**ARTS**: Available, Robust, and Trustworthy Software

**ARTS Overview**

- **Available, Robust and Trustworthy Software**
- **Goal**: improving software
  - Robustness
  - Availability
  - Security
- **Target software**: Large server programs (mostly C/C++ code)
- **Operating systems**: Platform dependent

**Dynamic**: CP-Miner/PR-Miner

- **Motivation**: Programs hold a lot of rules
  - Source code contains useful information for inferring rules
- **CP-Miner**: Detecting copy-pasted code and related bugs
  - Software bugs are expensive!
  - Account for 40% system failure
  - Induce large overhead (10X-100X)
  - Copy-paste detection time
  - 32.83 minutes
  - 6 minutes
  - 283 seconds
- **PR-Miner**: Extracting implicit programming rules and detecting violations
  - Memory bugs are most prevalent and difficult to catch
  - Memory related bugs contribute to most security issues
  - Memory usage behavior analysis to detect memory leaks
  - Memory corruption detection (reduction from 2-13 to 0)

**Interactive**: Flashback

- **Motivation**: Software bugs are hard to reproduce
  - Existing checkpointing solutions are heavy-weight, unsuitable for software debugging
  - Give the programmer the experience of a “flashback”, by replaying the bug again
  - Real-time checkpoints of programs
  - Deterministic replay in an interactive debugger
- **Results**: Less than 1% overhead

**Static**: Mining large program for specification and bugs

- **CP-Miner**
- **Motivation**: Programs hold a lot of rules
- **Source code contains useful information for inferring rules**
- **CP-Miner**
- **Detected copy-pasted code and related bugs**
- **Software**
  - #lines of code
  - #copy-paste
  - Copy-paste detection time
  - #bugs detected
  - **Linux**
    - #lines of code: 44,893
    - #copy-paste: 23.3%
    - Copy-paste detection time: 20 minutes
    - #bugs detected: 49
  - **FreeBSD**
    - #lines of code: 3.3 M
    - #copy-paste: 20.4%
    - Copy-paste detection time: 20 minutes
    - #bugs detected: 51
  - **Apache**
    - #lines of code: 224 K
    - #copy-paste: 17.7%
    - Copy-paste detection time: 15 seconds
    - #bugs detected: 5
- **PR-Miner**
- **Extracting implicit programming rules and detecting violations**
- **Software**
  - #lines of code
  - Time/sec
  - #bugs verified
  - **Linux**
    - #lines of code: 32,283
    - Time/sec: 42
    - #bugs verified: 16
  - **PostgreSQL**
    - #lines of code: 6,128
    - Time/sec: 5
    - #bugs verified: 6
  - **Apache**
    - #lines of code: 283
    - Time/sec: 1
    - #bugs verified: 1

**Dynamic**: iWatcher

- **Motivation**: Simple, General Architectural Support for Static Checking
  - Time-dependent: a particular inter-leaving sequence
- **iWatcher**
  - Trigger monitoring functions by hardware for all accesses to the watched memory locations with low overhead
  - Detects all the evaluated bugs with low overhead (4-80%)