Report on Session 2: "Design faults and intentional faults"

Bev Littlewood

Centre for Software Reliability, City University, London

Presentations considered:

"In pursuit of software faults: Status and challenges" - Bojan Cukic

"Security metrics" - Bill Sanders

Two extremes

- Bojan talked about a field where there has been extensive activity for many years
  - There have been some achievements but there are still large gaps
  - Some of the ‘obvious’ problems are only now being addressed successfully
- Bill talked about a field that is new - or does not even exist yet!
  - Huge *need* for security metrics
  - But very little exists
  - And the culture is not one that encourages quantitative measures

1 Bojan - outline

Useful - and usefully critical! - review of state of the art

- Fault distributions
  - Large scale, long term projects
- Software V&V methods and their effectiveness
  - Implications for failure detection and forecasting
- Streamlining V&V
  - Using diversity to our advantage

1 Bojan - challenges

- Detection and identification of changing requirements and contexts
- Adaptation specific model-driven environments
- Agile run-time assistance
- How would a developer organization argue they applied "expected care" in the assurance of adaptive applications?
- Risk aware adaptation?

My thoughts

- Link between “fault evidence” and “failure behaviour” is still quite weak
- Is there too much concentration on “process” rather than product dependability *behaviour*?
- Issues concerning “on average” versus “in particular”
  - Many of the existing results are heavily aggregated
  - Are we missing some important “explanatory variables”? E.g. problem difficulty
- Some complex interactions still not understood
  - Evidence on “marginal” efficacy - but not much on multi-variate

2 Bill

- Good account of why we need metrics
  - E.g. need for risk assessment
- Not just *absolute* metrics - *relative* ones also useful
  - E.g. aid to choice between design solutions
- Existing metrics are often lacking strong foundation, lack rigour
- Generally not predictive
  - In particular of the impact of those security flaws that are *still left*
- Doom and gloom? No! Opportunities for research, challenges…

2 Bill - challenges

- Define suitable metrics
- Methods for estimating them
- Security arguments
- Tools
- Legal/regulatory policy

My thoughts

- Much (too much?) of existing work is on "process" metrics of various kinds
  - As was the case for accidental faults in early days (and still) of SE
- Surely we can reuse some of the models and metrics we have developed over the years in reliability and safety?
  - "exposure" variable is problematic - *time* is rarely appropriate
- "Operational security" (w.r.t. faults *not yet found*) is the Holy Grail
  - But looks pretty hard

A current personal obsession

- Much of our modelling concentrates on *aleatory* uncertainty and neglects *epistemic* uncertainty (i.e. model uncertainty, parameter uncertainty)
- So we make claims about dependability, but rarely address issues of *how much confidence* can be placed in them (*even in safety cases!*)
  - Hypothesis: dependability claims based on process evidence (should) engender *low* confidence
  - Hypothesis: claims about *security* should earn less confidence than ones about *reliability*