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

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%