Information Security Requirements (from Michael T. Goodrich, Roberto Tamassia, Introduction to Computer Security, Pearson, 2011, p. 2-18)

Bilgi Güvenliği Gereksinimleri (Michael T. Goodrich, Roberto Tamassia , Bilgisayar Güvenliğine Giriş, Pearson, 2011, s. 2-18)

## Bilgi güvenliği kavramsal olarak GBE (gizlilik – bütünlük – erişilebilirlik) (C-I-A (confidentiality – integrity – availability)) olarak tanımlanmaktadır.

Gizlilik (Confidentiality)

Yetkisiz bilgi ifşasının önlenmesi

Gizlilik, verileri görme izni olan kişilere erişim sağlarken başkalarının bu verilerin içeriği veya varlığı hakkında herhangi bir şey öğrenmesini engeller

Hassas bilgileri korumaya yönelik araçlar:

* Şifreleme anahtarı adı verilen bir sırrı kullanarak şifreleme
* Erişim kontrolü: Gizli bilgilere erişimi yetkili kişilerle sınırlayan kurallar ve politikalar
* Kimlik doğrulama: Birinin kimliğinin veya rolünün belirlenmesi (jeton tabanlı, parola tabanlı, biyometrik)
* Yetkilendirme: Bir kişinin veya sistemin erişim kontrol politikasına dayalı olarak kaynaklara erişmesine izin verilip verilmediğinin belirlenmesi
* Fiziksel güvenlik: Korunan hesaplama kaynaklarına erişimi sınırlamak için fiziksel bariyerlerin oluşturulması (örneğin, bakır örgüler içeren duvarlara sahip odalar, Faraday kafesleri, böylece elektromanyetik sinyallerin muhafazaya girip çıkamaması)

Bütünlük (Integrity)

Bilgilerin yetkisiz bir şekilde değiştirilmediği bir mülk

Veri koruma araçları aynı zamanda veri bütünlüğü için de kullanılır. Ek araçlar:

* Yedeklemeler: Verilerin periyodik olarak arşivlenmesi
* Toplam Denetimleri: Bir dosyanın içeriğini sayısal bir değere eşleyen bir fonksiyonun hesaplanması; bu değer dosyayla birlikte tutulur. Dosya bütünlüğünü kontrol etmek için, toplam denetimi yeniden hesaplanır ve depolananla karşılaştırılır
* Veri düzeltme kodları: Verileri, küçük değişikliklerin kolayca tespit edilebileceği ve otomatik olarak düzeltilebileceği şekilde depolama yöntemleri

Tüm bu araçlar yedeklilik kullanır

Sadece veriler değil, meta veriler de korunmalıdır

Mevcutluk (Availability)

Bilginin yetkili kişiler tarafından zamanında erişilebilir olması özelliği

Örneğin, hisse senedi fiyatları taze olduklarında en faydalıdır. Başka bir örnek, çalınan kredi kartı numarası zamanında atılmalıdır.

Aletler:

* Fiziksel koruma: Fiziksel zorluklar durumunda bile bilgilerin erişilebilirliğini korumayı amaçlayan altyapı (fırtınalara, depremlere, bomba patlamalarına dayanıklı binalar ve elektrik kesintileri ve dalgalanmalarıyla başa çıkmak için jeneratörler ve diğer elektronik ekipmanlarla donatılmış binalar)
* Hesaplama yedeklilikleri: arıza durumunda geri dönüş olarak kullanılan bilgisayarlar ve depolama aygıtları (RAID, ucuz disklerden oluşan yedekli diziler; web sunucusu çiftlikleri)

Gizliliği veya bütünlüğü önemsemeyen bir saldırgan, kullanılabilirliğe yönelik bir saldırı ( DoS saldırısı, hizmet reddi saldırısı) seçebilir.

