

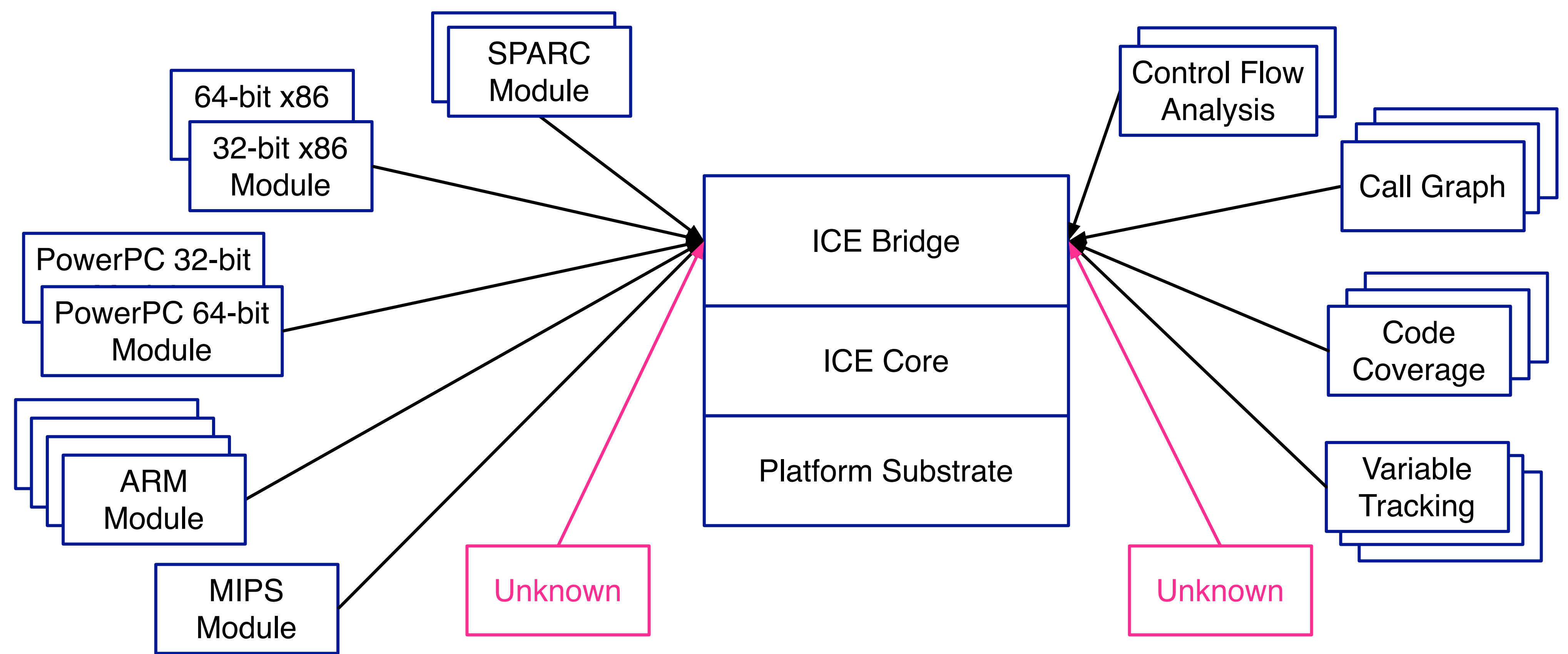
ICE: Circumventing Meltdown with an Advanced Binary Analysis Framework

The Need for Extensibility

Without extensibility, binary analysis tools are unable to adapt to the fluid world of software.

