FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Proactive Defenses through Program Hardening

Chao Zhang, Dawn Song

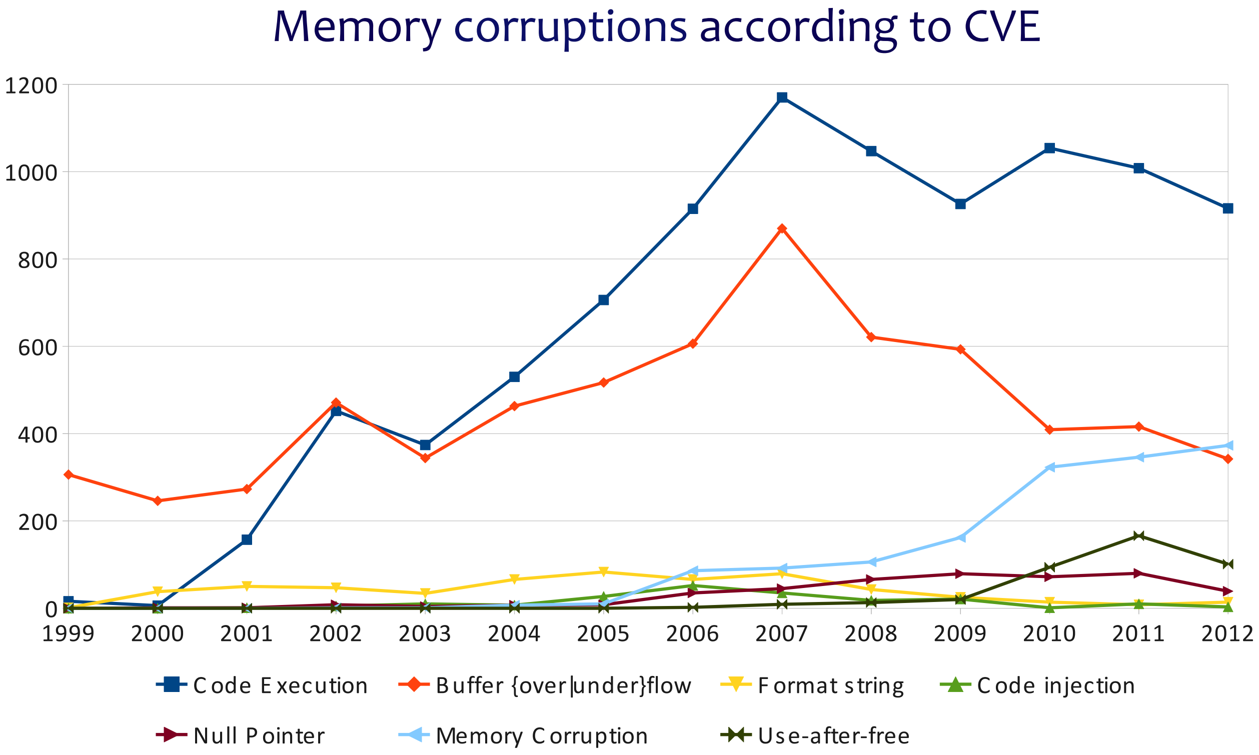
BitBlaze, UC Berkeley

Motivation

- Lots of attack targets

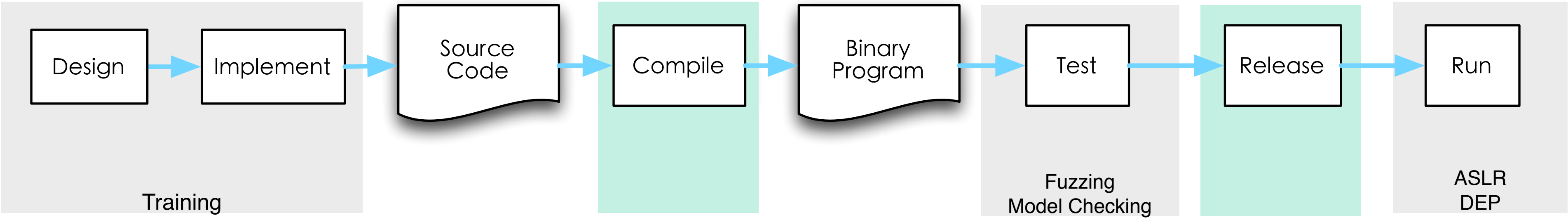
Motivation

- Lots of attack targets
- Increasing software vulnerabilities



Secure Development Cycle

- Existing solutions are not sufficient



  - Vulnerabilities are inevitable when designing and implementing.
  - Testing is not able to find out all potential vulnerabilities.
  - Runtime hardening is not sufficient, and has compatibility issues.

- Proactively hardening programs is a promising solution
  - source-code level
  - binary level

FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Program hardening

- Advantages
  - Automatic hardening: not affected by programmers' errors.
  - Strong protection: covers undiscovered bugs.

- Challenges
  - Performance: <10%
  - Protection
  - Compatibility: legacy code

Road map

- Binary level hardening
  - **Practical Control Flow Integrity & Randomization for Binary Executables.** Chao Zhang, Tao Wei, Zhaofeng Chen, Lei Duan, Stephen McCamant, László Szekeres, Dawn Song, and Wei Zou. *IEEE Security and Privacy, 2013*
  - **SoK: Eternal War in Memory.** László Szekeres, Mathias Payerz, Tao Wei, and Dawn Song. *IEEE Security and Privacy, 2013*

- Source code level hardening: future work

FORCES
FOUNDATIONS OF RESILIENT
CYBER-PHYSICAL SYSTEMS

Thanks!

Q&A

Berkeley
UNIVERSITY OF CALIFORNIA

Massachusetts
Institute of
Technology

NSF

MICHIGAN

VANDERBILT
UNIVERSITY