Universal Decompiler: Open Source By Force

John McMaster
RCOS
2/??/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...FLIRT technology, FLAIR toolkit I guess

Semester Milestones

- GOAL: FLIRT compatibility layer
- 1: elf2sig: ELF libraries/object files to
- 2: coff2sig: Windows PE analysis?
  - The IDA tool has similar name...should rename?
- 3: auto2sig: automatically use right tool

Current progress and goals

- Moved core code into a library
- Improving command line process
  - Need to keep same core arguments across multiple programs
  - Want to use a property based approach at core with traditional --/- names for common args
- Reworked build system with placeholder projects for each of the desired tools
- Basic research on ASCII format files

Questions?