Necmettin Erbakan Üniversitesi

Bilgi Güvenliği
2022-2023 Güz Dönemi

Dr. Alperen Eroğlu

aeroglu@erbakan.edu.tr

Kriptografi - Bazı önemli konular (tekrar)

Kriptografi , simetrik kriptografi ve asimetrik kriptografi (açık anahtarlı kriptografi) olarak ikiye ayrılır:

Simetrik sistemlerde, şifreleme ve deşifrelemede aynı anahtar veya birbirinden kolaylıkla elde edilebilen gizli bir anahtar kullanılır...

Açık anahtarlı kriptografi de, her kullanıcının açık ve gizli olmak üzere iki anahtarı vardır.

Kriptografi - Bazı önemli konular (tekrar)

Simetrik Kriptografi

Simetrik kriptografi , genellikle gizliliğin sağlanmasında kullanılmaktadır ve simetrik sistemler oldukça verimli sistemler olup blok şifreler (block cipher) ve akan şifreler (stream cipher) olarak ikiye ayrılır.

Blok şifrelerde anahtar boyutu genellikle 128, 192 veya 256 bit boyutlarında olup iletilmek istenen mesaj bu uzunluklara bölünüp şifreleme yapılır. Akan şifrelerde ise anahtar boyutu iletilmek istenen mesajın uzunluğuna eşit olup şifreleme, genellikle mesaj bitlerinin anahtar bitleri ile XOR işlemi yapılarak elde edilir.

Kriptografi - Bazı önemli konular (tekrar)

Simetrik Kriptografi

Pratikte mesaj boyutu uzunluğunda anahtar üretilip dağıtılması kolay değildir. Bundan dolayı akan şifrelerde anahtar dizisi adı verilen sözde rastgele sayı bitleri üretilir ve bu bitler mesaj bitleri ile işleme alınır. Burada haberleşmek isteyen tarafların ortak anahtar dizisini üretmek için daha küçük boylu gizli bir anahtar paylaşmaları gerekmektedir.

Kriptografi - Bazı önemli konular (tekrar)

Simetrik Kriptografi

Blok şifrelere örnek olarak 3DES, AES ve SERPENT gibi algoritmalar verilebilir. Diğer taraftan A5/1, A5/2, RC4, Salsa20 ve ChaCha gibi algoritmalar ise akan şifrelere örnektir.

Gönderici ve alıcı genellikle aynı anahtarı kullandıkları için haberleşmek isteyen her iki taraf aynı anahtara sahip olmak zorundadır.

Bir ağda *n* kişi varsa, toplam *n(n-1)/2* farklı anahtar oluşturulması gerekmektedir. Bundan dolayı, anahtarların oluşturulması ve güvenli bir kanalla dağıtılması sorun teşkil etmektedir. Ayrıca kullanılan anahtar tek bir kişide olmadığı için inkâr edememezlik gereksinimi bu sistemler ile sağlanamamaktadır.

Kriptografi - Bazı önemli konular (tekrar)

Senaryolar : Okuma Önerisi
https://medium.com/@muhammedkaralar/simetrik-ve-asimetrik-%C5%9Fifreleme-d57673284646

Asimetrik Kriptografi

Anahtar dağıtımı ve inkâr edememezlik gibi gereksinimler asimetrik kriptografi ile çözülebilmektedir. Bu tip kriptografi aynı zamanda açık anahtarlı kriptografi olarak adlandırılmaktadır.

Mesaj gönderilmek istenen kişinin herkes tarafından bilinen açık anahtarı, gönderici tarafından şifrelemede kullanılarak gizlilik sağlanırken, kullanıcı kendi gizli anahtarını kullanarak kimlik doğrulama ve inkâr edememezlik gereksinimlerini sağlayabilmektedir.

Kriptografi - Bazı önemli konular (tekrar)

Asimetrik Kriptografi

Şu anda gerçek hayat uygulamalarında kullanılan açık anahtar kriptografi başlıca üç gruba ayrılır. Bunlar çarpanlara ayırma kriptografi , sonlu cisim kriptografi ve eliptik eğri kriptografi olarak adlandırılır. Çarpanlara ayırma kriptografi sine örnek olarak RSA, sonlu cisim kriptografi sine örnek olarak ElGamal ve DSA, eliptik eğri kriptografisine örnek olarak ECDSA algoritmaları verilebilir.

