KRİPTOLOJİ SÖZLÜGÜ

açık anahtar (public key) : Açık anahtarlı bir kriptografik yöntem (algoritma) kullanan bir kullanıcının kendisine ait olan iki anahtarından kamuya açık olanı.

açık anahtar altyapısı-AAA (public key infrastructure-PKI) : Bilgi iletişiminde açık anahtarlı kriptografinin yaygın ve güvenli olarak kullanılabilmesini sağlamaya yarayan ve birbirleriyle eşgüdüm içinde çalışan anahtar üretimi, anahtar yönetimi, onay kurumu, sayısal noterlik, zaman damgası gibi hizmetlerin tümü.

açık anahtarlı kriptografi (public key cryptography) : Her kullanıcıya, sürekli kullanım için biri açık diğeri gizli iki anahtarın verildiği şifreleme/şifre çözme yöntemlerinin tümü. Asimetrik kriptografi ya da çift anahtarlı kriptografi adını da alır.

açık bilgisayar ağı (open computer network) : İsteyen herhangi bir bilgisayar kullanıcısının bağlanabileceği ve diğer kişilerle bilgisayar üzerinden iletişim kurabileceği, herkese açık elektronik iletişim ortamı. Örnek: İnternet.

anahtar (key) : Şifreleme ve şifre çözme sırasında kullanılan sayı dizisi.

anahtar üretimi (key generation) : Açık anahtarlı kriptografide, her kullanıcının açık/gizli anahtar çiftinin, kullanılan kriptografik yönteme bağlı matematiksel işlemlerle hazırlanması

anahtarı bulan kurum-ABK (key recovery agency-KRA) : Yasal erişime yardımcı olmak amacıyla kurulan ve yargının gerektirdiği durumlarda, zan altındaki kişinin gizli anahtarının matematiksel yöntemlerle elde edilmesini sağlayan kurum. Gizli anahtarını kaybeden herhangi bir kişi de, kimliğini belgeleyerek ABK'ye başvurursa anahtarını yeniden elde edebilir

anahtar yönetimi (key management) : Açık anahtarlı kriptografide her kullanıcıya farklı anahtar çiftleri verilmesi, kullanıcıların açık anahtarlarının herkesin ulaşı**** açık olarak saklanması ve kullanıcıların gizli anahtarlarının mutlak gizliliğinin sağlanmasından sorumlu düzen

access control : Ağ (network) üzerindeki herhangi bir bilgi kaynağına erişim konusunda yetkilendirilmiş kişiler, programlar, işlemler veya network içindeki diğer sistemler için konulan sınırlamadır.

attack signature : Ağ (network) üzerinden gelen bilgi paketlerini bazı modellere göre dikkatlice inceleyerek kötü niyetli aktiviteleri haber veren bir sistemdir.

authentication, authorization and accounting (AAA) : Kaynaklara güvenli erişimi sağlayıcı güvenlik unsurlarıdır.

Authentication : Server, switch ya da router kullanımlarında cihaz ya da kullanıcının kimliğinin onaylanmasıdır.

Authorization : Kullanıcı ya da kullanıcılara sisteme, programa ve network erişim hakkının verilmesidir. Accounting : Herhangi bir kullanıcının ne yaptığı, kullanıcı hareketleri kullanıcı data bağlantıları ve kullanıcı sistem kayıtlarının izlenebilmesi amacıyla yapılan işlemdir.

KRİPTOLOJİ SÖZLÜGÜ

authentication header : Paketin içeriğinin aktarım sırasında değişmediğini doğrulamak amacıyla kullanılan IPSec başlığıdır.

bilgi bütünlüğü (message integrity): Bilginin saklanması veya açık/kapalı iletişim ağlarından iletimi sırasında içerik açısından herhangi bir değişime uğratılmamış olması, özgün halinde korunması

bilgi güvenliği (information security) : Bilginin, i) kime ait olduğu belirlenmiş, ii) bütünlüğü korunarak, ve iii) gizliliği sağlanmış olarak iletimi ve saklanması.

çift anahtarlı kriptografi (double key cryptography) : Açık anahtarlı kriptografi veya asimetrik kriptografi.

CBAC (Context-Based Access Control) : Cisco IOS yazılımı içinde bulunan bu özellik sayesinde tüm yönlendirilebilir data akışı denetlenip kontrol edilmiş paketler halinde yapılabilir. ACL tarafından kontrol edilen data akışındaki paketlerin ilerlemesine izin verilebilir ya da yasaklanabilir.

