Engineering Graduate Symposium 2008

Testudo: Heavyweight Security Analysis via Statistical Sampling

Joseph L. Greathouse, Ilya Wagner, David A. Ramos, Gautam Bhatnagar, Todd Austin, Valeria Bertacco, and Seth Pettie

Electrical Engineering and Computer Science Department, University of Michigan

Software Security is Vital Research

$60,000,000,000

annual cost of buggy software to the US economy

15,000,000

annual identity thefts in the US

8000

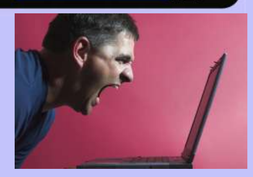
software vulnerabilities released publicly every year

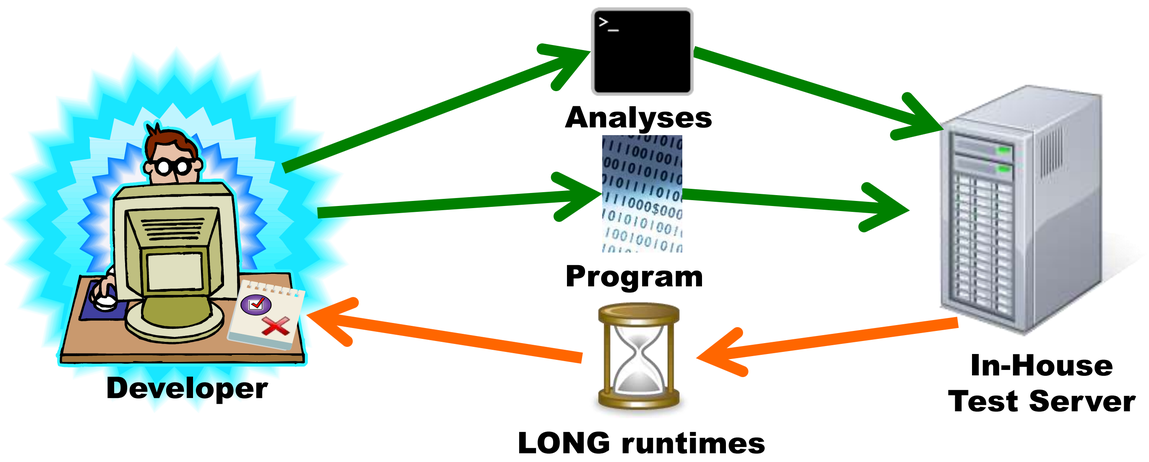
Tens of thousands of programmers who try to write safe code
A plethora of secure programming languages
Security vulnerabilities still exist.