Binary analysis tools must be extensible in three key areas:

- Instruction set architectures
- Software platforms
- Analysis techniques



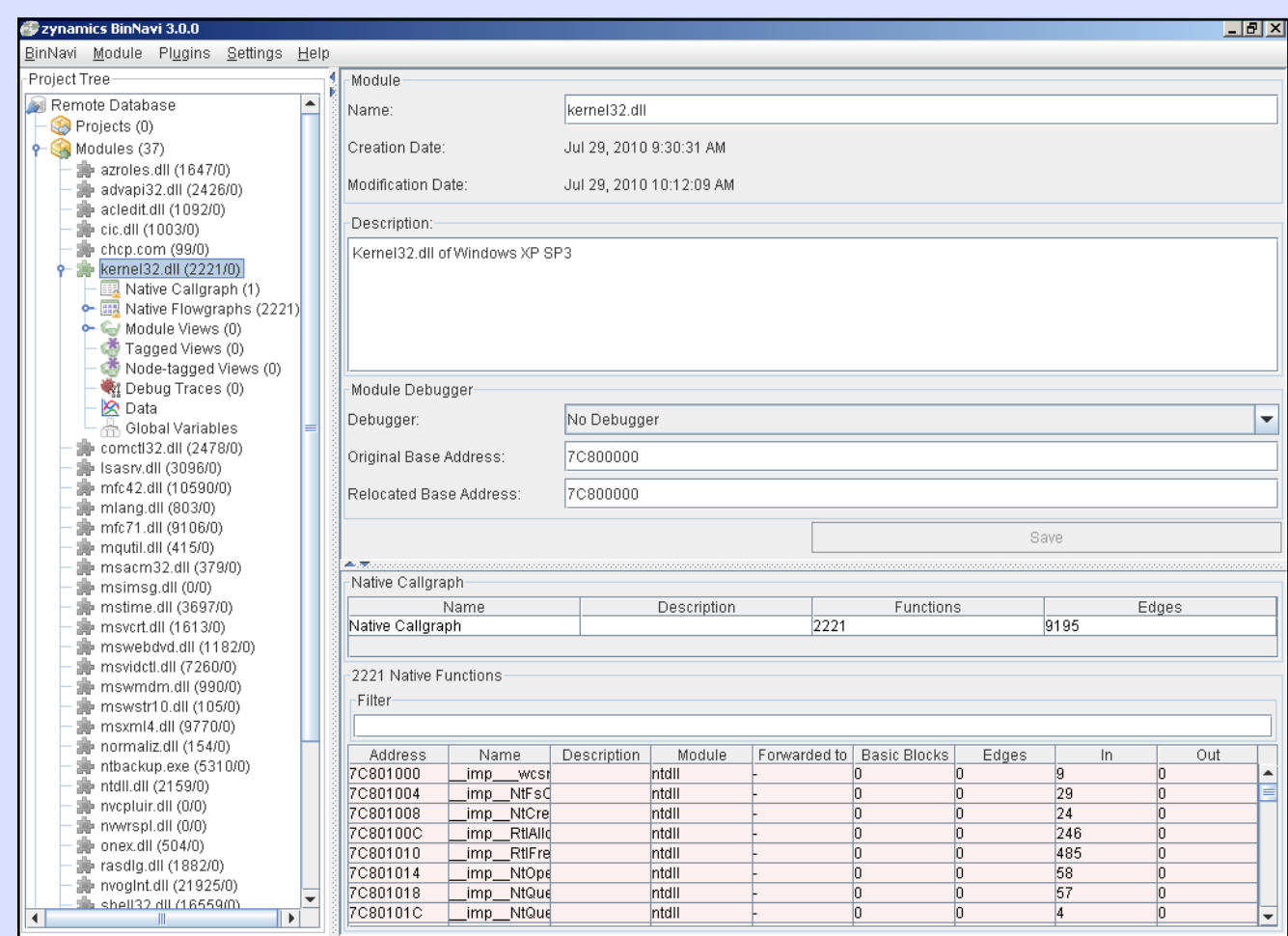
How do you understand the unknown?

Related Work

Evaluation Criteria for Binary Analysis Frameworks

1. Extensibility
2. Platform Independence
3. Static Analysis Tools
4. Dynamic Analysis Tools
5. Reliability of IL Translation
6. Architectures Supported
7. Instruction Set Completeness
8. Ease of Use & Documentation

