突破常规玩电脑系列丛书

智美利达

怎么样，动心了吧？如果是，请赶快翻到目录页寻找你感兴趣的内容仔细阅读。相信我们，读完之后你一定不会失望的

COMPUTER 工具技巧大曝光

计算机技术研究组　总策划

精彩内容导读

- 轻松使用SoftICE
- TRW2000与W32Dasm无师自通
- CrackCode与eXeScope过关斩将
- Hexedit和OllyDbg技巧大曝光

【特别提示】

本书荟萃了众多破解名家的“不传之秘”，旨在与读者朋友进行经验交流，切勿用于其他目的

内蒙古大学出版社

突破常规玩电脑系列丛书

工具技巧大曝光

计算机技术研究组　总策划

内蒙古大学出版社

书　　名：突破常规玩电脑系列丛书（1-7）
编　　著：武新华
出　　版：内蒙古大学出版社（呼和浩特市大学西路235号 邮编 010021）
责任编辑：赵英
封面设计：南永夫
发　　行：全国各地新华书店
印　　刷：河南省瑞光印务股份有限公司
开　　本：850×1168　　1/32
印　　张：7
字　　数：215千字
版　　期：2003年9月第1版　2003年9月第1次印刷
标准书号：ISBN 7—81074—508—5/TP·27
印　　数：1—5000册
定　　价：112.00元（本册定价16.00元）

为什么购买这本书

这是一本有关计算机加密与解密问题的书籍。这本书既是写给普通电脑迷的，同时更适合那些孜孜于计算机软硬件程序的探索者——Cracker。

对于普通的电脑迷，阅读本书的意义意味着你再也不需面对日益繁多的共享软件而茫然无措。我们知道，你曾经为它们心动，因为你确实需要它们的帮助去驾御你的计算机世界；但很多时候你又非常无奈，你无奈于你的钱财，更无奈于对加密解密技术的无知以及由此导致的对你心爱之物的不可获得。与你相似的苦恼我们也曾经历，更深知援助之手在这一时刻所具有的意义。我们无法助你钱财，但有时候知识却远比钱财重要。这本书便具有这样的作用。

我们相信，有这样一本书置于你的案头，那许许多多在你过去看来难于登天的事情，你会突然发现却原来如此简单。

而对于更高一级的电脑玩家 Cracker 来说，阅读本书的意义却另有不同。去不断地探索未知，是每一个 Cracker 心目中永远的诱惑。作为一个 Cracker，注定了你与未知的对抗，而不能掌握一些必要的软件破解技术，是你无法忍受的羞耻。

的确，有那么多的共享软件，而你却不明白它们的程序原理，这是有辱于 Cracker 的称号的。当然，Cracker 的目的不是单纯地破解软件，而是通过跟踪软件了解程序思路，从而写出更好的程序。

破解也不在于数量多寡，关键是掌握方法，弄清注册码计算原理。本书中，我们集合了数十位破解高手苦心钻研出来的心得，提供了一般加密解密书籍都无法教你的秘技与妙招，我们相信，当你翻阅完这些 Cracker“老鸟”们轻易不会示人的“私藏秘典”，你也会很快地加入他们的行列。

本书就是这样一本讲解各种破解实例的教科书，这也是我们推荐你购买与阅读本书的理由。

目 录

第 1 章 破解杂谈：寻找破解的理由

- WAREZ 的无形帝国
- 寻找破解的理由

盗版软件在我国是如此的肆虐，而且是难以遏制，简直就成了顽症。那么是什么原因使得盗版软件不能被彻底铲除呢？

从表面上看是因为我国人均收入还太低，无力支付购买软件的昂贵费用。而从实质上看，是因为我国的软件破解者太少了，以致于使盗版软件有了众多的客户。

如果我国的软件破解者较多，这时盗版软件的客源较少，使得它没有了经营的余地，那么盗版软件也就会自行消失了。当然，就目前来说，我国打击盗版软件的工作还是任重而道远的。

