New Defenses for Data-Only Attacks

PI: Jeff Huang, jeff@cse.tamu.edu

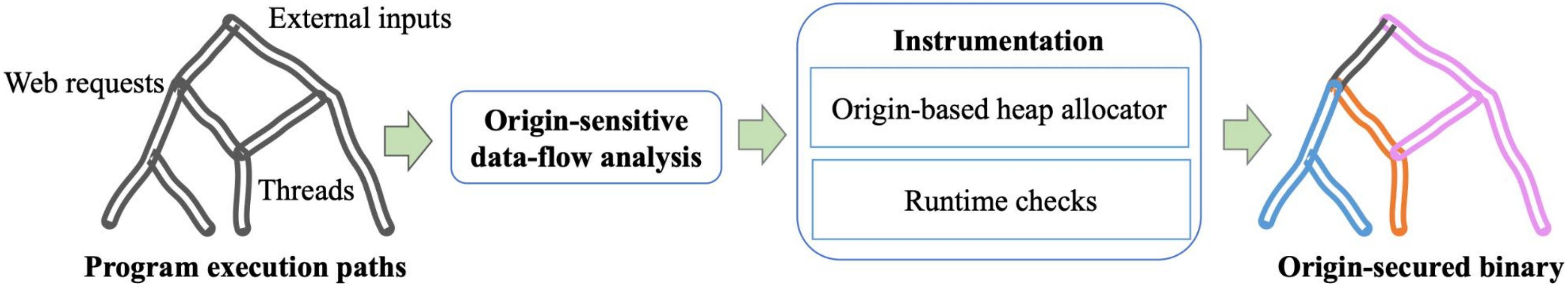
Challenge:

- Data-only attacks such as Heartbleed only tamper with data flow in software
- Existing solutions are either inapplicable or are too expensive for data-only attacks
- Advanced data-only attacks will become mainstream once control-flow defenses such as control-flow integrity are widely deployed

Scientific Impact:

This project proposes new, principled solutions to data-only attacks with acceptable overhead for deployment in practice

Solution: cross-origin data flow integrity (X-DFI)



External inputs

Web requests

Threads

Program execution paths

Origin-sensitive data-flow analysis

Instrumentation

Origin-based heap allocator

Runtime checks

Origin-secured binary

Broader Impact and Broader Participation:

- X-DFI implemented in LLVM for C/C++ and Rust programs
- An evaluation on a collection of recent CVEs (data-only vulnerabilities) shows high efficiency (< 9% runtime overhead).
- Origin-sensitive data-flow analysis adopted by a commercial product

Award No 1901482, TEXAS A&M ENGINEERING EXPERIMENT STATION