## Güvence (Assurance), Gerçeklik (Authenticity) ve Anonimlik (Anonymity)

CIA kavramlarının yanı sıra AAA kavramları da vardır (güvence, özgünlük, anonimlik)

Güvence: Bilgisayar sistemlerinde güvenin nasıl sağlandığı ve yönetildiği. Güven: İnsanların veya sistemlerin beklediğimiz şekilde davrandığına dair güvenimizin derecesi.

Güven, aşağıdakilerin etkileşimini içerir:

* İnsanların veya sistemlerin kendileri ve başkaları için sahip oldukları davranışsal beklentileri belirten politikalar. Örneğin, bir çevrimiçi müzik sisteminin tasarımcıları kullanıcıların şarkılara nasıl erişebilecekleri ve bunları nasıl kopyalayabilecekleri konusunda politikalar belirleyebilir
* Bir kişi veya sistemle etkileşim kuran aracıların izin verdiği davranışları tanımlayan izinler. Örneğin, bir çevrimiçi müzik mağazası, belirli şarkıları satın almış kişilere sınırlı erişim ve kopyalama için izinler sağlayabilir
* İzinleri ve politikaları uygulamak için uygulanan mekanizmaları tanımlayan korumalar. Çevrimiçi bir müzik mağazasının çalışan örneğimizi kullanarak, böyle bir sistemin insanların yetkisiz erişimini ve kaynaklarının kopyalanmasını önlemek için korumalar oluşturacağını hayal edebiliriz (güven sistemden kullanıcılara yönlendirilir)

Güvence, güvenin iki yönde yönetilmesini içerir: kullanıcılardan sistemlere (örneğin, şarkı satın almak için kredi kartı numaralarının geçerli kullanımı) ve sistemden kullanıcılara.

Bilgisayar sistemleri tasarımcıları, sistemlerinin kaynaklarını kullanan insanların bunu kendi politikaları doğrultusunda yapmasını isterler. Ayrıca tasarımcılar, kopyalarının kullanım süresini, izlenme sayısını veya müziklerinin yedek kopyalarının sayısını kısıtlamak isteyebilirler.

Bu nedenle güven yönetimi, etkili, uygulanabilir politikaların tasarımı, güvenilir kullanıcılara izin verme yöntemleri ve sistemdeki kaynakları korumak ve yönetmek için bu politikaları ve izinleri uygulayabilen bileşenlerle ilgilenir.

Sistem güvencesinin bir diğer önemli kısmı yazılım mühendisliğini içerir. Bir sistemin tasarımcıları, sistemlerini uygulayan yazılımın tasarımlarına uyacak şekilde kodlandığını bilmelidir. Örneğin, bir sistemin tasarımcısı, rastgele sayılarla şifreleme için bir Sahte Rastgele Sayı Üreticisi (PRNG) kullanılmasını belirtebilir. Uygulayıcı, PRNG için her zaman aynı başlangıç değerini kullanırsa, üretilen sayılar tekrar tekrarlanacaktır.

Bu nedenle iyi bir spesifikasyona sahip olmak ve uygulamaya koymak gerekmektedir.

Ayrıca güven için, yapılan işlemlerin bir takım delillerle desteklenmesi, bunların mahkemeye gidilmesi durumunda (örneğin bir web sitesi tarafından dolandırılma durumunda) kullanılabilmesi gerekmektedir.

Özgünlük

Kişiler veya sistemler tarafından verilen ifadelerin, politikaların ve izinlerin gerçek olduğunu belirleme yeteneğidir. Bu tür şeyler sahte olabiliyorsa, insanların ve sistemlerin çevrimiçi ürün satın alırken veya satarken girdiği zımni sözleşmeleri uygulamanın bir yolu yoktur.

İnkar edilemezlik, bir kişi veya sistem tarafından verilen gerçek ifadelerin reddedilemeyeceği özelliğidir. İnkar edilemezlik, dijital imzanın kullanılmasıyla elde edilir.

Anonimlik

Elektronik işlemlerde (tıbbi geçmiş, satın alma geçmişi, yasal kayıtlar, e-posta iletişimleri, istihdam kayıtları) kişisel kimliklerin kullanılmasının talihsiz bir yan etkisi vardır. Bu nedenle, belirli kayıtların veya işlemlerin herhangi bir bireye atfedilmemesi özelliği olan anonimliğe ihtiyaç vardır.

