Some Lessons Learned

- Context matters
- People power
- Focus on problems not solutions
- Exploit synergies and shoulders
- Plan carefully
- Cultivate champions
- Avoid the “root of all evil”
- Embedded verification experts

Context Matters

- **Microsoft culture change**
  - viruses, worms, security, privacy, …
  - Trustworthy Computing Initiative
  - security push and education
- **Microsoft Research** = basic research + product group impact
  - *Microsoft's researchers are brilliant, well-funded and free to advance … "the state of the art" in software and computer science.*
  - *By locating its researchers cheek by jowl with business managers, Microsoft hoped to encourage more effective transfer of new technologies from its labs to its range of products.*
  - 12 March 2004
    Financial Times
- **Programmer Productivity Research Center**
  - PREfix and PREfast tools
  - analysis infrastructure
  - tool pipeline to development organizations

Programmer Productivity Research Center (PPRC)

"Technology-based approach to software development"

Approach

- Focus on defect prevention and early detection
- Collect information about the development process
- Enable rapid research and tool development with rich infrastructures
- Achieve process automation through technology

Products that Microsoft ships have been touched by at least one of PPRC tools:

12.5% of bugs fixed in Windows 2003 Server were found with PPRC tools

Reliability Work

Static Analysis Tools, widely deployed

PREfix, PREfast, ESP, SLAM, Fugue, FxCop, MaX, ...

Dynamic Analysis Tools

BBT, Scout, LOP, coverage, ...

Annotation Languages

SAL – bounds checking

Modeling Languages

ASML, Spec#, TLA+

Recent News

Microsoft shifts researchers to Windows unit

By Ina Fried
CNET News.com
August 3, 2004, 11:57 AM PT
URL: http://zdnet.com.com/2100-1104-5295048.html

Microsoft is shifting about 70 technical staff from its research unit into its Windows effort as the company gears up for Longhorn, the next major release of the operating system.

The developers, who had been studying various ways of improving programmer productivity, will now focus their efforts on improving all phases of Windows development, including design, testing and sustained engineering. The move is among the largest shifts of workers from the company's research unit to a product group.

About 25 other workers that had been working on the programmer productivity project will remain in Microsoft Research.

People Power

Software Productivity Tools group members

- **Sriram Rajamani**, Manuvir Das, Rob DeLine, Jim Larus, Manuel Fahndrich, Rustan Leino, Jakob Rehof, Shaz Qadeer

SLAM summer interns

- Sagar Chaki, Todd Millstein, Rupak Majumdar (2000)
- Satyaki Das, Wes Weimer, Robby (2001)
- Jakob Lichtenberg, Mayur Naik (2002)
- Jakob Lichtenberg, Shuvendu Lahiri, Georg Weissenbacher, Fei Xie (2003)

SLAM Visitors

- Giorgio Delzanno, Andreas Podelski, Stefan Schwoon

Static Driver Verifier: Windows Partners

- Byron Cook, John Henry, Vladimir Levin, Con McGarvey, Bohus Ondrusek, Abdullah Ustuner
- Neill Clift, Nar Ganapathy, Adrian Oney, Johan Marien, Bob Rinne, Rob Short, Peter Wieland

Focus on Problems not Solutions

- Device driver problem
  - important to Microsoft
  - testing insufficient to ensure quality
  - many complexities but code of reasonable size
- Problem space guides search for solution
  - control-dominated properties ⇒ boolean programs
  - no annotations ⇒ counterexample-driven refinement

Exploit Synergies and Shoulders

- Diverse backgrounds of investigators
- SLAM built on strong foundations
  - program analysis
  - model checking
  - theorem proving
- Infrastructure
  - MS compiler front-end and alias analysis
  - CUDD BDD library
  - Simplify theorem prover
  - OCaml programming language

Plan Carefully

- Creativity = 10% inspiration + 90% perspiration
- Initial technical report
  - laid out plan, left open problems
  - recruiting/preparing interns
- Demo milestones
- Software process
  - open software architecture
  - code ownership, code reviews, code refactoring and cleanup
  - regression test suite
  - documentation

Cultivate Champions

- Device driver experts
  - Adrian Oney, Peter Wieland
  - explained subtleties of kernel
  - reviewed rules and error traces
- Management champions
  - Bob Rinne, Base OS
  - Amitabh Srivastava, PPRC

Avoid the "Root of All Evil"

- Premature optimization
  - easy to get caught up in new features
  - time/energy wasted on unprofitable features
  - optimizations introduce bugs
- Let application domain drive engineering
  - profiling gives data to help prioritize efforts
  - measure impact of new optimizations

Embedded Verification Experts

- Windows committed to hire two Ph.D.s with verification expertise
  - Byron Cook and Vladimir Levin
  - offices in both development and research
- Virtual team worked closely together for 1.5 years
- Product team now has 6 people full-time
- High bandwidth channel between groups

Conclusions

- The technology now exists for enforcing simple API contracts
- Rollout/adoption
  - first as out-of-band tools (i.e., SLAM/SDV)
  - next as in-band tools (part of language/compiler)
- Many variables in equation of technology transfer
  - keep your eyes wide open!

The Future (5 years?)

- If verification tools are successful, their use can be enforced by quality norms
- Professionals have to conform to such norms
- Tool automation makes it easy to conform to and difficult to ignore norms
- Third parties can audit to check for use of tool

Thanks to Patrick Cousot

The Future (10 years?)

- The *state of the art* will change toward complete automation
  - at least for common categories of bugs
- So responsibilities can be established
  - at least for automatically detectable bugs
- After which the law will change
  - by adjusting to the new state of the art
- To ensure at least partial software verification
- For the benefit of all of us

Thanks to Patrick Cousot