CE407 GÃ¼venli Programlama Hafta-13

Tigress ve Ã‡eÅŸitlilik Teknikleri

Yazar: Dr. Ã–Ğr. Ãœyesi UÄŸur CORUH

İçindekiler

Şekil Listesi

Tablo Listesi

1 CE407 GÃ¼venli Programlama

1.1 Hafta-13

1.1.0.1 Tigress ve Ã‡eÅŸitlilik Teknikleri

Ä°ndir PDF[1],DOCX[2], SLIDE[3], PPTX[4]

1.1.1 Outline

- Tigress ve Ã‡eÅŸitlilik Teknikleri
- Obfuscation YÃ¶ntemleri
- SaldÄ±rÄ±lara KarÅŸÄ± Savunma

1.1.2 Hafta-13: Tigress ve Ã‡eÅŸitlilik Teknikleri

Bu hafta, kodun analiz edilmesini zorlaÅŸtÄ±ran ve programÄ± saldÄ±rÄ±lara karÅŸÄ± daha direnÃ§li hale getiren Ã§eÅŸitlilik (diversification) tekniklerini ve Tigress gibi obfuscation araÃ§larÄ±nÄ± inceleyeceÄŸiz. Bu teknikler, programÄ±n Ã§alÄ±ÅŸtÄ±ÄŸÄ± her seferinde farklÄ±laÅŸmasÄ±nÄ± saÄŸlar, bÃ¶ylece saldÄ±rganlarÄ±n aynÄ± yÃ¶ntemlerle programÄ± analiz etmelerini zorlaÅŸtÄ±rÄ±r.

1.1.2.1 1. Tigress Ã‡eÅŸitlilik (Diversity) Teorik AÃ§Ä±klama: Tigress, bir programÄ± farklÄ± ÅŸekillerde dÃ¶nÃ¼ÅŸtÃ¼rerek, saldÄ±rÄ±lara karÅŸÄ± direnÃ§li hale getiren gÃ¼Ã§lÃ¼ bir obfuscation aracÄ±dÄ±r. Bir programÄ±n her Ã§Ä±ktÄ±sÄ± benzersiz bir yorumlayÄ±cÄ± (interpreter) oluÅŸturur. Bu, programÄ±n davranÄ±ÅŸÄ±nÄ± rastgeleleÅŸtirir ve analiz edilmesini zorlaÅŸtÄ±rÄ±r.

- **Tigressâ€™te KullanÄ±lan YÃ¶ntemler:**
  - **Instruction Dispatch TÃ¼rleri:**
    - Switch, direkt, endirekt, Ã§aÄŸrÄ± (call), if-else, lineer, binary, interpolasyon.
  - **Operand TÃ¼rleri:**

[1] ce407-week-13.tr_doc.pdf
[2] ce407-week-13.tr_word.docx
[3] ce407-week-13.tr_slide.pdf
[4] ce407-week-13.tr_slide.pptx

    - YÄ±ÄŸÄ±n (stack), registerlar.
  - **RastgeleleÅŸtirilen OperatÃ¶rler:**
    - FarklÄ± operandlar ve operator kombinasyonlarÄ± kullanarak kodun karmaÅŸÄ±klaÅŸtÄ±rÄ±lmasÄ±.
  - **Ã‡eÅŸitli DÃ¶nÃ¼ÅŸÃ¼mler:**
    - **Code Flattening:** ProgramÄ±n akÄ±ÅŸ kontrolÃ¼nÃ¼n dÃ¼zleÅŸtirilmesi.
    - **Merge/Split Fonksiyonlar:** BirleÅŸtirilen ya da bÃ¶lÃ¼nen fonksiyonlar.
    - **Opaque Predicates:** Kodda gizli ve deÄŸiÅŸtirilemeyen koÅŸul ifadeleri ekleme.

Uygulama Ã–rneÄŸi:

```
tigress --Transform=Virtualize --Functions=fib --VirtualizeDispatch=switch --out=v1.c test1.c
gcc -o v1 v1.c
```

2. Kodda Ã‡eÅŸitlilik SaÄŸlama Teorik AÃ§Ä±klama: Ã‡eÅŸitlilik, kodun analizini zorlaÅŸtÄ±rmak amacÄ±yla farklÄ± yÃ¶ntemlerle rastgeleleÅŸtirilmesini iÃ§erir. Bu yÃ¶ntemler, bir saldÄ±rganÄ±n programÄ± tersine mÃ¼hendislikle Ã§Ã¶zmesini zorlaÅŸtÄ±rÄ±r. Tigress ile bir program her Ã§alÄ±ÅŸtÄ±rÄ±ldÄ±ÄŸÄ±nda benzersiz bir sanal makine oluÅŸturulabilir.

3. SaldÄ±rÄ±lar ve KarÅŸÄ± SaldÄ±rÄ±lar Teorik AÃ§Ä±klama: Bir saldÄ±rgan, programÄ±n sanal talimat setini Ã§Ã¶zerek kodun nasÄ±l Ã§alÄ±ÅŸtÄ±ÄŸÄ±nÄ± anlamaya Ã§alÄ±ÅŸabilir. Bunun iÃ§in Ã§eÅŸitli saldÄ±rÄ± yÃ¶ntemleri geliÅŸtirilmiÅŸtir, ancak Tigress bu saldÄ±rÄ±lara karÅŸÄ± bazÄ± karÅŸÄ± saldÄ±rÄ± teknikleri sunar.

4. Algoritmik YÃ¶ntemler ve Ã‡eÅŸitlilik SaÄŸlama Teorik AÃ§Ä±klama: Ã‡eÅŸitlilik saÄŸlama algoritmalarÄ±, programÄ±n Ã§alÄ±ÅŸmasÄ±nÄ± karmaÅŸÄ±klaÅŸtÄ±rmak iÃ§in Ã§eÅŸitli seviyelerde uygulanabilir. Bu yÃ¶ntemler, bir saldÄ±rganÄ±n programÄ± Ã§Ã¶zme olasÄ±lÄ±ÄŸÄ±nÄ± azaltmak iÃ§in kullanÄ±lÄ±r.

SonuÃ§ Bu hafta, Ã§eÅŸitlilik saÄŸlama ve kendini deÄŸiÅŸtiren kod gibi ileri dÃ¼zey kod obfuscation tekniklerini Ã¶ÄŸrendik. Bu teknikler, programlarÄ±n saldÄ±rÄ±lara karÅŸÄ± daha direnÃ§li hale getirilmesini saÄŸlar ve saldÄ±rganlarÄ±n kodu Ã§Ã¶zmesini zorlaÅŸtÄ±rÄ±r. Tigress gibi araÃ§lar, kodu rastgeleleÅŸtirerek her seferinde farklÄ± bir yapÄ± oluÅŸturur, bu da kodun analizi ve tersine mÃ¼hendislik yapÄ±lmasÄ±nÄ± daha zor hale getirir.

$13. Hafta - Sonu$