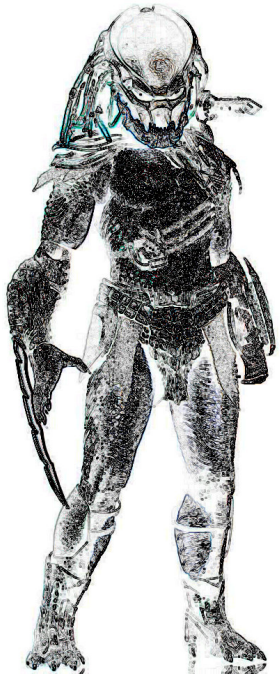
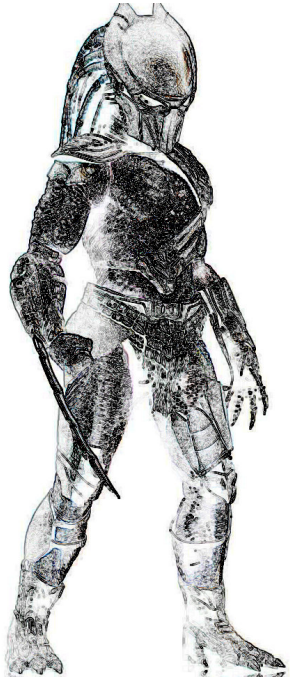
Predator Hunting Party

Ondřej Kinšt

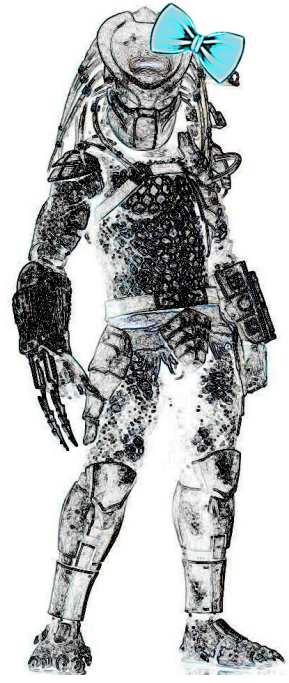


Petr Peringer



Tomáš Vojnar

Veronika Šoková



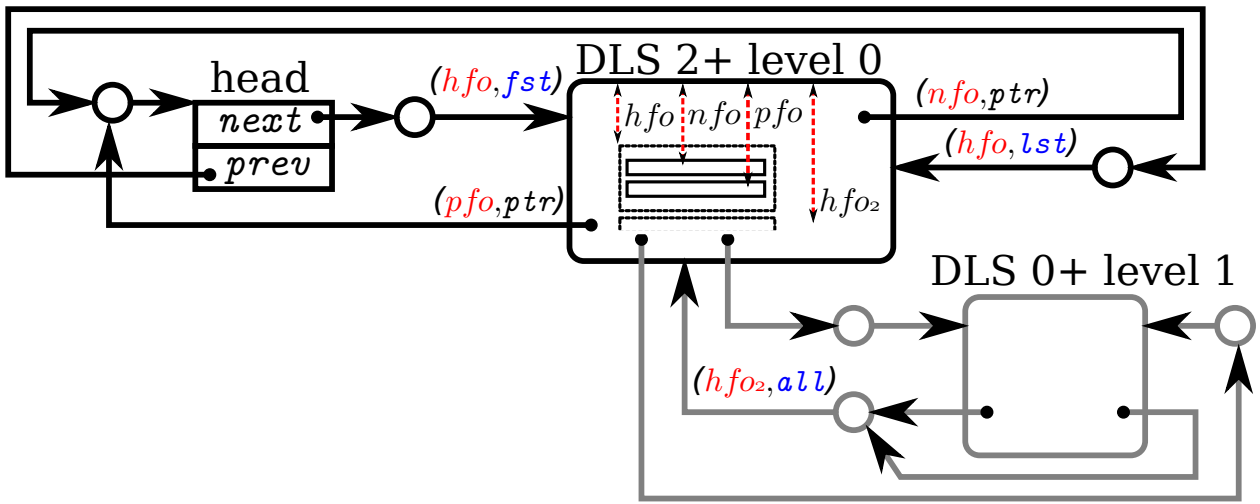
BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Predator: An Overview

- Focuses on shape analysis of low-level system code.

