Bilgi Güvenliği ve Kriptografi

Kriptografi

- Kriptografi,, kotu niyetli ucuncu taraflara karşı haberleşmenin guvenliğini sağlamak icin, uygulama ve teknikleri iceren calışmaların butununu ifade eder.

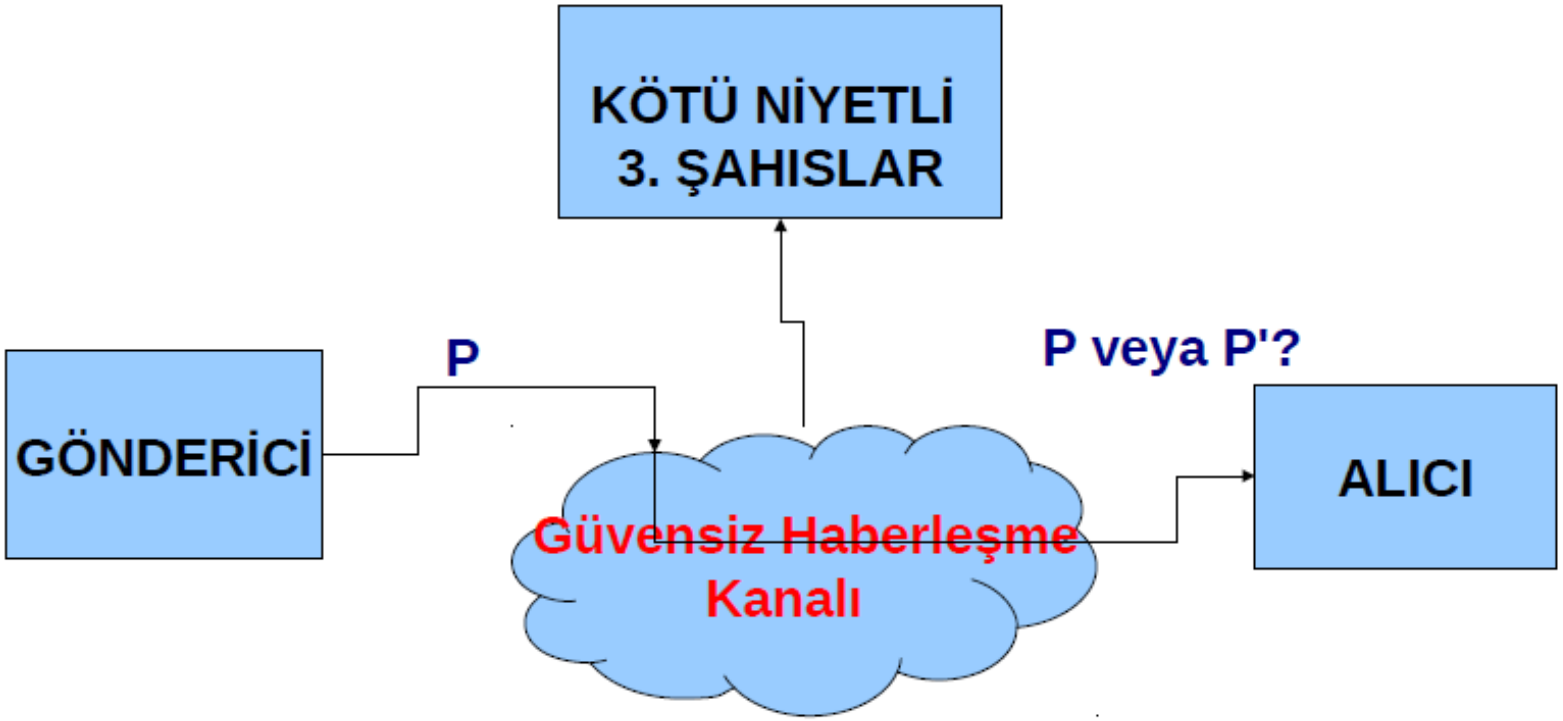
- Kriptoloji ise kriptografi ve kriptoanaliz–kriptografik algoritmalarını analizleri- ile ilgili bir bilim dalıdır.