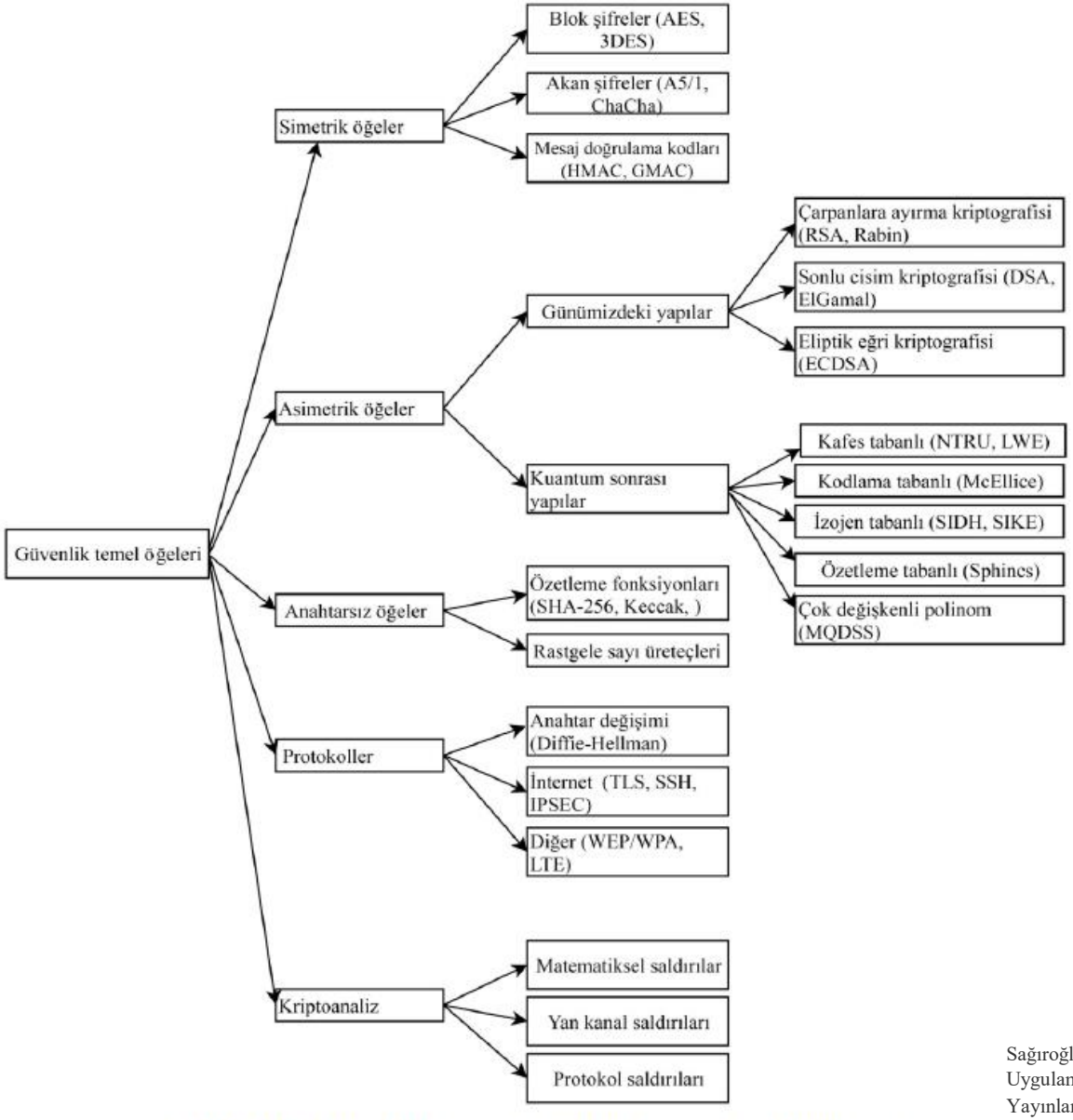
Kriptografi - Bazı önemli konular (tekrar)

Asimetrik Kriptografi
Birçok açık anahtar sistemi vardır. Bunların başlıcaları, çok değişkenli ikinci derece polinom kriptografi , kafes tabanlı kriptografi , kod tabanlı kriptografi , özet fonksiyon tabanlı kriptografi ve süper tekil izojen tabanlı kriptografi dir.

Son yıllara kadar özellikle verimlilik yönünden avantajlı olmadıkları için pek kullanılmayan bu sistemler kuantum bilgisayarların şu anda kullanılan çarpanlara ayırma kriptografiyi, sonlu cisim kriptografiyi ve eliptik eğri kriptografiyi güvensiz hale getirmesinden dolayı tercih edilmeye başlanmıştır ve bu sistemler kullanılarak yeni birçok sistem geliştirilmiştir.

Ayrıca, Amerika Birleşik Devletleri'nin Ulusal Teknoloji Standart Kurumu (NIST) hem klasik bilgisayarlar hem kuantum bilgisayarlar ile yapılan saldırılara karşı dayanıklı yeni açık anahtar kripto sistemleri seçme süreci başlatmıştır [4] ve bundan dolayı kuantum sonrası kriptografi ye olan ilgi artmıştır. Bu makalenin son bölümü bu konuya ayrılmıştır.