BinNavi



Pros

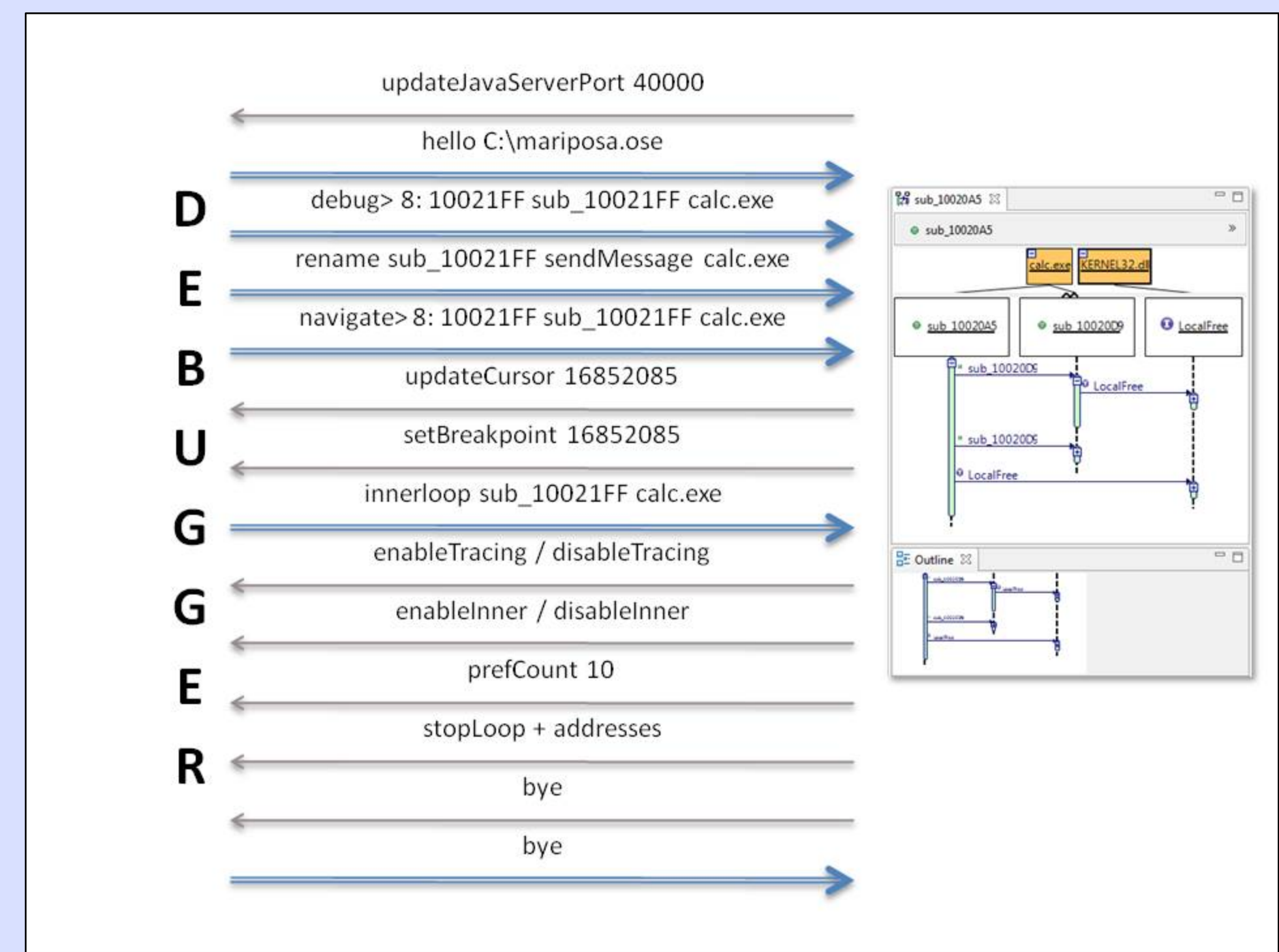
- Extensible
- Platform independent
- Visual static analysis tools
- Commercial product
- Clean GUI
- Excellent documentation

Cons

- Dynamic analysis is not feasible
- No support for IBM architectures
- No support for floating point, MMX or SSE
- No support for privileged instructions

