Özet

- Elektronik ticarette güvenlik konusunda ilk akla gelen konu tarafların birbirlerinin kimliklerinden emin olmaları gerektiğidir. Ayrıca kullanıcıların elektronik ortamda alışveriş yapmak için vermek durumunda kaldıkları kişisel bilgiler, adres bilgileri, kredi kartı bilgileri vb. bilgilerin üçüncü şahısların eline geçmesi tehlikesi de önemlidir.
- Elektronik ödemelerde güvenlik uygulamaları, sistem güvenliği ve bilgi güvenliği olarak iki ana başlık altında toplanabilir.
- E-ticarette güvenlik sağlanması için dört temel şartın yerine getirilmesi gerekir: *Gizlilik (Confidentiality), Bilgi Bütünlüğü (Integrity), Kimliğin Kanıtlanması (Authentication) ve İnkâr Edememe (Non-repudiation).*
- Kredi kartı bilgilerinin güvenliği PCI-DSS adı verilen bir standartla sağlanır. Payment Card Industry (PCI) Data Security Standart-DSS (Ödeme Kartları Endüstrisi Veri Güvenliği Standardı), Mastercard ve VISA tarafından belirlenmiş verinin kullanımı, korunması, saklanması ve iletimi ile ilgili ortak güvenlik standardıdır.
- Ödeme sistemlerinde güvenliği sağlamak için mantıksal yapılar da geliştirilmiştir. Bunlardan biri, Sanal POS uygulaması, diğeri de Secure 3D'dir. Sanal POS uygulamasında banka girilen kredi kartı bilgisinin doğruluğunu onaylar ve satıcıya bu işlemlerin gerçekleştirildiğine dair bilgi yollanır. 3D secure ise, siteden alışveriş yaparken kartı kullanan kişinin gerçekten kartın sahibi olup olmadığını anlamak amacıyla kullanılmaktadır.
- Bir güvenlik sistemi oluşturulurken kullanılan şifreleme algoritmalarının tanımlanması ve yeterince güvenli olup olmadığının ölçülmesi gerekir. Algoritmaların güvenilirliği,belirli standartlara uygunluğunun üçüncü tarafça (standartları üreten kuruluş) onaylanması ile sağlanmaktadır.
- Şifreleme algoritmalarında iki tür anahtar kullanılır. Bu anahtarlara, şifreleme ve şifreyi çözme işlemleri aynı anahtarla yapılıyorsa "Özel Anahtar", iki işlem için farklı anahtarlar kullanılıyorsa "Açık Anahtar" adı verilir.
- Dijital (sayısal) imza, bir elektronik mesaj veya iletiye eklenen ve taklit edilmesi neredeyse imkansız sayısal bir kodlama olup uygulamada en çok tercih edilen ve en güvenilir elektronik imza türlerindendir. Mesajın sayısal olarak imzalanmasının temel olarak iki amacı vardır. Birinci amaç veri bütünlüğünün (Integrity) korunmasıdır. İkinci amaç ise mesajı gönderen tarafın kimliğinin kanıtlanmasıdır (Authentication).
- Dijital sertifikalar; ağ üzerinde kullanıcı veya sunucu (server) bilgisayarların kimliğini tanımlamak ve kanıtlamak için kullanılan ve sertifika otoritesi adı verilen kurumlar tarafından üretilen özel yazılımlardır.
- SSL, web üzerindeki iletişim güvenliği için kullanılan ve bilgi transferinin gizliliğini ve bütünlüğünü sağlayan güvenlik protokolüdür. Web siteleri ve tarayıcılar tarafından yaygın olarak desteklenen SSL, müşteri ve mağaza arasındaki mesajların şifrelenmesini ve sadece doğru adreste deşifre edilmesini sağlar. Bilgisayarların birbirlerini tanıma işlemi, açık anahtarlı (public key) şifreleme ile sağlanır ve web sunucusunu tanımak için, dijital olarak imzalanan sertifikalar kullanır.
- SET, özellikle kredi kartı bilgilerinin çevrimiçi iletimi için geliştirilmiş bir standarttır. SET, kredi kartı ile yapılan online ödemelerde, bilgilerin internet üzerinden aktarımında gizliliği ve güvenliği sağlar. SET protokolü sadece müşteri (ürün siparişi veren kredi kartı sahibi) ile sanal dükkân (e-dükkân) ve kredi kartı şirketi arasındaki iletişimi şifreler. SET ile, ödeme işlemine taraf olan herkes birbirlerini tanırlar ve bu ispatlanabilir.

DEĞERLENDİRME SORULARI

1. Aşağıdakilerden hangisi e-ticarette ödeme sistemlerinde güvenlik sağlanması için gereken şartlar arasında yer almaz?
   a) Gizlilik
   b) Bilginin doğruluğu
   c) Bilgi Bütünlüğü
   d) Kimliğin Kanıtlanması
   e) İnkâr Edememe

2. E-ticarette güvenlik sağlanmasında "İşlem bilgilerinin üçüncü partiler tarafından değil sadece doğru kişi veya kuruluş tarafından görülebilmesi" aşağıdakilerden hangisiyle tanımlanabilir?
   a) Bilgi bütünlüğü
   b) Kimliğin kanıtlanması
   c) İnkâr edememe
   d) Erişim kontrolü
   e) Gizlilik

3. Aşağıdakilerden hangisi tescilli bir şifreleme algoritmasının ögelerinden değildir?
   a) Algoritmanın sahibi tarafından verilen ismi
   b) Onaylayan kuruluşun adı
   c) Onaylayan kuruluşun kuruluş tarihi
   d) Kayıt ve değiştirme tarihleri
   e) Varsa ihracat lisansı ve patent şartları

4. Aşağıdakilerden hangisi açık anahtarların özellikleri arasında bulunmaz?
   a) Asimetrik anahtar olarak da bilinir.
   b) Açık ve gizli olmak üzere iki anahtar kullanır.
   c) Açık anahtar tüm yetkili kullanıcılar tarafından bilinir.
   d) Şifreli mesajın çözülebilmesi için alıcının kullanılan anahtarı daha önceden bilmesi gerekir.
   e) Gizli anahtar, gizli anahtar sahibinin kendi bilgisayarında oluşturulur ve hiç kimseye gönderilmez.

