CERIAS

The Center for Education and Research in Information Assurance and Security

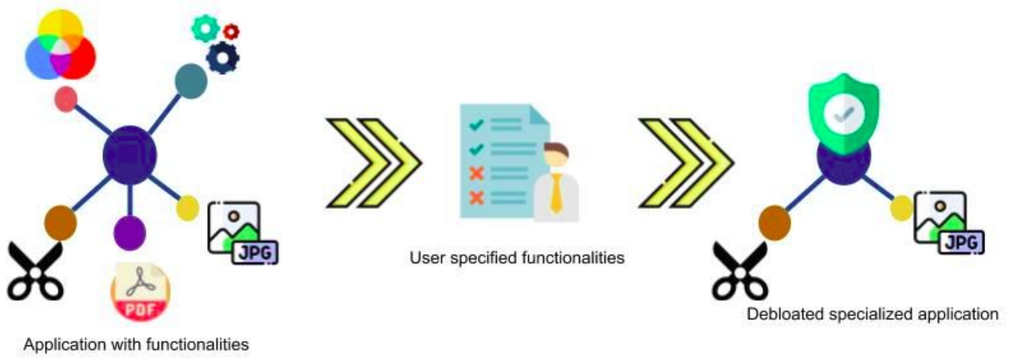
hexhive

Ancile: Attack Surface Reduction Through Application Specialization

Priyam Biswas Nathan Burow Mathias Payer

Motivation

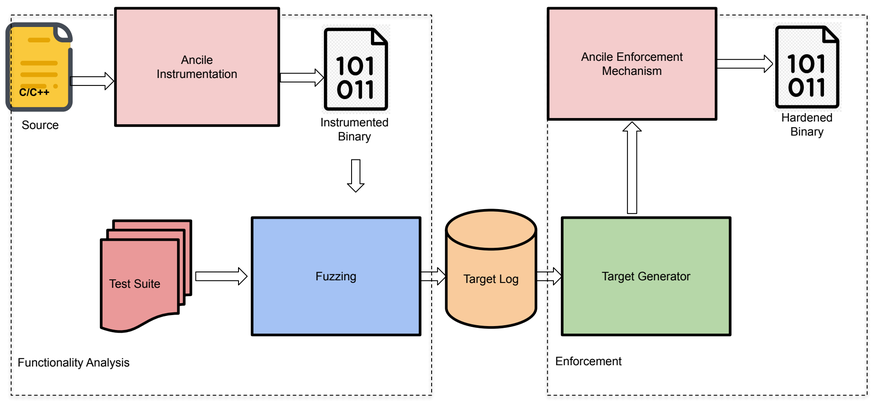
- Control-flow hijacking is the most common attack vector where attackers redirect execution to attacker chosen locations
- Existing mechanisms such as software debloating and control flow integrity (CFI) are incomplete; we need defense in depth
- Exercising only desired functionality discovers all required targets
- Stripping unused targets as well as functionalities minimizes attack surface



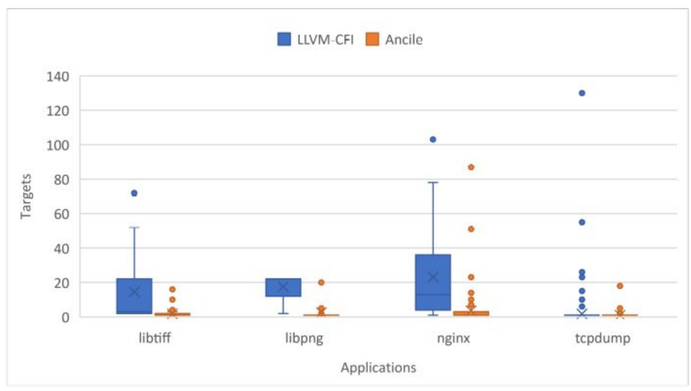
Goals

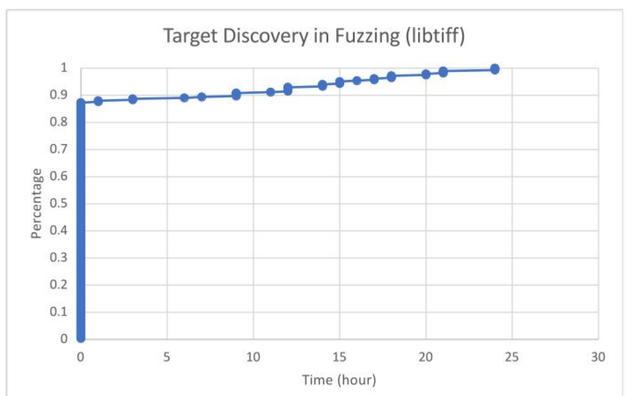
- Minimize target sets (while enabling correct execution)
- Move to dynamic analysis: Avoids over-approximation
  - Leverage fuzzing/unit tests to observe all required targets
  - Instrument binary to enforce observed target sets
- Remove unused functionality

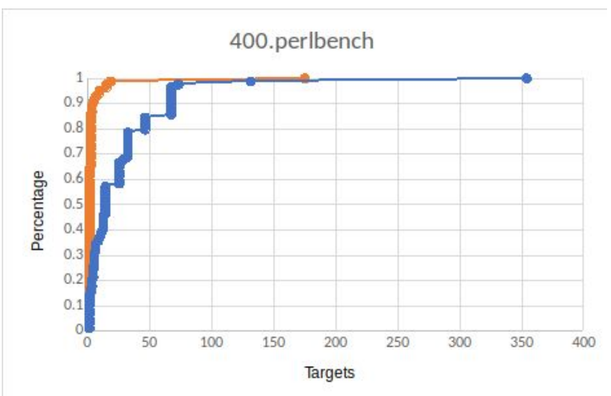
Design



Result







Steps

- **Application Profiling**:
  - Functionality-aware target analysis
  - Uses fuzzing to extract all valid control flows for a desired functionality
  - Allows only targets for the desired functionality
- **Enforcement:**
  - Leverages LLVM-CFI with the restricted target sets obtained during profiling phase

Conclusion

- Ancile builds context and flow-sensitive target sets
- Prunes unused functions
- Improves security bar by automatically specializing code for desired functionality

PURDUE UNIVERSITY Discovery Park

CERIAS