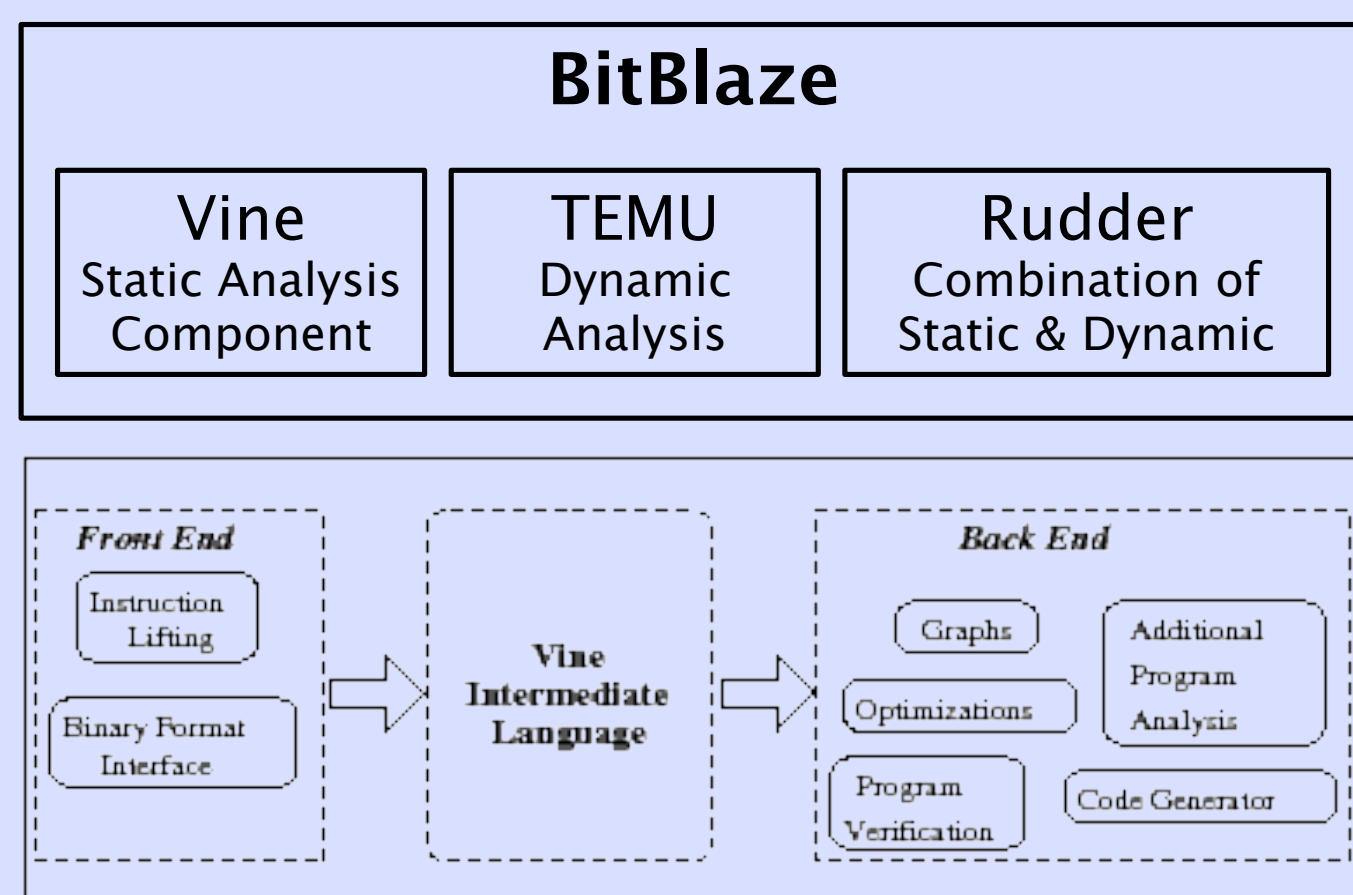
Current Progress

Tracks



- Leverages information provided by a debugger
- Enables dynamic analysis and navigation
- Integrates with Eclipse
- Communication between debugger and Eclipse plug-in uses the Tracks protocol
- Able to analyze several binaries simultaneously
- Able to analyze multithreaded binaries

