DivCon: Compiler-based Diversification Against Code-reuse Attacks

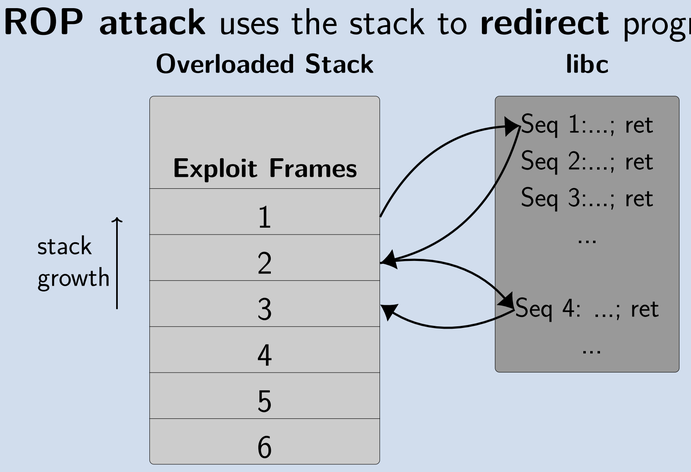
Rodothea Myrsini Tsoupidi

KTH Royal Institute of Technology, Sweden

Code-reuse attacks

- Evolved from **stack-smashing** attacks after introducing $W \oplus X$.
- **Return-oriented programming** (ROP) is a **code-reuse** attack that consists of **gadgets** code snippets with specific functionality.

Example: A **ROP attack** uses the stack to **redirect** program execution:



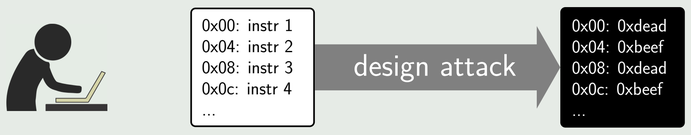
- **Variants**: JOP, COP, and more

Diversification

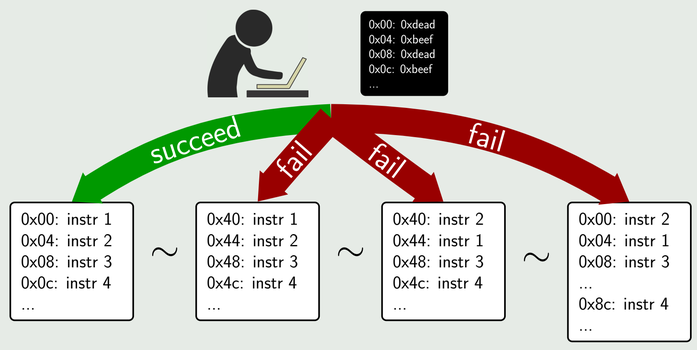
Diversification refers to diversity in software, i.e. the advantages of the existence of multiple **semantically equivalent** variants of a program.

- Diversity in **binaries** can **hinder** code-reuse attacks
- Common approach: **Randomization**

An **attacker** designs an **attack** for a **target** program

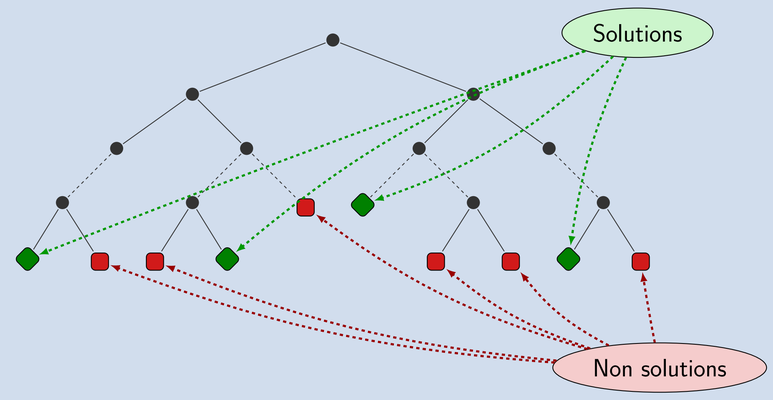


Diversified software **hinders** attacks that target identical programs



Constraint Programming

- **Constraint programming** (CP) is a method for solving **combinatorial** problems.
- Uses **search** to find one or all solutions
- CP is able to find the **optimal** solution
- The method considers **all solutions**