1.1 WAREZ 的无形帝国

就我国，乃至全世界来说，谁也不敢说自己的个人电脑里没有一个软件是非法的呢？因为如果电脑软件全部通过支付金钱的方法获取正版软件的话，对于每一个电脑使用者，特别是游戏玩家等一类需要经常更新软件或经常尝试使用新软件的电脑用户，购买软件的开支是相当大的。可以说没有盗版软件，我国乃至世界的 IT 业就不会有这么快的发展速度，这么说似乎也并不夸张。

那么是谁制作了那些盗版软件？，您想了解他们的身份和来历么？想了解他们的组织结构和体系么？笔者是在一个偶然的机会下，了解到了这一切，现在就听我一一道来吧。

1.1.1 了解软件盗版组织

最早的软件盗版组织在 70 年代末 80 年代初就已经出现了，它的成员是一些青少年电脑爱好者，他们是运用自己的技术破解各类机中运行的软件（包括个人电脑和电

这个本是用来对软件进行调试、跟踪、除错的工具，在 Cracker 手中变成了最恐怖的破解工具；TRW 2000 是中国人自己编写的调试软件，完全兼容 Soft-ICE 各条指令，由于现在许多软件能检测 Soft-ICE 存在，而对 TRW 2000 的检测就差了许多，因此目前它成了很多 Cracker 的最爱。

此外，TRW 2000 较还 Soft-ICE 功能更强，它不仅专门针对软件破解进行了优化，在 Windows 下跟踪调试程序，跟踪功能更强；而且可以设置各种断点，并且断点种类更多；它还可以像一些脱壳工具一样去除加密外壳，自动生成 EXE 文件，因此它在破解者手中对共享软件的发展威胁更大。

它还有在 DOS 下的版本，名为 TR。对于 Soft-ICE 和 TRW2000 来说，有些操作都很相似，一般精通其中一个，就能举一反三，触类旁通了。下面就让我们来看一下 Soft-ICE 的安装设置与基本的操作。

Soft-ICE 是 Numega 公司出品的强大的程序调试工具，它可以运行在 DOS、Windows 3.1、Windows 9x/NT/2000/XP 等多种操作系统，是跟踪调试程序的有力的工具（以下讲述的是 Soft-ICE for Win 2k 版本，其他版本和它大同小异）。

1．Soft-ICE 安装及设置

Soft-ICE 的安装并没有什么特殊的地方，与一般的软件一样，运行 setup 进行安装。安装过程中会出现几个配置 Soft-ICE 的对话框，它们都可以以后通过开始菜单中相应的程序重新配置，所以后面只说明通过程序配置的步骤，其实与安装时的配置对话框是一样的。

① Display Adapter Setup 显卡配置

Soft-ICE 现在支持许多的显卡，选择一款想对应于系统的显卡后，选择 TEST，以了解你现在选择的显卡驱程是否与自己的显卡匹配，如果冒失地选择一个与你的显卡并不匹配的驱动程序，当进入 Soft-ICE 调试状态时将会花屏。

推荐把 Universal Vidoe Driver 这一项选上，这样 Soft-ICE 就会在一个窗口里弹出来，而不会切换到全屏（那样容易花屏，而且当调试时显示器不断地在字符和图形两种模式下来回转换，对显示器不好。）

② Mouse Setup 鼠标配置

鼠标配置也相当重要，Soft-ICE 支持在它的调试窗口中使用鼠标，这对已经习惯于鼠标的朋友来说当然会更加方便。并且它有串行鼠标接口与 PS/2 鼠标接口等选择。

③ Startup Mode Setup Soft-ICE 启动模式设置

Soft-ICE 启动模式设置是选择 Soft-ICE 在什么时候启动，其中有 4 个选项：

Boot：在 Windows 启动之前加载 Soft-ICE，这个选项非常强大，甚至可以让你跟踪 Windows 启动的代码，主要是用于跟踪调试等级与 Windows 核心一样的驱动程序，当然也可以调试所有的应用级程序。

