PB173 - Tématický vývoj aplikací v C/C++ (podzim 2012)

Skupina: Aplikovaná kryptografie a bezpečné programování

https://minotaur.fi.muni.cz:8443/pb173_crypto

Petr Švenda, *svenda@fi.muni.cz*
Konzultace: G201, Pondělí 16-16:50

Reverse engineering

- Art of discovering principles through analysis of structure, functions and operation
- Legality
  - Own binary without documentation
  - Interoperability
  - Anti-virus research
  - Fair use, education
  - Forensics
- Problem with recent copyright laws
  - even attempt to circumvent is illegal
  - not only selling circumvented content

Disassembler vs. debugger

- Static vs. dynamic code analysis
- Debugger vs. Debugger with advanced modification tools (Visual Studio vs. OllyDbg)
- Assembler vs. bytecode
  - Instruction set
  - Register-based vs. stack-based execution

Lena tutorials

- Nice introduction tutorials for reversing/cracking
- Win32 binary
  - Lena tutorials 1 and 2
- Základy assembleru
- Name of the registers
  - (EAX 32bit, AX 16bit, AH/AL 8bit)
- Registers (FPU):
  - Z – zero flag, C – carry flag, S – sign flag
  - EIP ... next address to execute (instruction pointer)
  - EBX ... usually loop counter
- OllyDbg - zkratky, hinty

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

Practical assignment 1

- Reverse engineer file PB173CrackMe.exe
  - obtain information about its behavior
  - make program to continue successfully without error message
  - a) patching (binary modification)
  - b) creating valid license info (no binary modification)
- Provide short description of program behavior in text form or as **annotated** C source code
  - not only output of some disassembler
- Prepare patched crack me binary that let the program run every time successfully with no error even **without** valid license info
- Prepare valid license info that let program run successfully **without binary modification**

Practical assignment 2

- Prepare final demonstration for your project
  - will takes place 11.12.2012
  - 10-15 minutes every team
  - architecture and its change during projects
  - highlight problems
- + Finalize your code
  - otherwise no points will be awarded