MRLAB

**Address space layout randomization and Data execution prevention**

Azərbaycan Respublikası Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti - Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi - Malware Research Lab - F. Cəfərov - 29 aprel 2022

## Giriş

ASLR – yaddaşda icra olunan modulların adresini tələb edən bufer daşması hücumlarının yerinə yetirilməsini çətinləşdirən bir texnikadır. Bufer daşması proqram təminatında yaranan boşluqlardan irəli gəlir. Məsələn, tətbiq istifadəçisinin daxil etdiyi məlumatların gözlənilən uzunluğa uyğun gəlmirsə, bufer daşmasına gətirib çıxara bilər. İlk dəfə 2001-ci ilə "Pax Project" tərəfindən Linux əməliyyat sistemi üçün hazırlanıb. Windows əməliyyat sistemi isə 2007-ci ildə Vista versiyasından ASLR tətbiqinə başlayıb. Apple Mac əməliyyat sistemi üçün ASLR-i Mac OS 10.5 versiyasından tətbiq etməyə başlayıb. Apple İOS və Google Android isə 2011-ci ildən ASLR-in tətbiqinə başlayıb. ASLR daha yaxşı anlamaq üçün virtual yaddaş (**Virtual Memory**) haqqında məlumatımız olmalıdı.

## Virtual yaddaş

Virtual yaddaş, ikinci dərəcəli yaddaşın (misal üçün sərt disk) əsas yaddaşın bir hissəsi kimi istifadə oluna biləcəyi bir yaddaş idarəetmə texnikasıdır. Virtual yaddaş həm avadanlıq (hardware), həm də proqram təminatından istifadə edir. Virtual ünvan adlanan, proqram tərəfindən istifadə edilən yaddaş ünvanlarını fiziki ünvanlara uyğunlaşdırır. Faktiki olaraq proqramlar yalnız bir adres aralığın görürlər. Bir proqram, başqa proqramın yaddaşının görməsinə icazə verilmir. Bu proqramın işləməsini asanlaşdırır və təhlükəsiz edir. Proqramlar sadecə olaraq əməliyyat sistemindən əlavə yaddaş tələb edirlər. Proqram istifadə edildikdə, həmin proqramdan olan məlumatlar RAM istifadə edərək fiziki ünvanda saxlanılır. Yaddaş idarəetmə vahidi (MMU) virtual ünvanları fiziki ünvanlara tərcümə edir. (Şəkil 1)

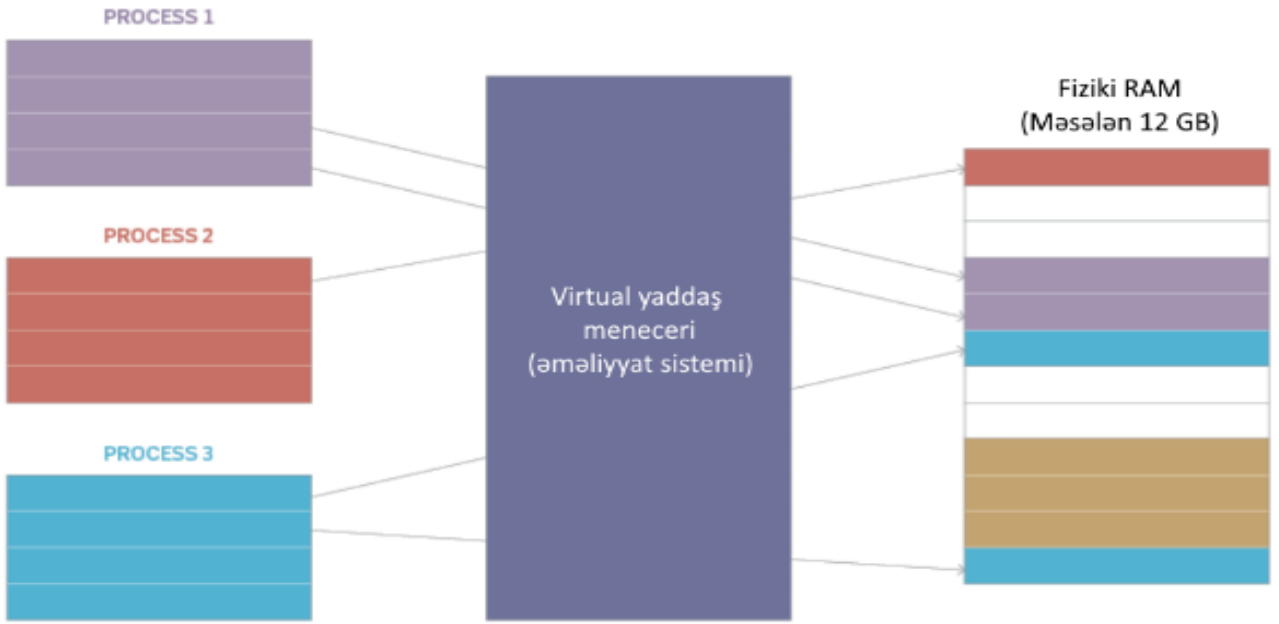
Virtual yaddaşın üstünlükləri:

- Bir neçə tətbiqi eyni anda istifadə etməyə imkan verir
- Proqramların bir birinin yaddaşlarına müdaxilə etməkdən qoruyur

- Fraqmentasiyaya ehtiyac yoxdur
- Shared yaddaşın idarə edilməyindən proqramı azad edir
- Əgər istifadədə olan proqramların istifadə etdiyi yaddaş olçüsü fiziki RAM ölçüsündən böyük olarsa, proqramların işləməsində məhdudiyyət qoymur

Virtual yaddaşın məhdudiyyətləri:

- Proqramlar virtual yaddaşdan işlıyirsə, daha yavaş işləyir
- Virtual və fiziki yaddaş arasında uyğunlaşdırılmalar əlavə apparat (hardware) dəstəyi tələn edir
- Kifayət qədər RAM olmadıqda kompüterin daha yavaş işləməsinə səbəb olacaq
- Mövcud sərt diskin həcmini azaldır




*Şəkil 1*

## Address space layout randomization (ASLR)

Daha əvvəl qeyd etdiyimiz kimi ASLR əsasən bufer daşması hücnumlarının reallaşmasını çətinləşdirmək üçün nəzərdə tutulub. Bufer daşması zamanı EİP reqistra şell kodun yaddaşdakı ünvanı qeyd olunur və JMP komandası ilə keçid olunur. Bu zaman ASLR modulların ünvanlarını təsadüfiləşdirir ki, buda JMP komandasına şel koda etibarlı çatmağa mane olur. Bu zaman kod icra olunmadan səhv qaytaracaq və proqram işini dayandıracaq. Əməliyyat sistemi yüklənən zamanı hər bir yüklənən modula əsas ünvan (base address) təyin olunur və ASLR qoşulu olan zaman hər dəfə əməliyyat sistemi yüklənən zaman bu adreslər yenilənir. Gəlin praktiki olaraq yoxlayaq. Process Explorer vasitəsilə IPHLPAPI.dll, kernel32.dll və KernelBase.dll əsas (base) ünvanına baxaq:

| Name | Base |
|---|---|
| IPHLPAPI.DLL | 0x73620000 |
| kernel32.dll | 0x75680000 |
| KernelBase.dll | 0x74C40000 |

Şəkil 2.

Daha sonra əməliyyat sistemini yenidən başladsaq və əsas ünvanların dəyişildiyini görəcəyik:

| Name | Base |
|---|---|
| IPHLPAPI.DLL | 0x738F0000 |
| kernel32.dll | 0x75490000 |
| KernelBase.dll | 0x74E40000 |

Şəkil 3.

İndi isə ASLR söndürüb test edək. ASLR söndürmək üçün registrdə **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management** ünvanında MoveImages dəyərinə (REG_DWORD) 0x00000000 mənimsədirik. Daha sonra əməliyyat sistemini yenidən başladırıq. Əməliyyat sistemi işə düşəndən sonra şəkil 2 və 3-də olan addımları təkrarlayırıq və nəticənin dəyişmədiyini görəcəyik:

| Name | Base |
|---|---|
| IPHLPAPI.DLL | 0x40C90000 |
| kernel32.dll | 0x77DE0000 |
| KernelBase.dll | 0x0DCE0000 |

Şəkil 4.

Şəkil 4-də əməliyyat sistemi işə düşəndən və yenidən başladılandan sonrakı modulların əsas ünvanların dəyişmədiyini görürük. ASLR exploytun yaddaş ünvana etibarlı şəkildə çatmasının qarşısını almaq məqsədi daşıyır. Bu hücumun müəyyən etmək məqsədi daşımır, sadecə hücumun gerçəkləşməsində çətinliklər yaradır. Yəni hücum cəhdləri haqqında heç bir məlumata malik deyil. Exployt səhv ünvana keçid etdikdən sonra davranışı qeyri-müəyyəndir. Proses istisna alıb dayana bilər.