- Bilgi guvenliği icin verinin yetkisiz değiştirilmeye, kullanılmaya, ifşa edilmesine, incelenmesine, kaydedilmesine, hasar verilmesine karşı koruma yontemleri (guvenlik hedeflerine ulaşılarak) calışılır.

- Ağ guvenliğinde, ağ erişimli sistemlere ve kaynaklara yetkisiz erişimleri izlemek ve onlemek icin uygulanan yontemler (kriptografik algoritmaların ağ protokollerinde kullanımı vb.) incelenir.

Gunumuzde kriptografik sistemler

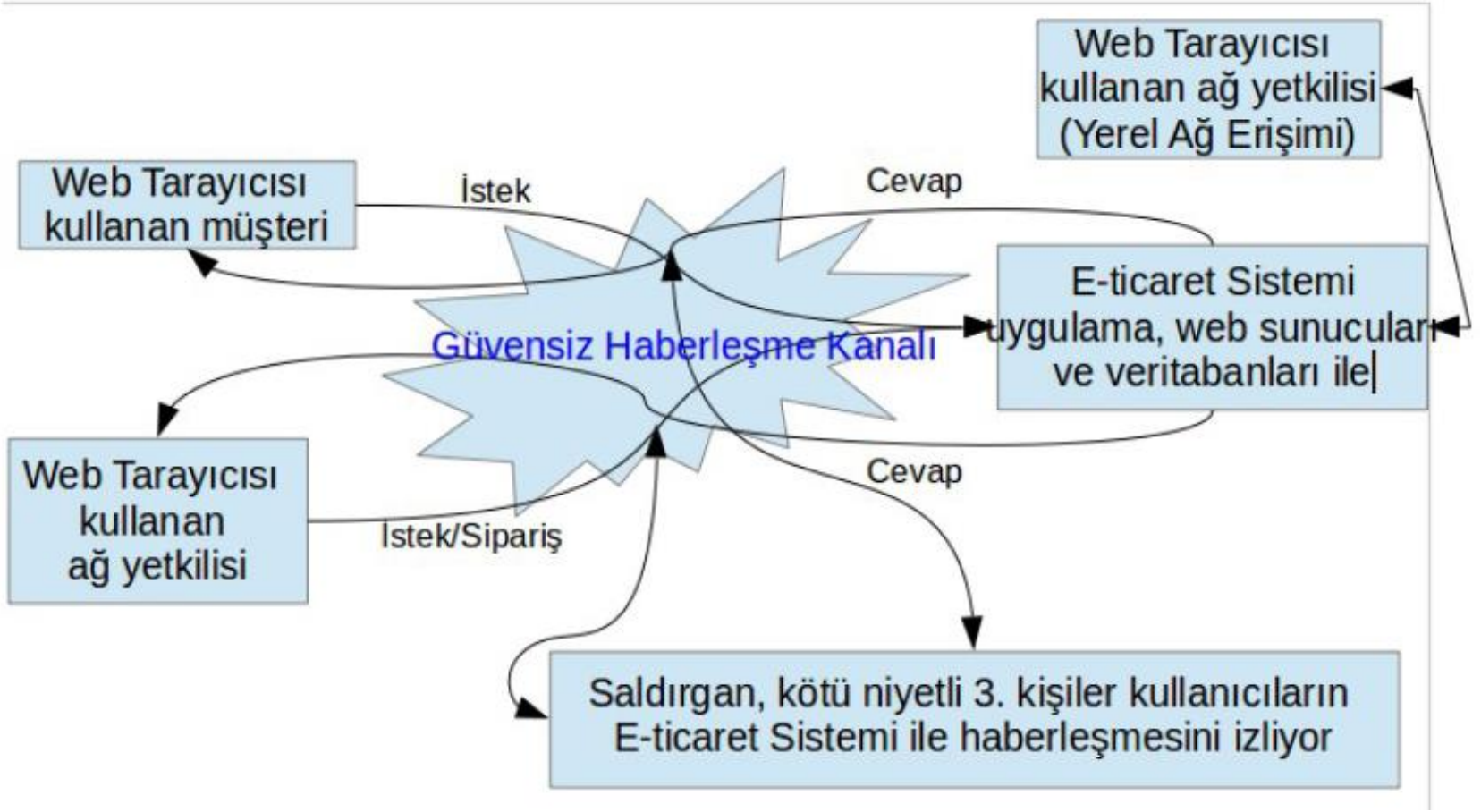
- Bugun, kriptografi cok geniş uygulama alanlarına dahil olarak gunluk hayatın onemli bir parcası olmuştur:
  - sim kartlar,
  - cep telefonları,
  - online bankacılık,
  - online alışveriş,
  - uydu alıcıları,
  - vs.