Kriptografi - Bazı önemli konular (tekrar)

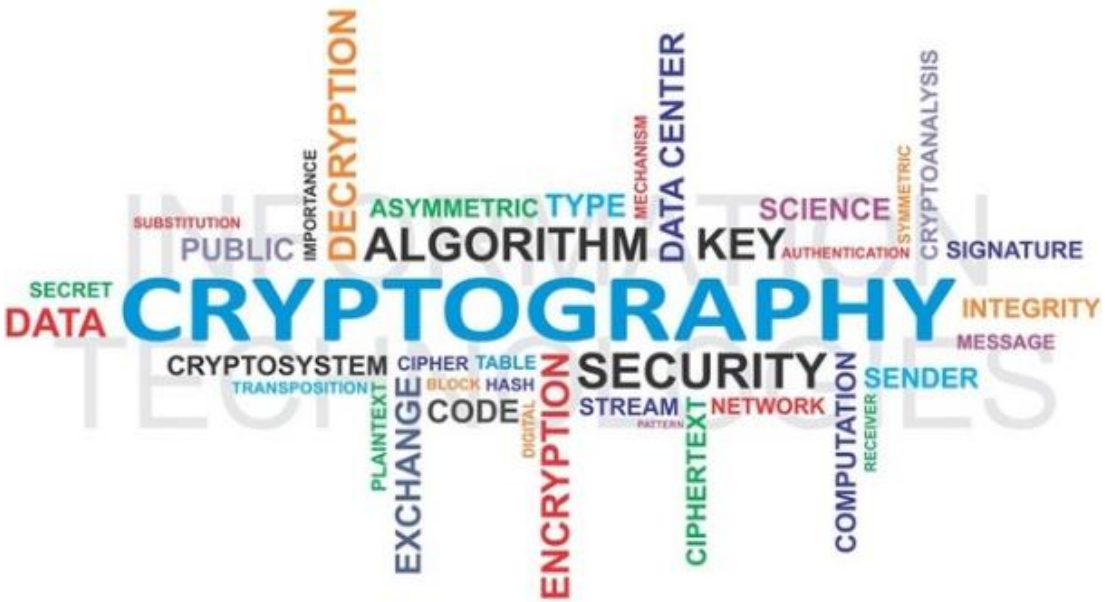


Şekil 2.1. Güvenlik temel öğelerinin sınıflandırılması

Sağıroğlu. Ş. (2022)., Siber Güvenlik ve Savunma: Standartlar ve Uygulamalar Kitap Serisi 2, ISBN: 978 605 2233 42 9, Grafiker Yayınları

Hafta-5

Siber Güvenliğin Temelleri – III (Şifre Bilim **(**Kriptografi**),** Özetleme(Hashing) Algoritmalları, Standartlar, Steganografi, Protokoller, Kuantum Şifreleme, E-imza (dijital imza)



https://www.enisa.europa.eu/news/enisa-news/cryptographic-tools-are-important-for-civil-society-and-industry

Hafta-5

- Şifre Bilim Standartları
- Steganografi
- Kuantum Şifreleme
- Güvenlik Protokolleri
    - PGP
    - SSL/TSL
    - SSH
    - S/MIME
    - IPSec
    - Kerberos
- Elektronik İmza (E-İmza)

Şifre Bilim Standartları

- Bilgisayar sistemlerinin ülke içi ve ülkeler arası haberleşmelerinde, bir uyum içerisinde problemsiz çalışmalarını sağlamak için ortak belirlenmiş olan kural ve politikalara ihtiyaç duyulmaktadır. Bu politikalar ve kurallar bütününe **standart** denilmektedir.

- Başka bir ifadeyle, kaliteyi tutturmak, verimliliği arttırmak, zaman kaybını azaltmak ve birlikte çalışabilirliği sağlamak için ortak kurallar, yani standartlar gereklidir.

Şifre Bilim Standartları

- Şifre biliminde bunun sağlanması için, devlet, özel sektör ve diğer organizasyonlar ortak standartlar belirlenmesine katkıda bulunmaktadırlar. Bazıları şu şekildedir:

- ✓ **ISO** : Uluslararası Standarlar Organizasyonu (International Standards Organization)
- ✓ **ANSI** : Amerikan Ulusal standartlar enstitüsü (American National Standards Institute)
- ✓ **IEEE** : Elektrik ve Elektronik Mühendisleri Odası (Institute of Electrical and Electronics Engineers)
- ✓ **NIST** : Ulusal Standartlar ve Teknoloji Enstitüsü
- ✓ (National Institute of Standards and Technology)
- ✓ **IETF** : İnternet Mühendisliği Çalışma Grubu (Internet Engineering Task Force)
- ✓ **EU** : Avrupa Birliği (European Union)

Şifre Bilim Standartları

- Şifre biliminde bunun sağlanması için, devlet, özel sektör ve diğer organizasyonlar ortak standartlar belirlenmesine katkıda bulunmaktadırlar. Bazıları şu şekildedir:

- ✓ **WTO** : Dünya Ticaret Örgütü (World Trade Organisation)
- ✓ **ICC** : Uluslar arası Ticaret Odası (International Commerce Chamber)
- ✓ **ITU** : Uluslararası Telekomünikasyon Birliği (International Telecommunications Union)
- ✓ **CEN** : Avrupa Standartlaşma Örgütü (European Committe for Standardization)
- ✓ **ETSI** : Avrupa Telekomünikasyon Standartları Enstitüsü (European Telecommunication Standards Institute)
- ✓ **UNCITRAL** : Uluslararası Ticaret Kanunu üzerine Birleşmiş Milletler Konferansı (United Nations Conference on
- ✓ International Trade Law)

Şifre Bilim Standartları

- Bilgi güvenliği Standartları

- **ISO/IEC Standartları**

Ülkemizde de Avrupa Birliğ i Uyum Kriterlerinde de adı geçen bu standartların uygulanması konusunda yapılan çalış malar kapsamında, ISO 27001:2005 standardı Türkçeye çevrilerek Türk Standardları Enstitüsü (TSE) tarafından TS ISO/IEC 27001 “Bilgi Güvenliğ i Yönetim Sistemi (BGYS)” standardı adı altında yayınlanmış ve belgeleme çalış maları baş latılmış tır. BGYS; insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir.