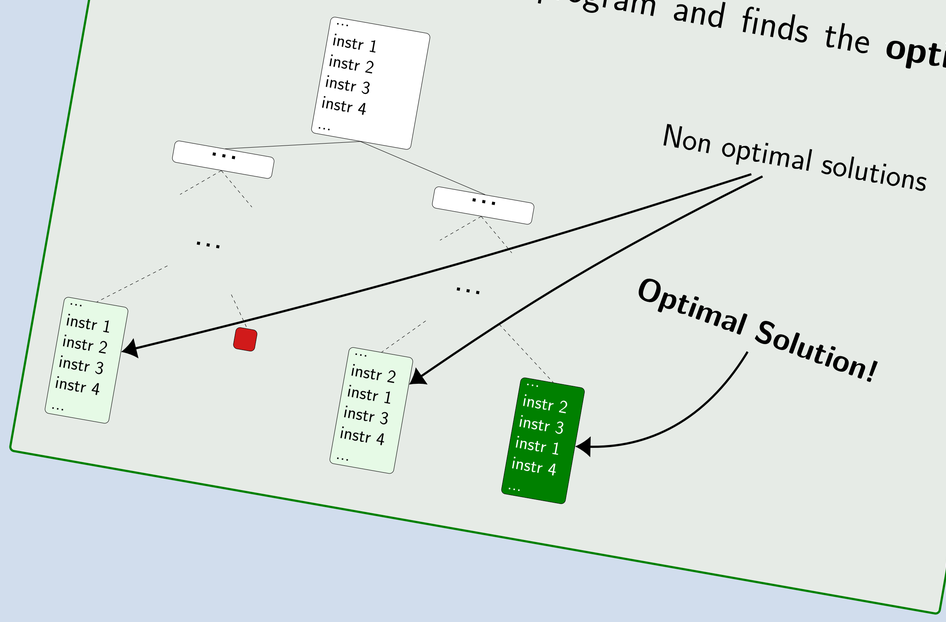


Unison

Tool that performs low-level **compiler optimizations** using **constraint programming**

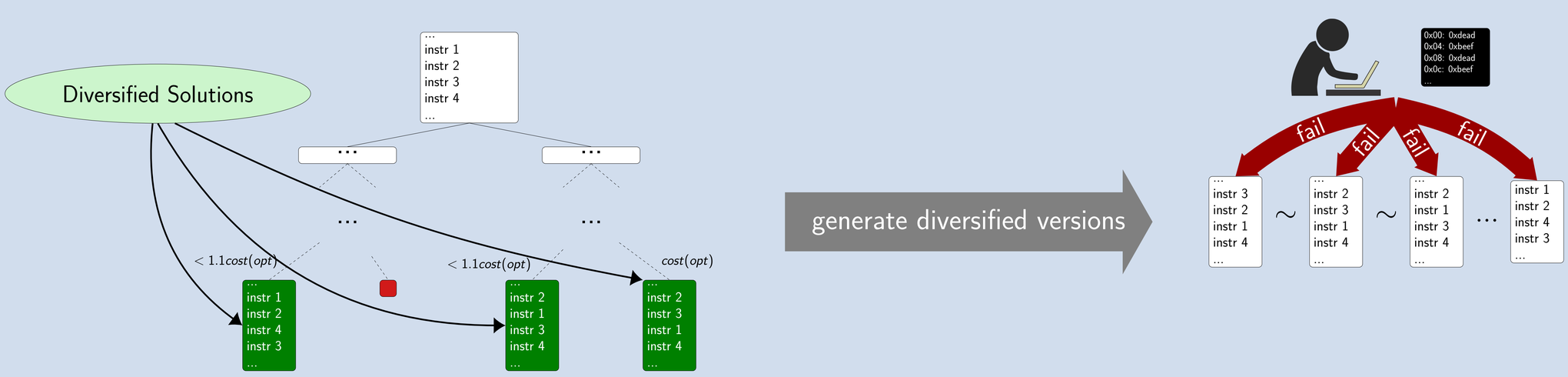
- Operates on **LLVM** intermediate representation
- **Optimizations**: Combined **register allocation** and **instruction scheduling**
- Finds the **optimal** solution

Unison considers an **input** program and finds the **optimal** solution:



Approach

- **Unison** provides a **structural** way to generate **variants** of a program by considering non-optimal solutions
- Considers compiler **optimizations**: speed (overhead $\leq 10\%$ optimal) or space (overhead $\leq 20\%$ optimal)
- Optimize based on **diversity** using a metric
  - Hamming distance
  - Levenschtein distance
  - Other metric



- Add additional **constraints** to the hardware model of Unison to **reduce** the gadgets