Güvenli Olmaya Kanal Üzerinden Haberleşme

P: Açık Metin

P': Açık Metin Değişmiş hali


Web Tarayıcısı kullanan ağ yetkilisi (Yerel Ağ Erişimi)
Web Tarayıcısı kullanan müşteri
İstek
Cevap
E-ticaret Sistemi uygulama, web sunucuları ve veritabanları ile
Güvensiz Haberleşme Kanalı
Web Tarayıcısı kullanan ağ yetkilisi
İstek/Sipariş
Cevap
Saldırgan, kötü niyetli 3. kişiler kullanıcıların E-ticaret Sistemi ile haberleşmesini izliyor

Bilgi Güvenliği Unsurları-Hedefleri

Bilgi Güvenliği Unsurları

I.Kimlik Sınaması (Authentication)

- Kullanıcının sisteme bağlanabilmesi için ilk başta yapılması gereken işlemdir. Sistem kullanımı sırasında cihaz veya kullanıcının kimliğinin doğrulanmasıdır.

- Bu işlem ile kullanıcının sahip olduğu **kullanıcı adının** sistemde kayıtlı olup olmadığı kontrol edilir. Daha sonra kullanıcıya verilen **parola** da kontrol edilerek doğrulama işlemi yapılır.

- Doğrulama sağlanırsa kullanıcıya sisteme giriş izni verilir. Bilgisayar ağları ve bilgisayar sistemleri dışında fiziksel sistemler için de çok önemlidir ve bu yüzden **akıllı kartlar veya biometrik teknolojilere dayalı kimlik sınama sistemleri** kullanılamaya başlanmıştır.

2. Yetkilendirme (Authorization):

- Kullanıcı adı ve parola doğrulaması sağlanan kullanıcıların sisteme, programa veya ağa hangi yetkilerle erişim hakkına sahip olduklarını belirten sistemdir.

- Sisteme kayıtlı olan kullanıcılar gruplanarak, bu gruplara çeşitli yetkiler verilir. Kullanıcı içerisinde bulunduğu grubun bütün yetkilerine sahiptir.

- Eğer bir kullanıcı birden fazla gruba üye ise bu gruplara verilen yetkilerin hepsine sahiptir. Güvenliğin tam sağlanabilmesi için kullanıcılara gerekenden fazla yetki verilmemelidir.

3.İzlenebilirlik/Kayıt Tutma (Accountability):

- Bir sorun ile karşılaşıldığında sorunun tespitinin sağlanabilmesi için kullanılan sistemdir.
- Sistemde bulunan kullanıcıların yaptıkları bütün işlemler ve erişim saatleri kayıt altına alınır.
  - Log: bir bilgisayarın gerçekleştirdiği etkinlik kayıtlarının tutulması anlamında kullanılır. Loglar sayesinde sistemlerin hataları uzmanlar tarafından görülür ve düzeltilir. Saldırı ya da güvenlik riskleri görülür ve tedbir alınır. İşlemleri gerçekleştirenlerin yaptıklarından sorumlu olmaları sağlanır.
- Bir problem çıktığında ise kullanıcı aktivitelerinin tutulduğu bu kayıtlardan sorun anlaşılmaya ve çözülmeye çalışılır.