## Data execution prevention (DEP)

DEP sistem səviyyəsində yaddaşın qoruması funksiyasıdır. Tətbiqi Windows XP versiyasından başlanıb. DEP sistemə bir və ya bir neçə yaddaş səhifələrinə (memory pages) icra olunmayan kimi qeyd etməyə imkan verir. Yaddaş səhifələrinin icra olunmayan kimi qeyd olunması, kodun yaddaşın həmin hissəsində icra olunmasının mümkünsüzlüyünü deməkdir. Əgər proqram orada kod icra etmək istəsə, yaddaşa girişin pozulması (access violation error) istisnası baş verəcək və procesin işini dayandırılacaq. Əgər kod qorunan yaddaşda icra olunmalıdırsa, bu zaman müvafiq virtual yaddaşın qorunması attributları yenidən təyin olunmalıdır. Yaddaşın attributları **PAGE_EXECUTE**, **PAGE_EXECUTE_READ**, **PAGE_EXECUTE_READWRITE** və ya **PAGE_EXECUTE_WRITECOPY** kimi qeyd edilməlidir. DEP, əməliyyat sistemi yüklənən zaman konfiqurasiya edilir. Konfiqurasiyanı əldə etmək üçün **Kernel32.dll**-də **GetSystemDEPPolicy** funksiyasını çağıraraq öyrənə bilərik (şəkil 5).

```
DEP_SYSTEM_POLICY_TYPE GetSystemDEPPolicy();
```

Funksiya **DEP_SYSTEM_POLICY_TYPE** tipli cavab qaytarır:

| | |
|---|---|
| **AlwaysOff 0** | DEP üçün aparat dəstəyindən asılı olmayaraq, sistemin bütün hissələri üçün sönülüdür. Yükləmə konfiqurasiya məlumatlarında PAE deaktiv edilmədiyi halda prosessor Windows-un 32-bit versiyaları ilə PAE rejimində işləyir. |
| **AlwaysOn 1** | DEP sistemin bütün hissələri üçün aktivdir. Proseslər üçün DEP deaktiv edilə bilməz. |

| | |
|---|---|
| **OptIn**<br>**2** | Aparat tərəfindən tətbiq edilən DEP, yalnız əməliyyat sistemi komponentləri üçün aktivləşdirilir. DEP seçilmiş proqram və ya cari proses üçün açıq şəkildə aktivləşdirilə bilər. |
| **OptOut**<br>**3** | DEP əməliyyat sistemi komponentləri və bütün proseslər üçün avtomatik aktivləşdirilir. Bu, Windows Server üçün standart parametrdir. DEP seçilmiş proqram və ya cari proses üçün açıq şəkildə aktivləşdirilə bilər. |

Cədvəl 1.

Gəlin python-da **GetSystemDEPPolicy** funksiyasın işə salaq:

```
>>> from ctypes import *
>>> windll.kernel32.GetSystemDEPPolicy()
2
```

Şəkil 6.

Şəkil 6-da alınan cavabı (2) cədvəl 1-dəki siyahıda tapsaq görərik ki OptIn cavabı ilə uyğun gəlir.

DEP funksiyasın söndürüb-yandırmaq üçün ardıcıllıq aşağıda göstərilən kimidir:

1. Sazlamalar (Settings) –> Sistem parametrləri (System) –> Sistem Qoruması (System Protection)
2. Açılan pəncərədə Advanced tabına keçirik.
3. Performance –> Settings:
4. Pəncərədə Data Execution Prevention tabına keçid edirik. Burada “Turn on DEP for essential Windows programs and services only” seçimində DEP-in yalnız əməliyyat sisteminin proqram və servislərinə tətbiq edilməsi seçimini görürük. Aşağıda isə “Turn on DEP for all programs and services except those I select” DEP-in bəzi proqramlar istisna olmaqla, bütün proqramlarına tətbiq edə biləcəyimiz seçim verilir.
5. Dəyişikliklərin qüvvəyə minməsi üçün əməliyyat sistemi yenidən başladılmalıdır.

**İstinadlar**

https://www.howtogeek.com/278056/what-is-aslr-and-how-does-it-keep-your-computer-secure/
https://www.ibm.com/docs/en/zos/2.4.0?topic=overview-address-space-layout-randomization
https://www.wallarm.com/what/what-is-aslr-address-space-layout-randomization