5. Aşağıdakilerin hangisi gizli anahtarın özelliklerinden değildir?
   a) Özel anahtar, simetrik anahtar gibi değişik adlarla da bilinir.
   b) Açık anahtara göre daha fazla güvenlik sağlar.
   c) Şifrenin hazırlanması ve çözülmesi için aynı anahtar kullanılır.
   d) En yaygın kabul görmüş gizli anahtar şifreleme algoritması, 1977 yılında IBM tarafından geliştirilen 64 bitlik DES algoritmasıdır.
   e) Bugüne kadar geliştirilmiş en güvenli anahtardır.

I. Gizlilik
II. Kimlik kanıtlama
III. İnkâr edememe

6. Kişi ve kuruluşların ticari ve kişisel işlemlerini iletişim ağları üzerinde güvenli bir şekilde gerçekleştirmelerini sağlayan dijital sertifikalar yukarıdakilerden hangisi ya da hangilerini karşılamak için kullanılır?
   a) I ve II
   b) Yalnız II
   c) Yalnız I
   d) II ve III
   e) I, II ve III

7. Aşağıdakilerden hangisi sertifikada yer alan bilgilerden değildir?
   a) Ana bilgisayarın açık anahtarı
   b) Sertifika seri numarası
   c) Sertifikanın geçerlilik süresi
   d) Sertifikaya erişimin hangi durumda yasaklanacağı
   e) Yayımcı kuruluşun dijital imzası

8. Aşağıdakilerden hangisi SSL protokolünün özellikleri arasında değildir?
   a) Web üzerindeki bilgilerin doğruluğunu garanti etmesi
   b) Web üzerindeki iletişim güvenliğini sağlaması
   c) Bilgi transferini gizliliğini ve bütünlüğünü sağlaması
   d) Web siteleri ve tarayıcılar tarafından desteklenmesi
   e) Mesajların şifrelenmesini ve sadece doğru adreste deşifre edilmesini sağlaması

9. SSL ile yapılan ve birçok adımda yürütülen güvenlik kontrolüne ne ad verilir?
   a) El sıkışma
   b) Anlaşma
   c) Sözleşme
   d) Kontrol
   e) İletişim

10. Aşağıdakilerin hangisi SET protokolünün özelliklerinden biri değildir?
    a) Bir endüstri standardı olması
    b) Online kredi kartı bilgileri iletimi için geliştirilmiş olması
    c) Bilgisayarların birbirlerini tanıma işleminin, açık anahtarlı şifreleme ile sağlanması
    d) Elektronik ticarette güvenliği sağlamak amacıyla geliştirilmiş olması
    e) Visa ve Mastercard'ın içinde bulunduğu bir konsorsiyum tarafından geliştirilmiş olması

Cevap Anahtarı

1.b,2.e,3.c,4.d,5.b,6.e,7.d,8.a,9.a,10.c

YARARLANILAN KAYNAKLAR

Barcelo, Julia, "Towards a Eurepan Framework For Digital Signatures And Encryption", Computer Law & Security Report, 1998, Sayı 14, No 2, ss. 79-86.

Beckett, Brian. a.g.e., s. 247.

Birch, Dave, (1997) "The Certificate Busines Public Key Infrastructure Will Be Big Business", Computer Law & Security Report, , Sayı 13, No 6, ss. 454-456.

FIPS Pub. 171, "Specifications for Key Management Using ANSI X9 17", Federal Information Processing Standard Publication, 27 Nisan 1992.

FIPS Pub. 180-1, "Announcing the Standard for SECURE HASH STANDARD", Federal Information Processing Standards Publication, 17 Nisan 1995, s. 1.

Glass Brett, (1991) "The Data Encryption Standard: Still Secure?," Infoworld, September 9,

http://csrc.nist.gov S.E.T. 07.02.2003.

http://www.globalsign.com.tr. S.E.T. 30.04.2003.

http://destek.kmk.net.tr/upload/filesContent/ETicarette_Gvenlik_Standartlar.pdf. S.E.T. 08.08.2019.

Koops, Bert-Jaab, (1997) "Crypto Regulation in Europe: Some Key Trends and Issues", Computer Networks and ISDN Systems, , Sayı 29

Mitchell, Chris, 1997, "Authentication Using Cryptography", Information Security Technical Report, Cilt 2, Sayı 2, ss. 25-32.

NIST Special Publications. SP800-4 .

Pounder, Chris, (1998) "Further Developments in the Field of Encryption and Digital Signatures", Computers & Security, , Sayı 17.

Senger, Matt, Providing Security through Secure Socket Layer, www.mrs.umn.edu, S.E.T. 10. 03.2003.

www.ykb.com, S.E.T. 07.02.2003.

www.eng.bahcesehir.edu.tr/css/bolum11, S.E.T. 12. 03.2003.