4.Gizlilik (Confidentiality):

- Bilginin yetkisiz kişilerin eline geçmesini engellemeyi amaçlamaktadır.
- Bilgi hem bilgisayar sistemlerinde, hem saklama ortamlarında, hem de ağ üzerinde gönderici ve alıcı arasında taşınırken 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.

5.Veri Bütünlüğü (Data Integrity):

- Amaç, veriyi olması gerektiği şekilde tutmak ve korumaktır.
- Bilginin bozulmasını, değiştirilmesini, yeni veriler eklenmesini, bir kısmının veya tamamının silinmesini engellemeyi hedefler.
- Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır.

6.Süreklilik (Availability):

- Bilginin her an ulaşılabilir ve kullanılabilir olmasını amaçlayan prensiptir.
- Bilişim sistemlerinin kendilerinden beklenen işi sürekli bir şekilde tam ve eksiksiz olarak yapmasını amaçlamaktadır.
- Süreklilik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek başarım düşürücü tehditlere karşı korumayı hedefler.
- Süreklilik hizmeti sayesinde, kullanıcılar, erişim yetkileri dâhilinde olan verilere, veri tazeliğini yitirmeden, zamanında ve güvenilir bir şekilde ulaşabilirler.

7. Güvenilirlik (Reliability-Consistency):

- Sistemin öngörülen ve beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur.

- Sistemin kendisinden beklenen şeyi eksiksiz/fazlasız olarak her çalıştırıldığında tutarlı şekilde yapmasıdır.

8. İnkâr Edememe (Non-repudiation):

- Bu prensip verinin iletildiği gönderici ve alıcı arasında ortaya çıkabilecek iletişim sorunları ve anlaşmazlıkları en aza indirmeyi amaçlar.
- İki sistem arasında bir bilgi aktarımı yapılmışsa ne gönderen veriyi gönderdiğini, nede alıcı veriyi aldığını inkâr edememelidir.
- Özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde kullanım alanı bulmaktadır.