Kuruluşların üyeleri veya müşterileri hakkında veri yayınlamaları gerekiyorsa, bunu aşağıdaki araçlardan bazılarını kullanarak gizliliği koruyacak şekilde yapmalarını beklemeliyiz.

* Toplama (toplam, ortalama, min, maks, sayım)
* Karıştırma: İşlemlerin, bilgilerin veya iletişimlerin herhangi bir bireye izlenemeyecek şekilde iç içe geçmesi
* Proxy'ler: Bir birey için, o kişiye kadar izlenemeyecek şekilde eylemlerde bulunmaya istekli güvenilir aracılar. İnternet arama proxy'leri, bireylerin örneğin bulundukları ülke nedeniyle engellenebilecekleri web sitelerini ziyaret edebilmeleri için bir İnternet tarayıcısı arayüzü sağlayan web siteleridir.
* Takma adlar: İletişim ve işlemlerde gerçek kimliklerin yerini doldurabilen, ancak başka türlü yalnızca güvenilir bir tarafça bilinen kurgusal kimlikler. Örneğin, birçok sosyal ağ kullanıcıların gerçek kimliklerini ifşa etmeden kullanıcı takma adlarıyla etkileşim kurmasına izin verir.

## Tehditler ve Saldırılar

**Tehdit** , güvenliği ihlal edebilecek ve zarara yol açabilecek bir durum, yetenek, eylem veya olay olduğunda ortaya çıkan bir güvenlik ihlali potansiyelidir. Yani, bir tehdit, bir güvenlik açığını istismar edebilecek olası bir tehlikedir.

**Saldırı** , akıllı bir tehditten kaynaklanan sistem güvenliğine yönelik bir saldırıdır: yani, güvenlik hizmetlerinden kaçınmak ve bir sistemin güvenlik politikasını ihlal etmek için kasıtlı bir girişim olan akıllı bir eylemdir

En yaygın saldırı türleri

* Dinleme (gizlilik konusunda)
* Değişiklik (bütünlük üzerinde)
* Hizmet Reddi (uygunluk durumuna göre)
* Maskeleme: Gerçekte yazar olmayan birine ait olduğu iddia edilen bilgilerin üretilmesi. Örneğin, gerçek bir banka veya başka bir e-ticaret sitesi gibi görünen bir web sitesi oluşturan kimlik avı. Parolaları toplamak ve sahtecilik yapmak (sahte dönüş adresleriyle ağ veri paketleri göndermek) için tasarlanmıştır. Gerçekliğe, gizliliğe (parolaları çalmak) ve/veya anonimliğe (gerçek bireyin verilerini elde etmek için parolaların kullanılması) yönelik bir saldırıdır.
* Reddetme: bir taahhüdün veya veri alımının reddedilmesi. Bu, farklı tarafların verinin alındığını onaylayan makbuzlar sağlamasını gerektiren bir sözleşmeden veya protokolden geri çekilme girişimini içerir. Bu, güvenceye bir saldırıdır.
* Korelasyon ve geri izleme : belirli bir veri akışının veya bilgi parçasının kaynağını belirlemek için birden fazla veri kaynağının ve bilgi akışının bütünleştirilmesi. Bu anonimliğe yönelik bir saldırıdır.

