**Scalable Security Vulnerability Analysis via Sampling**

Joseph Greathouse, Ilya Wagner, Valeria Bertacco, and Todd Austin, University of Michigan

**Motivation: Software Errors Abound**
- NIST: SW errors cost US $60 billion/year as of 2002
- FBI CCS: Security Issues $67 billion/year as of 2005

- >½ from viruses, network intrusion, etc.

**Our Solution: Dataflow Sampling**
- Lower overheads by skipping some analyses

**Dataflow Sampling Approach**
- Dataflow Sampling
- Non-Sampled Analysis
- Sampled analysis observes all states in aggregate

**Testudo: Hardware Dataflow Sampling**
- What happens when the cache overflows?
  - Use sampling to randomly remove meta-data
  - Reduces off-chip changes while facilitating meta-data sampling

**Other Applications and Future Work**
- Generalized hardware mechanism to find meta-data
  - Use hardware-supported watchpoints to speed up many analyses
  - To be presented at ASPLOS’12

- Simple hardware to accelerate data race detection
  - Performance counters enable SW race detector on-demand
  - Presented at ISCA’11

- Use dynamic sampling to improve static software analysis
  - Control paths near executed code are often exploited by hackers
  - Keep track of paths users don’t execute across entire population
  - Focus on these paths in static analysis tool