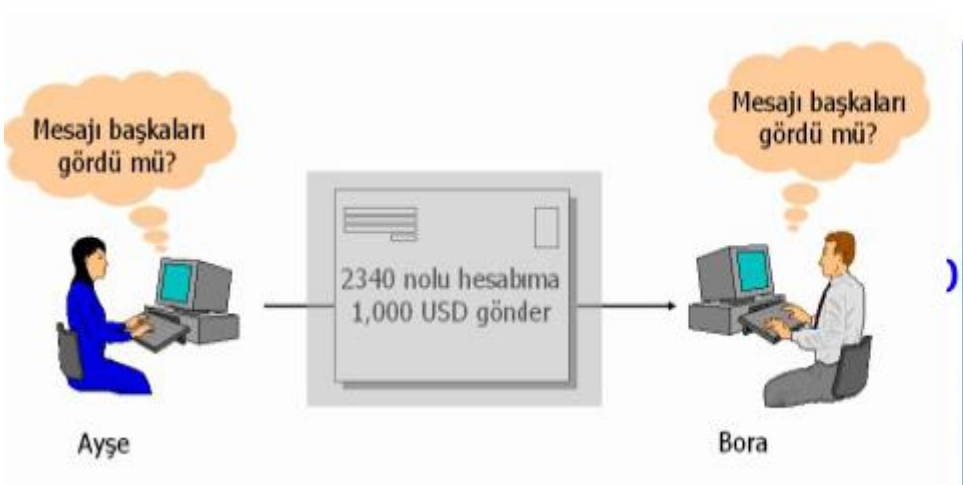
Güvenlik ihlallerine örnekler

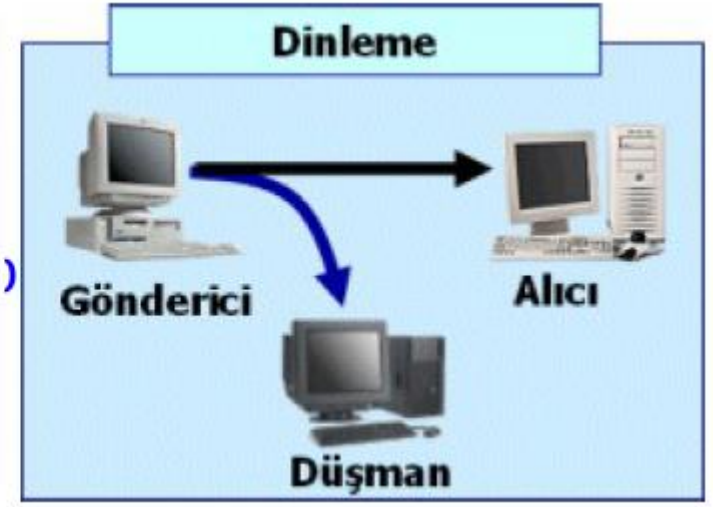
- Ornek 1 : Kullanıcı A, e-posta mesajı ekinde acığa cıkması / başka birinin eline gecmesi istenmeyen bir dosyayı kullanıcı B ye gonderir. Bu dosyayı okuma yetkisi olmayan Kullanıcı C, e-posta iletimini izleyebilir ve dosyanın transferi sırasında tarafların haberi olmadan bir kopyasını alabilir (Gizlilik ihlali)

  -Pasif Saldırı-

Gizlilik İhlali

- Haberleşme kanalını dinleyen saldırgan gonderici ile alıcı arasındaki mesaj trafiğini dinleyebilir ve elde ettiği mesajları okuyarak bu haberleşmenin gizliliğini bozar. Bu tehdit dinleme tehdidi olarak bilinir.





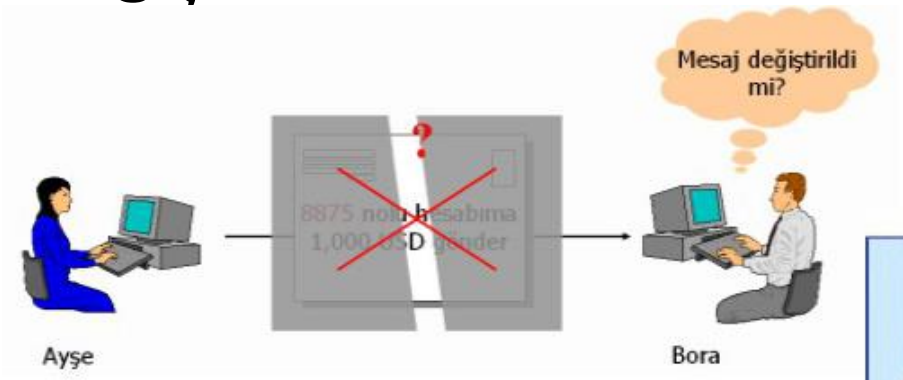
Güvenlik ihlallerine örnekler

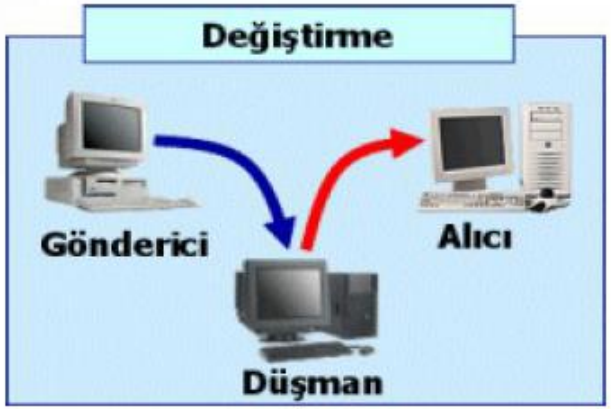
- Ornek 2 : Kullanıcı C, ornek 1 de yapılanların yerine e-posta iletimine mudahale edebilir ve bu dosyayı başka bir dosya ile değiştirip, sanki mesaj Kullanıcı A dan geliyormuşcasına tekrar Kullanıcı B ye gonderebilir (Butunluk ihlali, mesajın sahibi veya mesajı/dosyayı oluşturanın kontrol edilmemesi durumu)

–Aktif atak: araya girme ve tekrar gonderme

Bütünlük İhlali

- Haberleşmeye mudahale edip gondericinin mesajlarını değiştiren saldırgan, alıcıya giden mesajı istediği şekle sokabilir. Bu tehdit mesajın butunluğunu bozan değiştirme tehdididir.