## Kriptografik ilkeler

Bir kriptografik sistem yedi bileşenden oluşur

1. Olası düz metinlerin kümesi
2. Olası şifreli metinlerin kümesi
3. Şifreleme anahtarları kümesi
4. Şifre çözme anahtarları kümesi
5. Şifreleme anahtarları ile şifre çözme anahtarları arasındaki ilişki
6. Kullanılacak şifreleme algoritması
7. Kullanılacak şifre çözme algoritması

Örneğin, Sezar şifresi

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| D | E | F | G | H | I | J | k | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |

C =( p+3)mod26

P=(c-3 )mod26

Simetrik kripto sistemleri veya paylaşımlı anahtar kripto sistemleri

C=EK ( P ); P=DK ( C)

Asimetrik kripto sistemleri veya açık anahtarlı kripto sistemleri

C=E K1 (P); P=D K1 (C)

K1 ve K2 bir anahtar çifti oluşturur, bunlardan biri herkese açıktır, diğeri ise özeldir (gizlidir)

Asimetrik kriptografi için, şifreleme için gizli bir anahtarın kullanımı, anahtar sahibinin dijital imzası olarak hizmet eder. Diyelim ki Alice'in SA'sı (Alice'in sırrı), PA'sı (Alice'in geneli) ve Bob'un SB'si (Bob'un sırrı), PB'si (Bob'un geneli) var. O zaman Bob'un M mesajı için imzası C=E SB (M) olur, bu da Alice tarafından C'nin PB tarafından şifresinin çözülmesiyle kontrol edilir: M=D PB (С).

Açık anahtarlı şifrelemenin dezavantajı yüksek hesaplama karmaşıklığıdır, örneğin RSA'da yüzlerce ondalık basamaklı sayıların (300-500 basamak) üslenmesi gerekir. Esas olarak anahtar değişimi için kullanılır.

Kripto sistemleri, tüm olası anahtarların numaralandırılması varsayılarak kaba kuvvet saldırısıyla saldırıya uğrayabilir. 128 bit boyutundaki AES anahtarıyla, olası anahtar sayısı 2 128'dir, bu da numaralandırılması mümkün olmayan bir durumdur. Büyük anahtar boyutlarına sahip kripto sistemleri, hesaplama açısından (koşullu olarak) güvenli kabul edilir.

## Karma fonksiyonlar

Dijital imzalar genellikle tüm bir mesaj üzerinde yapılır ancak karma değeri üzerinde yapılır. Karma işlevi, h, şifreleme dönüşümüne benzerdir, ayrıca gizli anahtara sahip olabilir, ancak bire bir (tersine çevrilebilir) olan bir şifreleme dönüşümünün aksine, çoktan biredir (tek yönlü, tersine çevrilemez). Karma işlevi, herhangi bir giriş mesajı için sabit bir boyutta (örneğin, 64 bit) sonuç döndürür.

Bir mesajın, M, bir anahtar, K ile şifrelenmiş mesaj doğrulama kodu (MAC),

MAC( M,K)=h(K||M)

şifreli metinle birlikte aktarılır

C=EK ( M)

Şifre çözüldükten sonra,

M'=DK(C),

Alıcı, MAC'in yeniden hesaplanması yoluyla alınan mesajın gerçekliğini kontrol eder,

MAC( K,M')=h(K||M')

MAC( K,M) ile karşılaştırarak . Eğer eşleşirlerse, alıcı mesajın otantik olduğuna karar verir.

## Dijital sertifikalar

Açık anahtarlı kriptografi için, muhabirin güvenilir açık anahtarına sahip olmak gerekir. Bu amaçla güvenilir üçüncü taraflar (sertifika otoritesi, CA) tarafından verilen dijital sertifikalar (DC) kullanılır. DC genellikle aşağıdaki verileri içerir:

- CA'nın adı (örneğin, Thawte)

- sertifikanın düzenlenme tarihi (örneğin, 29.09.2016)

- son kullanma tarihi (örneğin, 28.09.2018)

- web sitesinin adresi (örneğin, mail.google.com)

- web sitesini işleten kuruluşun adı (örneğin, Google, Inc.)

- web sunucusunun kullandığı genel anahtar (örneğin, bir RSA 1024-bit anahtarı)

- kullanılan şifreleme işlevinin adı (örneğin, SHA-256)

- dijital imza

Kimlik avı saldırılarına karşı korunmanın bir yolu, dijital sertifikanın web sitesiyle ilişkili kuruluşun adını içerdiğinden emin olmaktır.