



Saldırgan, sistem üzerinde kodu analiz edebilir, belleği okuyabilir ve işleme işlemlerini takip edebilir. Beyaz kutu kriptografi, bu durumlarda bile güvenli saılayacak teknikler sunar.

- **Kara Kutu Modeli (Blackbox):** Anahtar ve veri, işleme işlemi sırasında sistemde gizli kalır. Saldırganın işleme algoritmasınına erişimi yoktur.
- **Beyaz Kutu Modeli (Whitebox):** Saldırgan sistemde tam erişime sahiptir. İşleme algoritması ve anahtarlar saldırgan tarafından güvenli olarak elde edilir.

#### Uygulama Örnekleri:

1. Beyaz kutu ortamında bir işleme algoritmasını nasıl gizlenebileceğini analiz etmek.
2. Kara kutu ve beyaz kutu modelleri arasındaki farkları karşılaştırarak açıklamak.

**1.1.2.2 2. Beyaz Kutu İşleme Yöntemleri Teorik Açıklama:** Beyaz kutu işleme, özellikle simetrik işleme algoritmaları için kullanılır. Beyaz kutu ortamında işleme yapıldıktan, işleme anahtarının bellekten işleme karışması veya tahmin edilmesi zorlaştırılır.

- **Whitebox AES:** AES işleme algoritmasını, beyaz kutu ortamlarında güvenli bir şekilde uygulanmasını sağlar.
- **Whitebox DES:** DES algoritmasını benzer şekilde beyaz kutu güvenli işleme saılanmış hali.

#### Uygulama Örnekleri:

1. **Whitebox AES** ile bir metni işleme ve işleme işlemi.
2. **Whitebox DES** kullanarak verilerin işlenmesi ve işleme işleme işlemi.

**1.1.2.3 3. Whitebox AES ve DES Teorik Açıklama:** AES ve DES, simetrik işleme algoritmalarıdır. Beyaz kutu uygulamalarında, bu algoritmaların işleme yapıları gizlemek için işleme teknikler kullanılır.

- **Whitebox AES:** Normalde güvenli bir ortamda işleme AES algoritması, saldırganın tüm belleğe ve koda erişebildiği durumlarda dahi anahtarlar gizli tutacak şekilde değiştirilir. Bu, değiştirilmiş tablosu kullanılarak yapılır.
- **Whitebox DES:** DES algoritması da benzer bir yaklaşımla izlenir, ancak AES'e göre daha düşük güvenlik seviyelerine sahiptir.

#### Uygulama Örnekleri:

1. Whitebox AES algoritmasını nasıl işleme işleme işlemi analiz etme.
2. Whitebox DES'in yapılarını ve güvenli açıkların tartışma.

**1.1.2.4 4. Beyaz Kutu Kriptografisinde Kullanılan Teknikler Teorik Açıklama:** Beyaz kutu kriptografisi, saldırganın anahtarları elde etmesini zorlaştıran işleme teknikler kullanır.

- **Tablo Dönüşümü (Table Lookups):** Anahtar işlemleri, tabloya dayalı dönüşümlerle gerçekleştirilir ve böylece anahtarlar kod içinde saklanmaz.
- **Obfuscation:** Kodun karmaşıklığı artırılarak, işleme işlemlerinin izlenmesini zorlaştırılır.
- **Çoklu Maskeler (Multiple Masking):** Anahtarlar, birden fazla maskeleyme katmanıyla korunur, böylece saldırganın tek bir anahtar ele geçirmesi yeterli olmaz.

#### Uygulama Örnekleri:

1. **Tablo Dönüşümü** yöntemi ile işleme işlemi beyaz kutuda nasıl güvenli hale getirebiliriz?
2. **Obfuscation** teknikleri kullanarak işleme algoritmasını karmaşıklığı artırma.

**1.1.2.5 5. Beyaz Kutu Kriptografisinde G $\frac{1}{4}$ venlik Tehditleri Teorik A $\frac{1}{2}$ S $\frac{1}{2}$ klama:** Beyaz kutu kriptografisi, tam g $\frac{1}{4}$ venlik sunamayabilir ve  $\frac{1}{2}$ Şe $\frac{1}{2}$ Yitli sald $\frac{1}{2}$ r $\frac{1}{2}$  t $\frac{1}{4}$ rlerine kar $\frac{1}{2}$ Y $\frac{1}{2}$  savunmas $\frac{1}{2}$ z kalabilir.