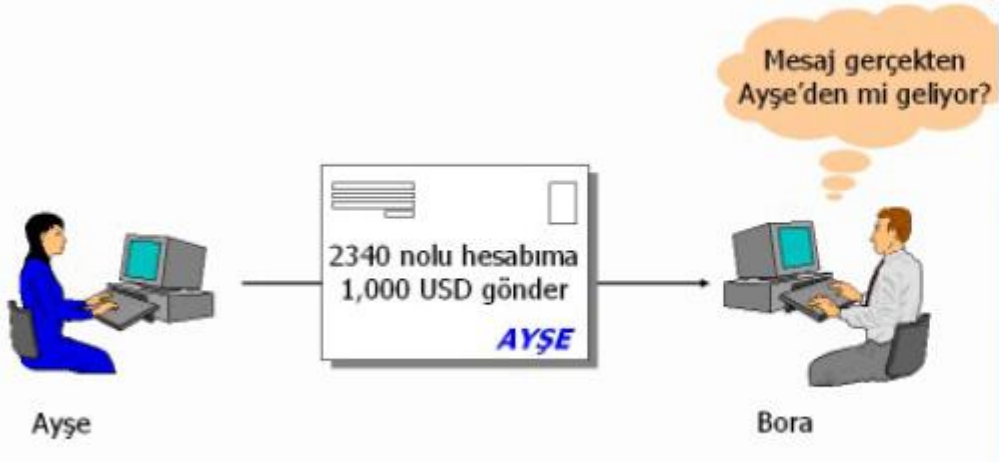
Güvenlik ihlallerine örnekler

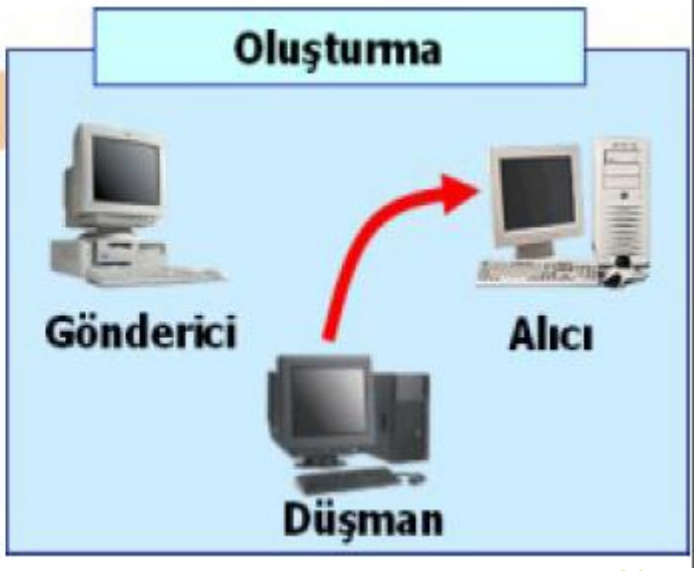
- Ornek 3 : Kullanıcı C nin, Kullanıcı A yerine (Kullanıcı A boylesine bir mesajı Kullanıcı B ye gondermemektedir), Kullanıcı B ye e-posta mesaj gondermesi (Kimlik denetimi ihlali, mesajın sahibi veya mesajı/dosyayı oluşturanın kontrol edilmemesi durumu)

– Aktif Saldırı: başkasını taklit etme

Kimlik Doğrulama İhlali

- Saldırgan, alıcıya gondericinin kimliğini taklit ederek bir mesaj gonderebilir. Bu durumda eğer alıcı guvenilir bir kimlik doğrulaması yapmıyorsa yanlış mesajlarla kandırılabilir.





