bir ağdaki veya ana bilgisayardaki etkinliđi izleyebilen, şüpheli etkinlikleri izleyebilen ve gördüklerine göre otomatik eylem gerçekleştirebilen özel bir yazılım kategorisi.



06. E-Ticaret Ağlarının Güvenliđi

- Bal Ađı (Honeynet)
 - Bal kp ađı (A network of honeypots.)
 - Bal kpleri (Honeypots)
 - Gerekte alıřıyormuř gibi grnen ancak bir tuzak gibi davranan ve ađa izinsiz giriřlerin nasıl gerekleřtiđini incelemek iin izlenen retim sistemi (rneđin, gvenlik duvarları, ynlendiriciler, Web sunucuları, veritabanı sunucuları).



07. Dolandırıcı Tüketici & Satıcı Koruması

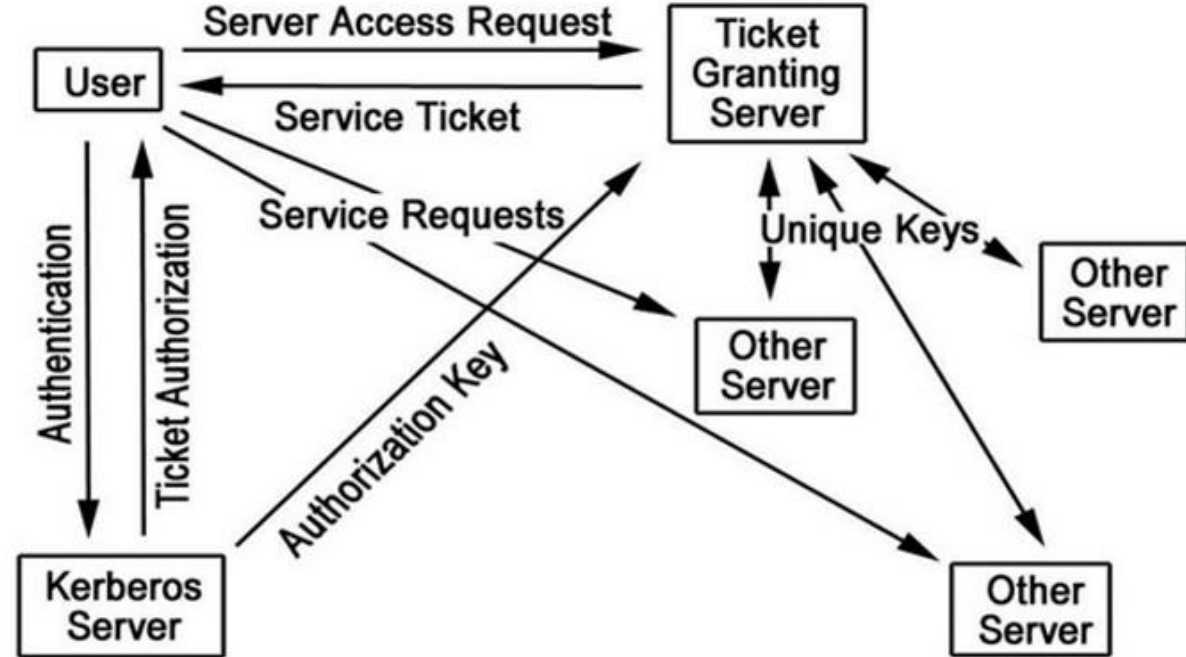
- İnternette dolandırıcılık
 - Tüketici koruması
 - Satıcı koruması
 - Üçüncü taraf güvence hizmetleri

07. Dolandırıcı Tüketici & Satıcı Koruması

•Kerberos sistemleri

DKKAT!!

- Kerberos, fiziksel olarak güvensiz ağlardaki birincil kullanıcıların kimliklerini doğrulamanın bir aracı sağlayan bir ağ doğrulama hizmetidir.
-
- Kerberos , ağ trafiğinin yakalanmasına, incelenmesine ve yerine koymaya açık olduğu varsayımının altında karşılıklı kimlik doğrulaması, veri bütünlüğü ve gizlilik sağlar.



