# Summary of Workshop on MACS

## Reported by John Meyer

- Taxonomies
- Formal methods
- Informal methods
- Model-based quantification
- Measurement-based quantification

# T/A/V Taxonomies

- Measurement-oriented
  - Top-down  OK for conceptual taxonomies
  - Bottom-up better for measurement oriented taxonomies
- Anomaly-oriented
  - AC - DC
  - Desire a bijection between AC and DC classifications?
- Curiously, the term “intrusion” was not used in either of these taxonomy discussions

# Formal and Informal Methods

- Formal
  - Key - Keep the trusted part very simple in the sense that application of formal verification methods is feasible
  - Depth of formalization process
- Informal
  - Red Team experiments (tests)
  - Subjective measures such as CSR

# Model-Based Quantification

- Model diversity
  - Diversity is omnipresent
  - Attack diversity - defense diversity
  - Use of diversity can beat statistical independence (if covariance is negative)
- Quantification of survivability properties (SPs)
  - Survivability models need to represent
    - system functionality (including intrusion tolerance mechanisms)
    - workload
    - attack effects
  - Probabilistic measures quantify various properties

# Total Assurance Case

- Various types of evidence are needed
  - Some evidence is quantitative; other evidence can take the form of desired properties
  - Means of obtaining such evidence likewise differ widely.
  - Again, a call for diversity
- The problem: How to effectively combine diverse evidence in the construction of a total assurance case
- Example tool for this purpose: SEAS

# Measurement-Based Quantification

- Analysis of vulnerabilities
  - FSMs, pFSMs
- Relative vulnerabilities
  - Compare “base” system with one that’s enhanced with some form of intrusion prevention, count vulnerabilities for each and consider the ratio
  - How to count Vs is an issue
  - RV  of an application
- Quantitative evaluation of security
  - Use of both modeling and measurement

# Questions

- What are appropriate assurance measures?
- In what environment will the assessment/validation be performed?
- How will the attacks/intrusions be modeled?
- Level of detail of scheme?
- Assumption coverage?
- What existing techniques can be used? What new techniques are needed?