InlineEgg Changelog

v1.08 - Nov 17, 2004

- fixed a bug in Variable (leading to a bug in IfInlineEgg)
- added long conditional jumps
- setString() now uses a call over the string and pop to set the string when the string is long enough to justify it - thanks spoonm

v1.07 - Sep 1, 2004

- inner eggs can now inherit syscall's symbols (useful for WindowsSyscall)
- added paramer leave to freeStack() (how many words to leave in the stack)
- fixed a bug which was unbalancing the stack
- renamed setVarPtr() to setRegFromVarPtr()

v1.06 - Jun 16, 2004

- added iadd() to InlineEgg. Now, instead of doing egg.addCode(X) you can do egg += X. Which leads to cleaner and nicer code :-)
- added subValue() and addValue() to Microx86, you can do egg += egg.micro.addValue('eax',1234), for example

v1.05

- example1.py, README and InlineEgg.html
  - changed it to execute "/bin/ls -la" instead of "/bin/sh -i". Now it's easier to test.

v1.04

- Microx86:
  - incReg and decReg track the changes in the registers. This is a bug fix, not only an optimization: incorrect tracking was introducing bugs when assuming incorrect values for registers.
- InlineEgg, Linuxx86Syscall, OpenBSDx86Syscall:
  - inet_addr and make_sockaddr moved from InlineEgg to the OS dependant lasses, because there are differences from os to os. Solaris implementation is still missing (I just forgot to do it).
- InlineEgg:
  - fork() just a comment
  - write() suggestion from Philippe Biondi, write() can be used with just two arguments, in which case the count to write is len(buf)
  - fcntl() added
  - ptrace() fixes in handling arguments
  - prctl() added
  - added a way to call any syscall if it's defined in the syscall class (read the code for InlineEgg.getattr())

v1.03

- WindowsSyscall:
  - added the method initResolver(), which will walk the linked lists of loaded modules to find the adresses of kernel32.dll, GetProcAddress() and LoadLibraryA().

v1.02

- WindowsSyscall:
  - fixed a missing microClass field

v1.01

- Makefile: added $(VERSION)
    - added Changelog
    - added InlineEgg.html
- inlinegg: added Syscall.microClass
    - removed microClass from InlineEgg.init()
    - added Microx86.nop()
    - added InlinEgg.dumpBin()
    - renamed InlineEgg.popReg() to pop(), and fixed a bug in it.
    - added Microx86.pushString(), this makes InlineEgg.save() work with strings
- examples:
    - added example6.py (getAndExecuteEgg(). It will download a file from a URL, save it and execute it.