System：与 Windows 一起启动，适用于跟踪调试 Windows 应用程序。

Automatic：自动启动，与 Windows 一起启动，适用于跟踪调试 Windows 应用程序。

Manual：手工启动，运行【开始】→【Soft-ICE】→【Start Soft-ICE】才启动 Soft-ICE，当然它不能调试内核驱动程序。

一旦加载了 Soft-ICE，只有重新启动计算机才可以“卸载”Soft-ICE。建议如果不是要调试内核驱动程序的话，最好选择 Manual，如选择每次启动 Widnows 时都加载 Soft-ICE，在不调试时，就很浪费资源还有可能造成系统不稳定。

④ Symbol Loader 符号加载器

在调试程序前必须要运行符号加载器。它的功能是通知 Soft-ICE 加载将要调试的程序，然后转换程序的调试符号表，使 Soft-ICE 能够在源码级上进行调试（这当然要求编译的程序是调试编译即 Debug Build 的）。

它主要有以下的操作命令：

Open：打开需要调试的程序，一般说有以下几种：用户级程序有*.exe，*.dll，*.OCX，*.vbx；内核级程序有*.sys（Win2K/nt），*.vxd，*.386，*.drv（Win Me/9x）。

Load：将所打开的程序加载。

Translate：将源码转换为 Soft-ICE 识别的 NMS 符号文件。如果你在编译或汇编时指定了 Debug Build（即调试编译），那么可执行程序中将包括函数输入输出符号表和源码路径等调试需要的信息，所以不需要特意指定你的源码路径，Soft-ICE 能够找到它。

LoadExpoffs：加载 32 位的输出动态文件，它包括驱动程序、win32 应用程序、dll 程序等。Load Exports 在调试没有调试信息的 dll 时格外有用。

Soft-ICE Initialization Setting：初始化 Soft-ICE 设置。我们可以在这里修改一些 Soft-ICE 预设的设置，像快捷键等。

还可以使用快捷键在 Soft-ICE 中代替一些常用命令，以下为预设的快捷键：

F1——显示帮助

F2——打开/关闭寄存器窗口

F3——切换当前源码的模式

F4——回到 Windows

F5——执行

F6——在命令窗口和源码窗口切换

F7——执行到光标所在行

F8——单步执行，如果调用过程，则跟踪进入进程

F9——在光标所在行设中断点

F10——单步执行，如果调用过程，则跳过过程

F11——执行到 SS：EIP

F12——从当前的过程中返回

Shift +F3——改变数据窗口内的数据的格式

Alt +Fl——打开或关闭寄存器窗口

Alt +F2——打开或关闭数据窗口

Alt +F3——打开或关闭代码窗口

Alt +F4——打开或关闭监视窗口

Alt +F5——清除命令窗口

2．使用 Soft-ICE 调试程序

现在来介绍一下调试程序的一般步骤：

首先要确认是否根据需要调试的程序（应用程序还是内核程序）而设置好了 Soft-ICE 的正确的启动模式。如果不是则需要运行【Soft-ICE】→【StartUp ModeSetup】重新设置。

使用 Ctrl+D 组合键调出 Soft-ICE 窗口，确认已经加载了 Soft-ICE 后，可以进行需要调试程序的加载。

① 打开 Soft-ICE+SymbolLoader 工具。

② 用【File】菜单中的【Open Module…】菜单项打开需调试的可执行文件。

③ 用【Module】菜单中的【Load】菜单项装载调试符号文件。如果目的文件并没有调试信息的话，Symbol Loader 会发出警告，只能够进行汇编级调试，而不可以进行源码级调试。

