Universal Decompiler: Open Source By Force

John McMaster

RCOS

3/26/10

Project Goals

Architecture retargettable decompile
Geared towards embedded platforms (8051, BlackFin, ARM, etc)
Architectures can be defined through a config file or through a loadable module
Repurpose the Candela laser!

FLAIR/FLIRT Background

"Fast Library Identification and Recognition Technology"

"FLAIR is a collection of tools for generating library function signatures which are later used by IDA to identify library functions in statically compiled binaries"

http://www.phreedom.org/research/reverse-challenge/analysis.html

Used as synonyms, but technically FLIRT technology, FLAIR toolkit

Semester Milestones

GOAL: FLIRT compatibility layer
1: obj2pat: object file to editable .pat file
2: pat2sig: .pat file to binary .sig file version
3: misc assembly (IR) engine enhancements

Current progress and goals

- obj2pat
  - libbfd based implementation based on modified rpat
  - partial implementation based on config files
- Improved command line process
  - Scales: multiple executables, large number of args
- Memory leaks: learned to use Valgrind
  - Some hard leaks still present, but much better
- Unit testing: some basic CppUnit unit tests
- Figuring out some of the legal stuff

Questions?

Thanks to Sean O'Sullivan and RCOS for funding the development of this project!