Bilgi Güvenliğine Giriş ve Adli Bilişim

Ahmet Haşim Yurttakal

Kurumsal Veri Türleri

- Geleneksel Veri
  - Personel — uygulama materyalleri, bordro, teklif mektubu, çalışan sözleşmeleri
  - Fikri — patentler, ticari markalar, ürün planları, ticari sırlar
  - Finansal — gelir tabloları, bilançoları, nakit akış tabloları
- Nesnelerin İnterneti ve Büyük Veriler
  - IoT — sensörler gibi fiziksel nesnelerin geniş ağı
  - Büyük Veri — IoT verileri

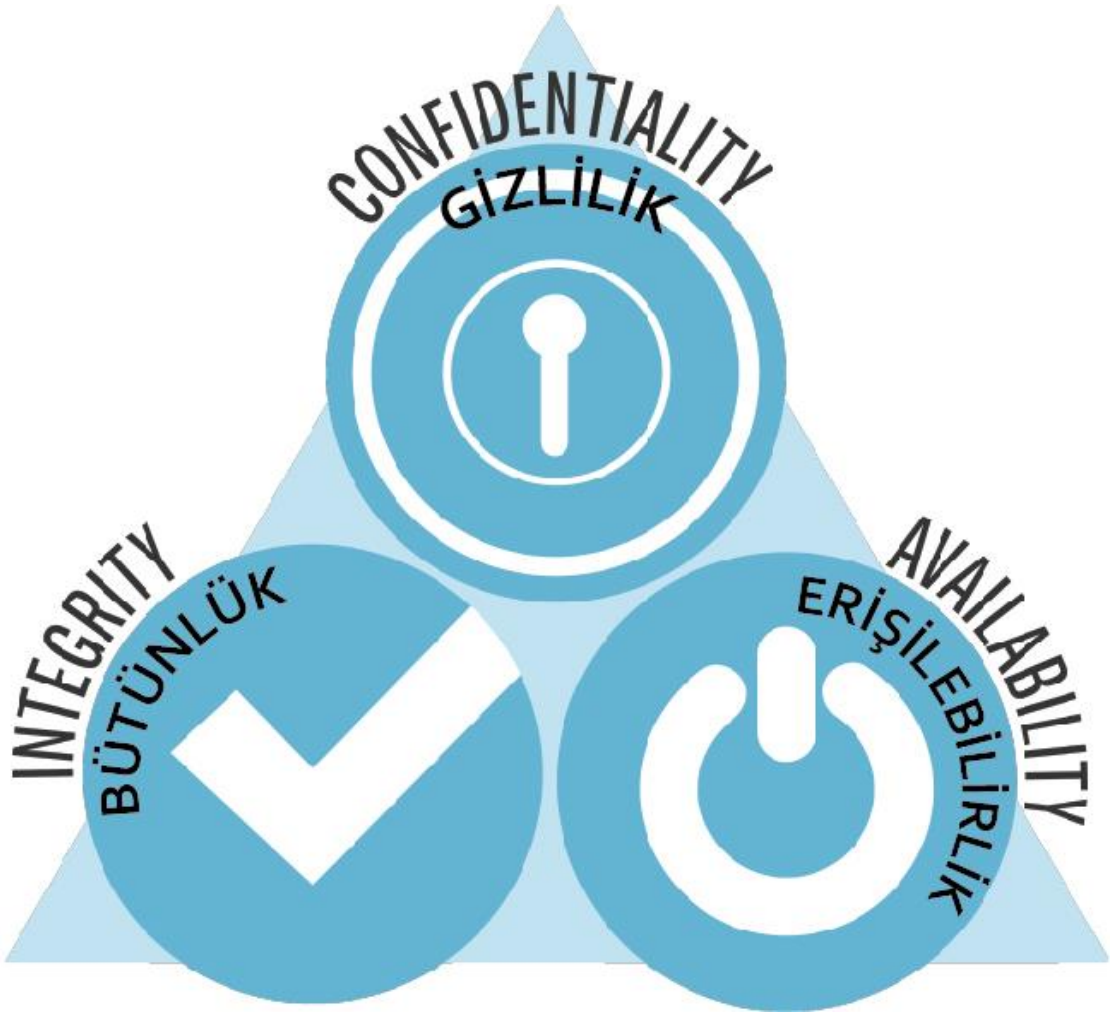
Çevrimiçi ve Çevrimdışı Kimliğiniz

- Çevrimdışı Kimliğiniz
  - Evde,
    okulda veya işte düzenli olarak etkileşime giren kimliğiniz
- Çevrimiçi Kimliğiniz
  - Siber uzaydayken kimliğiniz
  - Sizin hakkınızda sadece sınırlı miktarda bilgi ortaya koymalıdır
  - Kullanıcı adı veya takma ad
    - Herhangi bir kişisel bilgi içermemeli
    - Uygun ve saygılı olmalı
    - İstenmeyen dikkatleri üzerine çekmemeli