BitBlaze



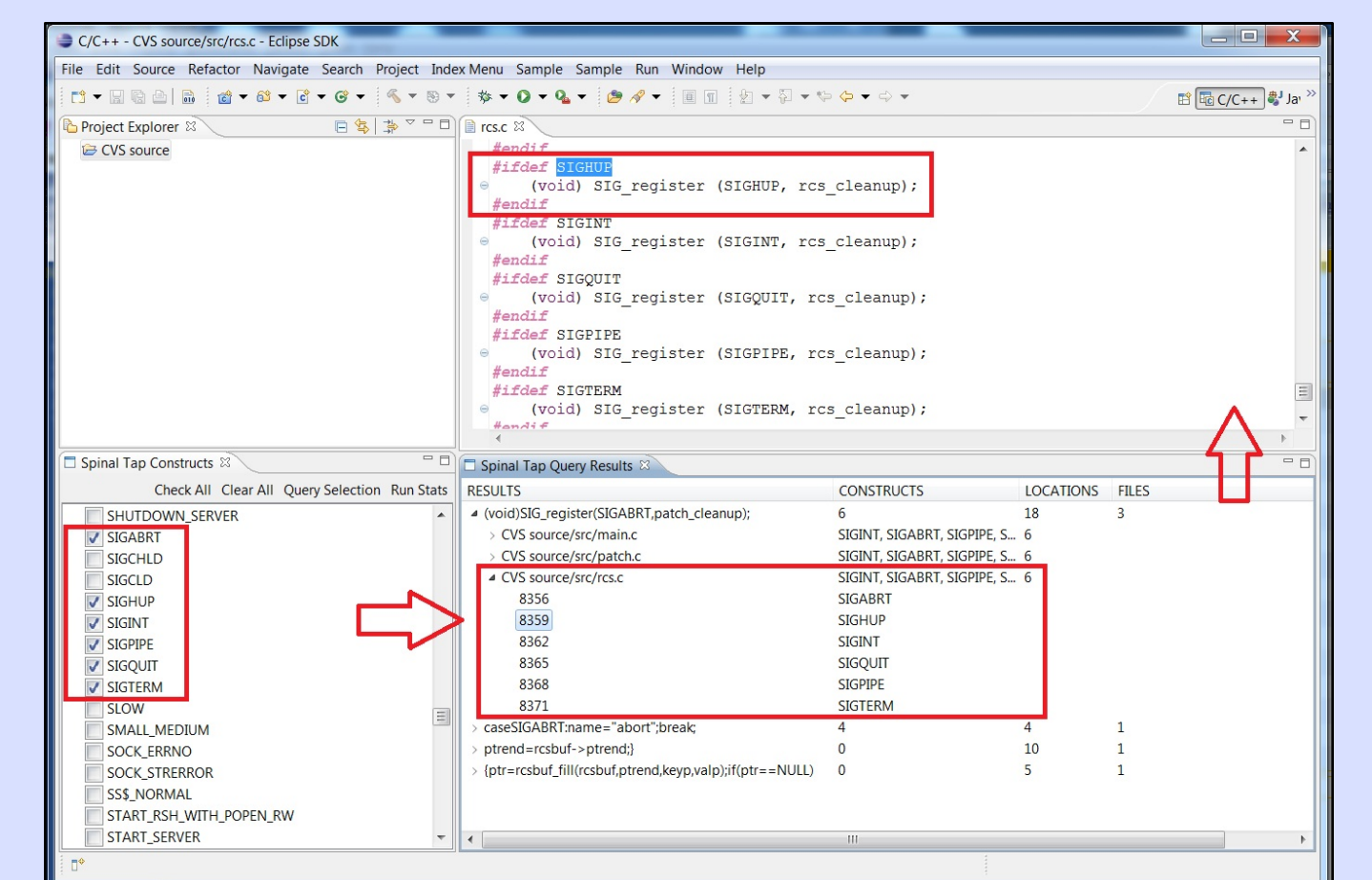
