بررسی الگوریتم رمزنگاری پسورد های ذخیره شده ی وایرلس و دیکد آنها با خط فرمان powershell و زبان C

تقدیم به :

سازمان نظام صنفی رایانه ای استان کردستان

نویسنده : مسلم حقیقیان

ایمیل : moslem.haghighian@yahoo.com

وب سایت : wininfo.ir

Kurdistan ,sanandaj

1393

شاید بار ها و بارها برنامه های مختلفی رو برای اینکار دیده باشید به عنوان مثال ۲ برنامه ی زیر از معروف ترین آنها هستند

http://www.nirsoft.net/utils/wireless_key.html

http://securityxploded.com/wifi-password-decryptor.php

بعد از وارد کردن پسورد WIFI و ورود به آن تمامی آن پسورد ها در داخل فایل هایی با پسورد XML در داخل پوشه ی زیر ذخیره می شوند

C:\ProgramData\Microsoft\Wlansvc\Profiles\Interfac

در این فایل ها مشخصات هر WiFi نیز آورده شده محتویات این فایل ها به شکل زیر می باشد.

```
<?xml version=”1.0”?>
<WLANProfile xmlns=”http://www.microsoft.com/networking/WLAN/profile/v1”>
<name>Cisco</name>
<SSIDConfig>
<SSID>
<hex>436998736F3236312338</hex>
<name>Cisco</name>
</SSID>
</SSIDConfig>
<connectionType>ESS</connectionType>
<connectionMode>auto</connectionMode>
<MSM>
<security>
<authEncryption>
<authentication>WPA2PSK</authentication>
<encryption>AES</encryption>
<useOneX>false</useOneX>
</authEncryption>
<sharedKey>
<keyType>passPhrase</keyType>
<protected>true</protected>
<keyMaterial>0907A788C15949A010C2B54654f555dfg5666d6fg85858jh521f3</keyMaterial>
</sharedKey>
</security>
</MSM>
</WLANProfile>
```

همون طور که میبینید اطلاعاتی را می توان از طریق این XML فایل ها در مورد یک WiFi بدست آورد مانند Name , connectionType , connectionMode , authenticationو ... اما بحث اصلی در مورد مقدار keyMaterialاست که همان پسورد ما بوده منتها به صورت رمزنگاری شده است.

طریقه ی رمز نگاری با استفاده از تابع CryptProtectData انجام شده به شکل زیر

```
// Encrypt data from DATA_BLOB DataIn to DATA_BLOB DataOut.
//-------------------------------------------------------------------
// Declare and initialize variables.
DATA_BLOB DataIn;
DATA_BLOB DataOut;
BYTE *pbDataInput =(BYTE *)"Hello world of data protection.";
DWORD cbDataInput = strlen((char *)pbDataInput)+1;
//-------------------------------------------------------------------
// Initialize the DataIn structure.
DataIn.pbData = pbDataInput;
DataIn.cbData = cbDataInput;
//-------------------------------------------------------------------
// Begin protect phase. Note that the encryption key is created
// by the function and is not passed.
if(CryptProtectData(
&DataIn,
L"This is the description string.", // A description string
// to be included with the
// encrypted data.
NULL, // Optional entropy not used.
NULL, // Reserved.
NULL, // Pass NULL for the
// prompt structure.
,۰
&DataOut))
{
printf("The encryption phase worked.\n");
}
else
{
printf("Encryption error using CryptProtectData.\n");
exit(1);
}
```

خوشبختانه خود ویندوز تابع دیکدینگ این الگوریتم رمزنگاری را در اختیار ما گذاشته است . ما باید جهت decryptکردن آن از تابع CryptUnprotectData استفاده کنیم.

```
// Decrypt data from DATA_BLOB DataOut to DATA_BLOB DataVerify.
//-------------------------------------------------------------------
// Declare and initialize variables.
DATA_BLOB DataOut;
DATA_BLOB DataVerify;
LPWSTR pDescrOut = NULL;
//-------------------------------------------------------------------
// The buffer DataOut would be created using the CryptProtectData
// function. If may have been read in from a file.
//-------------------------------------------------------------------
// Begin unprotect phase.
if (CryptUnprotectData(
&DataOut,
&pDescrOut,
NULL, // Optional entropy
NULL, // Reserved
NULL, // Here, the optional
// prompt structure is not
// used.
,`
&DataVerify))
{
printf("The decrypted data is: %s\n", DataVerify.pbData);
printf("The description of the data was: %s\n",pDescrOut);
}
else
{
printf("Decryption error!");
}
```

