CEN429 GÃ¼venli Programlama Hafta-10

Beyaz Kutu Kriptografisi

Yazar: Dr. Ã–ÄŸr. Ãœyesi UÄŸur CORUH

İçindekiler

Şekil Listesi

Tablo Listesi

1 CEN429 GÃ¼venli Programlama

1.1 Hafta-10

1.1.0.1 Beyaz Kutu Kriptografisi Ä°ndir

- PDF[1]
- DOC[2]
- SLIDE[3]
- PPTX[4]

1.1.1 Outline

- Beyaz Kutu Kriptografisi Nedir?
- Beyaz Kutu Åžifreleme YÃ¶ntemleri
- Uygulama AlanlarÄ± ve Tehditler

1.1.2 Hafta-10: Beyaz Kutu Kriptografisi

Bu hafta, ÅŸifreleme iÅŸlemlerinin aÃ§Ä±k sistemlerde gÃ¼venli bir ÅŸekilde nasÄ±l uygulandÄ±ÄŸÄ±nÄ± inceleyen Beyaz Kutu Kriptografisi'ni ele alacaÄŸÄ±z. Beyaz kutu kriptografisi, Ã¶zellikle dijital hak yÃ¶netimi (DRM) ve mobil uygulamalarda veri gÃ¼venliÄŸini saÄŸlamak iÃ§in Ã¶nemli bir tekniktir.

1.1.2.1 1. Beyaz Kutu Kriptografisinin Temelleri Teorik AÃ§Ä±klama:

Beyaz kutu kriptografisi, Ã¶zellikle saldÄ±rganÄ±n sistemin tÃ¼m kaynaklarÄ±na eriÅŸimi olduÄŸu durumlarda gÃ¼venliÄŸi saÄŸlamak amacÄ±yla geliÅŸtirilmiÅŸtir. Buradaki temel amaÃ§, şifreleme anahtarlarÄ±nÄ± ve iÅŸlemlerini dÄ±ÅŸarÄ±dan gelebilecek saldÄ±rÄ±lara karÅŸÄ± gizli tutmaktÄ±r.

[1] pandoc_cen429-week-10.tr_doc.pdf
[2] pandoc_cen429-week-10.tr_word.docx
[3] cen429-week-10.tr_slide.pdf
[4] cen429-week-10.tr_slide.pptx

SaldÄ±rgan, sistem Ã¼zerinde kodu analiz edebilir, belleÄŸi okuyabilir ve ÅŸifreleme iÅŸlemlerini takip edebilir. Beyaz kutu kriptografi, bu durumlarda bile gÃ¼venliÄŸi saÄŸlayacak teknikler sunar.

- **Kara Kutu Modeli (Blackbox):** Anahtar ve veri, ÅŸifreleme iÅŸlemi sÄ±rasÄ±nda sistemde gizli kalÄ±r. SaldÄ±rganÄ±n ÅŸifreleme algoritmasÄ±na eriÅŸimi yoktur.
- **Beyaz Kutu Modeli (Whitebox):** SaldÄ±rgan sistemde tam eriÅŸime sahiptir. Åžifreleme algoritmasÄ± ve anahtarlar saldÄ±rgan tarafÄ±ndan gÃ¶rÃ¼nÃ¼r.

Uygulama Ã–rnekleri:

1. Beyaz kutu ortamÄ±nda bir ÅŸifreleme algoritmasÄ±nÄ±n nasÄ±l gizlenebileceÄŸini analiz etmek.
2. Kara kutu ve beyaz kutu modelleri arasÄ±ndaki farklarÄ± karÅŸÄ±laÅŸtÄ±rarak aÃ§Ä±klamak.

1.1.2.2 2. Beyaz Kutu Åžifreleme YÃ¶ntemleri Teorik AÃ§Ä±klama:

Beyaz kutu ÅŸifreleme, Ã¶zellikle simetrik ÅŸifreleme algoritmalarÄ± iÃ§in kullanÄ±lÄ±r. Beyaz kutu ortamÄ±nda ÅŸifreleme yapÄ±lÄ±rken, ÅŸifreleme anahtarÄ±nÄ±n bellekten Ã§Ä±karÄ±lmasÄ± veya tahmin edilmesi zorlaÅŸtÄ±rÄ±lÄ±r.