Certificate : Güvenilir bir otorite tarafından özel açıklama ile belirli bir kalıp ve isim altında belirlenen özelliklere sahip olunduğunu bildirir.

certificate authority (CA) : Bağımsız çalışarak dijital sertifikaları onaylar ve bu nedenle yetkilendirilmiş diğer kullanıcıları da tanır.

compromise : Ağ'a (Network'e) yapılan saldırı ve güvenliği aşma olaylarında güvenlik sisteminin kullandığı prosedürlerdir.

computer emergency response team (CERT) : Bilgisayar ve network güvenliği konularında öncelikli olarak servis sağlayan, sistem yöneticilerinden oluşan resmi bir organizasyondur.

cryptographic key : Şifreleme, şifre çözümü ve bilgi onaylamak için kullanılan dijital bir şifredir.

cryptography : Mesajları şifreleme ve şifreli mesajları okuma bilimidir.

doküman (********) : Bir verinin üzerine kayıt edildiği, insan ya da makine tarafından okunabilen, (değişmez) veri taşıyıcı.

data confidentiality : Sadece bilgi paketlerine ulaşma yetkisi olanların bunları kolayca ulaşılabilir formatta görmelerinin garanti edilmesidir.

elektronik kimlik belgesi-EKB (digital certificate) : Onay kurumunun hazırladığı ve sayısal olarak imzaladığı, hangi açık anahtarın hangi kişiye ait olduğunu gösteren belge.

elektronik veri değişimi-EVD (electronic data interchange-EDI) : Standart bir formda yazılmış olan bilgilerin bilgisayarlar arasında aktarımı ve otomatik olarak yorumlanıp işlenebilmesi.

erişim (access) : Herhangi bir sistemi kullanmaya başlama, örneğin bir elektronik ticaret sistemine bilgisayar üzerinden bağlanarak iletişim kurma.

KRİPTOLOJİ SÖZLÜGÜ

EVD kurumu (EDI association) : Bir ülkede EVD kullanı**** düzenleyen kuruluş, örneğin, ABD'deki EDIA, Avustralya'daki EDICA, Kanada'daki EDICC veya Yeni Zelanda'daki EDIANZ

EVD servis sunucusu (EDI server) : Bir EVD servisinin merkezinde olan bilgisayar sistemi.

elektronik veri değişimi (Electronic Data Interchange) : Standart bir yapıda bilgisayardan – bilgisayara veri (ticari) transferi.

gizlilik (privacy) : İletişim kuran iki taraf arasındaki yazışmaların üçüncü kişilerden gizli tutulması, veya bir kişiye ait bilgilerin kendisi dışında herkesten gizli tutulması.

gizli -özel, kişisel- anahtar (private key) : Açık anahtarlı kriptografi kullanan bir kullanıcının, kendisine ait olan iki anahtarından gizli tutulanı.

güvenilir üçüncü kuruluş, kurum veya kişi-GÜK (trusted third party-TTP) : Bir çeşit onay kurumu. Onay kurumlarının yaptığı gibi kişilerin kimliğini güvenli olarak belirleyip, elektronik kimlik belgelerini hazırlamaya ve anahtar yönetimini sağlamaya ek olarak, kişilerin gizli anahtarlarını çok güvenli bir ortamda saklayan ve gerektiğinde yargı kararıyla yetkili makamlara veren kuruluş.

kanal (channel) : Bilginin bir kullanıcıdan diğerine iletimi için gereken fiziksel iletişim ortamı, örneğin, bilgisayar bağlantısı, telefon kablosu, radyolink ve uydu üzerinden diğer kullanıcıya ulaşan bağlantının tümü

kapalı bilgisayar ağı (closed computer network) : Kullanıcılarından biri olmak için belirli koşulların sağlanması gerektiği, herkese açık olmayan bilgisayar ağları. Örnek: Bankalar ve bankamatikler arasındaki bağlantı.

kimlik belirleme (authentication) : Herhangi bir servisi almak isteyen birinin, gerçekten de kendi iddia ettiği kişi olduğunun belirlenmesi.

kriptografik algoritma (cryptographic algorithm) : Şifreleme / şifre çözmede kullanılan belirli bir yöntemin ayrıntılı içeriği, bu içeriğin matematiksel adımları.

kriptoloji (cryptology) : Güvenli bilgi iletişimi ve/veya saklanması için sifreleme ve sifre çözme yöntemleri türeten, geliştiren, inceleyen bilim dalı. Kriptoloji genel bir ifade ile bilgileri gizli tutma bilimidir. Örneğin haberleşme yapılırken mesaj bir algoritma vasıtası ile şifrelenerek gizliliği sağlanır. Şifreleme işlemi sonucunda alıcının aynı anahtarı kullanarak açabileceği şifreli mesaj ortaya çıkar. Anahtar iki taraf arasında gizli tutulmalıdır. Kriptoloji uygulamalarının hemen hepsinde en önemli problem bu anahtarları gizli tutmak ve anahtarların dağıtı**** sağlamaktır.

kod : (a) Bilginin kısaltılarak kayıt edildiği ya da tanımlandığı karakter dizisi (b) Bilgisayarın tanıyacağı formda özel semboller kullanılarak bilginin gösterilmesi ya da tanımlanması

mesaj (message) : Bilgiyi taşımak üzere planlanmış sıralı (düzenli) karakter serisi

onay kurumu-OK (certifying authority-CA) : Kişilerin kimliğini güvenli olarak belirleyip elektronik kimlik belgelerini hazırlayan ve anahtar yönetimini sağlayan kuruluş.