- **Yan Kanal Sald $\frac{1}{2}$ r $\frac{1}{2}$ lar $\frac{1}{2}$  (Side-Channel Attacks):** Sald $\frac{1}{2}$ rgan,  $\frac{1}{2}$ Yifreleme i $\frac{1}{2}$ Ylemi s $\frac{1}{2}$ ras $\frac{1}{2}$ nda enerji t $\frac{1}{4}$ ketimi, elektromanyetik yay $\frac{1}{2}$ l $\frac{1}{2}$ m veya zamanlama bilgilerini analiz ederek  $\frac{1}{2}$ Yifreleme anahtarlar $\frac{1}{2}$ n $\frac{1}{2}$  elde etmeye  $\frac{1}{2}$ Şal $\frac{1}{2}$  $\frac{1}{2}$ Yabilir.
- **Kapsaml $\frac{1}{2}$  Sald $\frac{1}{2}$ r $\frac{1}{2}$ lar (Brute Force):** T $\frac{1}{4}$ m olas $\frac{1}{2}$  anahtar kombinasyonlar $\frac{1}{2}$ n $\frac{1}{2}$  deneyerek do $\frac{1}{2}$ Yru anahtar $\frac{1}{2}$  bulmaya  $\frac{1}{2}$ Şal $\frac{1}{2}$  $\frac{1}{2}$ Yan sald $\frac{1}{2}$ r $\frac{1}{2}$ lard $\frac{1}{2}$ r.
- **Differential Fault Analysis (DFA):** Sald $\frac{1}{2}$ rgan,  $\frac{1}{2}$ Yifreleme i $\frac{1}{2}$ Ylemi s $\frac{1}{2}$ ras $\frac{1}{2}$ nda bellek veya i $\frac{1}{2}$ Ylemcide k $\frac{1}{4}$  $\frac{1}{2}$ Ş $\frac{1}{2}$ k hatalar olu $\frac{1}{2}$ turarak,  $\frac{1}{2}$ Yfre  $\frac{1}{2}$ Ş $\frac{1}{2}$ zme s $\frac{1}{2}$ recini manip $\frac{1}{2}$ le eder ve anahtar bilgilerini elde edebilir.

**Uygulama  $\frac{1}{2}$ -rneklere:**

1. Yan kanal sald $\frac{1}{2}$ r $\frac{1}{2}$ lar $\frac{1}{2}$ na kar $\frac{1}{2}$ Y $\frac{1}{2}$  beyaz kutu ortam $\frac{1}{2}$ nda nas $\frac{1}{2}$ l koruma sa $\frac{1}{2}$ Ylanabilir?
2. Brute force sald $\frac{1}{2}$ r $\frac{1}{2}$ lar $\frac{1}{2}$ n $\frac{1}{2}$  etkilerini ve korunma y $\frac{1}{2}$ ntemlerini analiz etme.

**1.1.2.6 6. G $\frac{1}{4}$ venlik Kapsam $\frac{1}{2}$ nda Beyaz Kutu Kriptografisinin Avantaj ve Dezavantajlar $\frac{1}{2}$  Teorik A $\frac{1}{2}$ S $\frac{1}{2}$ klama:** Beyaz kutu kriptografisi, dijital hak y $\frac{1}{2}$ netimi ve mobil uygulamalarda s $\frac{1}{2}$ k $\frac{1}{2}$ Şa kullan $\frac{1}{2}$ lsa da, her durumda m $\frac{1}{4}$ kemmel bir  $\frac{1}{2}$ Ş $\frac{1}{2}$ z $\frac{1}{2}$ m sunmaz. Avantajlar ve dezavantajlar  $\frac{1}{2}$ Yunlard $\frac{1}{2}$ r:

- **Avantajlar:**
  - Sald $\frac{1}{2}$ rgan $\frac{1}{2}$ n t $\frac{1}{4}$ m sisteme eri $\frac{1}{2}$ Yimi oldu $\frac{1}{2}$ Yu durumlarda dahi g $\frac{1}{4}$ venlik sa $\frac{1}{2}$ Ylar.
  - Dijital hak y $\frac{1}{2}$ netimi (DRM) gibi uygulamalarda yayg $\frac{1}{2}$ n olarak kullan $\frac{1}{2}$ l $\frac{1}{2}$ r.
- **Dezavantajlar:**
  - Yan kanal sald $\frac{1}{2}$ r $\frac{1}{2}$ lar $\frac{1}{2}$  gibi  $\frac{1}{2}$ Şe $\frac{1}{2}$ Yitli sald $\frac{1}{2}$ r $\frac{1}{2}$  t $\frac{1}{4}$ rlerine kar $\frac{1}{2}$ Y $\frac{1}{2}$  hala savunmas $\frac{1}{2}$ z olabilir.
  - Performans a $\frac{1}{2}$ Ş $\frac{1}{2}$ s $\frac{1}{2}$ ndan maliyetli olabilir,  $\frac{1}{2}$ Ş $\frac{1}{2}$ nk $\frac{1}{2}$  ek maskeler ve d $\frac{1}{2}$ Şn $\frac{1}{2}$  $\frac{1}{2}$ Y $\frac{1}{2}$ mlerle i $\frac{1}{2}$ Ylem yap $\frac{1}{2}$ l $\frac{1}{2}$ r.

**Uygulama  $\frac{1}{2}$ -rneklere:**

1. Beyaz kutu kriptografisinin avantajlar $\frac{1}{2}$ n $\frac{1}{2}$  ve dezavantajlar $\frac{1}{2}$ n $\frac{1}{2}$  tart $\frac{1}{2}$  $\frac{1}{2}$ Yma.
2. Beyaz kutu ve kara kutu g $\frac{1}{4}$ venlik modellerinin kar $\frac{1}{2}$ Y $\frac{1}{2}$ la $\frac{1}{2}$ Yt $\frac{1}{2}$ r $\frac{1}{2}$ lmas $\frac{1}{2}$ .

**1.1.2.7 7. Beyaz Kutu Kriptografisinin Uygulama Alanlar $\frac{1}{2}$  Teorik A $\frac{1}{2}$ S $\frac{1}{2}$ klama:** Beyaz kutu kriptografisi,  $\frac{1}{2}$ Şe $\frac{1}{2}$ Yitli uygulama alanlar $\frac{1}{2}$ nda kullan $\frac{1}{2}$ l $\frac{1}{2}$ r:

- **Dijital Hak Y $\frac{1}{2}$ netimi (DRM):** M $\frac{1}{4}$ zik, film ve yaz $\frac{1}{2}$ l $\frac{1}{2}$ m gibi dijital i $\frac{1}{2}$ Şeriklerin korsan kullan $\frac{1}{2}$ m $\frac{1}{2}$ n $\frac{1}{2}$   $\frac{1}{2}$ Şnlemek i $\frac{1}{2}$ Şin kullan $\frac{1}{2}$ l $\frac{1}{2}$ r.
- **Mobil Uygulama G $\frac{1}{4}$ venli $\frac{1}{2}$ Yi:** Mobil cihazlarda  $\frac{1}{2}$ Şal $\frac{1}{2}$  $\frac{1}{2}$ Yan uygulamalarda,  $\frac{1}{2}$ Şzellikle finansal uygulamalarda hassas bilgilerin korunmas $\frac{1}{2}$ n $\frac{1}{2}$  sa $\frac{1}{2}$ Ylar.
- **IoT G $\frac{1}{4}$ venli $\frac{1}{2}$ Yi:** Nesnelerin interneti (IoT) cihazlar $\frac{1}{2}$ nda veri g $\frac{1}{4}$ venli $\frac{1}{2}$ Yini sa $\frac{1}{2}$ Ylamak i $\frac{1}{2}$ Şin kullan $\frac{1}{2}$ l $\frac{1}{2}$ r.