Şifre Bilim Standartları

ISO/IEC Standartları

Uluslararası Elektroteknik Komisyonu 1906, Uluslararası Standartlar Organizasyonu ise 1947 yılında uluslararası alanda ticari ve elektroteknik standardizasyonun sağlanması için, İsviçre'nin Cenova şehrinde kurulmuştur.

ISO ve IEC birlikte teknik çalışma grupları
oluşturarak (Joint Technical Committee-JTC) ve Bilimsel Komiteler (SC) koordinasyonunda tüm dünyada geçerli olacak standartları geliştirmektedirler.

Bu standartlarla ilgili olarak detay bilgiye
https://www.iso.org/ics/35/ adresinden erişebilirsiniz.

Şifre Bilim Standartları

ISO/IEC Standartları

ISO tarafından BT (Biliş im Teknolojileri) Güvenlik Standartları ile ilgili çalış malar JTC–1 BT Komitesine bağ lı SC-27'ye bağlı olarak çalışan BT Güvenlik Teknikleri Alt Komisyonunda ele alınmaktadır.
Bu komisyonun sorumluluk alanları ise aşağıda verilmiştir:

- BT sistemleri güvenlik hizmetlerinin ve ihtiyaçların tanımlanması,
- Güvenlik teknikleri ve yapılarının geliş tirilmesi,
- Güvenlik rehberlerinin geliş tirilmesi ve
- Yönetim destek dokümanları ile standartların geliş tirilmesidir.

Şifre Bilim Standartları

ISO/IEC Bilgi Güvenliğ i Standartları Ailesi

Kişisel ve kurumsal bilgi güvenliğ inin üst düzeyde sağ lanması için gerekli olan bilgi güvenliğ i yönetiminde kullanılan uluslararası standartlara http://www.iso27001security.com/index.html kısaca özetlenmiştir.

ISO/IEC 27000: teknik terimler ve açıklamalarının yer aldığ ı genel bir sözlüktür.
ISO/IEC 27001: BGYS için gereklilikleri ortaya koyan bir standartt ır.
ISO/IEC 27002: bilgi güvenliği kontrol hedefl erini ve kontrollerini açıklayan bilgi güvenliği kontrolleri için iyi uygulamaları kapsar.

Okuma Önerisi
Kitap Serisi 3 - Bölüm 2

Şifre Bilim Standartları

Steganografi

- Bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir.

- Ses, sayısal resim, video görüntüleri üzerine veri saklanabilir. Bu veriler metin dosyası olabileceği gibi, görüntü veya ses dosyaları da olabilir.

- Vektör kuantalama, k-n eşikleme yöntemi ve çeşitli dönüşümler kullanarak (Ayrık Kosinüs Dönüşümü (DCT) gibi) gerçekleştirilen, steganografik uygulamalar mevcuttur.

Şifre Bilim Standartları

- Steganografik işlemleri daha iyi anlamak için, temel yöntem olan en az öneme sahip bit (LSB: Least Significant Bit) kavramının bilinmesi gereklidir.

- Bir resmin piksellerinin son bitlerinin mesaj bitleriyle yer değiştirmesiyle bu işlem gerçekleştirilir.

- Mesela, Şekil'de verilen resimde bulunan piksellerin LSB'leri ile mesaj bitleri sırasıyla değiştirilebilir. Bu sayede bir resim içerisine bir mesaj veya doküman kolaylıkla saklanabilir. Daha sonra yerleştirilen bu bitlerin tekrar sırasıyla geri elde edilmesiyle, deşifreleme işlemleri gerçekleştirilerek, verilerin tekrar elde edilmesi sağlanmaktadır.

Şifre Bilim Standartları

- İçerisine doküman gizlenmiş bir resim e-posta veya başka bir elektronik iletişim yoluyla karşı tarafa gönderildiğinde arada giden mesajımızı izleyen veya elde eden herhangi bir kişi sadece resmi görebilecektir. Bu resim içine doküman gizlendikten sonra, beklendiği gibi, boyutlarda bir değişim gözlenmemektedir. Boyut değişikliğinin olmaması, şifreleme işleminin başarısının ayrı bir göstergesidir. Gizlenen dokümanın tekrar elde edilmesi için yine geliştirilen programda yapılan bir ters işlem ile gizlenen doküman otomatik olarak geri elde edilir. Bu yaklaşımda ses içerisine ses, resim ve doküman gizlenebilir.