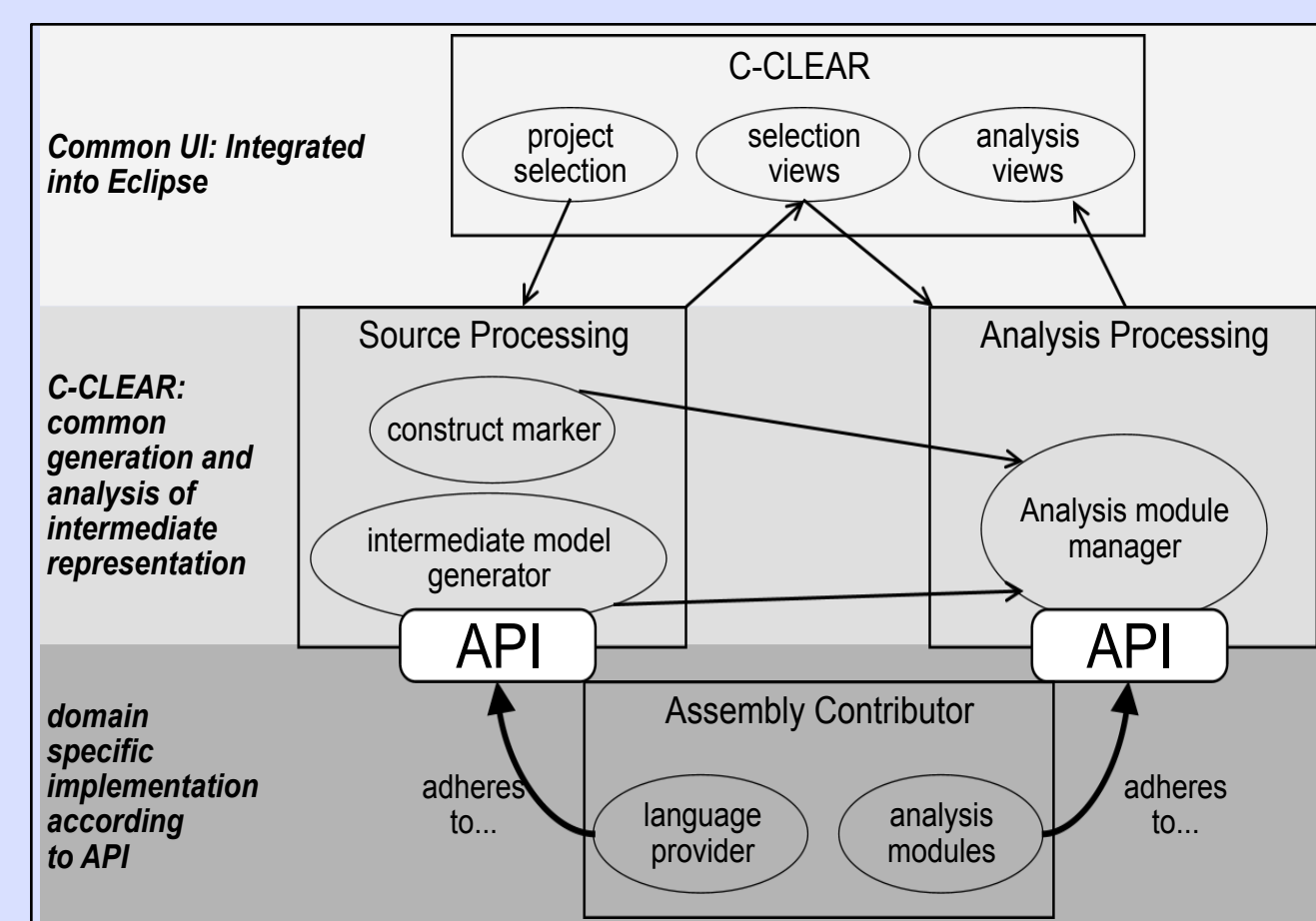
Pros