④ 用【Module】菜单中的【Translate】菜单项将需要调试的文件转换成 Soft-ICE 的 NMS 调试符号文件。

⑤ 现在调试文件的加载工作已经完成，可以按 Ctrl+D 组合键激活 Soft-ICE，加入断点，进行调试了。

⑥ 窗口一开始是有点小，所以可以先调整窗口，使用 lines X 命令可以将调试窗口设置为 X 行，使用 width X 命令可以将调试窗口设置为 X 列。

⑦ 使用 file 命令显示目前符号表中的源码文件，进而使用 file XXX.C 在源码窗口中打开 XXX.C 源码文件。

⑧ 使用 bpx XXX 来设置断点。XXX 为 XXX.C 文件中存在的函数。

⑨ 退出 Soft-ICE 窗口，执行需要调试的程序，程序执行到预先设置的断点处将自动进入 Soft-ICE 窗口，进行跟踪操作，这时就可以使用 Soft-ICE 中的各种命令来跟踪程序的流程。

下面对 Soft-ICE 一些常用命令进行说明。由于 Soft-ICE 中有在线的参数提示，所以在这里就没有提及各命令的参数。

① 窗口控制命令

如果能够使用鼠标的话，很方便就可以改变窗口的大小。

LINES 改变 Soft-ICE 窗口的显示行数

WIDTH 改变 Soft-ICE 窗口的显示列数

WL 打开或关闭局部变量窗口；设置局部变量窗口的大小

WR 打开或关闭寄存器窗口

WW 打开或关闭监视窗口或改变监视窗口的大小

WD 打开或关闭数据窗口或改变数据窗口大小

WC 打开或关闭代码窗口或改变代码窗口大小

CLS 清除命令窗口中的字符

DATA 显示另一个数据窗口

② 数据/代码监视命令

以下的命令是用来监视目前程序中的数据或变量的。

FORMAT 改变数据窗口的显示格式

DEX 在数据窗口中显示(或赋予)某个表达式

WATCH 加入一个变量到监视窗口中

LOCALS 从当前栈中列出局部变量

STACK 显示某个调用栈

③ Windows 系统信息命令

在调试程序的时候当然不能脱离调试的环境，所以就有了以下极其有用的命令用来显示目前 Windows 系统的内部状态。

GDT 显示全局描述符表

CLASS 显示 Windows 的类的信息

CPU 显示寄存器内容

HEAP 显示 Windows 全局堆

HWND 显示窗口句柄的信息

IDT 显示中断描述符表

LDT 显示局部描述符表

LHEAP 显示 Windows 局部堆

MOD 显示 Windows 模块列表.

PAGE 显示页表信息

PCI 显示系统中每个 PCI 设备的情况.

PROC 显示系统中所有进程的简要信息

QUERY 显示某个进程的虚拟地址映象

TASK 显示 Windows 任务列表

THREAD 显示线程信息

PHYS 显示某个物理地址对应的所有虚拟地址.

④ 跟踪调试控制命令

这里的大部分命令都是大名鼎鼎的 Debug 也有的，当然 Soft-ICE 已经将它们的功能大大加强了。

G 执行到某一地址

X 从 Soft-ICE 窗口中退出

HERE 运行到当前光标所在行

P 单步执行程序，在汇编模式中，当遇到 CALL，INT，LOOP，REP 指令时，P 将不跟踪进去，直到这些指令执行完毕，控制才返回 Soft-ICE。

T 单步跟踪

R 显示或更改寄存器的内容

S 在内存中搜寻特定数据

A 写入汇编代码

C 比较内存中两块区域的内容

D 用最后一次指定的形式显示内存

DB 以字节的形式显示内存

DW 以字的形式显示内存

DD 以双字的形式显示内存

E 用最后一次指定的形式编辑内存

EB 以字节的形式编辑内存

EW 以字的形式编辑内存

ED 以双字的形式编辑内存

F 填充某一块内存区域

U 显示反汇编后的汇编码

⑤ 断点命令

中断是 Soft-ICE 中重要的功能。中断点的触发可以由内存某地址的读取、内存范围的存取、程序的执行及端口的存取来达成。Soft-ICE 赋与每个中断点一个一位的 16 进制号码（0-F）。这个中断点号码是当你对中断点做启动、删除、中止、编辑等动作时使用。Soft-ICE 的所有中断点在启动后不会自动消失。