Kuantum Şifreleme

Okuma Önerisi:
Sağıroğlu. Ş. (2022)., Siber Güvenlik ve Savunma: Standartlar ve Uygulamalar Kitap Serisi 2, ISBN: 978 605 2233 42 9, Grafiker Yayınları

- Haberleşmenin gizli veya açıktan dinlenme tehdidini tamamen ortadan kaldırma söz konusudur!
- Bu yaklaşım, optik haberleşmede fotonların kuantum özelliklerini temel almalarından dolayı mutlak güvenliği garanti etmektedir.

- Şifreleme ve şifre çözme yöntemlerinin etkinliği, kriptolama algoritması ile birlikte kullanılan anahtarın uzunluğuna bağlıdır. Eğer amaç, iletilen mesajların gizliliği ise algoritmaların tersine çevrilebilir olması gereklidir. Kuantum anahtar dağıtımında, tek fotonluk alıcılar ve vericiler kullanılarak, kırılamayan anahtarlar iki taraf arasında güvenli ve hızlı bir şekilde değiş tokuş edilir.

Kuantum Şifreleme

- Kuantum yaklaşımıyla şifrelenen bir verinin, iki taraf arasındaki iletim sırasında, bir saldırgan tarafından, araya girilerek okunmaya çalışılması halinde, kuantum fizik yasalarına göre, ortaya çıkan “kuantum gürültüsü” saldırganın veriyi çözebilmesini imkansız kılmaktadır. Buna karşın gerçek alıcı, elindeki anahtar sayesinde, kuantum gürültüsünü ortadan kaldırarak orijinal veriye ulaşır.

Kuantum Şifreleme

- Sayısal veri içindeki her bitin değeri, fotonlara polarizasyon uygulanarak belirlenir ve polarizasyon, elektrik alanının osilasyon yönüdür. Düşey ve yatay fotonları birbirinden ayırt etmek için, bir filtre ve diyagonal fotonlar için de, ikinci bir filtre kullanılabilir. Foton, doğru filtreden geçirilirse, polarizasyonu değişmez, aksi durumda polarizasyon rasgele bir değişime uğrar. İşte bu nedenle, iletim yolu üzerinde, istenmeyen üçüncü bir şahıs veya saldırgan fotonları gözetlemeye çalışırsa, yüksek bir olasılıkla, fotonların polarizasyonunu değişikliğe uğratacaktır. Bu girişim, alıcı tarafından kolaylıkla öğrenilebilecek ve sonuç olarak verici ve alıcı taraflar gerekli önlemleri alabilecekltir.

- Kuantum kriptolama kullanılarak gerçekleştirilen iletişimde, fiber optik ortam kullanılmasının yanında, uydu haberleşmelerinde de, bu yaklaşım kullanılmaya başlanacaktır. Bu sayede, gelecek yıllarda saniyede Gigabit mertebesinde akan trafiği de şifreleyebilmek mümkün olabilecektir.

Güvenlik Protokolleri

- PGP (Pretty Good Privacy)
- SSL/TLS (Secure Socket Layer) / (Transport Layer Security)
- SSH (Secure SHell)
- S/MIME
- IPSec
- Kerberos

Güvenlik Protokolleri

PGP

Güvenli bir e-posta yazılımı olan PGP'nin, ücretsiz ve açık kodlu olması ve güçlü şifreleme algoritmaları içermesi en önemli üstünlükleridir. Kullanımı çok da kolay olmayan bu yazılımın, kendine has ve oldukça karmaşık bir güven ve sertifika modeli bulunmaktadır. Bu sayede, güvenlik konularında az da olsa bilgi sahibi olan birisi, kendi güven sistemini istediği şekilde oluşturabilmektedir.

Güvenlik Protokolleri

SSL/TLS

SSL, genel amaçlı kullanım için geliştirilmiş bir endüstri standardıdır. Güvenli HTTP bağlantısı sağlaması ve yaygın olarak tarayıcı (browser) programlar tarafından desteklenmesiyle, büyük bir kullanıcı kitlesine sahiptir. SSL ve TLS protokolleri, genel olarak TCP/IP protokollerine güvenlik katmak amacıyla geliştirilmiştir.

Güvenlik Protokolleri

SSL, kendi başına çok karışık bir protokol olmamasına rağmen, bir kaç farklı opsiyon ve varyasyon sunmaktadır. SSL'in en basit hali, iletişim hattının şifrelenmesi durumudur. Bu protokol, bağlantı kuran iki uç arasındaki kimlik doğrulamayı, doğrulama işlemini şifrelemeden ayırmayı ve daha önceki bağlantının kaldığı yerden devam etmesini sağlamayı içeren daha karmaşık seçenekler sunmaktadır. SSL protokolü, bir birlerine gönderilen ya da gönderilmeyen bir dizi mesaj kümesinden oluşur.

Okuma ve İnceleme Önerisi
https://tr.godaddy.com/blog/ssl-nedir-ne-ise-yarar/

Güvenlik Protokolleri

SSL protokolü, Netscape tarafından geliştirilmiş olmasına rağmen, bu protokolün internette yaygın kullanımından dolayı, IETF için çok kritik bir hale gelmiştir. SSL protokolünün IPSec araştırmalarından ayrılmasını da içeren çeşitli nedenlerden dolayı, IETF bu protokolü biraz daha geliştirerek TLS (Ulaşım Katmanı Güvenliği-Transport Layer Security) olarak değiştirmiştir. TLS protokolü SSL'e göre çok az değiştirilmiş, güvenliği daha da arttırılmıştır.

