Fun with Bin Patching

Andrew Zonenberg, Alex Radocea

Tools of the trade

- Hex editor. I personally use ICY Hexplorer (http://sourceforge.net/projects/hexplorer/). Other good tools: hte, gdb -write
- gdb

x86 machine code: Conditionals

- Common conditionals:
  - 0x 7? xx
  - 0x 0f 8? xxxxxxxx
- Flip the low order bit of a conditional to invert it
  - 0x 74 = jz xx
  - 0x 75 = jnz xx
  - 0x 0f 82 = jc xxxxxxxx
  - 0x 0f 83 = jnc xxxxxxxx

Other useful opcodes

- 0x90 (nop). Does absolutely nothing.
- 0xEB FE (jmp -2).
- 0xC3 (ret). Returns from the current function.
- 0xCC (int3). Triggers a software breakpoint.

Basic procedure

- Find targets
- Patch
- EB FC