Reverse code engineering

Powerfull tool, lot of fun and legal for several purposes! We will work with OllyDbg (www.ollydbg.de) program that is easy-to-use disassembler and debugger.

- Basic information available in Wikipedia article on reverse engineering (IS copy REWiki.pdf)
- Download OllyDbg 1.10 (freeware) either from http://www.ollydbg.de/ or (better) from IS (OllyDbg.zip).
- Download tutorials I and II. by Lena from IS (tut1.rar and tut2.rar). Remaining tutorials can be obtained from www.tuts4you.com.
- Download Assembler basics from IS (BasicsOfAssembler.pdf).
- Download homework crackme (LabakCrackMe).

OllyDbg shortcuts & most important commands

F3 ... Open binary file
F2 ... Toggle breakpoint (on opcodes, or double click)
F9 ... Run debugged program
Ctrl+F2 ... Restart program
F8 ... Step over
F7 ... Step into
Spacebar or double click ... allows to set new opcode
Alt+BkSp ... Undo change
Rightclick->Search for->All referenced text strings ... Constant text strings referenced in code.
Rightclick->Find references to->Address constant ... will find references to particular memory elsewhere in the code – use when you like to know where the memory is set or changed.
Ctrl+F1 ... Help on API (WIN32 API help file already prepared in OllyDbg directory (WIN32.HLP))
; ... add or edit your comment for specific code line

Registers (FPU): Z – zero flag, C – carry flag, S – sign flag. Invert bit flag by double click.
EIP ... next address to execute (instruction pointer)
EBX ... usually loop counter

Startup resources

The Reverse Code Engineering Community: http://www.reverse-engineering.net/
Tutorials for You: http://www.tuts4you.com
RE on Wikipedia: http://en.wikipedia.org/wiki/Reverse_engineering

Homework

The goal of this assignment is to reverse engineer supplied crack me file (LabakCrackMe.exe), obtain information about its behavior and make program to continue successfully without error message by a) patching, b) creating valid license

info. More principally different solutions for the same problem will be awarded by extra points.

Hints:
- You may use OllyDbg or any other disassembler.
- Function *fread* fail by null exception if invalid file handle is supplied.

Submit:
- Short description of program behavior in text form or as **annotated** C source code (not only output of some disassembler) (source code version will be awarded by 1 extra point).
- Patched crack me binary that let the program run every time successfully with no error **without** valid license info.
- Valid license info that let program run successfully **without binary modification**.
- Deadline is 15.5.2009{10 points + bonuses}