ÖZETLEYELİM

Dr. Fatih KALEMKUŞ

E-Ticaret Güvenliđi

- E-ticarete karşılıklı iki taraf birbirinin kimliklerinden emin olmalıdır.
 - Sayısal imza,
 - Sayısal sertifikalar,
- Kredi kartı bilgilerinin güvenliđi ve gizliliđi,
 - SSL,
 - SET.
 - SSL(Secure Socket Layer) ve SET(Secure Electronic Transfer) 128 bit şifreleme anahtarı kullanmaktadırlar.

E-Ticaret Güvenliđi-SSL

- 3 temel güvenliđi sađlar
 - Asıllama
 - Őifreleme
 - Veri bütünlüğü
- Bilgi sadece dođru adreste deŐifre edilir.
- Her iki tarafta asıllama yapılır.
- Bilgisayarların birbirini tanıması açık anahtar tekniđiyle yapılır.
- SSL, Őimetrik Őifreleme algoritması, mesaj özeti fonksiyonu ve kimlik tanımlaması seđiminde esnektir.

E-Ticaret Güvenliđi-SSL

- SSL işlemleri:
 - İstemci (örnekte browser) sunucu portuna bir bağlantı açarak 'ClientHello' mesajı gönderir.
 - Sunucu 'ServerHello' mesajı ile cevap verir.
 - Sunucu sertifikasını gönderir.
 - Sunucu istemci sertifikası isteđi gönderir (seçime bađlı).
 - İstemci sertifikasını gönderir (seçime bađlı).
 - İstemci 'ClientKeyExchange' mesajı gönderir.
 - İstemci 'CertificateVerify' mesajı gönderir (seçime bađlı).
 - Hem istemci hemde sunucu 'ChangeCipherSpec' mesajı gönderir.
 - Hem istemci hemde sunucu 'finished' mesajı gönderir.

E-Ticaret Güvenliđi-SET

- SET her müşteriye bir e-cüzdan verilmesini öngörür.
- Açık anahtar şifrelemesini,DES ve RSA birleşimini kullanır.
- SET protokolu müşteri,banka ve sanal mağaza arasındaki ödeme fazını şifreler.

E-Ticaret Güvenliđi-SET

- SET protokolunu kullanmak isteyenler,
 - Kullanmak istedikleri her bir kredi kartı için sertifika otoritesinden birer SET sertifikası almalı,
 - Bankadan sanal cüzdan programını alıp yüklemeli ve kredi kartlarını tanıtmalı,
- SET, SSL e göre daha güvenlidir.
- DES ve RSA şifrelemesi yapar.

E-Ticaret Güvenliđi-SET ile SSL arasındaki farklar

- SSL de kart bilgilerini gönderen kişinin kart sahibi olduđu garanti edilememektedir.SET de garanti edilir.
- SSL de kart ve POS un ait olduđu bankalar bu modelde yoktur.
- SSL de kart bilgileri internet üzerinden şifrelenmektedir. Mađaza kart bilgilerini görebilir. SET de kart bilgilerini mađaza göremez. Sadece banka görebilir.

E-Ticaret Güvenliđi-SET ile SSL arasındaki farklar

- SSL de kart bilgilerini gönderen kişinin kart sahibi olduđu garanti edilememektedir.SET de garanti edilir.
- SSL de kart ve POS un ait olduđu bankalar bu modelde yoktur.
- SSL de kart bilgileri internet üzerinden şifrelenmektedir. Mađaza kart bilgilerini görebilir. SET de kart bilgilerini mađaza göremez. Sadece banka görebilir.

Özetle E-Ticaret Protokolleri

1. **SSL/TLS (Secure Sockets Layer / Transport Layer Security)** – Güvenli veri iletimi
2. **SET (Secure Electronic Transaction)** – Güvenli ödeme işlemleri
3. **3D Secure** – Online kredi kartı işlemleri için ek güvenlik
4. **EDI (Electronic Data Interchange)** – İşletmeler arası elektronik veri değişimi
5. **PKI (Public Key Infrastructure)** – Dijital sertifikalar ve güvenlik

SSL/TLS (Secure Sockets Layer / Transport Layer Security) – Güvenli veri iletimi



Müşteri güvenli bir bağlantı talep ediyor, sunucu SSL sertifikasını sunuyor, tarayıcı sertifikayı doğruluyor ve güvenli şifreli iletişim başlatılıyor.