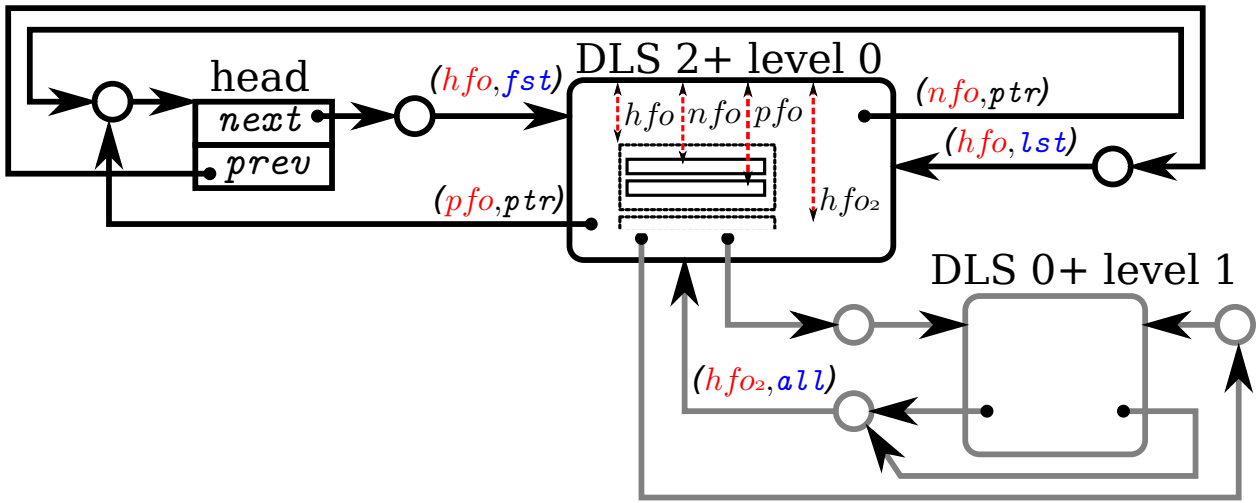
Predator: An Overview

- Focuses on shape analysis of low-level system code.
- Uses symbolic memory graphs (SMGs) to encode sets of heap configurations with various kinds of (nested) lists:



Predator: An Overview

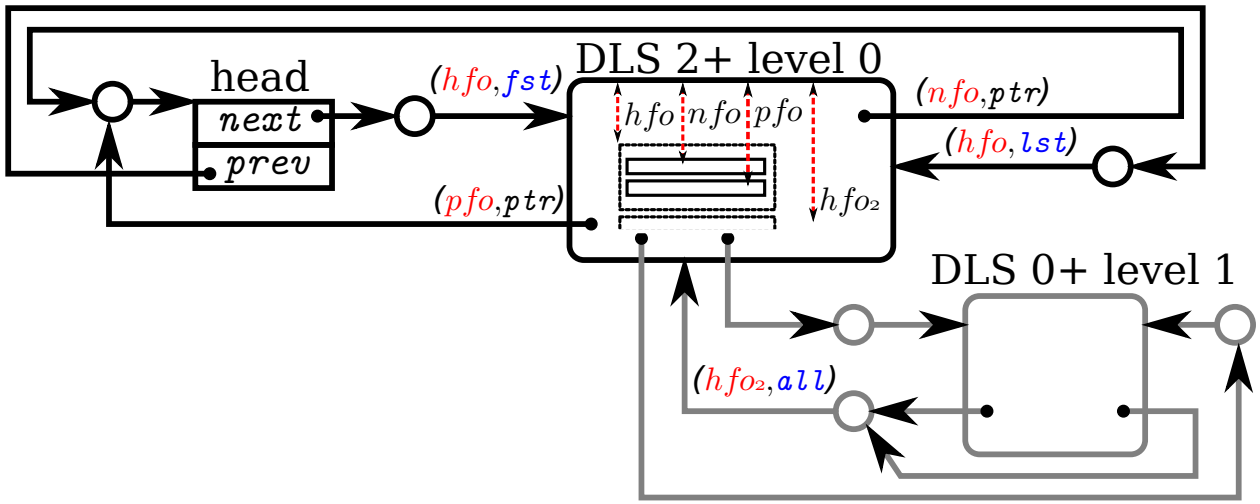
- Focuses on shape analysis of low-level system code.
- Uses symbolic memory graphs (SMGs) to encode sets of heap configurations with various kinds of (nested) lists:



- Uses efficient graph-based algorithms to implement all needed operations: join, abstraction, entailment, ...