Bilgi Güvenliği

- Bilgilerin izinsiz erişimlerden, kullanımından, ifşa edilmesinden, yok edilmesinden, değiştirilmesinden veya hasar verilmesinden korunması işlemidir.

CIA


CONFIDENTIALITY
GİZLİLİK
INTEGRITY
BÜTÜNLÜK
AVAILABILITY
ERİŞİLEBİLİRLİK

CIA X DAD

- Disclosure (İfşa) X Confidentiality
- Alteration (Yetkisiz Değişiklik) X Integrity
- Destruction (İmha / Tahribat) X Availability

Gizlilik (**Confidentiality**)

- Bilginin **yetkisiz kişil**erin eline geçmesini engellemeyi amaçlamaktadır.
- Bilgi **işlenirken** (process), saklama ortamlarında **depolanırken** (storage), gönderici ve alıcı arasında **taşınırken** (transport) yetkisiz erişimlerden korunmalıdır.
- Saldırgan bir yapılandırma veya yazılım hatasını istismar ederek yahut Sosyal Mühendislik teknikleri ile yetkili insanların hatalarını istismar ederek bilgilere izinsiz olarak erişebilir.

Bütünlük **(Integrity)**

- Bilginin **bozulma**sını, **değiştirilme**sini, yeni veriler **eklenme**sini, bir kısmının veya tamamının **silinme**sini engellemeyi hedefler.
- Bu amaçla kritik bilgi için **erişim kontrolü**nün gerçekleşmesi ve belli aralıklarla **yedekleme**nin gerçekleşmesi gerekmektedir.
- Bütünlük prensibi temel olarak Sistem Bütünlüğü ve Veri Bütünlüğü olarak ikiye kısımda incelenebilir.

Erişilebilirlik **(Availability)**

- Bilginin **belirlenen / beklenen / hedeflenen / ihtiyaç duyulan süre** (SLA – Service Level Agreement) boyunca ulaşılabilir ve kullanılabilir olmasını, **tam** ve **eksiksiz** olarak yapılmasını amaçlayan prensiptir.
- Erişilebilirlik; bilişim sistemlerini, kurum içinden ve dışından gelebilecek başarım düşürücü tehditlere karşı korumayı hedefler.
- Erişilebilirlik hizmeti sayesinde, kullanıcılar, **erişim yetkileri dahilinde** olan verilere, **veri güncelliğini kaybetmeden**, zamanında ve **güvenilir** bir şekilde ulaşabilirler.

Bilgisayar Adli Analiz (Computer Forensics)

- Bilişim sistemleri ve üzerinde bulunan depolama ünitelerinin herhangi bir suçu işlemede kullanılıp kullanılmadığını tespit etme işlemleridir.
- Adli bilişim uzmanları suçla ilgili verileri toplayıp uygun formatta mahkemeye sunmalıdır.
- Bilinçli firmalar Siber Olaylara Müdahale Ekibi oluşturmalıdır.

Adli Analiz Süreci

- Adli analiz uzmanı ve yasa uygulayıcının sınırlı zamanı vardır.
- Bilgi elle tutulmayan soyut bir şeydir.
- Soruşturma organizasyonun normal iş akışını engelleyebilir.
- Kanıtı toplamak zor olabilir.
- Suçla ilgili bilgiler normal bir bilgisayarda olabilir.
- Adli analiz uzmanı tüm bilişim sistemini analiz edemeyebilir.
- Suçun işlendiği yerler farklı coğrafi yerlerde farklı yasalara tabi olabilir.
- Elektronik bilgi de dahil birçok şeyin mülkiyet hakları sorgulanabilir. Uzun süreli davalar olabilir.