SET (Secure Electronic Transaction) – Güvenli ödeme işlemleri



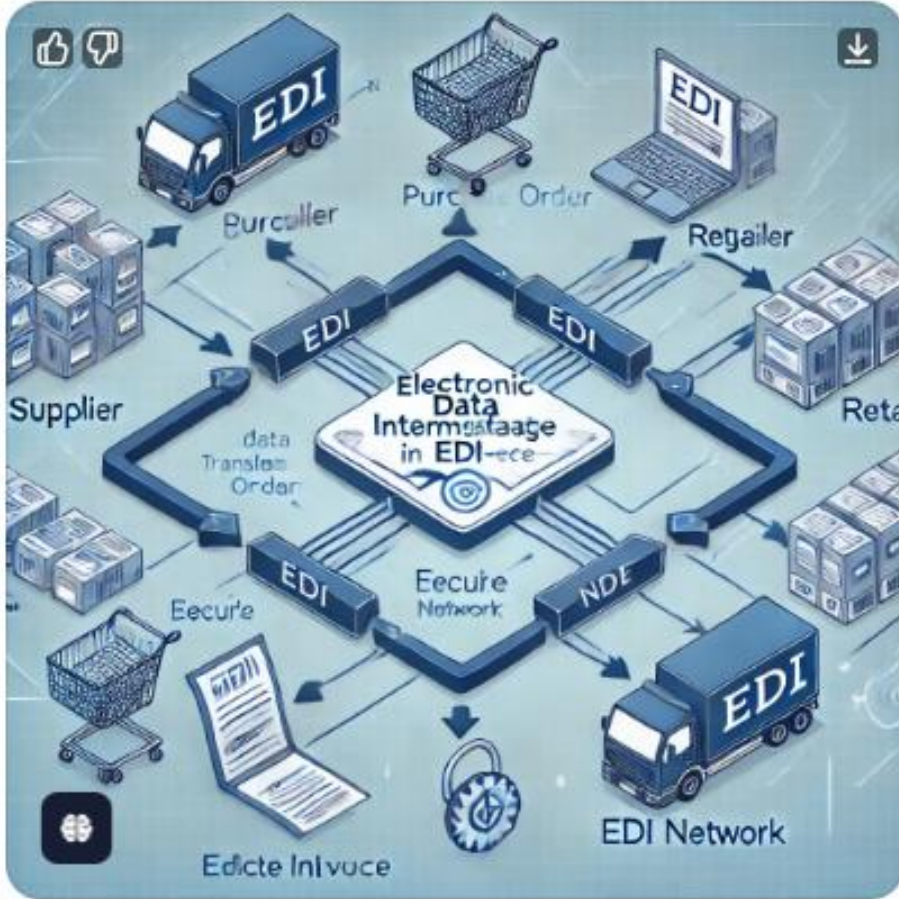
Müşteri sipariş veriyor, satıcı ödeme yetkilendirmesi istiyor, ödeme geçidi işlemi bankaya iletiyor ve banka işlemi onaylıyor veya reddediyor.

3D Secure – Online kredi kartı işlemleri için ek güvenlik



Müşteri kredi kartı bilgilerini giriyor, satıcı müşteriyi 3D Secure doğrulama sunucusuna yönlendiriyor, müşteri kimliğini doğruluyor ve banka işlemi onaylıyor veya reddediyor.

EDI (Electronic Data Interchange) – İşletmeler arası elektronik veri değişimi



Tedarikçi sipariş gönderiyor, EDI ağı veriyi çevirerek perakendeciye iletiyor, perakendeci siparişi işleyerek tedarikçiye elektronik fatura gönderiyor.

PKI (Public Key Infrastructure) – Dijital sertifikalar ve güvenlik



Kullanıcı dijital sertifika talep ediyor, Kayıt Otoritesi (RA) kimlik doğrulaması yapıyor, Sertifika Otoritesi (CA) sertifika veriyor ve kullanıcı bunu güvenli iletişim için kullanıyor.

Sonuç



Sorular



Dr. Fatih KALEMKUŞ

TEŐEKKÜRLER

Dr. Fatih KALEMKUŐ