# Session 2 Summary

## Mustaque Ahamad “Challenges in Data-Driven Characterization of Cyber Attacks”

- Emphasis on challenges in risk evaluation
- Today risk is anecdotal, “in the eye of the beholder”
  - there is no 'MTTF' equivalent
- Improve resilience via data-driven assessment:
  - Create warehouse of combined attack data
    - public & private, successful & failed
    - access to real data is challenge #1
  - Create analytics (challenge #2)
    - today's risk & predictive, visualization
    - dependent upon value of target, mitigation, etc.

# Session 2 Summary

## Salvatore Stolfo “An Empirical Approach to Measure Defense-in-Depth as a Cloud-Based Service”

- Evaluate security of a specific architecture
  - Real system and real threats
- Defense-in-depth: visualize all products and levels
  - Relative coverage of evolving system
  - Ability to prevent, detect, react and/or repair
  - Threats vs product coverage (e.g., degree of overlap)

- Make adversary effort multiplicative not additive
- Monitor outbound traffic, exfiltration of data
- Embedded systems are wide-open exposure
- Clouds introduce opportunity for complete testing

# Session 2 Summary

- Customer for both Sal and Mustaque is executive level
  - Top-down perspective
    - Dashboard view, not a lot of numbers and clutter
  - To make bottom line decisions
    - Risk/investment trade-off and value
  - Valuable for technical staff too
    - improve architecture, product choice
    - identify emerging threats,etc.