Kanıt

- Kanıtların toplanması, korunması kontrol edilmesi önemlidir. Soyut, geri döndürülemez olabilir. Kanıt zincirinin temel unsurları:
  - Kanıtın yeri, bulunduğu yer,
  - Kanıtın alınma zamanı
  - Kanıtı tespit eden bireyin kimliği
  - Kanıtı toplayan bireyin kimliği
  - Kanıtı kontrol eden, saklayan, işleyen kişinin kimliği

Kanıt Yaşam Döngüsü

- Keşif ve tanıma
- Toplama
  - İlgili tüm medyaları topla
  - Eneri kesmeden tüm sabit disklerin imajını al
  - Ekran çıktısı al
  - Verileri silme
- Etiketleme
- Koruma
  - Manyetik etkilerden koru
  - Uygun koşullarda sakla
- Taşıma
- Mahkemede sunma
- Kanıtı sahibine geri verme

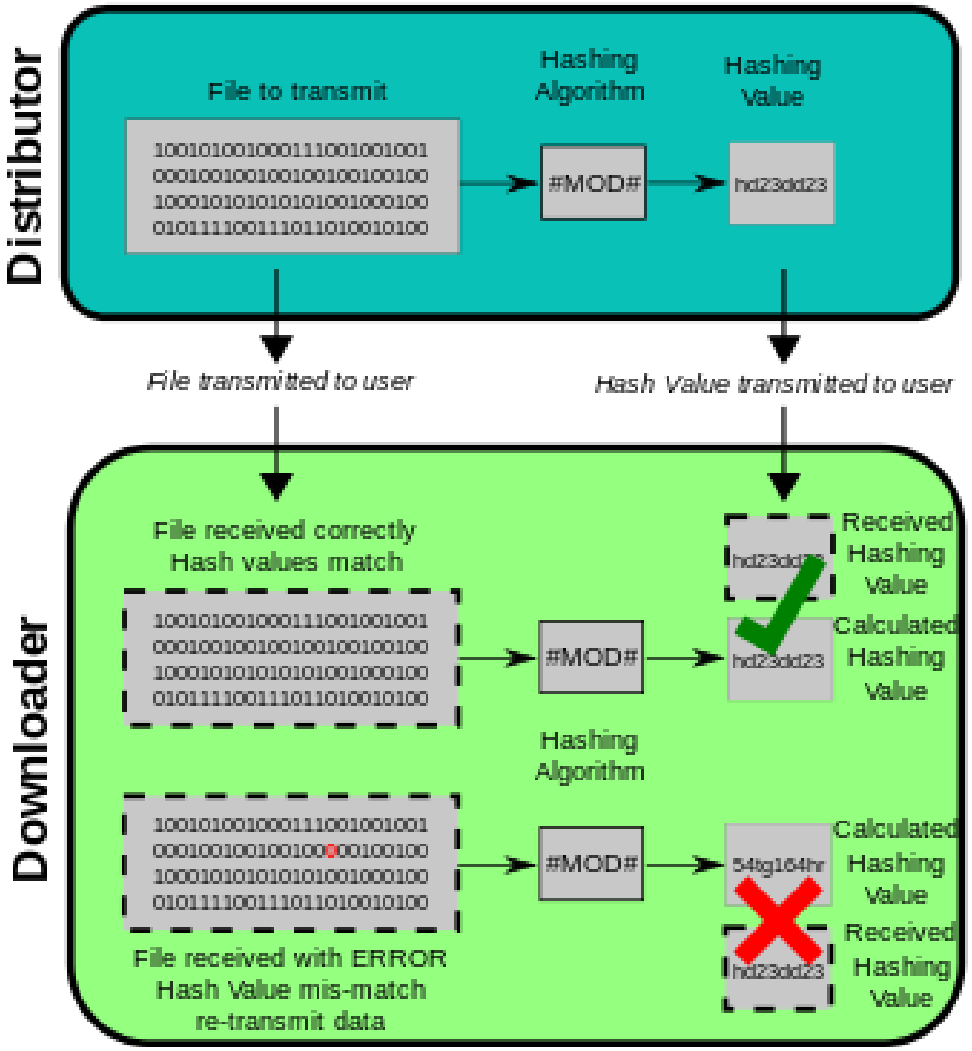
Kanıtın Kabul Edilebilirliği

- Suçla ilgili olmalı
- Yasal yollarla elde edilmiş olmalı
- Uygun tanımlanmış olmalı, kalıcı kalemle etiketlenmeli, seri numarası marka modeli tanımlanmalı, mühürlü paketlerde saklanmalı
- Zarar görmemeli veya yok edilmemeli, Yedek alınmalı, Saklama ortamı dumansız tozsuz olmalı, Hash algoritmaları ile doğrulanmalı

Hash Algoritmaları

- Hashing, bir dosyadan sabit boyutlu bir bit dizisi değeri hesaplayan bir algoritmadır. Orjinal veriyi temsil eden çok daha kısa sabit uzunluklu değere veya anahtara özetler.
- Bir karma genellikle birkaç karakterden oluşan onaltılık bir dizedir.
- Hashing tek yönlü bir işlemdir. Orijinal verileri geri almak için geriye doğru çalıştıramazsınız
- İyi bir hash algoritması, iki farklı girdiden aynı hash değerini üretmeyecek kadar karmaşık olmalıdır. Olursa, bu bir karma çarpışması olarak bilinmektedir.

