Vulnerability Assessment for Cyber-Crime Prevention

Motivation

- Software vulnerabilities are pervasive – they are not limited to any particular platform, vendor or industry
- Exploitation of vulnerabilities leads to massive social disruption and/or immense financial costs
- Identifying and remediating vulnerabilities is a complex challenge owing to large code-sizes and various platform as well as architectural dependencies
- Aim to build an automated, platform and architecture agnostic vulnerability assessment framework

Project Description

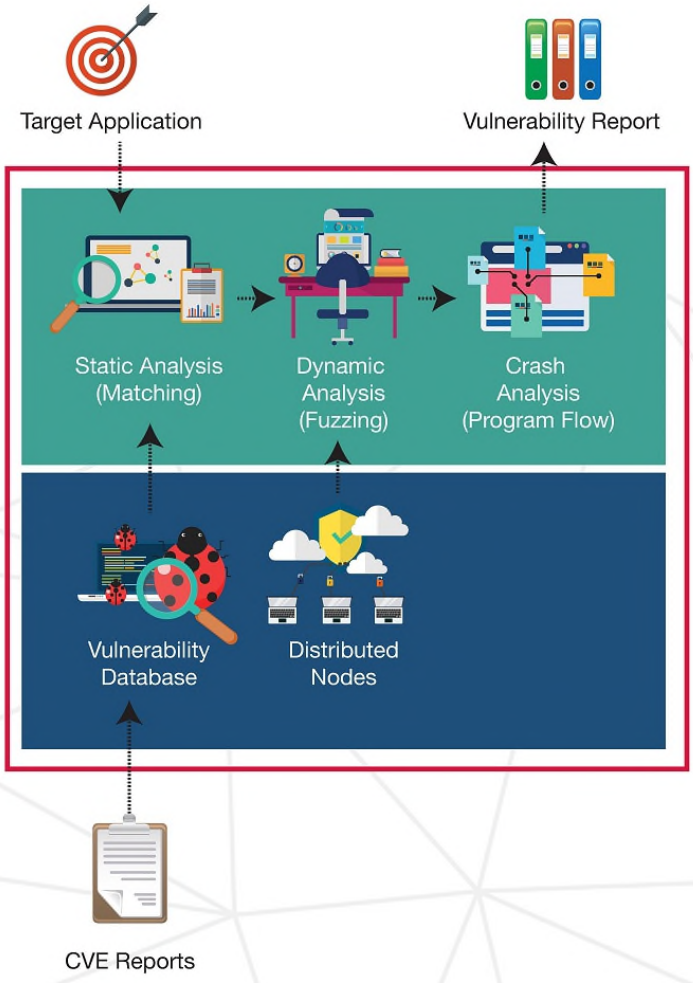
A comprehensive 3-step approach to vulnerability assessment in a scalable, distributed environment

1. Static Analysis
A source-code/binary-level analysis to uncover known as well as potential vulnerabilities using smart matching techniques

2. Dynamic Analysis
A run-time binary analysis to confirm vulnerabilities found during the static analysis using distributed fuzzing

3. Crash Analysis
A program-flow analysis to understand the vulnerability's root cause so as to better identify security fixes

Vulnerability Assessment Framework



Future Work

Expanding support to include all major platforms (Windows, Linux, Mac, Android, iOS) and architectures (Intel x86/x64, ARM/ARM64, MIPS, PPC)

Real-world application and validation for systems across public (defence, critical infrastructure) as well as private sectors (banking, IoT, CPS, ICS)

Liu Yang

Supported by NRF's National Cybersecurity Research Grant.