KRİPTOLOJİ SÖZLÜGÜ

sayısal imza (digital signature) : Elektronik ortamdaki yazışmalara eklenen, yazıyı gönderenin kimliğini ve gönderilen yazının iletim sırasında bozulmadığını kanıtlamaya yarayan bölüm. Sayısal imza, yazının içeriğine ve imzalayanın gizli anahtarına bağlı bir kriptografik yöntemle atıldığı için, sayısal imzanın doğrulanmasında, imzayı atanın açık anahtarı kullanılır.

sayısal noter (digital notary) : Bilgisayar ağlarında iletilen bilgileri tarafların isteği ile saklayıp, kendisine başvurulduğunda belgeleyebilen kuruluş.

steganografi : Eskiden sadece askerler şifrelemeyi kullanırken günümüzde artık çok sayıda kişi ve kurum taraından kullanılmakta ve hatta zorunlu hissedilmektedir. Şifreleme (kriptografi) ve Steganografi latince'den türemiş hecelerdir. "Kripto" yada "kryptos" "gizli", "sakli", "grafi" yada "graphia" is "yazma" anlamina gelmektedir. Bir başka deyişle kriptografi, gizli yazım sanatıdır. Şifreli uygulamaların amacı mesajın gizliliğini koruyarak sadece belli bir kişi tarafından okunmasını sağlamaktır. Steganografi de başka bir yazma tekniğidir. Latince de "steganos" "görünmeyen" anla**** gelmektedir. Böylece steganografi, herkes tarafından görünmeyen bir iletişim çesitidir. Steganografi aslında şifrelemenin alternatifi değil onun tamamlaıcısıdır. Bugünün steganografi teknikleri güvenliği daha da arttırmak için şifrelenmiş verileri gizlemek için genelde görsel yada ses dosyalarını kullanmaktadır. Şifrelenmiş veriler kendi başlarına hacker'ların dikkatini çekerken görsel yada ses dosyalarının içine gizlenmiş olduklarında hiç kimse fark etmeyeceğinden kırılmaya da çalışılmayacaktır. Konusunda dünya lideri olan ve Türkiye ortaklığını yaptığımız Steganos'un Security Suite ürünü size steganografi uygulamanızın yanında bir çok ek güvenlik özellikleri de sunar. (Kaynak:Tursign)

şifre : Şifre, bir metin bloğunun belirli genel bir kural dahilinde başka bir metin bloğu ile değiştirilmesidir. Mesela bir metindeki tüm harfleri, alfabede kendisinden bir sonra gelen harf ile değiştirmek basit bir şifredir. (A yerine B, B yerine C gibi)

tek anahtarlı kriptografi (single key cryptography) : Şifreleme ve şifre çözme için aynı anahtarı kullanan kriptografik yöntemlerin tümü. Simetrik kriptografi veya gizli anahtarlı kriptografi adını da alır. Kullanılan gizli anahtarı mesajı gönderen ve alan kişilerin paylaşması gerektiği için, tek anahtarlı kriptografinin güvenilirliği, her kullanıcı çiftine ayrı bir anahtar verilebilmesine bağlıdır. Bu durumda, bir kullanıcı, haberleşeceği herkes için farklı bir anahtar kullanmak zorundadır; bu ise önemli bir anahtar dağıtımı problemine yolaçar. Çift anahtarlı kriptografi , bu sorunu ortadan kaldırmıştır.

yasal erişim (lawful access) : Devletin, açık anahtarlı bir kriptografik algoritma kullananların gizli anahtarlarına, yasaların gerektirdiği durumlarda ve yargı kararıyla ulaşabilme yetkisi.

veri : Bilginin, iletişim, yorum, ya da işlem için uygun olarak formülize edilmiş şekilde gösterilmesi

veri elemanı : Verinin, tanımlamak, değer göstermek için özellikleri belirlenmiş bir birimi.

veri elemanı niteliği (data element attribute) : Veri elemanının tanımlanmış özelliği

veri elemanı rehberi (Data element directory) : Tanımlanmiş, isimlendirilmiş veri elemanı niteliklerinin, uygun veri elemanı değerinin nasıl simgeleneceğine ilişkin spesificasyonları içeren liste.

zaman damgası (time stamp) : Bilgisayar ağlarında iletilen mesajlara eklenen ve mesajın yazıldığı zamanı güvenli olarak belgeleyen damga.

ALINTIDIR.