اگر نوع رمزنگاری در سیستم به صورت WPA/WPA2 باشد باید اول آن را به دودویی تبدیل کنید و سپس می توانید مقادیر را با استفاده از تابع CryptStringToBinary به binary تبدیل کنید.

```
//
// Decrypt data from DATA_BLOB DataOut to DATA_BLOB DataVerify.
//-------------------------------------------------------------------
// Declare and initialize variables.
DATA_BLOB DataOut;
DATA_BLOB DataVerify;
LPWSTR pDescrOut = NULL;
//-------------------------------------------------------------------
// The buffer DataOut would be created using the CryptProtectData
// function. If may have been read in from a file.
//-------------------------------------------------------------------
// Begin unprotect phase.
if (CryptUnprotectData(
&DataOut,
&pDescrOut,
NULL, // Optional entropy
NULL, // Reserved
NULL, // Here, the optional
// prompt structure is not
// used.
```

سپس با استفاده از تابع CryptUnprotectData آنرا رمزگشایی کنید.

معمولا در برخی از سیستم ها پیش میاید که سیستم عامل به ما دسترسی کامل برای اجرای کد های خود را ندهد و Access Denied بدهد به همین خاطر شما می توانید کد را با سطح دسترسی بالا تری اجرا کنید و می توانید از تابع زیر استفاده کنید

```
int privileges(){
HANDLE Token;
TOKEN_PRIVILEGES tp;
if(OpenProcessToken(GetCurrentProcess(), TOKEN_ADJUST_PRIVILEGES | TOKEN_QUERY, &Token)){
LookupPrivilegeValue(NULL, SE_TCB_NAME, &tp.Privileges[0].Luid); //SE_TCB_NAME is to check
then set the exe as PART OF THE SYSTEM
tp.PrivilegeCount = 1;
tp.Privileges[0].Attributes = SE_PRIVILEGE_ENABLED;
if (AdjustTokenPrivileges(Token, 0, &tp, sizeof(tp), NULL, NULL)==0){
return 1; //FAIL
}else{
return 0; //SUCCESS
}
}
return 1;
}
```

با استفاده از فرامین CMD و powershell

خوب تا اینجا کد نویسی و طریقه ی ساخت آن را گفتیم اما فکر کنید که ما پشت یک سیستم قرار گرفتیم و دسترسی به هیچ کامپایلری نداریم ؟ خوب اینجا باید از طریق همان کد نویسی در ویندوز این کار را انجام بدیم من در اینجا از کد های powershell اینکار را با چند خط انجام میدیم.

اول از همه فرمانnetsh wlan export profile

```
PS C:\Users\Administrator\Desktop> netsh wlan export profile
Interface profile "moslem" is saved in file ".\Wi-Fi- moslem.xml" successfully.
Interface profile "l4tr0d3ctism is saved in file ".\Wi-Fi- l4tr0d3ctism.xml" successfully.
Interface profile "offsec" is saved in file ".\Wi-Fi- offsec.xml" successfully.
Interface profile "wininfo " is saved in file ".\Wi-Fi- wininfo.xml" successfully.
PS C:\Users\Administrator\Desktop>
```

حال به تعداد تمامی WiFi هایی که روی سیستم ورد آن شدید یک فایل XML که بالا گفته شد در مسیر جاری powershell ایجاد می شود . که همان فایل XML می باشد اما پسورد به صورت رمزنگاری شده می باشد اما نیازی به رمزگشایی نیست کافیست یک خط را به فرمان اضافه کنید تا کی ها را در داخل keyMaterialبه صورت Clear به ما نمایش دهد و خود سیستم عامل آنرا رمزگشایی کند . فرمان زیر

```
netsh wlan export profile key=clear
```

با وارد کردن این فرمان پسورد ها در داخل فایل XML به صورت clear به ما داده می شوند.

حال ما می خواهیم بعد از وارد کردن فرمان لیست تمام WiFi ها و Password ها را به صورت عادی و رمزگشایی شده به ما نشان دهد . پس یک پوشه در TEMP می سازیم و مسیر ذخیره شدن فایل های XMLرا به آن تغییر می دهیم.

```
new-item $env:TEMP\moslem -itemtype directory | Out-Null
netsh wlan export profile key=clear folder="$env:TEMP\moslem" | Out-Null
```

فرمان out-null هم برای این می زنیم که در حین ایجاد فرمان خروجی مربوط به این دستور به ما نشان داده نشود.