必须以 BC 或 BD 命令来消除或关闭它。Soft-ICE 一次最多可以处理 16 个中断点。同种类型的中断点最多可以有 10 个。但内存地址的中断点（BPM）因 80386 处理器之寄存器的缘故，最多只能设 4 个。设置中断点时可以设个计数参数。计数参数是中断点真正触发作用前被忽略的次数。

具体指令：

BPMBPMBBPMWBPMD——在内存地址被存取或执行时触发中断

BPR——对内存地址范围设置中断点

BPIO——对 I/O 端口存取时触发中断

BPINT——呼叫中断时触发中断

BMSG 在 WIN95 的消息上设置断点

BPX——设置/清除执行中断点

CSIP（16 位程序才有用）为所有断点设定一个界限（CS：EIP 在其内）（16 位程序）

BPAND——等待复合中断点的发生

BD——中止中断点

BE——启动中断点

BL——列出中断点

BPE——编辑中断点

BPT——把中断点当样板

BC——清除中断点

⑥ 内存/端口存取命令

Soft-ICE 甚至提供了在 Windows 下直接存取物理内存的能力，当然你得知道应该怎么用，否则就是号称永不死机的 Windows 2000 也会轻松崩溃。

I 从输入/输出（I/O）端口读入数据

O 向 I/O 端口输出数据

PEEK 从物理内存中读数据

POKE 向物理内存写数据

ADDR 在 Soft-ICE 中显示或是切换内存区域

⑦ 符号/源码命令

以下命令是对 Soft-ICE 中的源码及符号表进行操作的。Soft-ICE 可以一次将多个符号表装入内存。

Soft-ICE 支持 16、32 位 WINDOWS 程序，DLLs，VxDs，Sys 内核驱动程序. 但每一时刻只能从一个符号表中取得符号，你若是要用某个符号表中的符号，必须先用 TABLE 命令选中。FILE 则是用来选择当前显示的源文件。

源文件可以有 3 种不同的格式显示：源程序、反汇编代码及两者混和。使用 SRC 可以使它在这 3 种不同格式中切换。

FILE 显示或切换当前源文件

TABLE 显示或切换当前符号表

SRC 在源程序，反汇编代码，两者混和之间切换显示

SS 在源程序文件中查找字符串

EXP 显示 DLL 中的出口函数

SYM 显示或设置符号

SYMLOC 重定位符号基址

⑧ 其他操作命令

计算一个表达式的值，并以十六进制、十进制、带符号的十进制显示结果。当代码窗口可见时，此命令使得当前的 CS：EIP 所指向的指令可见，并且高亮显示

EXIT 强行退出 DOS 程序或 Windows 程序

1.1.2　反汇编工具 Win32dasm 和 Hiew

Cracker 常将 Soft-ICE 和 TRW2000 比作屠龙刀，将 Win32Dasm 8.93 比作倚天剑。Win32Dasm 能够同时支持 Windows 9x 和 NT 两个操作系统平台。Win32Dasm 8.93 是一个反编译工具，能够方便地反汇编程序。它不仅能静态分析程序流程，而且可以动态分析程序。Win32Dasm 8.93 版是在原有的普通版的基础上开发出的黄金版，它加强了对中文字符串的提取，这样对国产共享软件的威胁也就更大了。

例如开心斗地主这个共享软件，用 Win32Dasm 8.93 黄金版对其反汇编可以直接看到注册码，普通版则不能。

Hiew 是一个十六进制工具，它除了普通十六进制的功能外，它还有一个特色，能反汇编文件，并可以用汇编指令修改程序，用它修改程序，方便快捷！这也是 Cracker 们常用的静态反汇编工具。

