

CEN429 G4venli Programlama Hafta-13

Tigress ve 4te4itlilik Teknikleri

Yazar: Dr. 4-4Yr. 4e4yesi U4Yur CORUH

İçindekiler

1 CEN429 G4venli Programlama	1
1.1 Hafta-13	1
1.1.1 Outline	1
1.1.2 Hafta-13: Tigress ve 4te4itlilik Teknikleri	1

Şekil Listesi

Tablo Listesi

1 CEN429 G4venli Programlama

1.1 Hafta-13

1.1.0.1 Tigress ve 4te4itlilik Teknikleri 4ndir

- PDF¹
- DOC²
- SLIDE³
- PPTX⁴

1.1.1 Outline

- Tigress ve 4te4itlilik Teknikleri
- Obfuscation Y4ntemleri
- Sald4r4lara Kar4Ş4 Savunma

1.1.2 Hafta-13: Tigress ve 4te4itlilik Teknikleri

Bu hafta, kodun analiz edilmesini zorla4t4ran ve program4 salda4r4lara kar4Ş4 daha diren4Şli hale getiren 4Şe4itlilik (diversification) tekniklerini ve Tigress gibi obfuscation ara4Şlar4n4 inceleyece4Yiz. Bu teknikler, program4n 4sal44t44Y4 her seferinde farklıla4Ymas4n4 sa4Ylar, b4Ylece salda4rganlar4n ayn4 y4ntemlerle program4 analiz etmelerini zorla4t4r4r.

1.1.2.1 1. Tigress 4te4itlilik (Diversity) Teorik AAŞ4klama: Tigress, bir program4 farklı 4Yekillerde d4n44t4rerek, salda4r4lara kar4Ş4 diren4Şli hale getiren g4Şl4 bir obfuscation arac4d4r. Bir program4n her 4Ş4kt4s4 benzersiz bir yorumlay4c4 (interpreter) olu4turur. Bu, program4n davran44Y4n4 rastgelele4tirir ve analiz edilmesini zorla4t4r4r.

¹[pandoc_cen429-week-13.pdf](#)

²[pandoc_cen429-week-13.docx](#)

³[cen429-week-13.pdf](#)

⁴[cen429-week-13.pptx](#)

- **Tigressâ€™te Kullanılan Yâ¶ntemler:**
 - **Instruction Dispatch Tâ¼rleri:**
 - * Switch, direkt, indirekt, Å§aÄŸrÅ± (call), if-else, linear, binary, interpolasyon.
 - **Operand Tâ¼rleri:**
 - * Yâ±ÄŸÄ±n (stack), registerlar.
 - **RastgeleleÅŸtirilen Operatâ¼rler:**
 - * FarklÅ± operandlar ve operator kombinasyonlarÅ± kullanarak kodun karmaÅŸlaÅŸtırÅ±lmasÅ±.
 - **ÄŸeÅŸitli Dâ¶nâ¼ÄŸâ¼mler:**
 - * **Code Flattening:** ProgramÄ±n akÄ±ÅŸ kontrolâ¼n dâ¼zleÅŸtirilmesi.
 - * **Merge/Split Fonksiyonlar:** BirleÅŸtirilen ya da bâ¶lâ¼nen fonksiyonlar.
 - * **Opaque Predicates:** Kodda gizli ve deÅŸiÅŸtirilemeyen koÅŸul ifadeleri ekleme.

Uygulama Å–rneÅŸi:

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

2. Kodda ÄŸeÅŸitlilik SaÄŸlama Teorik AÅŸÅ±klama: ÄŸeÅŸitlilik, kodun analizini zorlaÅŸtırmak amacÅ±yla farklÅ± yâ¶ntemlerle rastgeleleÅŸtirilmesini iÅŸerir. Bu yâ¶ntemler, bir saldırganÄ±n programÅ± tersine mâ¼hendislikle ÅŸâ¶zmesini zorlaÅŸtırÅ±r. Tigress ile bir program her ÅŸalÅ±ÅŸtırÅ±ldÅ±ÄŸÄ±nda benzersiz bir sanal makine oluÅŸturulabilir.
3. Saldırganlar ve KarÅŸı Saldırganlar Teorik AÅŸÅ±klama: Bir saldırgan, programÄ±n sanal talimat setini ÅŸâ¶zerek kodun nasıllı ÅŸalÅ±ÅŸtırÅ±ÄŸÄ± anlamaya ÅŸalÅ±ÅŸabilir. Bunun iÅŸin ÄŸeÅŸitli saldırgan yâ¶ntemleri geliÅŸtirilmiÅŸtir, ancak Tigress bu saldırganlara karÅŸı bazÅ± karÅŸı saldırgan teknikleri sunar.
4. Algoritmik Yâ¶ntemler ve ÄŸeÅŸitlilik SaÄŸlama Teorik AÅŸÅ±klama: ÄŸeÅŸitlilik saÄŸlama algoritmalarÅ±, programÄ±n ÅŸalÅ±ÅŸtırmasÄ±nı karmaÅŸlaÅŸtırmak iÅŸin ÄŸeÅŸitli seviyelerde uygulanabilir. Bu yâ¶ntemler, bir saldırganÄ±n programÅ± ÅŸâ¶zme olasılıÄŸÄ±nı azaltmak iÅŸin kullanılabılır.

SonuÅŸ Bu hafta, ÄŸeÅŸitlilik saÄŸlama ve kendini deÅŸiÅŸtiren kod gibi ileri dâ¼zey kod obfuscation tekniklerini ÅŸâ¶yrendik. Bu teknikler, programlarÄ±n saldırganlara karÅŸı daha direnÅŸli hale getirilmesini saÄŸlar ve saldırganlarÄ±n kodu ÅŸâ¶zmesini zorlaÅŸtırÅ±r. Tigress gibi araÅŸlar, kodu rastgeleleÅŸtirerek her seferinde farklÅ± bir yapı oluÅŸturur, bu da kodun analizi ve tersine mâ¼hendislik yapılmamasÄ±nı daha zor hale getirir.