Hashing


Distributor
File to transmit
Hashing Algorithm
Hashing Value
#MOD#
hd23dd23
File transmitted to user
Hash Value transmitted to user
Downloader
File received correctly
Hash values match
#MOD#
Received Hashing Value
Calculated Hashing Value
Hashing Algorithm
#MOD#
Calculated Hashing Value
Received Hashing Value
File received with ERROR
Hash Value mis-match
re-transmit data

Hashing Türleri

- Amaç, İki belge dosyasını açmadan dosyayı karma değer üzerinden eşitlik için karşılaştırmaktır.
- Dosyanın bütünlüğünü doğrulamak için kullanılır
- SyncBack gibi bir dosya yedekleme programı
- Dosya bütünlüğü kontrolleri için kullanılan en yaygın karma türü MD5, SHA'dir.

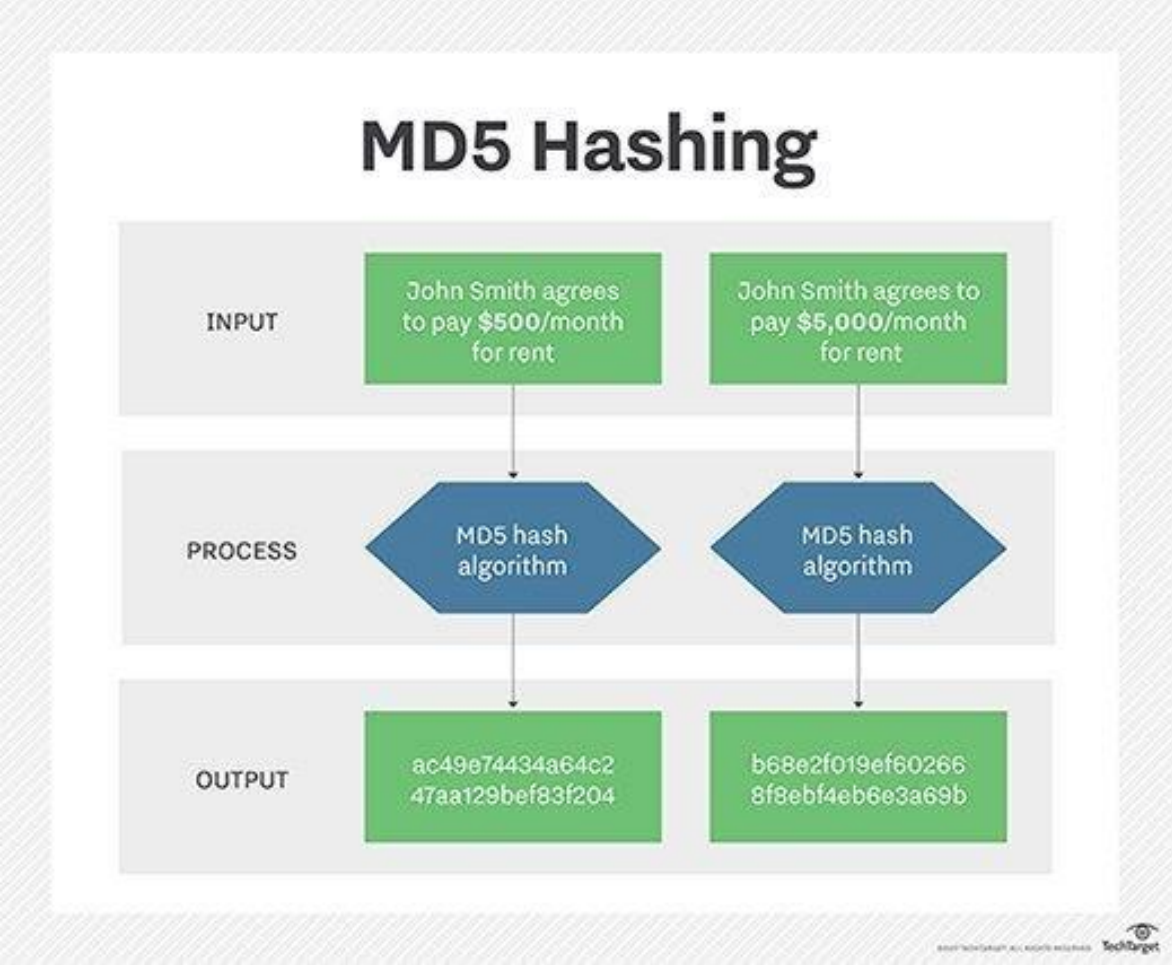
SHA

- ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından geliştirilen Secure Hash Algorithm (SHA) Güvenli Karma Algoritma, belirtilen bir şifreleme hash fonksiyonları ailesidir.
- Federal Bilgi İşleme Standardı (FIPS 180-2) dört adet güvenli karma algoritmasını (SHA-1, SHA-256, SHA-384 ve SHA-512) belirtir.
- Bir mesaj özeti olarak adlandırılan 160 ile 512 bit yoğunlaştırılmış gösterimi üretir.
- SHA-1, MD5 algoritmasına benzeyen yaygın olarak kullanılan 160 bitlik bir karma işlevdir.

MD5

- Message Digest (MD5)Mesaj Özeti, Ron Rivest tarafından geliştirilmiştir.
- İsteğe bağlı bir uzunluk dizesinden 128 bitlik bir dize değeri oluşturmak için kullanılabilecek bir şifreleme karma algoritmasıdır.
- MD5 algoritması, bir girişi isteğe bağlı uzunlukta bir mesaj alır ve çıktı mesajı olarak 128-bit bir “parmak izi” veya “mesaj özeti” üretir.
- Güvenlik protokollerinde ve SSH, SSL ve IPSec gibi uygulamalarda yaygın olarak kullanılır.

MD5


MD5 Hashing
INPUT
John Smith agrees to pay $500/month for rent
John Smith agrees to pay $5,000/month for rent