- **Whitebox AES:** AES ÅŸifreleme algoritmasÄ±nÄ±n, beyaz kutu ortamlarÄ±nda gÃ¼venli bir ÅŸekilde uygulanmasÄ±nÄ± saÄŸlar.
- **Whitebox DES:** DES algoritmasÄ±nÄ±n benzer ÅŸekilde beyaz kutu gÃ¼venliÄŸi saÄŸlanmÄ±ÅŸ hali.

Uygulama Ã–rnekleri:

1. **Whitebox AES** ile bir metni ÅŸifreleme ve Ã§Ã¶zme iÅŸlemi.
2. **Whitebox DES** kullanarak verilerin ÅŸifrelenmesi ve ÅŸifre Ã§Ã¶zÃ¼lmesi.

1.1.2.3 3. Whitebox AES ve DES Teorik AÃ§Ä±klama:

AES ve DES, simetrik ÅŸifreleme algoritmalarÄ±dÄ±r. Beyaz kutu uygulamalarÄ±nda, bu algoritmalarÄ±n iÃ§ yapÄ±larÄ±nÄ± gizlemek iÃ§in Ã§eÅŸitli teknikler kullanÄ±lÄ±r.

- **Whitebox AES:** Normalde gÃ¼venli bir ortamda Ã§alÄ±ÅŸan AES algoritmasÄ±, saldÄ±rganÄ±n tÃ¼m belleÄŸe ve koda eriÅŸebildiÄŸi durumlarda dahi anahtarlarÄ± gizli tutacak ÅŸekilde dÃ¶nÃ¼ÅŸtÃ¼rÃ¼lÃ¼r. Bu, dÃ¶nÃ¼ÅŸÃ¼m tablosu kullanÄ±larak yapÄ±lÄ±r.
- **Whitebox DES:** DES algoritmasÄ±nda da benzer bir yaklaÅŸÄ±m izlenir, ancak AES'e gÃ¶re daha dÃ¼ÅŸÃ¼k gÃ¼venlik seviyelerine sahiptir.

Uygulama Ã–rnekleri:

1. Whitebox AES algoritmasÄ±nÄ±n nasÄ±l Ã§alÄ±ÅŸtÄ±ÄŸÄ±nÄ± adÄ±m adÄ±m analiz etme.
2. Whitebox DES'in zayÄ±f yÃ¶nlerini ve gÃ¼venlik aÃ§Ä±klarÄ±nÄ± tartÄ±ÅŸma.

1.1.2.4 4. Beyaz Kutu Kriptografisinde KullanÄ±lan Teknikler Teorik AÃ§Ä±klama:

Beyaz kutu kriptografisi, saldÄ±rganÄ±n anahtarlarÄ± elde etmesini zorlaÅŸtÄ±ran Ã§eÅŸitli teknikler kullanÄ±r.

- **Tablo DÃ¶nÃ¼ÅŸÃ¼mÃ¼ (Table Lookups):** Anahtar iÅŸlemleri, tabloya dayalÄ± dÃ¶nÃ¼ÅŸÃ¼mlerle gerÃ§ekleÅŸtirilir ve bÃ¶ylece anahtarlar kod iÃ§inde aÃ§Ä±kÃ§a gÃ¶rÃ¼nmez.
- **Obfuscation:** Kodun karmaÅŸÄ±klaÅŸtÄ±rÄ±lmasÄ±, ÅŸifreleme iÅŸlemlerinin izlenmesini zorlaÅŸtÄ±rÄ±r.
- **Ã‡oklu Maskeler (Multiple Masking):** Anahtarlar, birden fazla maskeleme katmanÄ±yla korunur, bÃ¶ylece saldÄ±rganÄ±n tek bir anahtarÄ± ele geÃ§irmesi yeterli olmaz.

Uygulama Ã–rnekleri:

1. **Tablo DÃ¶nÃ¼ÅŸÃ¼mÃ¼** yÃ¶ntemi ile ÅŸifreleme iÅŸlemini beyaz kutuda nasÄ±l gÃ¼venli hale getirebiliriz?
2. **Obfuscation** teknikleri kullanarak ÅŸifreleme algoritmasÄ±nÄ± karmaÅŸÄ±klaÅŸtÄ±rma.