Okuma Önerisi:
https://www.kaspersky.com.tr/resource-center/definitions/what-is-a-ssl-certificate

Güvenlik Protokolleri

SSH

Daha çok telnet ve ftp gibi uzaktan erişim protokolleri yerine kullanılan ve sunucu ile istemci arasındaki iletişimi şifrelemeye yarayan bir protokoldür. İstemci, sunucuya ilk bağlantı sırasında sunucunun gönderdigi açık anahtarı çevrim dışı yollarla doğrulayıp listesine ekleyebilir. Böylelikle, sertifika gerektirmeden, sunucunun açık anahtarı istemci tarafından öğrenilmiş olur. Bu işlem bir seferlik olup, SSH sisteminin kullanım amacı; sunucuda hesabı bulunan kısıtlı sayıdaki kullanıcıya hizmet vermektir.

Güvenlik Protokolleri

S/MIME (Secure/Multipurpose Internet Mail Extensions, Güvenli/Çok Amaçlı İnternet Posta Uzantıları)

Bu protokol, güvenli e-posta ortamı oluşturmak için kullanılan bir standarttır. Bu yapı PKCS#7 yapısı üzerine kurulmuştur ve RSA-DSA ve MIME standartlarını içerir. Bu protokolde mesaj içeriği açıktır, fakat tüm yapı şifrelenmiştir. Mesaj alındı teyidi, güvenlik etiketleri, posta listeleri, anahtar belirleme gibi işlemleri destekler. MD2, MD4, DES, 3DES, SHA-1, MD5, RSA, DSA, Diffie-Hellman gibi özetleme, imzalama, şifreleme ve anahtar şifreleme algoritmaları bu yapı içerisinde kullanılır.

https://en.wikipedia.org/wiki/PKCS_7

Güvenlik Protokolleri

IPSec

IP adresini taklit etme, veri trafiğini izleme ve veri paketlerini değiştirme gibi işlemlerin, internet ortamında kolaylıkla yapılabildiği bilinmektedir. Bu protokol iki bilgisayar arasındaki haberleşmeden, IP paketlerinin şifrelenmesi, online anahtar dağıtımı, **sanal özel ağ (VPN)** haberleşmesi, bilgisayar ile şifreleme cihazlarının haberleşmesine kadar, internet tabanlı tüm haberleşmelerde güvenliği sağlamak veya güvenli bir ortam oluşturabilmek için kullanılır.

Güvenlik Protokolleri

IPSec

Bu protokolun, **IPv4** ve **v6'ya** uygulandığını burada belirtmekte fayda vardır. IPSec işlemi, IP doğrulama başlığı ve IP zarflama modları olmak üzere iki türde gerçekleştirilebilir. Değiştirilmiş veriyi ve taklit edilen IP adreslerini anlama ve tüm paketlerin bütünlüğünün ve kimlik doğrulamasının yapılması, birinci türde gerçekleştirilmektedir. İzlemeyi önleme için, şifreleme ve paketteki verinin bütünlüğü ve kimlik doğrulama işlemi ise, ikinci türde gerçekleştirilir.

Bu protokolde şifreleme ve kimlik doğrulama, işlemlerini hızlandırmak, simetrik algoritmalarla yapılır. Bu işlemler yapılırken, SKIP veya IKE gibi protokoller de kullanılmaktadır.

Okuma ve inceleme önerisi

https://berqnet.com/blog/dns-nedir-dns-ayarlari-nasil-yapilir

https://community.fs.com/blog/ipv4-vs-ipv6-whats-the-difference.html

Güvenlik Protokolleri

Kerberos

Bu protokol, Needham ve Shroeder tarafından 1978 geliştirilmiştir. Simetrik anahtarların, bir anahtar sunucusu tarafından dağıtılması için kullanılır. Bu işleme, anahtar dağıtım merkezinden bir bilet almayla başlanır. Anahtar dağıtımı için önemli olan bu merkezin, her zaman aktif tutulması gereklidir. AAA ve sertifika kullanılması halinde bu protokole gerek kalmaz.

Güvenlik Protokolleri

İnceleme Önerileri:

OSI Katmanları:
https://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/osi-katmanlar%C4%B1

Domain/DNS/IP Adresi:
https://www.hosting.com.tr/bilgi-bankasi/domain-nedir/

Https vs http:
https://www.hosting.com.tr/blog/http-vs-https/

Güvenlik Protokolleri

Elektronik İmza (e-imza)

Ülkemizde "**e-imza**", "**dijital imza**", "**sayısal imza**" veya "**elektronik imza**" olarak da isimlendirilen bu yaklaşım, artık sadece elektronik ticaret yapanları, bankacıları, özel ve kamu hukukçularını değil herkesi ilgilendirmektedir**.**

"***elektronik veri*: elektronik, optik veya benzeri yollarla üretilen, taşınan veya saklanan kayıtları**", "***elektronik imza*: başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veri**"

5070 sayılı Yasanın 3. Maddesinde Tanımlar

Güvenlik Protokolleri

Elektronik İmza (e-imza)