PROCESS
MD5 hash algorithm
MD5 hash algorithm
OUTPUT
ac49e74434a64c2 47aa129bef83f204
b68e2f019ef60266 8f8ebf4eb6e3a69b
TechTarget

SHA ve MD5 Farkı

- MD5 her ne kadar iyi tanınan şifreleme hash fonksiyonlarından biri olsa da, güvenlik temelli servisler ve uygulamalar ya da çarpışma direncine dayanan dijital imzalar için uygun değildir.
- SHA-1 birçok açıdan MD5'ten daha güvenli görünüyor. SHA-1'e bazı bilinen saldırılar olmasına rağmen, MD5'teki saldırılardan daha az ciddidirler.
- Şu anda SHA-256, SHA-384 ve SHA-512 gibi daha güvenli ve daha iyi hash fonksiyonları mevcut olup, bunlar önceden kendilerine hiçbir saldırı geçmişi olmadığından güvenlidir.
- SHA algoritması MD5'ten biraz daha yavaştır, ancak daha büyük ileti özeti uzunluğu, inversiyon saldırılarına ve kaba kuvvet saldırılarına karşı daha güvenli olmasını sağlar.

Kanıt Türleri

- En iyi kanıt: Kanıtın orijinal hali
- İkincil kanıt: Kanıtın kopyası, suçlu veya suçsuz bulmak için güçlü görülmez
- Doğrudan kanıt: Şahitlerin tanıklığı
- Kati kanıt
- Koşulsal kanıt:Orta düzeyde, 2 saat sonra bir siteyi devre dışı bırakacağını söylemesi
- Tamamlayıcı kanıt: destekleyici nitelikte
- Uzman kanıt: Bir konuda uzmanın konuya açıklık getirmesi
- Dolaylı kanıt: Kulaktan doğma

Honeypot

- Firmalar kendi sistemlerine yapılabilecek saldırıları izlemek ve gerekli önlemleri alabilmek için bilgisayar sistemlerinin yanına yeterince güvenlik önlemi alınmamış, üzerinde açıklık bulunan benzer bir sistem kurarlar.
- Korsanlar bu sistemi gerçek sanıp saldırırlar.
- Firma balküpüne saldıran bilgisayar korsanını olay kayıtlarıyla birlikte mahkemeye verebilir.
- Burada firmanın korsanın dikkatini çekmek için yaptığı ayartma yasaldır. Korsanın sisteme saldırması suçtur.

SON