

# Automated Generation of High-Quality Attack Signatures and Patches

Tzi-cker Chiueh



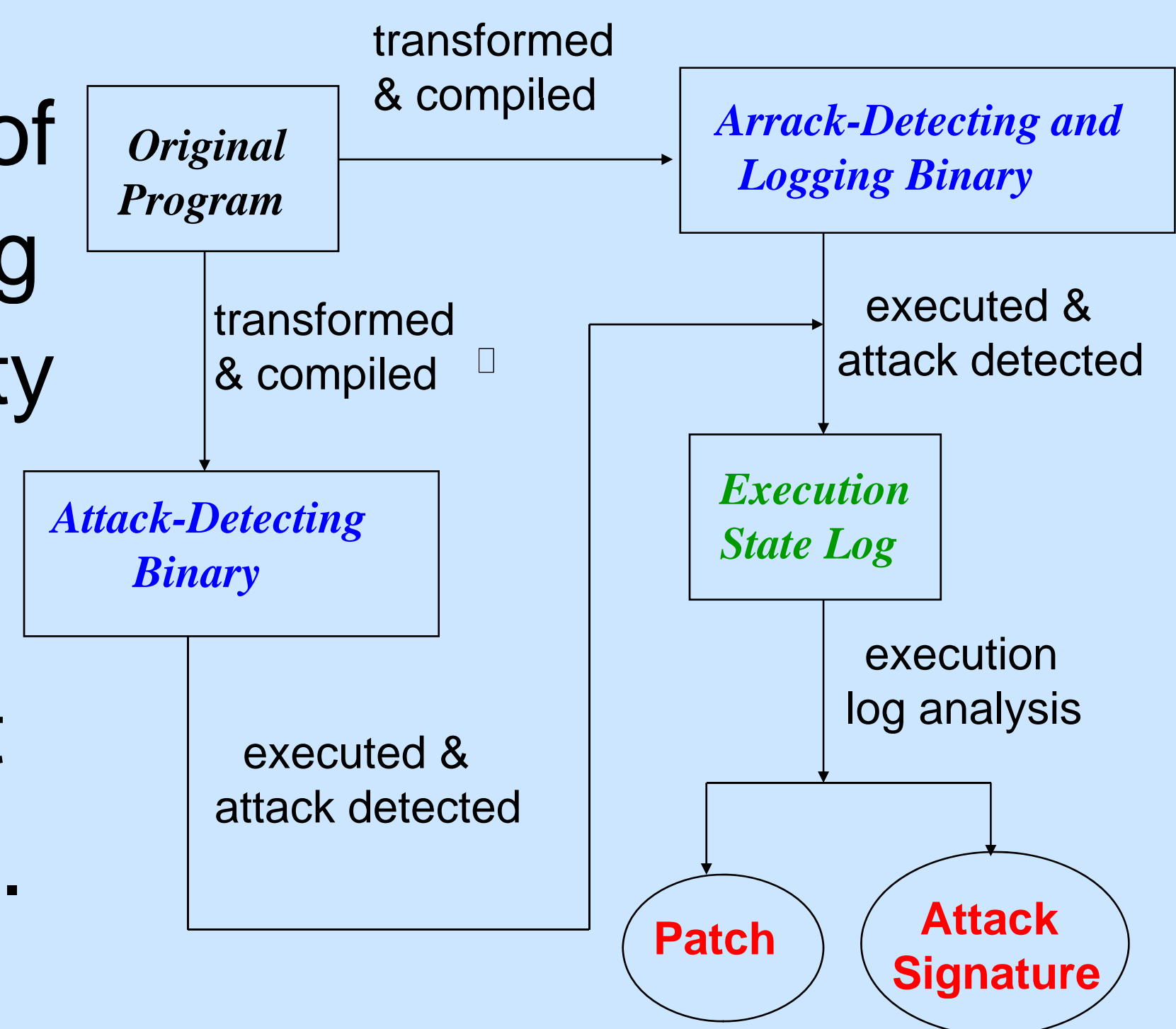
Stony Brook University (<http://www.ecsl.cs.sunysb.edu/~dira>)

## Project Goal

The DIRA project aims to develop a complete system that can automatically generate attack signatures and patches for a wide variety of attacks including control-hijacking attacks such as buffer overflow attacks, web server attacks such as SQL injection and browser attacks such as cross-site scripting (XSS) attacks.

## Approach

Analyze the root cause of each type of vulnerability, derive the corresponding attack pattern, identify the vulnerability site being attacked through data and control flow analysis, and extract the portion of victim application code that uniquely characterizes a given attack.



## Approach and Impact

### Automated Logging and Analysis

- Minimal execution state logging
- Vulnerability type-specific analysis
- Exploit bi-directional traffic

### Research Impact

- First known automated patch creation tool
- Applicable to multiple vulnerability types
- Used in Symantec's Response group

**Description:** The two key ideas in the DIRA project are (a) a unified execution state logging framework that can simultaneously detect attacks, create signatures/patches for detected attacks, and erase the side effects left by the attacks, and (2) an extensible vulnerability type-specific execution log analysis framework that can be tailored to different types of vulnerabilities used in control-hijacking attacks, web server attacks and browser attacks.

**Main Use Case:** After a vulnerability of a program is reported, the publisher of the program can use DIRA to automatically determine where the vulnerability site is, create an initial patch to seal that vulnerability, and generate an IPS signature to protect its customers before the final patch is published and deployed.