uvudec: Open Source By Force

John n' Alex
RCOS
10/16/09

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 (in progress)
- 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: brute force

- Binary function comparison
- Copyright issue: requires distributing binaries to other people for them to make same comparisons you are
- Every possible variation of function is requires for successful analysis
- May require statistical byte matching to get any reasonable results

Static function analysis: hash

- Supported analysis technique
- Currently using libc MD5 implementation
- Fast comparisons
- Gets around copyright issues from distributing binaries you don't have right to

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

Distributing analysis files

- Ideally would like to distribute as .tar.bz2 or similar archives so easy to manipulate and compressed
- Archives will simply be collection of the binaries and supporting data used for analysis
- Archives could also include processor support files

Generating analysis files

- Template files can be generated from a given executable
- Tools like ld and text editors can be used to shape them to more friendly forms (combine into CRT, add source code, etc)
- Will add utilities to aid in analysis DB creation as they are needed

????