1.1.2.5 5. Beyaz Kutu Kriptografisinde GÃ¼venlik Tehditleri Teorik AÃ§Ä±klama: Beyaz kutu kriptografisi, tam gÃ¼venlik sunamayabilir ve Ã§eÅŸitli saldÄ±rÄ± tÃ¼rlerine karÅŸÄ± savunmasÄ±z kalabilir.

- **Yan Kanal SaldÄ±rÄ±larÄ± (Side-Channel Attacks):** SaldÄ±rgan, ÅŸifreleme iÅŸlemi sÄ±rasÄ±nda enerji tÃ¼ketimi, elektromanyetik yayÄ±lÄ±m veya zamanlama bilgilerini analiz ederek ÅŸifreleme anahtarlarÄ±nÄ± elde etmeye Ã§alÄ±ÅŸabilir.
- **KapsamlÄ± SaldÄ±rÄ±lar (Brute Force):** TÃ¼m olasÄ± anahtar kombinasyonlarÄ±nÄ± deneyerek doÄŸru anahtarÄ± bulmaya Ã§alÄ±ÅŸan saldÄ±rÄ±lardÄ±r.
- **Differential Fault Analysis (DFA):** SaldÄ±rgan, ÅŸifreleme iÅŸlemi sÄ±rasÄ±nda bellek veya iÅŸlemcide kÃ¼Ã§Ã¼k hatalar oluÅŸturarak, ÅŸifre Ã§Ã¶zme sÃ¼recini manipÃ¼le eder ve anahtar bilgilerini elde edebilir.

Uygulama Ã–rnekleri:

1. Yan kanal saldÄ±rÄ±larÄ±na karÅŸÄ± beyaz kutu ortamÄ±nda nasÄ±l koruma saÄŸlanabilir?
2. Brute force saldÄ±rÄ±larÄ±nÄ±n etkilerini ve korunma yÃ¶ntemlerini analiz etme.

1.1.2.6 6. GÃ¼venlik KapsamÄ±nda Beyaz Kutu Kriptografisinin Avantaj ve Dezavantajları Teorik AÃ§Ä±klama: Beyaz kutu kriptografisi, dijital hak yÃ¶netimi ve mobil uygulamalarda sÄ±kÃ§a kullanÄ±lsa da, her durumda mÃ¼kemmel bir Ã§Ã¶zÃ¼m sunmaz. Avantajlar ve dezavantajlar ÅŸunlardÄ±r:

- **Avantajlar:**
  - SaldÄ±rganÄ±n tÃ¼m sisteme eriÅŸimi olduÄŸu durumlarda dahi gÃ¼venlik saÄŸlar.
  - Dijital hak yÃ¶netimi (DRM) gibi uygulamalarda yaygÄ±n olarak kullanÄ±lÄ±r.
- **Dezavantajlar:**
  - Yan kanal saldÄ±rÄ±larÄ± gibi Ã§eÅŸitli saldÄ±rÄ± tÃ¼rlerine karÅŸÄ± hala savunmasÄ±z olabilir.
  - Performans aÃ§Ä±sÄ±ndan maliyetli olabilir, Ã§Ã¼nkÃ¼ ek maskeler ve dÃ¶nÃ¼ÅŸÃ¼mlerle iÅŸlem yapÄ±lÄ±r.

Uygulama Ã–rnekleri:

1. Beyaz kutu kriptografisinin avantajlarÄ±nÄ± ve dezavantajlarÄ±nÄ± tartÄ±ÅŸma.
2. Beyaz kutu ve kara kutu gÃ¼venlik modellerinin karÅŸÄ±laÅŸtÄ±rÄ±lmasÄ±.