حال شما می تونید به داخل فایل های XML بروید و سپس پسورد را مشاهده کنید اما بهتر است که در داخل صفحه powershell به صورت گروه بندی شده تمامی لیست را برایمان بیاورد برای این کار باید فایل xmlرا باز کنیم و محتویات داخل آن را نشان دهیم از فرمان زیر استفاده می کنیم

```
New-Object PSObject -Property @{
WifiName = $data.WLANProfile.name
SSID = $data.WLANProfile.SSIDConfig.SSID.name
connectionType = $data.WLANProfile.connectionType
connectionMode = $data.WLANProfile.connectionMode
authentication = $data.WLANProfile.MSM.security.authEncryption.authentication
encryption = $data.WLANProfile.MSM.security.authEncryption.encryption
useOneX = $data.WLANProfile.MSM.security.authEncryption.useOneX
KeyType = $data.WLANProfile.MSM.security.sharedKey.keyType
protected = $data.WLANProfile.MSM.security.sharedKey.protected
Password = $data.WLANProfile.MSM.security.sharedKey.keyMaterial
}
```

و سپس برای اینکه این کار برای تمامی فایل ها انجام شود در C# از فرمان foreach استفاده می کنیم ولی در powershell از فرمان Get-ChildItem استفاده می کنیم.

```
Get-ChildItem $env:TEMP\moslem\*.xml | % {
$data = [xml] (gc $_)
New-Object PSObject -Property @{
WifiName = $data.WLANProfile.name
SSID = $data.WLANProfile.SSIDConfig.SSID.name
connectionType = $data.WLANProfile.connectionType
connectionMode = $data.WLANProfile.connectionMode
authentication = $data.WLANProfile.MSM.security.authEncryption.authentication
encryption = $data.WLANProfile.MSM.security.authEncryption.encryption
useOneX = $data.WLANProfile.MSM.security.authEncryption.useOneX
KeyType = $data.WLANProfile.MSM.security.sharedKey.keyType
protected = $data.WLANProfile.MSM.security.sharedKey.protected
Password = $data.WLANProfile.MSM.security.sharedKey.keyMaterial
}
Write-Host "-------------------------"
}
pause
```

در نهایت با کشیدن یک خط ـــــ مقادیر درون فایل ها را از هم جدا و سپس فرمان pause را می زنیم تا صفحه بسته نشود مانند system.consol.readkey() در#C کل کد به شکل زیر می باشد.

```
new-item $env:TEMP\moslem -itemtype directory | Out-Null
netsh wlan export profile key=clear folder="$env:TEMP\moslem" | Out-Null
Get-ChildItem $env:TEMP\moslem\*.xml | % {
$data = [xml] (gc $_)
New-Object PSObject -Property @{
WifiName = $data.WLANProfile.name
SSID = $data.WLANProfile.SSIDConfig.SSID.name
connectionType = $data.WLANProfile.connectionType
connectionMode = $data.WLANProfile.connectionMode
authentication = $data.WLANProfile.MSM.security.authEncryption.authentication
encryption = $data.WLANProfile.MSM.security.authEncryption.encryption
useOneX = $data.WLANProfile.MSM.security.authEncryption.useOneX
KeyType = $data.WLANProfile.MSM.security.sharedKey.keyType
protected = $data.WLANProfile.MSM.security.sharedKey.protected
Password = $data.WLANProfile.MSM.security.sharedKey.keyMaterial
}
Write-Host "-------------------------"
}
Pause
```

در این صورت دیگر نیازی به نوشتن کد های طولانی و یا استفاده از هیچ ابزاری نیست و می توانید با استفاده از اسکریپت نویسی در خود ویندوز این کار را انجام دهید خروجی به شکل زیر می باشد.

```
KeyType : passPhrase
WifiName : moslem
encryption : AES
Password : P4ssw0rd00
connectionMode : manual
protected : false
SSID : moslem
connectionType : ESS
useOneX : false
authentication : WPA2PSK
-------------------------
KeyType :
WifiName :felani
encryption : none
Password :passwordddddddd
connectionMode : manual
protected :
SSID : offsec
connectionType : ESS
useOneX : false
authentication : open
-------------------------
Press Enter to continue...:
```

موفق باشید

Author:moslem haghighian
Nike name: l4tr0d3ctism
Email: l4tr0d3ctism@gmail.com , moslem.haghighian@yahoo.com
Website: wininfo.ir
Microsoft security researcher and developer