Report on Session 4

Karama Kanoun

LAAS-CNRS

65tht meeting of the IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance
Sorrento, Italy, January 23-27, 2014

Robin Bloomfield

Security Risk Assessment: Between Snake Oil and Science

Assessment provide useful outputs, an estimate is not the only one

- ☞ Safety: damage = system → environment
- ☞ Security : damage = environment → system

  … why not looking for the safety of the environment

- ☞ Carrot diagram: Effort/investment ←→ risk level
- ☞ Problem of legacy systems
- ☞ Impact of security on safety cases
- ☞ Some success stories

- ☞ Solution = layered analysis
- ☞ Uncertainty in structure is enormously important

  … what about the uncertainty due to the nature of application itself
- ☞ Factorization of attacker capabilities
- ☞ Attack scenarios, grading of scenarios → table

  ←→ similar to:

  Failure Mode Effects and Criticality Analysis spreadsheets

  FMECA

Laurie Williams

Where should I look?
Using metrics to prioritize verification efforts

- ☞ Application of software engineering approaches to security engineering
- ☞ Metrics: to predict the presence of security vulnerabilities
  - ☞ Vulnerability databases
- ☞ Collect internal metrics
  - → static analysis tools → statistical correlations
- ☞ Machine learning: training period
  - → identification of vulnerability prone components

- ☞ Empirical studies
- ☞ 3 impacting classes of metrics (discriminative power)
  - Code complexity (14)
    - ☞ Size /volume, cyclomatic complexity, comments
  - Code churn / change metris (3)
    - ☞ Frequency / number of changes, etc
  - Developer metrics (11)
    - ☞ Closeness, betweenness, number, etc
- ☞ Static analysis alerts → indicative of security vulnerabilities
- ☞ Can we rely only on these alerts?
- ☞ Should be completed? How?