SE 464 Lecture, May 9th, 2011

3 Questions:

1. What is Design
2. How Design is represented
3. How do we know design’s good? Revisit

4 Analytical Criteria:

1. Fitness for purpose
2. Fitness for future
3. Cost of Production
4. Cost of Operation

Evidence used in SoftEng to argue for the above criteria:

1. Demo
2. User Testimony
   1. User installed base (Bigger version), a.k.a. number of hours of field operations, or number of units installed
3. Formal Verification (Critical software)
4. Testing to some coverage criteria
   1. e.g. US Military DOD178B/MCDC common criteria
   2. Use a testing suite
5. Vendor Reputation (50 years ago, no one got fired for buying IBM)
6. Warranty (not commonly offered in SW)
7. Whitepapers
8. Source Code (Open/Free Source Software)
   1. controversy: Voting Machines
   2. Enron Case: Accenture
9. Trial/Shareware Sneak Peeks
10. Normal Components
11. Product family lines
    1. Microsoft Office, Windows, Visual Studio, etc.
12. Benchmark testing
13. Certification from independent third party
    1. less so in software, but more so in other disciplines
    2. Review by a trusted source
14. Word of Mouth/personal referral/anecdotes
15. Systematic derivation
    1. common in 1970s/1980s
    2. Refinement Calculus
16. Comparison to alternatives

Administrative break.

seL4 Case Study (refer to slides on Repo)

Monolithic and Microkernel:

Criteria for OS:

1. Purpose
   1. Run applications
   2. Interact with hardware
   3. Tell time
   4. Multi-tasking
   5. Manage memory
   6. Interact with the user
   7. Default font
   8. Scheduling
2. Fitness for Future
   1. Easy to upgrade (SW, and HW)
      1. Apple moving from PowerPC to Intel
      2. MSFT Windows Vista and Hardware Drivers
      3. ITS vs Unix

Mach:

1. Kernel in User Space
2. Asynchronous IPC is more expensive than synchronous IPC