E-imza ve açık anahtar altyapısı; gelişmiş teknolojiler kullanarak, elektronik ortamda gönderilen veya alınan bilgilerin, bunları gönderen kişi veya kuruma ait olduğunun ***doğrulanmasını***, iletilen veya alınan verilerin bilinmeyen kişiler (başkaları) tarafından gönderilmediğini veya bildiğimiz kişiler tarafından gönderildiğinin *belirlenmesini*, verileri gönderenlerin gönderdiğini ve alanların aldığını ***inkar edememesini***, gönderilen veya alınan bilgilerin *içeriğinin değiştirilmemesini*, başkaları tarafından elde edilse bile, içeriğin başkaları tarafından *anlaşılamamasını* sağlamayı garanti eden, elektronik ortamda bit katarlarından oluşturulmuş **güvenli haberleşme ortamı**na verilen addır.

Güvenlik Protokolleri

Elektronik İmza (e-imza)

Bir e-imzada bulunması gereken önemli özellikler;
- güvenilirlik,
- taklit edilemezlik,
- yeniden kullanılamazlık,
- inkar edilemezlik,
- içerik değiştirilemezlik ve
- yardıma gerek duyulmadan kullanılabilirlik

olarak sıralanabilir.

Güvenlik Protokolleri

Elektronik İmza (e-imza)

Amerikan "Electronic Signatures in Global and National Commerce Act (E-Sign)", e-imza'yı; "*elektronik bir ses, sembol veya veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan verileri değiştirmek veya işlemek için kişinin verileri imzalama (işaretleme) girişimi*" olarak ifade etmektedir.

Güvenlik Protokolleri

Elektronik İmza (e-imza)

Normal (ıslak) imzalarda olduğu gibi, e-imza tiplerinde de farklılıklar mevcuttur. İnkar edilemeyen imza, tuzak imza, sahte imza, vekalet imza, ve kör imza bunlardan bazılarıdır.

İnkar edilemez imza, imzayı atanın bilgisi olmadan doğruluğu kanıtlanamayan veya e-imzaların kopyalanmasını engellemek için kullanılır.

Bir kimsenin, içeriğini görmeden veya bilmeden bir belgeyi imzalamasına imkan veren e-imza tipi ise *kör imza* olarak bilinir.

Atılan bir e-imzanın sahte olduğunu kanıtlamaya çalışan e-imza yaklaşımı ise *tuzak imza* olarak isimlendirilir.

Bir diğer imza şekli de *vekalet imza*'dır. E-imza kullanacak kişiye, kendi gizli anahtarını açmadan bir başkasına imzasını kullandırma hakkı tanıyabilmesine imkan veren imza şeklidir.