下面来看一下 Win32dasm 的基本情况和操作初步。

上面我们已经讲到：Win32Dasm 是个反编译工具，它可以将应用程序静态反编译为 WIN 32 汇编代码。利用 Win32Dasm Cracker 们可以轻松地对程序进行静态分析，帮助快速找到程序的破解突破口，有时甚至可以直接用它来破解软件。

不过 Win32Dasm 只能对应用程序进行静态反汇编，如果原程序经过了加密变换处理或者是被 EXE 压缩工具压缩过，那么用 Win32Dasm 对程序进行反汇编就没有任何意义了。

Win32Dasm 不需要复杂的安装过程，直接将下载的压缩文件解压到目录下就可以立即使用了。

在主程序界面中选择【Disassembler】下的【Open File To Disassemble...】打开需要反汇编的程序就可以开始反编译了。

在对较大的应用程序进行反汇编时通常会耗费不少的时间，为了能保存 Win32Dasm 反汇编的结果，便于下次查阅而不用再次进行重复反汇编，可以选择【Disasserhbler】下的【Save Disassembly Text Fileand Create Project File】选项将结果存到文件中，下次需要打开时可以用【Project】下的【Open Porject File...】打开所保存的反汇编结果。

分析程序时经常需要搜索程序中的特定字符串，了解字符串被调用的情况，这时选择【Search】下的【Find Text】就可以了，【Find Next】（或按功能键 F3）能帮助找

到程序中其它调用此字符串的地方。

【Goto】菜单下提供了4种快速跳到指定程序地方的功能：Goto Code Start——跳到程序代码开始处，快捷键为CTRL+S；Goto Program Entry Point——跳到程序进入点，快捷键为F10；GotoPage——跳到指定页，快捷键为F11；Goto Code Location——跳到指定地址代码处，快捷键为Shift+F12，用得比较多的是"Goto Code Location"，即跳到指定地址代码处，在Win32dasm中按住SHIFT+F12即可。其中需要输入的代码地址"Code Offset（Hex）"和Softice中显示的代码地址一样。

【Functions】下的【Imports】功能显示了反汇编程序中所调用到的WIN32API函数。双击指定的行可以直接跳到程序中这个WIN32API函数被调用的代码处。

"HexData"下的"Hex Display Of Data Objects/Segments"和"Hex Display Of Code Data"可以分别查看十六进制形式的数据段和代码段数据。

【Refs】菜单对于程序的分析是很有用处的，【Menu References】显示程序中的菜单资源，【Dialog References】显示程序中的对话框资源，【String Data References】显示程序中的字符串资源。

【Refs】菜单下的各个功能中都可以通过双击鼠标跳到指定行资源被调用的代码地址处，其中【String Data References】是最有用的，可以通过查找程序中出现的特定字符串，从而快速跳到可疑字符串被调用的代码处，分析程序的运行机制。

1.1.3 Visual Basic 程序调试工具 SmartCheck

SmartCheck是一个针对Visual Basic程序的调试程序，由于Visual Basic程序执行时从本质上讲是解释执行，它们只是调用VBRUNxxx.DLL中的函数，因此VB的可执行文件是伪代码，程序都在VBXXX.DLL里面执行。

若用Soft-ICE跟踪调试只能在dll里面用打转转，看不到有利用价值的东西，而且代码质量不高，结构还很复杂。当然只要了解其特点用Soft-ICE也可破解，但SmartCheck的出现，为Cracker破解软件提供了极大的方便。SmartCheck是NuMega公司出的一款出色的调试解释执行程序的工具，目前最新版是6.03。

它非常容易使用，甚至不需要懂得汇编语言都能轻易驾驭它。它可将Visual Basic程序执行的操作完全记录下来，使破解者轻而易举的破解大部分Visual Basic程序。

下面是SmartCheck的基本用法。