آموزش اول-مهندسی معکوس چیست

به فرایند درک و بهینه سازی و تغییر در یک پروس کامپایل شده ی باینری را مهندسی معکوس میگویند،وقتی یک برنامه نویس با یکی از زبان های سطح بالا مانند (C++,VB) و خدایی نکرده (Delphi) ،ازآنجایی که کامپیوتر نمیتواند این کد ها را بفهمد، باید به زبان ماشین تبدیل شوند،البته کد های تبدیل شده به زبان ماشین ،مانند سورس کد اصلی ،خیلی قابل فهم نیستند ، و نیاز به تجربه و تفکر است که بتوان ذهن برنامه نویس حدس زد.

مهندسی معکوس در چه مواردی استفاده میشود؟

قطعا مهندسی معکوس استفاده های گوناگونی در علم کامپیوتر دارد که در اینجا سعی کرده ایم آن ها را دسته بندی کنیم :

۱- مکان اشکال زدایی برنامه هنگامی که سورس کد اصلی در دست رس نیست
۲- شکستن محدودیت های برنامه برای حفظ منافع مالی $$
۳-مطالعه و انالیز ویروس ها و بدافزارها
۴-ارزیابی کیفیت نرمافزار
۵-اضافه کردن و بهینه کردن قابلیت به نرمافزار

IRANLED.COM

در مورد دسته ی اول، که سورس کد در دسترس نیست بحث نمیکنیم چون هم خسته کننده هست و هم ،جهت دار با این مقاله نیست

دسته ی دوم، باید بگویم که بحث اصلی حول همین محور است که شامل :(عبور از انواع محدودیت ها،برنامه هایی با محدویت زمان،اجرا،رمز عبور،پنجره های مزاحم باشو) که البته مبحث کوچکی هم نیست

درمورد دسته سوم ،حقیقتی وجود دارد و آن این است که کنکاش برای رفتار شناسی صورت میگرد و بسیار هیجان انگیز هست ،اما خیلی درمبحث مهندسی معکوس نیست ،از طرفی نسبت به مهندسی معکوس دانش وسیع تری را میطبلد ،لذا از حوصله ی این مقاله خارج است

دسته ی چهارم ،بیشتر در محصولات بزرگ و تجاری مانند "سیستم عامل ها و برنامه های بزرگ" کاربرد دارد که توسعه دهندگان ویا متخصصان اطمینان حاصل یابند که محصول هیچ گونه آسیب پذیری یا نقص های امنیتی که به کرکر اجازه ی سوء استفاده دهد را ندارد

دسته ی آخر، اضافه کردن قابلیت به برنامه ،شخصا فکر میکنم که یکی از سرگرم کننده ترین و البته یکی از مهم ترین قسمت هاست،برای مثال آیا از گرافیک برنامه تان خوشتان نمی آید؟ تغییرش بدید ویا آیا میخواهید آیتمی به برنامه اضافه کنید؟انجامش دهید
در این سری آموزش تعدادی از این تکنیک ها را بررسی خواهیم کرد

پیش نیازها

خوشبختانه دانش زیادی برای شروع لازم نیست ،البته به شدت توصیه میکنم که حداقل با منطق برنامه نویسی و کمی از هر زبان آشنا باشید ،همینطور با نحوه ی کار کردن ابزارهای مهنوسی معکوس ،البته در طی این سری آموزشی با آنها آشنا خواهیم شد اما یک واقعیت موجود این است به دلیل گستردگی مباحث مهندسی معکوس و عدم دسته بندی آن روش یکپارچه ایی وجود ندارد لذا نیاز به عزم جدی و تلاش و آزمون خطا برای کسب مهارت و تجربه است، در هر چالش ما نکاتی را فرار خواهیم گرفت که مارا در کسب مهارت و تجربه بیشتر کمک میکنند

IRANIED.COM

در مهندسی معکوس چه ابزار هایی استفاده میشود؟

بسته به نوع هدف ابزار های متفاوت هستند اما به طور کلی سعی کرده ایم آنها را دسته بندی کنیم :

Disassemblers

برنامه‌ای است که زبان ماشین را به زبان اسمبلی ترجمه می‌کند، عملیات معکوس آن از یک اسمبلر است. یک دیس اسمبلر با دی کامپایلر تفاوت‌هایی دارد که هدف یک زبان سطح بالا به جای زبان اسمبلی است .جداسازی قطعات، خروجی از یک اسمبلر اغلب برای انسان فرمت بندی شده است_قابلیت خواندن به جای مناسب بودن برای ورودی به اسمبلر، آن را عمدتاً یک ابزار مهندسی معکوس می‌سازد.