- Supports static analysis
- Supports dynamic analysis

Cons

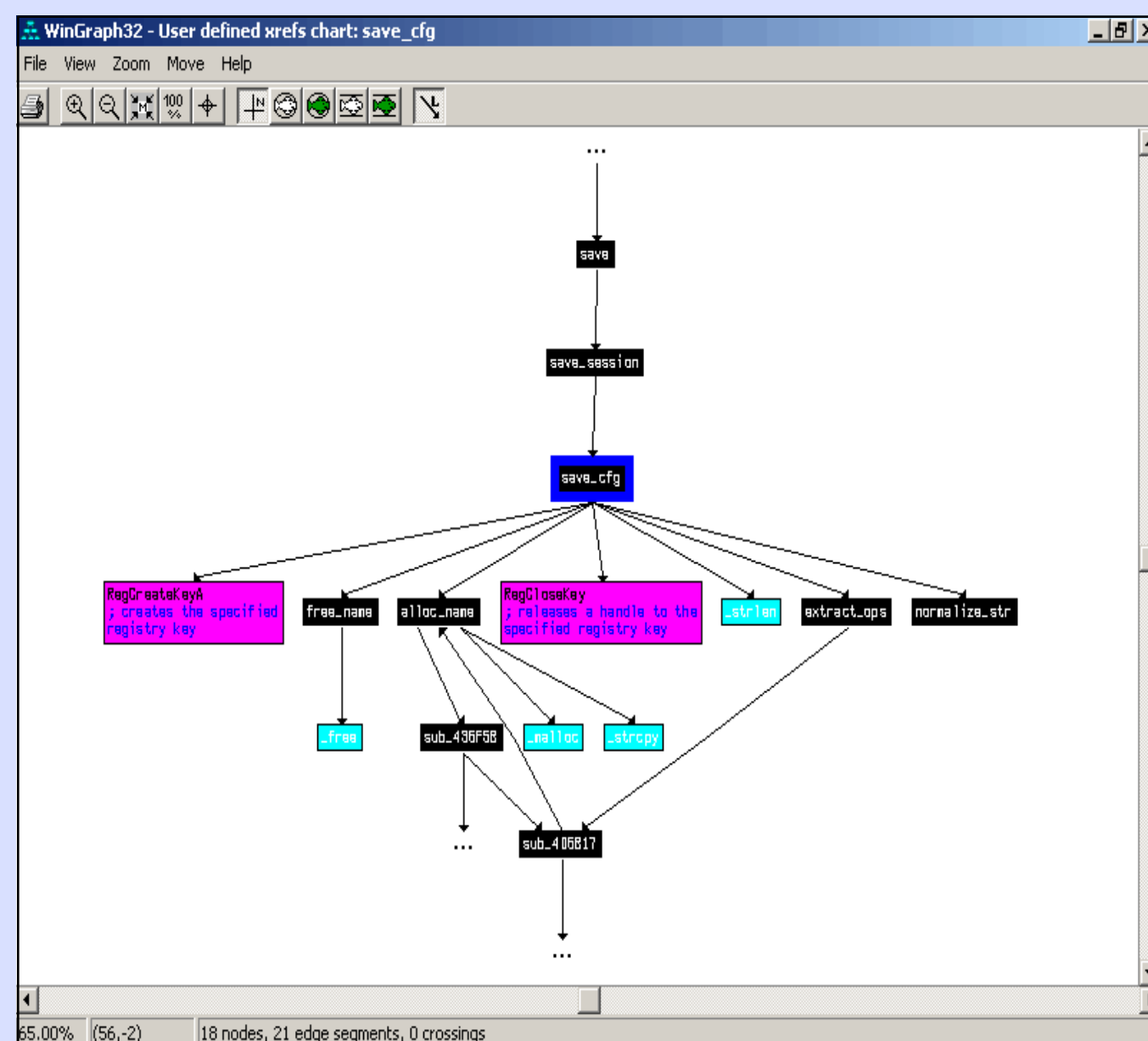
- Extensible only in terms of analyses
- Platform dependent
- No GUI
- Several translations to generate IL
- Only 32-bit x86 is supported
- Must define external function calls
- Unclear documentation
- Intricate third-party dependencies

C-CLEAR



- Integrated with Eclipse
- Common UI for selecting analysis and viewing results
- Intermediate model defined as a Syntax Tree
- Assembly Contributor provides tokens and other information required for analysis

IDA Pro



Pros

- Plug-in architecture
- Platform independent
- Visual static analysis tools
- Dynamic analysis
- Many architectures supported

Cons

- Dynamic analysis prone to errors
- IBM architectures not supported
- Many tools are difficult to use
- Difficult to use documentation