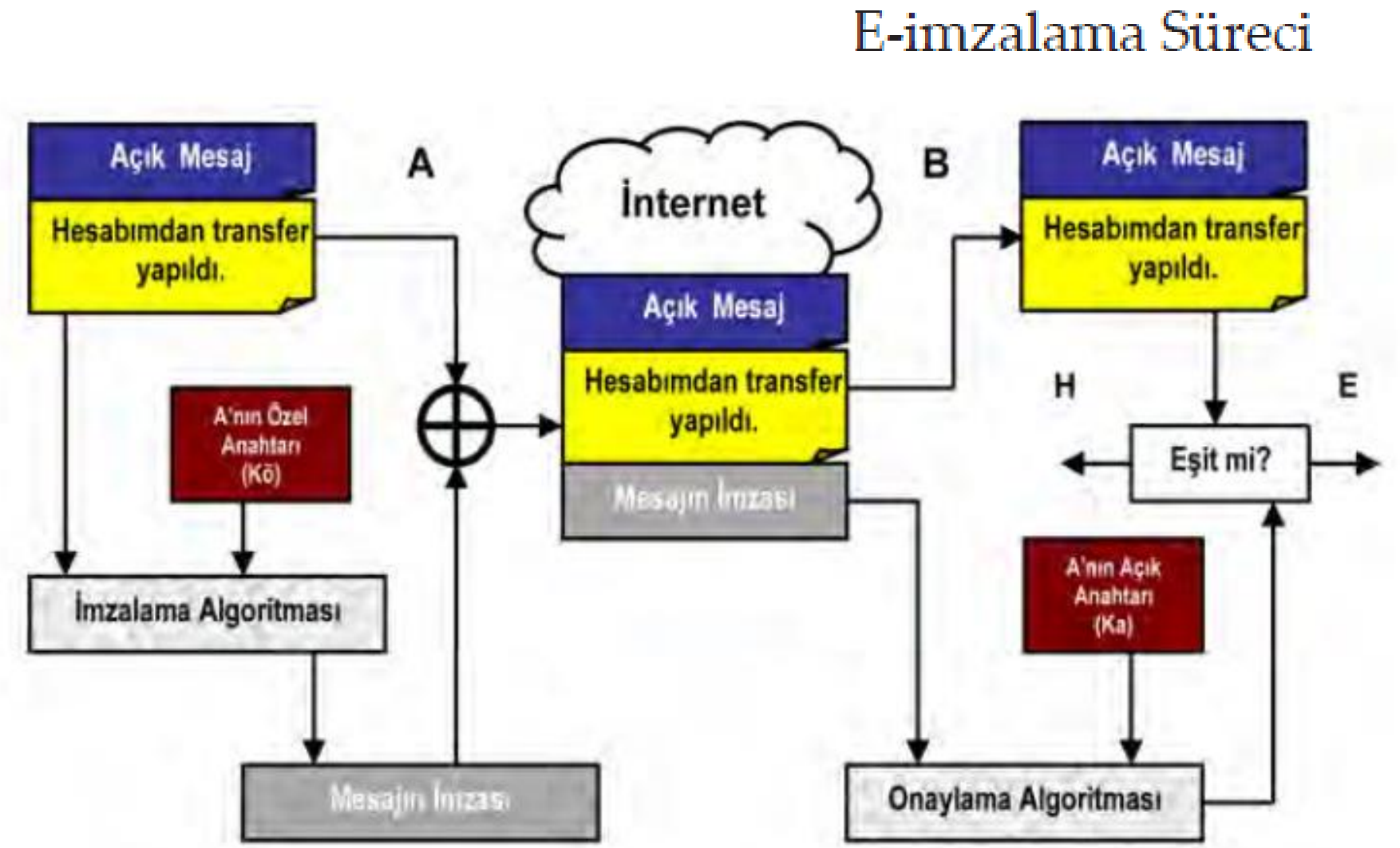
Güvenlik Protokolleri

Elektronik İmza (e-imza)

İnternet/intranet ortamında gönderilen mesajlar, iletiler veya dokümanlar, çoğu zaman "düz metin" veya "açık metin" olarak isimlendirilirler. İnternet/intranet uzayında yapılan haberleşmelerin aktif veya pasif olarak dinlenilmesini önlemek için, mesaj içeriklerinin gizlenmesi veya kolaylıkla algılanamayacak bir formata dönüştürülmesi gerekir. **Bu metinlerin saklanması, başka bir forma dönüştürülmesi işlemine, daha önceki bölümde de vurgulandığı gibi *şifreleme* denir. Bu işlem ile, mesaj güvenli olarak iletilebilir ama tam bir güvenlik için, yalnız şifreleme yeterli değildir. Bunlara ilave olarak, kimlik doğrulama, belirlenen kişi olduğunu ispatlama, bütünlük ve aldığını veya gönderdiğini reddetmeme gibi işlemlerin de haberleşme sırasında sağlanması gereklidir.**

Güvenlik Protokolleri

Elektronik İmza (e-imza)



Güvenlik Protokolleri

Elektronik İmza (e-imza)

(1) Mesajı göndermek isteyen A, mesajını oluşturduktan sonra bu mesajı kendi özel anahtarı (Kö) ile imzalama algoritmasından geçirerek şifreler.
(2) Bu işlem sonucu oluşan şifreli mesaj, orjinal mesajın sonuna mesaj imzası olarak eklenir.
(3) Mesaja, imzayı ekleyerek B'ye (karşı tarafa) gönderir.
(4) B mesajı aldığında, imzayı onaylamak için mesajın imzasını A'nın açık anahtarı (Ka) ve onaylama algoritmasını kullanarak çözer. Eğer şifreli mesaj imzasını A'nın açık anahtarı ile çözebilirse, bu mesajın, gerçekten A'dan geldiğinden emin olur. A'nın açık anahtarı ile sadece, A'nın özel anahtarı ile şifrelenmiş mesajların çözebileceğini hatırlatmakta fayda vardır. A'nın özel anahtarı da, yalnız kendisindedir.

Güvenlik Protokolleri

Elektronik İmza (e-imza)

(5) Bu işlem sonucunda, orjinal mesajın elde edilip edilmediği karşılaştırılır. Eğer onaylama işlemi sonucu elde edilen imza mesajı ile, açık olarak gelen orjinal mesaj aynı ise, mesajın A'dan geldiği garanti edilmiştir.
(6) Şekilde gösterildiği gibi mesajın değiştirilip değiştirilmediğinin (bütünlüğü), burada kontrol edildiğini belirtmekte fayda vardır. Kimlik doğrulamaya ek olarak, bütünlüğün de kontrol edilmesi beraberinde bir problemi açığa çıkarmaktadır. Doğal olarak bu problem, e-imza mesaj uzunluğunu iki katına çıkarmaktadır. Bu sorunu çözmek için ise özetleme fonksiyonları kullanılır.

https://kamusm.bilgem.tubitak.gov.tr/dokumanlar/belgeler/

Okuma ve inceleme önerisi

https://kamusm.bilgem.tubitak.gov.tr/dokumanlar/belgeler/kitaplar/temel_kavramlar.jsp

https://kamusm.bilgem.tubitak.gov.tr/dosyalar/makaleler/EDevletUygulamalariIcinElektronikImzaFormatlari.pdf

Sorular

Bir sonraki ders Kötü Amaçlı Yazılımlar, Siber Tehditler ve Saldırılar (DDOS Ataklar vb.) ve Analizi konusuna giriş yapılacak.