

CEN429 GÃ¼venli Programlama Hafta-13

Tigress ve ÃžeÃžitlilik Teknikleri

Yazar: Dr. Ã–Ãžr. Ãœyesi UÃžur CORUH

Ãžindekiler

1 CEN429 GÃ¼venli Programlama	1
1.1 Hafta-13	1
1.1.1 Outline	1
1.1.2 Hafta-13: Tigress ve ÃžeÃžitlilik Teknikleri	1

Åekil Listesi

Tablo Listesi

1 CEN429 GÃ¼venli Programlama

1.1 Hafta-13

1.1.0.1 Tigress ve ÃžeÃžitlilik Teknikleri

- PDF¹
- DOC²
- SLIDE³
- PPTX⁴

1.1.1 Outline

- Tigress ve ÃžeÃžitlilik Teknikleri
- Obfuscation YÃžntemleri
- SaldÃžrÃžlara KarÃžÃž Savunma

1.1.2 Hafta-13: Tigress ve ÃžeÃžitlilik Teknikleri

Bu hafta, kodun analiz edilmesini zorlaÃžtÃžran ve programÃž saldÃžrÃžlara karÃžÃž daha direnÃžli hale getiren ÃžeÃžitlilik (diversification) tekniklerini ve Tigress gibi obfuscation araÃžlarÃžnÃž inceleyeceÃžiz. Bu teknikler, programÃžn ÃžalÃžÃžtÃžÃž her seferinde farklılaÃžmasÃžnÃž saÃžlar, bÃžylece saldÃžrganlarÃžn aynÃž yÃžntemlerle programÃž analiz etmelerini zorlaÃžtÃžrÃžr.

1.1.2.1 1. Tigress ÃžeÃžitlilik (Diversity) Teorik AÃžÃžklama: Tigress, bir programÃž farklı Ãžekillerde dÃžnÃžtÃžrerek, saldÃžrÃžlara karÃžÃž direnÃžli hale getiren gÃ¼venli bir obfuscation aracÃždÃžr. Bir programÃžn her ÃžÃžktÃžsÃž benzersiz bir yorumlayÃžcÃž (interpreter) oluÃžturur. Bu, programÃžn davranÃžÃžnÃž rastgeleleÃžtirir ve analiz edilmesini zorlaÃžtÃžrÃžr.

¹pandoc_cen429-week-13.pdf

²pandoc_cen429-week-13.docx

³cen429-week-13.pdf

⁴cen429-week-13.pptx

- **Tigressâ€™te Kullanılan Yâ¼ntemler:**
 - **Instruction Dispatch Tâ¼rleri:**
 - * Switch, direkt, indirekt, ÅšaÅ½râ¼ (call), if-else, lineer, binary, interpolasyon.
 - **Operand Tâ¼rleri:**
 - * Yâ¼n (stack), registerlar.
 - **RastgeleleÅ½tirilen Operatâ¼rler:**
 - * Farklâ¼ operandlar ve operator kombinasyonlarâ¼ kullanarak kodun karmaÅ½tâ¼râ¼lmasâ¼.
 - **Å½eÅ½itli Dâ¼nâ¼mlemler:**
 - * **Code Flattening:** Programâ¼n akâ¼ kontrolâ¼n dâ¼zleÅ½tirilmesi.
 - * **Merge/Split Fonksiyonlar:** BirleÅ½tirilen ya da bâ¼len fonksiyonlar.
 - * **Opaque Predicates:** Kodda gizli ve deÅ½iÅ½tirilemeyen koÅ½ul ifadeleri ekleme.

Uygulama Å½rneÅ½i:

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

2. Kodda Å½eÅ½itlilik SaÅ½lama Teorik AÅ½klama: Å½eÅ½itlilik, kodun analizini zorlaÅ½tâ¼rmak amacâ¼yla farklâ¼ yâ¼ntemlerle rastgeleleÅ½tirilmesini iÅ½erir. Bu yâ¼ntemler, bir saldâ¼rganâ¼n programâ¼ tersine mâ¼hendislikle Å½zmesini zorlaÅ½tâ¼râ¼r. Tigress ile bir program her Å½alâ¼tâ¼râ¼ldâ¼nda benzersiz bir sanal makine oluÅ½turulabilir.
3. Saldâ¼rganlar ve KarÅ½ Saldâ¼rganlar Teorik AÅ½klama: Bir saldâ¼rgan, programâ¼n sanal talimat setini Å½zerek kodun nasâ¼l Å½alâ¼tâ¼râ¼nâ¼ anlamaya Å½alâ¼tâ¼râ¼bilir. Bunun iÅ½in Å½eÅ½itli saldâ¼rgan yâ¼ntemleri geliÅ½tirilmiÅ½tir, ancak Tigress bu saldâ¼rganlara karÅ½ bazâ¼ karÅ½ saldâ¼rgan teknikleri sunar.
4. Algoritmik Yâ¼ntemler ve Å½eÅ½itlilik SaÅ½lama Teorik AÅ½klama: Å½eÅ½itlilik saÅ½lama algoritmalarâ¼, programâ¼n Å½alâ¼tâ¼râ¼nâ¼ karmaÅ½tâ¼râ¼mak iÅ½in Å½eÅ½itli seviyelerde uygulanabilir. Bu yâ¼ntemler, bir saldâ¼rganâ¼n programâ¼ Å½zme olasâ¼lâ¼nâ¼ azaltmak iÅ½in kullanâ¼lâ¼r.

SonuÅ½ Bu hafta, Å½eÅ½itlilik saÅ½lama ve kendini deÅ½iÅ½tiren kod gibi ileri dâ¼zey kod obfuscation tekniklerini Å½â¼rendik. Bu teknikler, programlarâ¼n saldâ¼rganlara karÅ½ daha direnÅ½li hale getirilmesini saÅ½lar ve saldâ¼rganlarâ¼n kodu Å½zmesini zorlaÅ½tâ¼râ¼r. Tigress gibi araÅ½lar, kodu rastgeleleÅ½tirerek her seferinde farklâ¼ bir yapâ¼ oluÅ½turur, bu da kodun analizi ve tersine mâ¼hendislik yapâ¼lmasâ¼nâ¼ daha zor hale getirir.