Heavyweight Analysis Tools Help, but…

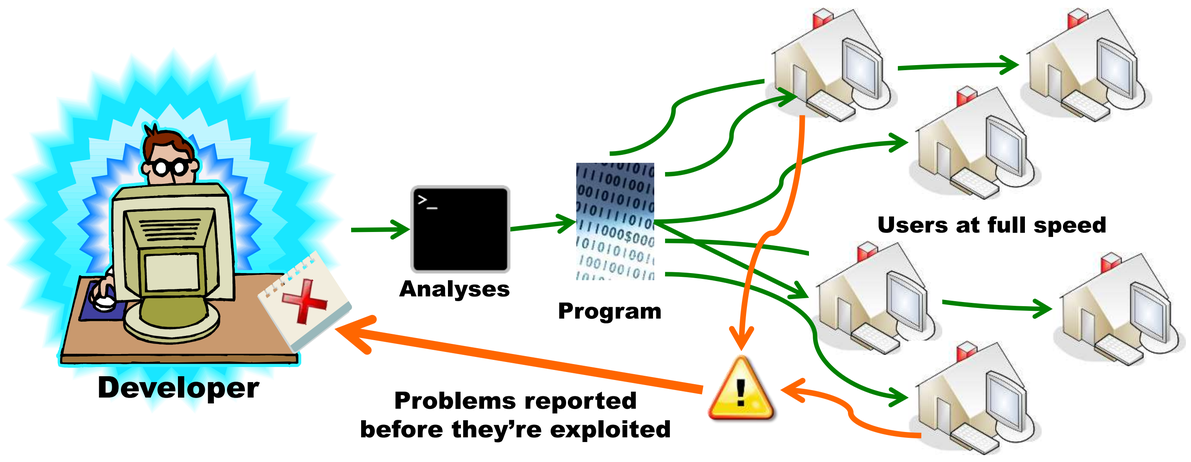
Existing Tools:
- GDB
- Valgrind
- Pin

Weaknesses:
- Runtime overhead
- Cannot predict end-user behavior





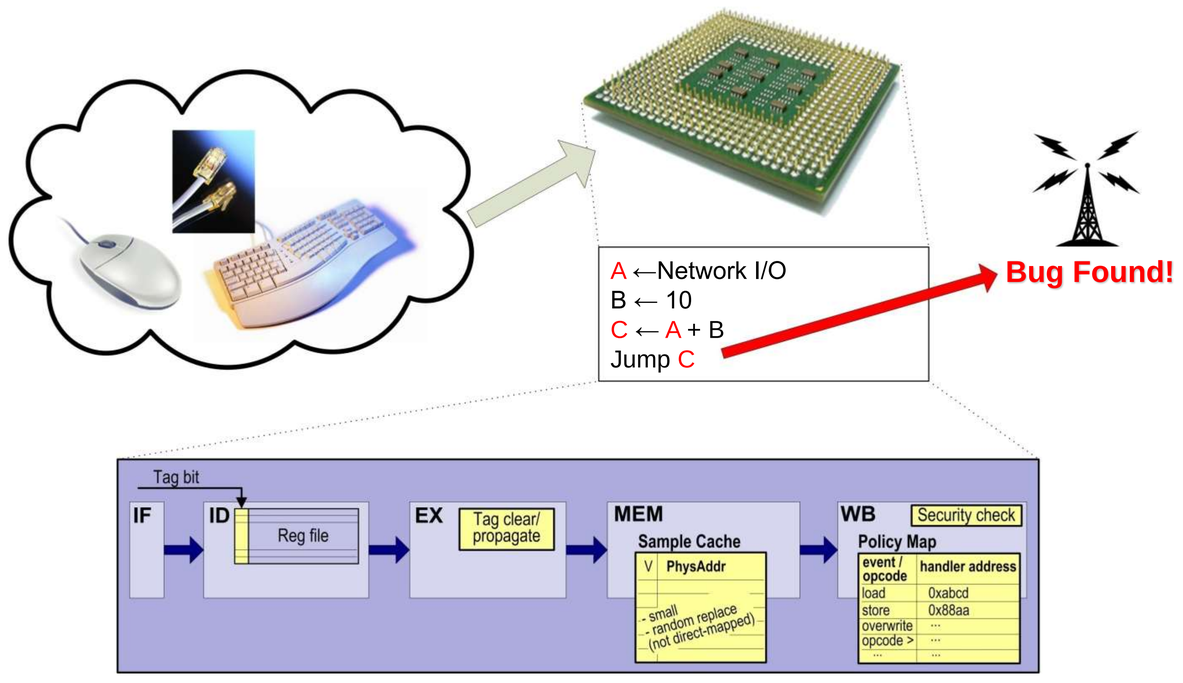
In **Traditional Heavyweight Analysis**, the developer runs tests on his program, then waits to receive feedback. This loop continues until the software is released.



With Testudo's **Distributed Dynamic Debugging**, users run small parts of the total examination *at full speed*, which leads to much stronger security analyses.

Contributions of Testudo:

- Inexpensive method for deploying analyses to end-user systems
- Novel approach to security using distributed debugging
- Employs only a small, fixed-size sample cache
- Especially beneficial to enterprise users



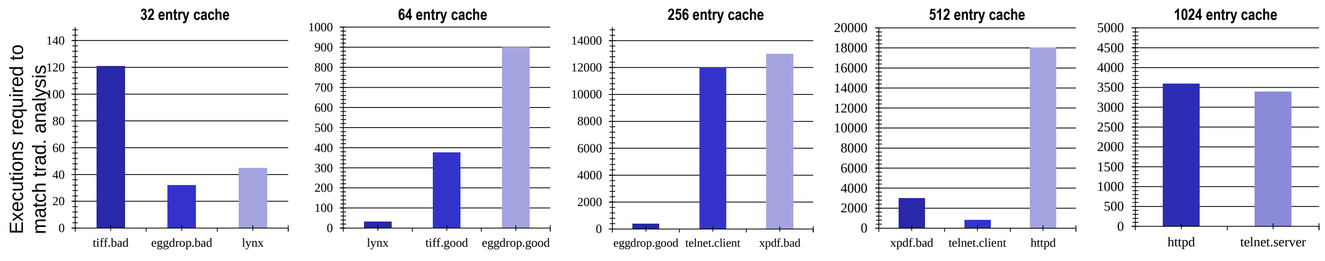
Future Work:

- Multiprocessor compatibility
- Software-based analysis

Statistical Sampling Eliminates Analysis Overhead

Taint Analysis

Traditional Overhead: 30x | **Testudo Overhead: 0**



Dynamic Bounds Checking

Traditional Overhead: 100x | **Testudo Overhead: <1%**

Aerospace Engineering • Applied Physics • Biomedical Engineering • Chemical Engineering • Civil and Environmental Engineering • Computer Science Engineering • Electrical Engineering • Industrial and Operations Engineering • Interdisciplinary Programs • Macromolecular Science and Engineering • Materials Science and Engineering • Mechanical Engineering • Naval Architecture and Marine Engineering • Nuclear Engineering and Radiological Sciences

RACKHAM · MichiganEngineering · KAIST · intel · Exponent · TAUBER INSTITUTE FOR GLOBAL OPERATIONS · BUSINESS ▪ ENGINEERING ▪ LEADERSHIP · Schlumberger · THE AEROSPACE CORPORATION · TOYOTA