Predator: An Overview

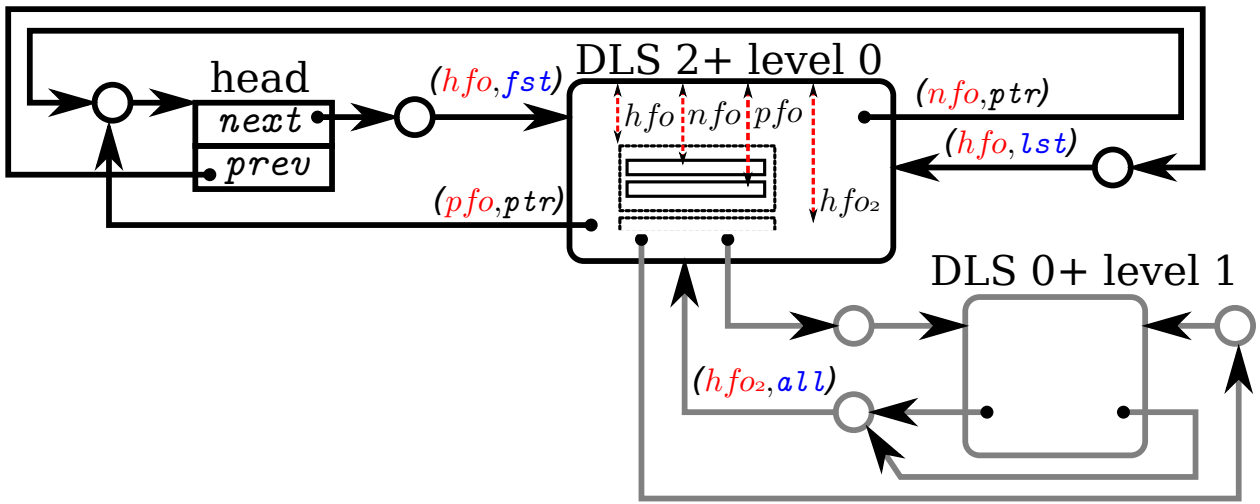
- Focuses on shape analysis of low-level system code.
- Uses symbolic memory graphs (SMGs) to encode sets of heap configurations with various kinds of (nested) lists:



- Uses efficient graph-based algorithms to implement all needed operations: join, abstraction, entailment, ...
- Looks for memory safety errors: invalid dereferences, out-of-lifetime accesses, double frees, memory leaks, ...

