Self-Healing vs. Fault Tolerance

Phil Koopman
Carnegie Mellon University

WADS, May 2003
Overview

- Perhaps this isn’t even the right question
  - But people are going to ask it anyway

- Is some Fault Tolerance also Self Healing? – Yes

- Is all FT also Self Healing – No

- Is all Self Healing also FT – Maybe
  - Assume “yes” until proven otherwise?
Is This Even The Right Question?

- “Fault Tolerance” is an emergent property
  - Systems are fault tolerant (or not), to varying degrees
  - It is perhaps a measurable property
    - Fault injection experiments to see which faults can really be tolerated
    - But this is a difficult area

- “Self Healing” seems like an approach (or point of view)
  - What is an “injury”, and what isn’t?
  - Are there unifying themes to “self-healing”
  - Are there self-healing outcomes that are *not* fault tolerance?
    - (That are *not* dependability?)

  - BTW, can we measure “healability?”
Is Some Fault Tolerance *also* Self Healing?

Bouricius, W.G., Carter, W.C. & Schneider, P.R.,
“Reliability modeling techniques for self-repairing computer systems,”

- **An early self-healing idea: Standby sparing**
  - One or more operating units
  - Pool of reserve units
  - When one unit breaks, standby spare used to replace an operating unit
  - If that isn’t healing, then we need a tighter definition of “healing”

- **What about Byzantine Generals algorithms?**
  - They take data sets with arbitrary defects and produce a clean output

- **What about error correcting codes?**
Is *All* FT Really Self Healing?

- **Many FT techniques are probably not self healing**
  - Using highly reliable components (bullet-proof vests are not “healing”)
  - Fail-fast, fail-silent components (component suicide is not “healing”)
    – But, such components can facilitate healing at the system level

- **Emphasis might be different**
  - Fault tolerance tends to emphasize 100% functionality (does self-healing?)
  - But, much of FT is arguably self healing
Is *All* Self Healing Really FT?

- **Narrow question: historical FT research**
  - Things like incomplete systems and human+computer systems are not emphasized
  - Someone could draw up a research area map based on DSN papers … but is there a point to that?

- **Broad question: could it be FT research**
  - Probably yes – I do “graceful degradation” and I’m from the FT community

- **Broadest question: is it all “dependability”**
  - The definition of dependability grows over time
  - “Dependability” has recently come to include security
  - Probably it is all “dependability;

  But the question I care about is research community interactions, not turf battles