1.1.2.7 7. Beyaz Kutu Kriptografisinin Uygulama AlanlarÄ± Teorik AÃ§Ä±klama: Beyaz kutu kriptografisi, Ã§eÅŸitli uygulama alanlarÄ±nda kullanÄ±lÄ±r:

- **Dijital Hak YÃ¶netimi (DRM):** MÃ¼zik, film ve yazÄ±lÄ±m gibi dijital iÃ§eriklerin korsan kullanÄ±mÄ±nÄ± Ã¶nlemek iÃ§in kullanÄ±lÄ±r.
- **Mobil Uygulama GÃ¼venliÄŸi:** Mobil cihazlarda Ã§alÄ±ÅŸan uygulamalarda, Ã¶zellikle finansal uygulamalarda hassas bilgilerin korunmasÄ±nÄ± saÄŸlar.
- **IoT GÃ¼venliÄŸi:** Nesnelerin interneti (IoT) cihazlarÄ±nda veri gÃ¼venliÄŸini saÄŸlamak iÃ§in kullanÄ±lÄ±r.

Uygulama Ã–rnekleri:

1. **DRM** sistemlerinde beyaz kutu kriptografinin nasÄ±l kullanÄ±ldÄ±ÄŸÄ±nÄ± inceleme.
2. Mobil uygulamalarda beyaz kutu kriptografinin uygulanmasÄ± ve test edilmesi.

1.1.2.8 8. Beyaz Kutu Kriptografi AraÃ§larÄ± Teorik AÃ§Ä±klama: Beyaz kutu kriptografisini uygulamak iÃ§in Ã§eÅŸitli araÃ§lar ve kÃ¼tÃ¼phaneler kullanÄ±labilir. Bu araÃ§lar, ÅŸifreleme iÅŸlemlerini karmaÅŸÄ±klaÅŸtÄ±rarak gÃ¼venliÄŸi artÄ±rÄ±r.

- **Tigress:** C/C++ programlarÄ± iÃ§in obfuscation (kod karmaÅŸÄ±klaÅŸtÄ±rma) ve beyaz kutu kriptografi teknikleri saÄŸlayan bir araÃ§.
- **Whitebox Toolkits:** Beyaz kutu AES ve diÄŸer ÅŸifreleme algoritmalarÄ±nÄ± uygulayan Ã§eÅŸitli aÃ§Ä±k kaynak ve ticari kÃ¼tÃ¼phaneler.

Uygulama Ã–rnekleri:

1. **Tigress** kullanarak bir ÅŸifreleme algoritmasÄ±nÄ± karmaÅŸÄ±klaÅŸtÄ±rma.
2. Beyaz kutu kriptografi araÃ§larÄ±yla basit bir uygulama geliÅŞtirme.

1.1.2.9 9. Beyaz Kutu Kriptografisinde Gelecek YÃ¶nelimleri Teorik AÃ§Ä±klama: Beyaz kutu kriptografisi, dijital hak yÃ¶netimi ve gÃ¼venli mobil uygulamalar iÃ§in kritik bir rol oynamaya devam ediyor. Gelecekte, beyaz kutu gÃ¼venlik tekniklerinin daha da geliÅŞtirilmesi ve yeni saldÄ±rÄ± tÃ¼rlerine karÅŞÄ± daha direnÃ§li hale getirilmesi bekleniyor.

- **Post-Kuantum Kriptografi:** Kuantum bilgisayarlarÄ±n ortaya Ã§Ä±kmasÄ±yla birlikte, mevcut ÅŞifreleme algoritmalarÄ±nÄ±n gÃ¼venliÄŞi sorgulanmaktadÄ±r. Beyaz kutu kriptografisi, bu yeni tehditlere karÅŞÄ± daha gÃ¼venli hale getirilmeye Ã§alÄ±ÅŞÄ±lÄ±yor.

Uygulama Ã–rnekleri:

1. Beyaz kutu kriptografisinin gelecekteki gÃ¼venlik tehditlerine karÅŞÄ± nasÄ±l geliÅŞtirilebileceÄŞini analiz etme.

1.1.3 SonuÃ§

Bu hafta, beyaz kutu kriptografisinin temellerini, uygulama alanlarÄ±nÄ± ve gÃ¼venlik tehditlerine karÅŞÄ± nasÄ±l koruma saÄŞlandÄ±ÄŞÄ±nÄ± Ã¶ÄŞrendik. Beyaz kutu kriptografisi, dijital iÃ§eriklerin ve hassas bilgilerin gÃ¼venliÄŞini saÄŞlamak iÃ§in Ã¶nemli bir araÃ§tÄ±r.

$$10. Hafta - Sonu$$