Մեքենայական լեզվով ծրագրերի պաշտպանությունը վերծանումից

Խումբ՝ Հ055-2
Ուսանող՝ Բաբկեն Վարդանյան
Ղեկավար՝ տ.գ.թ, դոցենտ Ռ. Գ. Հակոբյան

Հայաստանի Պետական Ճարտարագիտական Համալսարան
Քոմփյութերային Համակարգերի և Ինֆորմատիկայի Ֆակուլտետ

Երևան 2014

Ներածություն

- Ծրագրերի մեծամասնությունը պաշտպանության կարիք ունի
- Պաշտպանությունը դժվար գործ է, բայց անհրաժեշտ
- Հնարավոր չէ ծրագիրը 100%-ով պաշտպանել
- Բայց հնարավոր է վերծանման ժամանակը ավելացնել

Սպառնալիքներ

Ծրագրային ապահովմանը սպառնալիքներ

1. Վերծանում
2. Փոփոխություններ
3. Ապօրինի օգտագործում

Վերծանման միջոցներ

Ստատիկ վերծանում

Դինամիկ վերծանում

Պաշտպանության միջոցներ

Պաշտպանության միջոցների տեսակներ

1. Ջրանշում
2. Ծրագիրը որպես ծառայություն
3. Օբֆուսկացիա

Օբֆուսկացիա

Ստատիկ հարձակման դեմ

- Ինքնաձևափոխվող կոդ
- Գաղտնագրում
- Սեղմող ծրագրեր

Դինամիկ հարձակման դեմ

- Կարգաբերիչների առկայության ստուգում
- Բազմաձևություն (պոլիմորֆիզմ)
- Ձուգահեռացում

Պաշտպանության գնահատում

- Կարողություն՝ մարդու դեմ
- Ճկունություն՝ ավտոմատացված ծրագրի դեմ
- Տվյալների թաքցնում
- Գին (Բացասական ազդեցություններ)
  1. Ծրագրի սպասարկման վրա ծախսեր
  2. Արագագործության կորուստ
  3. Կարգաբերման բարդացում
  4. Ֆայլի չափի մեծացում

PE ֆայլի կառուցվածքը

Պաշտպանության ալգորիթմը

1. Սեկցիաների անունների հասցեները պահվում են զանգվածի մեջ
2. Խառնվում են Կնուտի ալգորիթմով
3. Արդյունքը հետ է գրվում ֆայլի մեջ

Պաշտպանությունից առաջ

Պաշտպանությունից հետո

Կնուտի ալգորիթմ

Միջ.	Պատահ.	Մնացածը	Արդյունքը
		1 2 3 4 5 6 7 8	
1–8	6	1 2 3 4 5 **8** 7	**6**
1–7	2	1 **7** 3 4 5 8	**2** 6
1–6	6	1 7 3 4 5	**8** 2 6
1–5	1	**5** 7 3 4	**1** 8 2 6
1–4	3	5 7 **4**	**3** 1 8 2 6
1–3	3	5 7	**4** 3 1 8 2 6
1–2	1	**7**	**5** 4 3 1 8 2 6

Արդյունք՝ 7 5 4 3 1 8 2 6

Օգտագործված գրականություն

1. http://aerokid240.blogspot.com/2011/03/windows-and-its-pe-file-structure.html
2. http://en.wikipedia.org/wiki/Fisher–Yates_shuffle
3. http://www.ollydbg.de/
4. Project URL: github.com/axper/shuffle-pe-section-names