یکی از این ابزارها IDA است که میتوانید از آدرس http://www.hex-rays.com آن را دریافت کنید

Debuggers

دیباگرها یکی از ابزار اصلی مهندسی معکوس است که درجهت اجرای دستورهای زبان اسمبلی و برای ایجاد، آزمایش، اجرا، تغییر و اشکال یابی برنامه، به زبان اسمبلی کمک میکند.

دیباگر های متفاوت و زیادی وجود دارند که میتوان به (*Immunity*

WINDBG,OllyDBG,X64DBG,) اشاره کرد

در این آموزشها از OllyDBG استفاده خواهیم کرد که میتوانید از آدرس http://www.ollydbg.de/

آن را دریافت کنید

Hex editors

Hex Editorها برنامه هایی هستند که با انها محتویات فایلها و دیسک ها را میتوان بـصورت بـاینری (در مبنای ۱۶ = hex)مشاهده و در صورت نیاز تغییر داد . در این برنامه ها هر بایت درون فایل بصورت یک عدد دورقمی در مبنای ۱۶ نمایش داده میشود.

PE and resource viewers/editors

هر فایل باینری (در سیستم عامل ویندوز و لینوکس) دارای یک بخش خاص در ابتدای آن است که ویندوز لودر هنگام بارگذاری فایل و مقدار دهی به آن رجوع میکند ،این اطلاعات شامل :

مقدار حافظه ی مورد نیاز

Dllهای مورد نیاز وغیره...

که مختصرا آن را PEیا Portable Executable میشناسیم ،در دنیای مهندسی معکوس درک ساختار فایل های اجرایی بسیار مهم و حیاتی است،ابزار های متنوعی برای نمایش ساختار این فایلها وجود دارد که من از CFF Explorer استفاده میکنم که میتوانید آن را از آدرس زیر دریافت کنید :

http://www.ntcore.com/exsuite.php

System Monitoring tools

گاهی اوقات (مطالعه بد افزارها و ویروس ها) ،نیاز ه رفتار شناسی داریم ،بدین معنی که هرحرکتی اعم از (دسترسی،ساهت،ویرایش،حذف) خارج از چهارچوب برنامه باید بررسی شود ،گاهی ممکن است یک برنامه مقداری را از ریجیستری ویندوز بخواند یا بنویسد که کلید حل مشکل باشد

ابزارهایی که میتواند در این قسمت به ما کمک کند :

ProceMon
Regshot
Process Explorer
Process Hacker

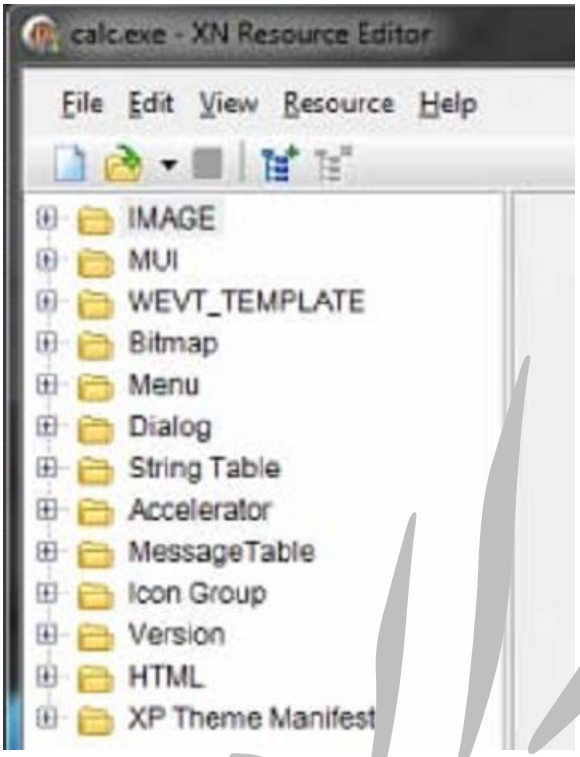
Miscellaneous tools and information

ابزار های شناسایی،مانند شناسایی نوع پکر و گاهی کمک در Unpack میتواند کمک کند

بیایید شروع کنیم:

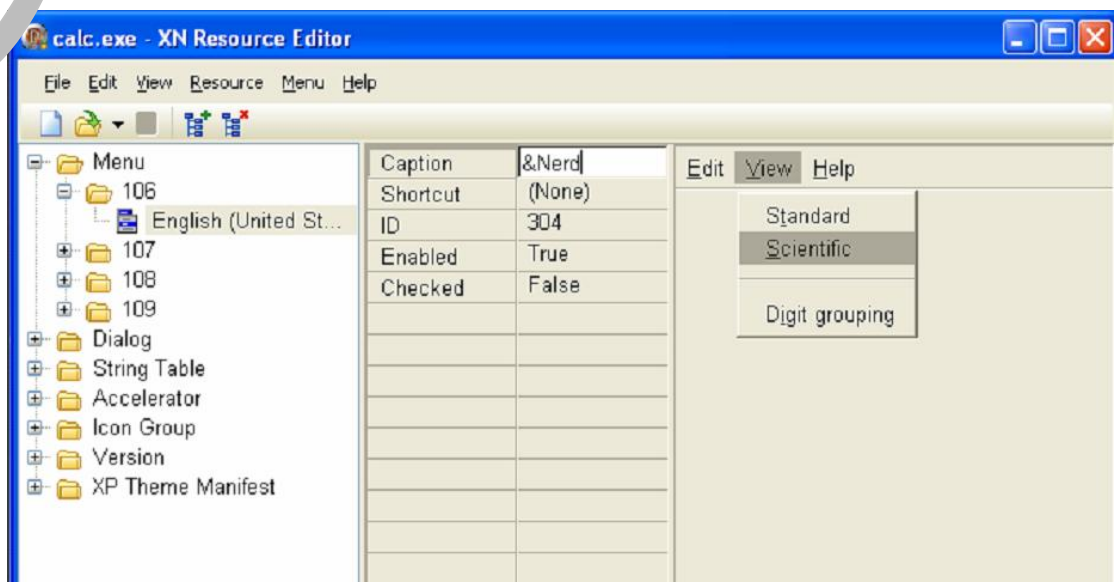
حتی اگر شما دانش اندکی درباره ی مهندسی معکوس داشته باشید میخواهم طعم آن را بچشید در این قسمت ما از یک ابزاری ریسورسر viewer/edit به نام XN Resource Editor استفاده خواهیم کرد،این برنامه میتواند فایل های اجرایی را ریسورس کند و تغییرات ظاهری در شکل برنامه (menus, icons, graphics, dialogs) ایجاد و ذخیره کند

بروی آیکن load کلیک کنید و فایل calc.exe واقع در \indows\System32\ را بارگذاری کنید

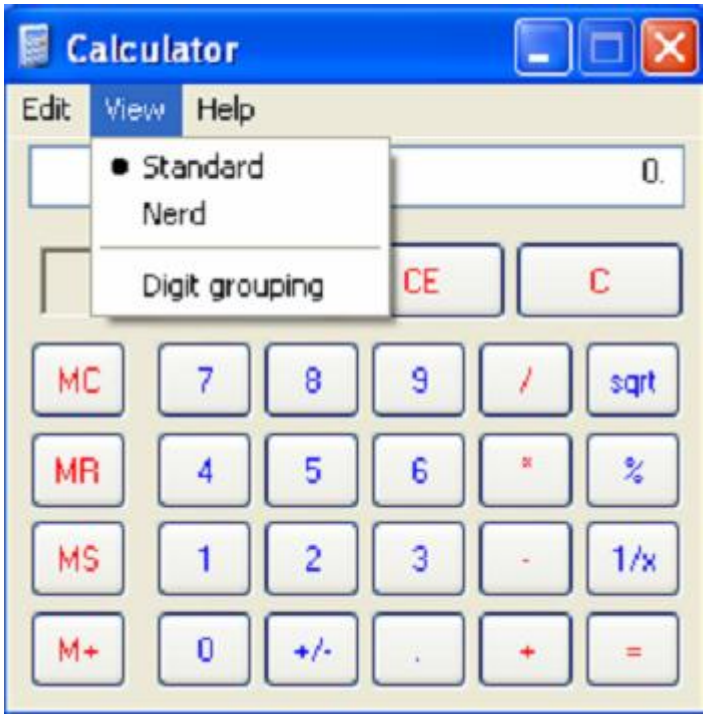


در شکل بالا شما هرنوع(گرافیک،منو،دیالوگ باکس و دکمه ها ،رشته ها،آیکن ها و...) استفاده شده در برنامه رو میتوانید ببینید

روی + از قسمت Menu کلیک کنید تا گسترش یابد،فولدری با یک عدد نمایش داده میشود که نمایانگر شناسه ی پنجره است،ویندوز با استفاده از این شناسه به ان دسترسی پیدا میکند، که حاوی "English (United States)" یا چیزی شبیه این است ،اگر روی آن کلیک کنید پنجره ایی در سمت راست خواهید دید:



حال بروی menu option کلیک کنید و "Scientific" را انتخاب کنید و Caption field حاوی مقدار "&Scientific" خواهد شد علامت & به معنای میانبر(hotkeys) است با جایگزین & در قسمت های دیگر عبارت ها مانند ("Sci&entific") میتوان کلید میانبرها(hotkeys) را تغییر داد

حالا عبارت &Scientific را به "&Nerd" تغییر بدهید به همین شکل تمام منو ها را به شکل دلخواه تغییر دهید (البته به یاد داشته باشید که کلید های میانبر باهم همسان نباشد) و تغییرات را ذخیره کنید

وسپس فایل را "Save As..." کنید و بانام دیگری ذخیره کنید :