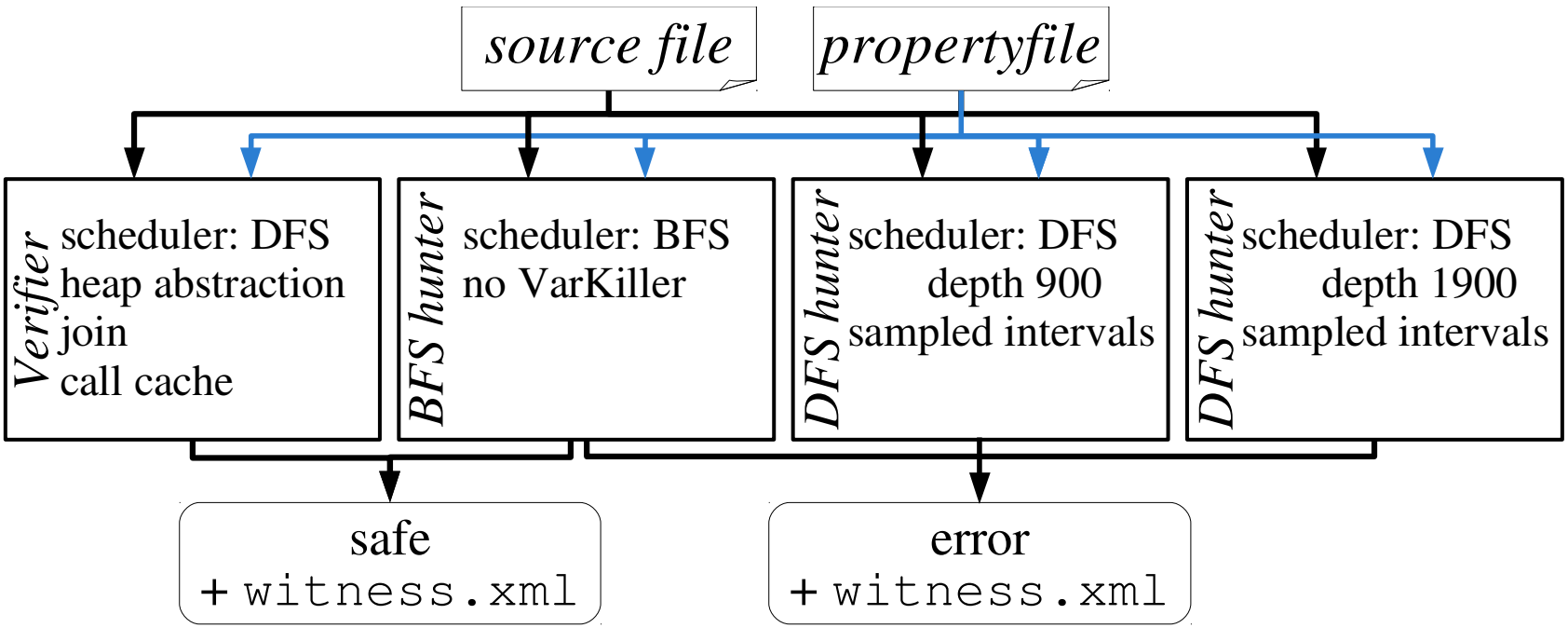
Predator: An Overview

- Focuses on shape analysis of low-level system code.
- Uses symbolic memory graphs (SMGs) to encode sets of heap configurations with various kinds of (nested) lists:



- Uses efficient graph-based algorithms to implement all needed operations: join, abstraction, entailment, ...
- Looks for memory safety errors: invalid dereferences, out-of-lifetime accesses, double frees, memory leaks, ...
- Implemented as an open source GCC plug-in.

Predator Hunting Party v3.1415



Competition Results

- MemSafety: gold.
  - Best results in MemSafety-Heap and MemSafety-LinkedLists.
- ReachSafety:
  - Implemented as an assertion category.
  - Best results in ReachSafety-Heap.

Competition Results

- MemSafety: gold.
  - Best results in MemSafety-Heap and MemSafety-LinkedLists.
- ReachSafety:
  - Implemented as an assertion category.
  - Best results in ReachSafety-Heap.
- Errors reported by Predator Hunters only:
  - Many false alarms suppressed (except 4).

Competition Results

- MemSafety: gold.
  - Best results in MemSafety-Heap and MemSafety-LinkedLists.
- ReachSafety:
  - Implemented as an assertion category.
  - Best results in ReachSafety-Heap.
- Errors reported by Predator Hunters only:
  - Many false alarms suppressed (except 4).
- Soundness preserved:
  - Only Predator Verifier can claim infinite-state programs correct.
  - Some finite-state programs proved correct by the BFS Hunter.

Competition Results

- MemSafety: gold.
  - Best results in MemSafety-Heap and MemSafety-LinkedLists.
- ReachSafety:
  - Implemented as an assertion category.
  - Best results in ReachSafety-Heap.
- Errors reported by Predator Hunters only:
  - Many false alarms suppressed (except 4).
- Soundness preserved:
  - Only Predator Verifier can claim infinite-state programs correct.
  - Some finite-state programs proved correct by the BFS Hunter.
- Support for Linux/macOS.


2+DLS