Universal Decompiler: Open Source By Force

John (n' Alex?)
RCOS
12/11/09

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!

Milestones

- 1: Config file retargettable disassembler (DONE)
- 2: Static function analysis: nearly finished
- 3: Basic assembly -> C
- 4: Advanced control flow analysis (ie for loops, more intelligent conditionals)
- 5: Add more processors and analysis features

Status as of last presentation

- Tests currently implemented at 8051 (80C32)
- Retargettable disassembler
- Basic assembly analysis
- Some R&D on function signature analysis

Static function analysis: relocatable objects

- Convert to the form used in .o files before linking into executable
- Literally making ELF .o files since it allows processing by bintools (ld and friends)
- Supporting data will either go in config file or embedded in the object file
- Resulting file could also be hashed

Static function analysis: symbol analysis

- (unstable) support for getting relocations from simple instructions:
- NAME=LCALL
- ...
- ACTION=CALL(u16_0)
-
- But not (yet):
- NAME=ACALL
- ...
- ACTION=CALL(%PC&0x1F00+u8_0+0x0000)

Demo and then ????