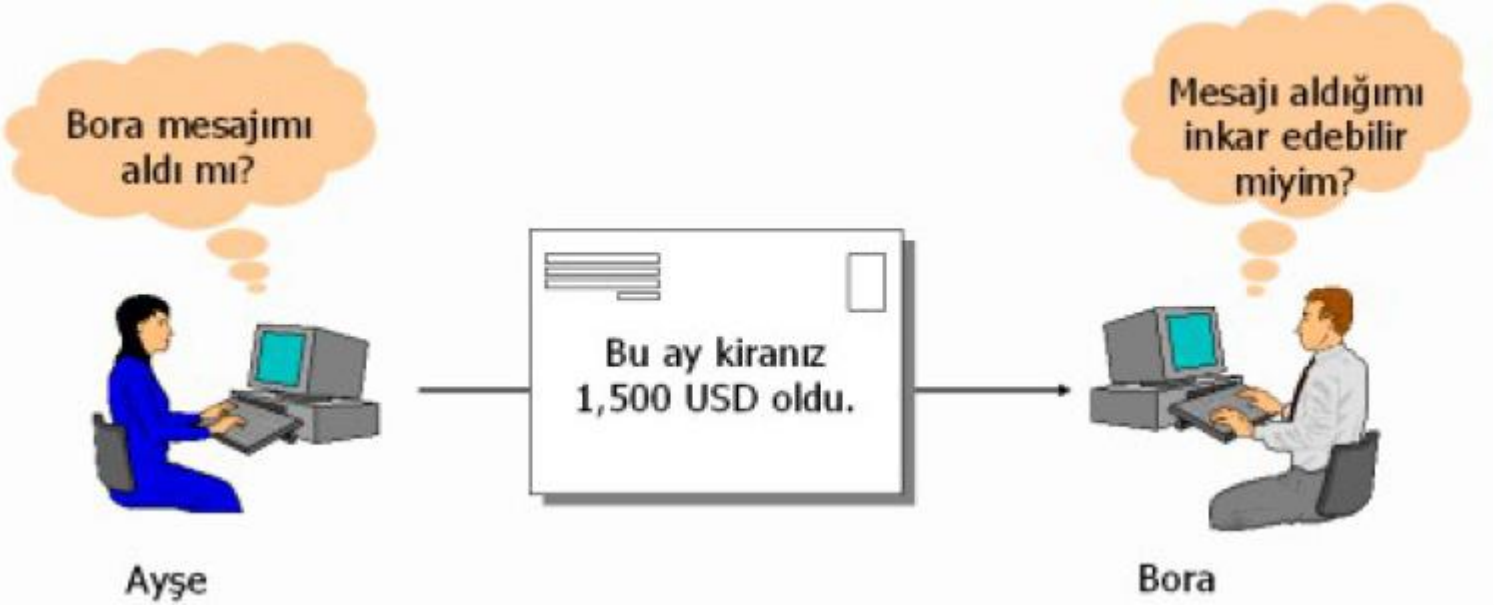
Güvenlik ihlallerine örnekler

- Ornek 4 : Muşteri B nin, cağrı merkezi uzerinden muşteri temsilcisi G ye bir talimat vermesi ve G nin bu talimatı yerine getirmesi. Fakat Muşteri B nin bu talimatı verdiğini inkar etmesi (İnkar edilemezlik ihlali, talimatı verenin inkar etmemesini icin kanıtın oluşturulmaması)

- Ornek 5 : Muşteri B nin, cağrı merkezi uzerinden muşteri temsilcisi G ye bir talimat vermesi ve G nin bu talimatı yerine getirmemesi. G nin bu talimatı aldığını inkar etmesi (İnkar edilemezlik ihlali, talimatı alanın, aldığını inkar etmemesini icin kanıtın oluşturulmaması)

İnkar Edilemezlik İhlali

- Mesajı gonderen veya alan tarafın bu işi yaptığını inkar etmesi soz konusu olabilir. Bu kotu niyetli girişimi boşa cıkaracak mekanizmalara ihtiyac vardır.



