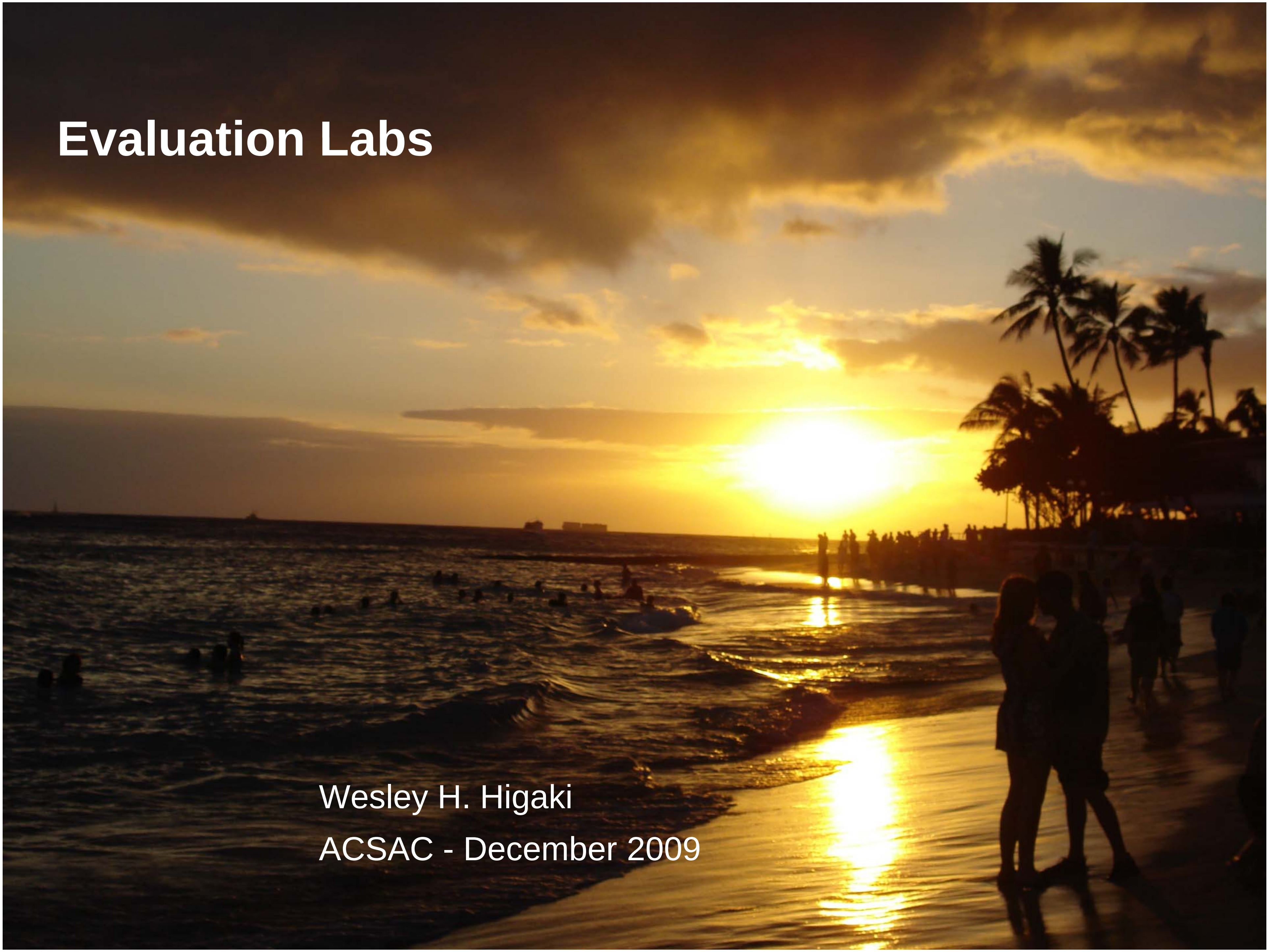
Evaluation Labs



Wesley H. Higaki

ACSAC - December 2009

Assertions

- Vendors pay the evaluation labs and should expect satisfactory service
- Evaluation labs make it difficult to comparison shop
- Lab “lock-in” is common

Evaluation Lab Selection Criteria

- Total cost of evaluation
  - Fixed or T&M evaluation costs
  - Hidden costs
  - Rework costs
- Probability of successful evaluation
  - Lab track record
  - Demonstrated expertise in technology
- Timeliness
  - Availability of resources
  - Turnaround times

Symantec Experience

- 15 successful CC evaluations
  - 4 failures
  - EAL 2, 3 and 4
- International labs
  - US
  - UK
  - Canada
- Consultants
  - Evidence preparation

Issues with Labs

- Focus on documentation errors, not security issues
- Learning curve on product/technology
- Each Scheme, Lab and Evaluator are unique
- Disputes with consultants/writers

NIST NVLAP Accreditation

- NVLAP accredits CCTLs against general quality criteria, not CC capabilities
- Have any labs lost accreditation?
- Are labs accreditation reviewed on schedule?
- Where do you go when you have a dispute with the lab?

International Considerations

- Labs are accredited by national Schemes using national criteria
- International lab evaluations vary greatly
  - Partly due to Scheme biases
  - Partly due to evaluation lab biases
- CEM is used, but …
  - Is CEM enough?
  - Differing evaluation focus

Cost Reductions or Improved Security?

- Vendors pay the labs so what do they expect?
  - Improved product security?
  - Lowest evaluation costs?
  - Accurate evaluation?
- What do Validators/Certifiers expect from labs?

Conflicting Objectives and Drivers

- Vendors are commercial entities
  - Profit-driven
  - Protect their IP/competitive advantage
- Validators/Certifiers are government entities
  - Security standard bearers
  - Also need to justify their existence
- CCTL/CLEF are also commercial entities
  - Must balance satisfying vendors and validators

Is CEM Enough?

- Interpretation of CEM will always exist
- There is some weak oversight of labs internationally
- More international lab standardization could remove the inconsistencies between Schemes and Labs