

# Estimating Types in Binaries using Predictive Modeling

Omer Katz

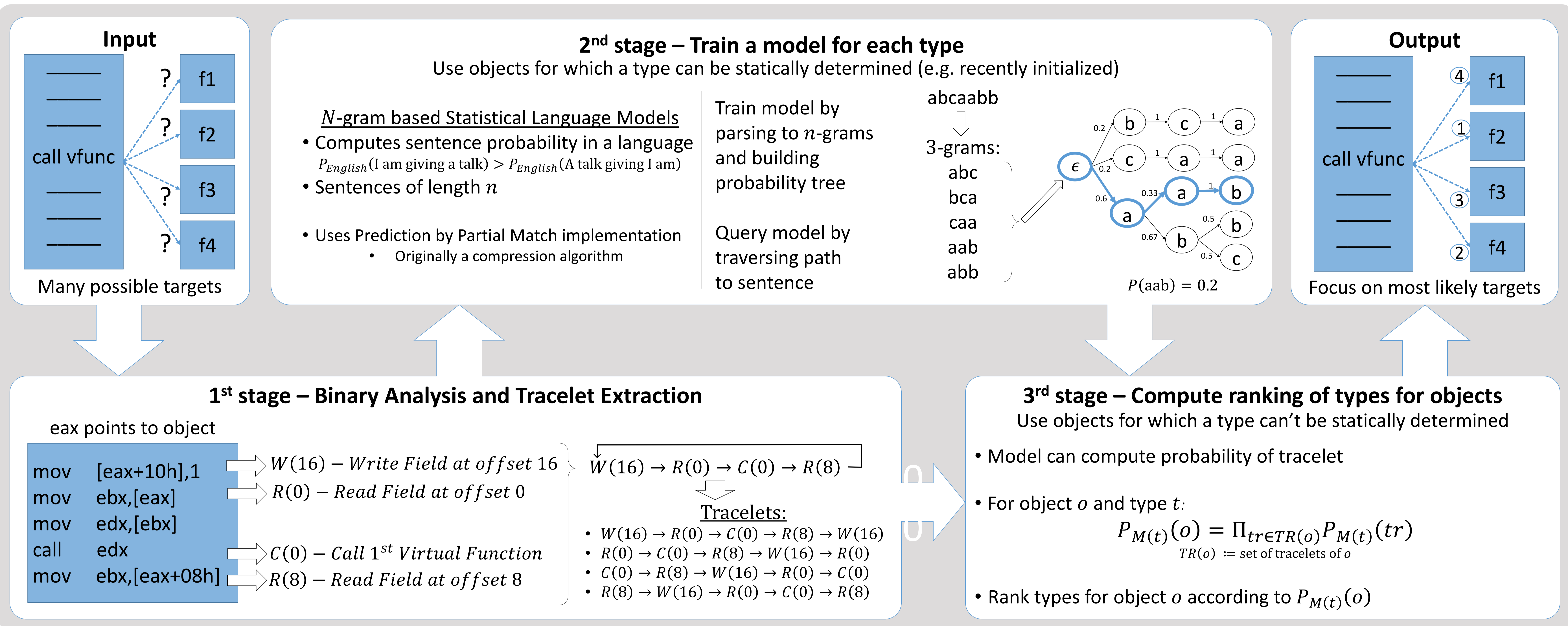
Ran El-Yaniv

Eran Yahav

**Problem:** Calls to virtual functions break the control flow of programs and hinder reverse engineering (RE) efforts

**Goal:** Statically determine most likely targets of each virtual function call

**Solution:** Determine types of objects used in virtual function calls based on how they are used



## Evaluation:

- Evaluated over 20 benchmarks
- Compared to ground truth from manual RE
- **Objective:** rank expected target highest
- Across all benchmarks, for over 80% of calls to virtual functions, expected target ranked in top 3

## Benchmark results:

- **X** axis – maximum rank
- **Y** axis – percentage of calls to virtual functions for which the expected target was ranked below the maximum rank

