Software for Dependable Systems: Research Needs and NSF Perspectives

Jeannette M. Wing
Assistant Director
Computer and Information Science and Engineering Directorate
and
President’s Professor of Computer Science
Carnegie Mellon University

Software for Dependable Systems: Sufficient Evidence? Symposium
National Academy of Sciences
October 23, 2007
U.S Broader Research Agenda and Priorities

- **PCAST/NITRD report [August 2007]**
  - Dan Reed and George Scalise
  - 8 priority areas listed, with the recommendation that the first 4 get disproportionately larger funding increases.

- **#1 Priority: Cyber-Physical Systems**
  - Our lives **depend** on them.

- **#2 Priority: Software**
  - Software is **everywhere** and in **everything**.

- **#6 Priority: CyberTrust**
  - In particular, foundations, e.g., models and logics for reasoning.
NSF Relevant Programs: New FY08

• **Software for Real-World Systems (CISE-wide)**
  - Goal: Bring foundations of software researchers and systems researchers together. Working with industry encouraged.
  - $10M, 12-20 awards, proposals due Jan. 17, 2008

• **Cyber-Enabled Discovery and Innovation (NSF-wide)**
  - Goal: Computational Thinking for science and engineering
  - Three dimensions
    • From Data to Knowledge
    • *Understanding Complexity* in Natural, Built, and Social Systems
    • Virtual Organizations
  - $52M, with $20M from CISE, FY08 is first of five years
CISE Relevant Ongoing Core Programs

- **Computing Processes and Artifacts (in CCF Division)**
  - Includes formal methods, programming languages, static and dynamic analysis, software engineering

- **Computer Systems Research (in CNS Division)**
  - Includes cyber-physical systems

- **Cybertrust (in CNS Division)**
  - Includes security, reliability, privacy, usability

- **Information and Intelligent Systems (IIS) Division**
  - Includes foci on human, team, and social roles in systems development
The Harder Question

Computer scientists have been researching [formal methods] for at least four decades. What could make a real difference to the speed at which [formal methods] permeate industrial and commercial software development?
High-Level Answers

• **Lightweight formal methods [Jackson and Wing 1996]**
  - Laser beam vs. light bulb approach
    • Focus on one critical property (at a time)
    • Focus on one critical component (at a time)

• **Training and education**
  - Teach formal methods to undergrads. Engage them in your research.

• **Academics-Industry-Government Partnerships**
  - Academics have to work with domain experts from industry or a gov’t lab
  - Industry and/or gov’t lab have to be willing to work with academics.
  - Successful collaborations start at the grassroots
    • Embed academics in industry/gov’t lab and v.v.
    • SLAM story. Two Ph.D.s in formal methods hired in the development org.
  - Also need buy in from the top
  - Models of collaboration/consortia
    • Many consortia have failed. We should understand why.
    • Semiconductor Research Corporation model—successful for hardware!
    • Flower model (see next slide)
A Model for Expediting Progress
Scientific Research Challenges

• **We need new advances in software foundations.**
  - What does “correctness” mean?
    - Factor in context of use, unpredictable environment, emergent properties, dynamism
  - What are the desired properties of and metrics for both software (e.g., weak compositionality) and systems (e.g., power)?
  - What is a complexity theory for real-world systems as we have a complexity theory for algorithms?

• **We need new advances in formal models and logics**
  - For complex systems, e.g., hybrid systems
  - For a richer set of properties, e.g., privacy, cost, power
  - For multiple purposes, e.g., verification, simulation, prediction
Engineering Research Challenges

• We need new advances in verification tools for systems builders and domain engineers
  - Push-button
  - Usable
  - Integrated with rest of system development process

• We need new engineering processes for creating software-intensive systems.
  - Traditional ones won’t work.
A Model for Expediting Progress

Do we have the courage and commitment to do something like this?
Thank you!