**Uygulama  $\frac{1}{2}$ -rneklere:**

1. **DRM** sistemlerinde beyaz kutu kriptografinin nas $\frac{1}{2}$ l kullan $\frac{1}{2}$ ld $\frac{1}{2}$  $\frac{1}{2}$ Y $\frac{1}{2}$ n $\frac{1}{2}$  inceleme.
2. Mobil uygulamalarda beyaz kutu kriptografinin uygulanmas $\frac{1}{2}$  ve test edilmesi.

**1.1.2.8 8. Beyaz Kutu Kriptografi Ara $\frac{1}{2}$ Şlar $\frac{1}{2}$  Teorik A $\frac{1}{2}$ S $\frac{1}{2}$ klama:** Beyaz kutu kriptografisini uygulamak i $\frac{1}{2}$ Şin  $\frac{1}{2}$ Şe $\frac{1}{2}$ Yitli ara $\frac{1}{2}$ Şlar ve k $\frac{1}{4}$ t $\frac{1}{4}$ phaneler kullan $\frac{1}{2}$ labilir. Bu ara $\frac{1}{2}$ Şlar,  $\frac{1}{2}$ Yifreleme i $\frac{1}{2}$ Ylemlerini karma $\frac{1}{2}$ Y $\frac{1}{2}$ kl $\frac{1}{2}$ Yt $\frac{1}{2}$ rarak g $\frac{1}{4}$ venli $\frac{1}{2}$ Yi art $\frac{1}{2}$ r $\frac{1}{2}$ .

- **Tigress:** C/C++ programlar $\frac{1}{2}$  i $\frac{1}{2}$ Şin obfuscation (kod karma $\frac{1}{2}$ Y $\frac{1}{2}$ kl $\frac{1}{2}$ Yt $\frac{1}{2}$ rma) ve beyaz kutu kriptografi teknikleri sa $\frac{1}{2}$ Ylayan bir ara $\frac{1}{2}$ Ş.
- **Whitebox Toolkits:** Beyaz kutu AES ve di $\frac{1}{2}$ Yer  $\frac{1}{2}$ Yifreleme algoritmalar $\frac{1}{2}$ n $\frac{1}{2}$  uygulayan  $\frac{1}{2}$ Şe $\frac{1}{2}$ Yitli a $\frac{1}{2}$ Ş $\frac{1}{2}$ k kaynak ve ticari k $\frac{1}{4}$ t $\frac{1}{4}$ phaneler.

**Uygulama  $\frac{1}{2}$ -rneklere:**

1. **Tigress** kullanarak bir Ğifreleme algoritmasġnġ karmaġġklaġtġrma.
2. Beyaz kutu kriptografi araġġlarla basit bir uygulama geliġtirme.

**1.1.2.9 9. Beyaz Kutu Kriptografisinde Gelecek Yġnelimleri Teorik Aġġklama:** Beyaz kutu kriptografisi, dijital hak yġnetimi ve gġvenli mobil uygulamalar iġin kritik bir rol oynamaya devam ediyor. Gelecekte, beyaz kutu gġvenlik tekniklerinin daha da geliġtirilmesi ve yeni saldġrġ tġrlarına karġġ daha direnġli hale getirilmesi bekleniyor.

- **Post-Kuantum Kriptografi:** Kuantum bilgisayarlarġn ortaya ġġkmasġyla birlikte, mevcut Ğifreleme algoritmalarġn gġvenliġi sorgulanmaktadġr. Beyaz kutu kriptografisi, bu yeni tehditlere karġġ daha gġvenli hale getirilmeye ġsalġġyor.

#### Uygulama ġrnekleri:

1. Beyaz kutu kriptografisinin gelecekteki gġvenlik tehditlerine karġġ nasġl geliġtirilebileceġini analiz etme.

#### 1.1.3 Sonuġ

Bu hafta, beyaz kutu kriptografisinin temellerini, uygulama alanlarġn ve gġvenlik tehditlerine karġġ nasġl koruma saġlandıġnġ ġġrendik. Beyaz kutu kriptografisi, dijital iġeriklerin ve hassas bilgilerin gġvenliġini saġlamak iġin ġnemli bir araġtıġtır.