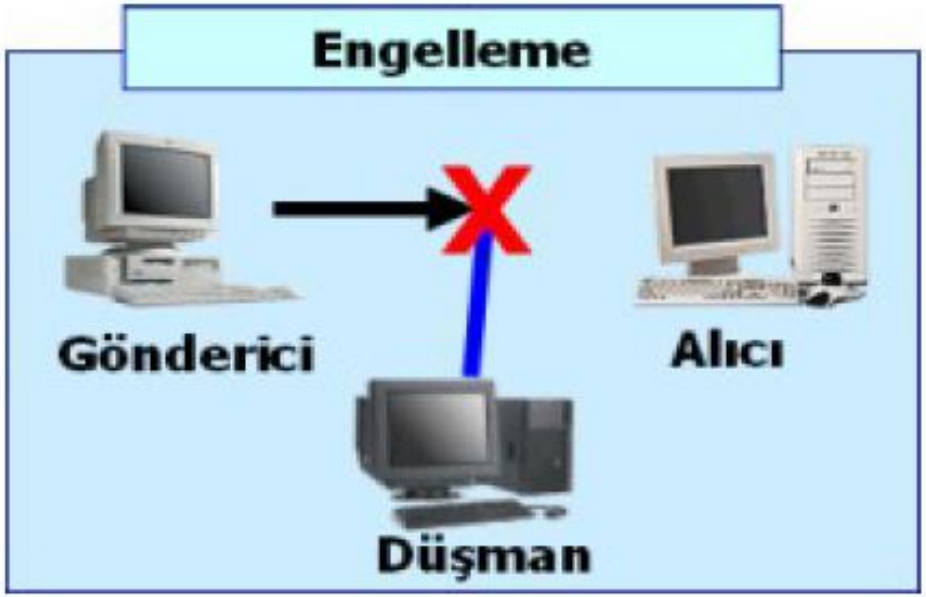
Güvenlik ihlallerine örnekler

- Ornek 6 : Yonetici D, calışanı E yi işten cıkarır ve E nin firma sistemlerine ulaşma yetkisinin kaldırılma emrini iceren e-posta mesajını gonderir. Fakat hala yetkili olan E, bu mesajın yerine ulaşmasını bir sureliğine engeller. Bu sure boyunca da firma kaynaklarına zarar verir ve bu zarar sonrası, yonetici D nin e-posta mesajının yerine ulaşmasına izin verir (Sureklilik ihlali)

-Aktif saldırı

Süreklilik İhlali

- Saldırgan, haberleşen iki taraf arasındaki hattı veya haberleşme araclarını kullanılmaz hale getirerek haberleşmenin surekliliğini engellemeye calışır.



Güvenlik Hedeflerine Ulaşmanı Yolu: Kriptografi

- Gizlilik hedefi: Simetrik şifreleme (buyuk dosyalar) ve Asimetrik Şifreleme (kucuk mesajlar)
- Butunluk hedefi: Mesaj Kimlik doğrulama (MAC-Message Authentication Code) algoritmaları, Ozet (Hash) fonksiyonları
- İnkar edilememezlik hedefi: Dijital imza ve X.509 sertifikaları (dolayısıyla Asimetrik şifreleme, ozet fonksiyonları ve Acık anahtarlı Altyapısı)
- Kimlik Denetimi hedefi: Mesaj Kimlik doğrulama (MAC) algoritmaları, Ozet fonksiyonları ve dijital imza
- Sureklilik hedefi: Erişim ve Yetkilendirme kontrolu, dolaylı yoldan: Mesaj Kimlik doğrulama (MAC) algoritmaları, Ozet fonksiyonları ve dijital imza
- İzlenebilirlik hedefi: İnkar edilememezlik kanıtı icin, dijital imza