Automated Cyber-Readiness Evaluation (ACE)

Rotem Guttman

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0004109

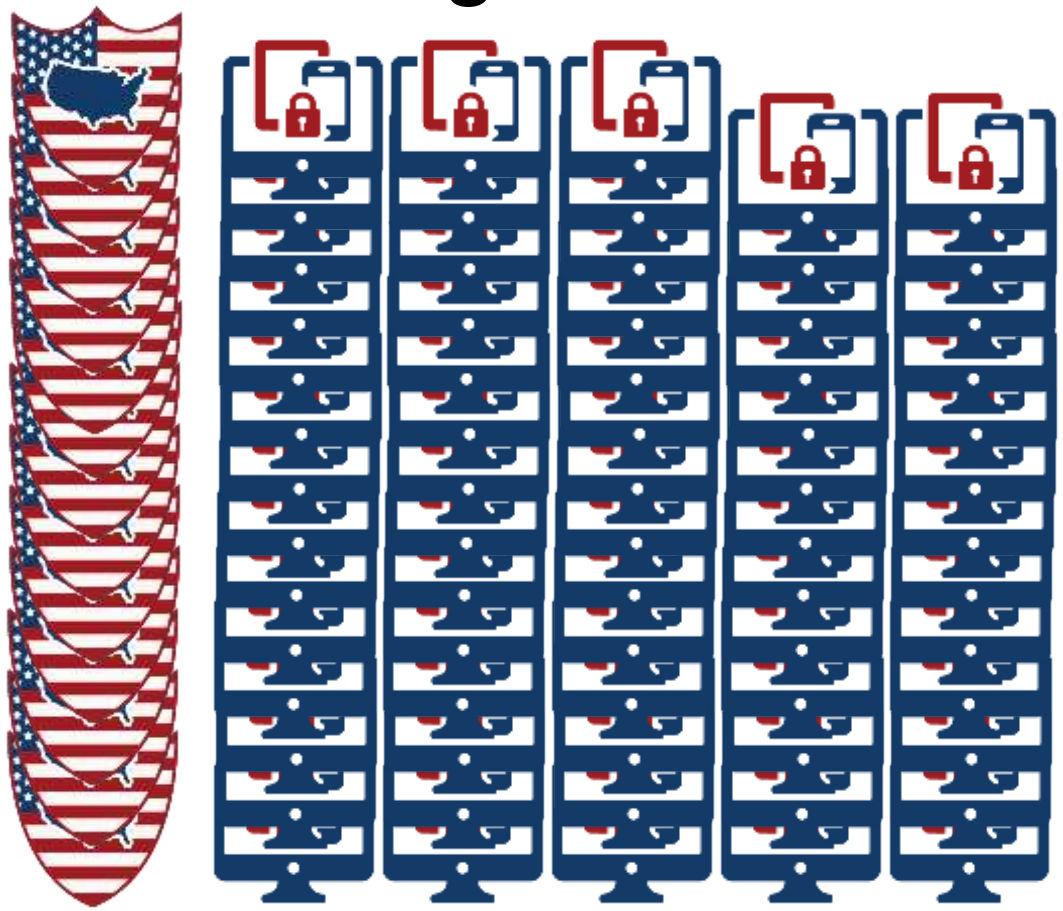
DoD Challenge Problem

Evaluating Mission-Readiness for Cyber Operators at Scale

- **Scalable**
- **Objective**
- **Reliable**
- **Valid**

13 National Mission Teams (Defend the Nation)

DoD Challenge Problem



68 Cyber Protection Teams (Defend DoD Networks)

Evaluating Mission-Readiness for Cyber Operators at Scale

- **Scalable**
- **Objective**
- **Reliable**
- **Valid**

DoD Challenge Problem

27 Combat Mission Teams
(Support Combatant Commands)

Evaluating Mission-Readiness for Cyber Operators at Scale

- **Scalable**
- **Objective**
- **Reliable**
- **Valid**

DoD Challenge Problem

+25 Support Teams

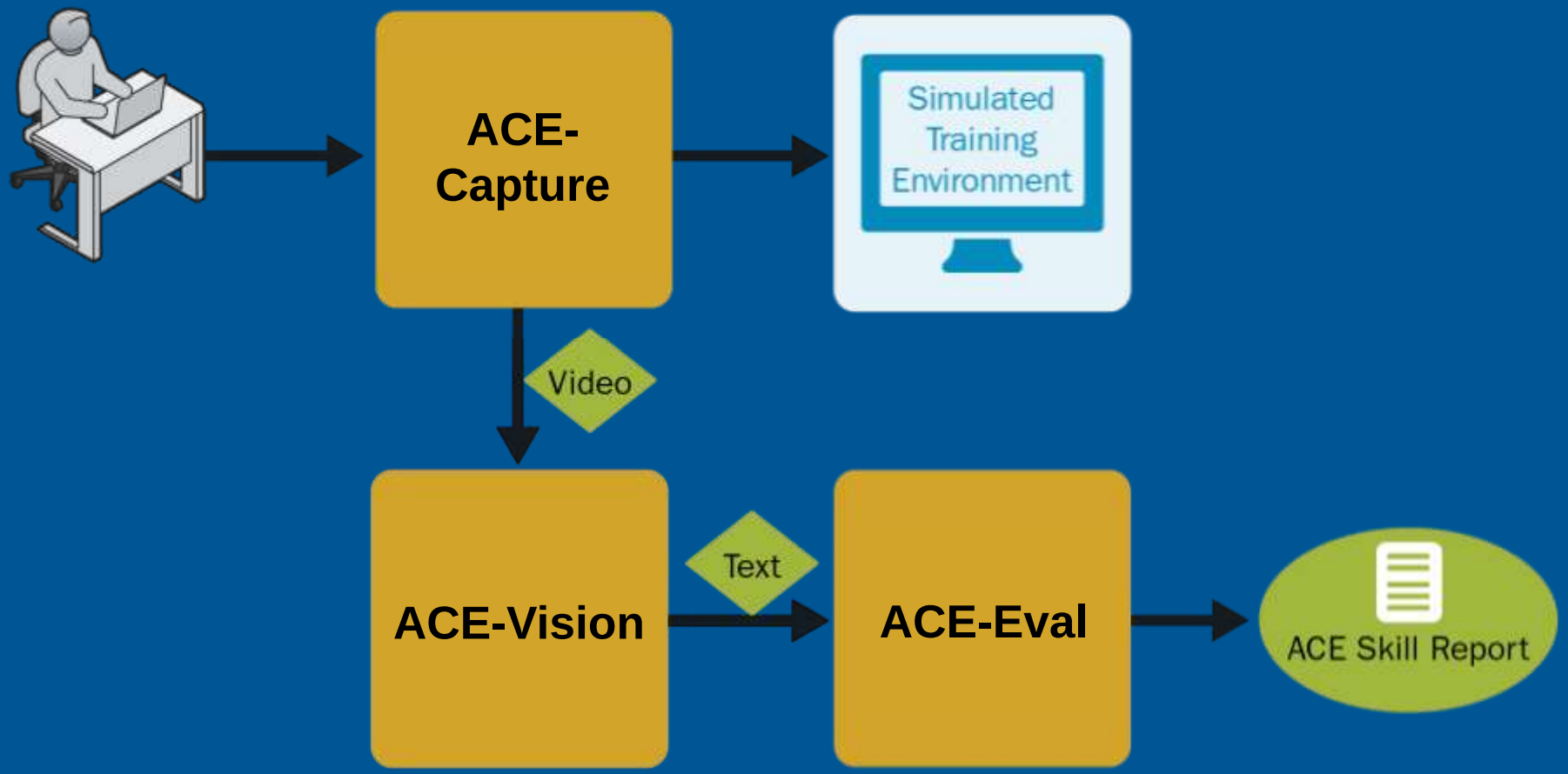
Evaluating Mission-Readiness for Cyber Operators at Scale

- Scalable
- Objective
- Reliable
- Valid

ACE Philosophy

- **Train as you fight?**
- **Evaluate as you fight!**
  - Place cyber operators in familiar environment
  - Task cyber operators with realistic mission
  - Understand actions taken within scenario
  - Verifiably assess mission-readiness based on actions taken
- **Benefits**
  - Automated analysis
  - Specific deficiencies isolated
  - Automated remediation plans
  - Recording available for future review

ACE Architecture Overview



Role Choice

Joint Cyberspace Training &

Certification Standards (JCT&CS)

Forensic Analyst

- 2 Hours
- Existing DoD Standard*
- Self-Contained

* During the course of the project more specific readiness criteria became available

Scenario Development

Scenario I

- **Missing Person**
  - Apartment Searched
  - Laptop Drive Recovered
  - Foul Play Suspected

Scenario II

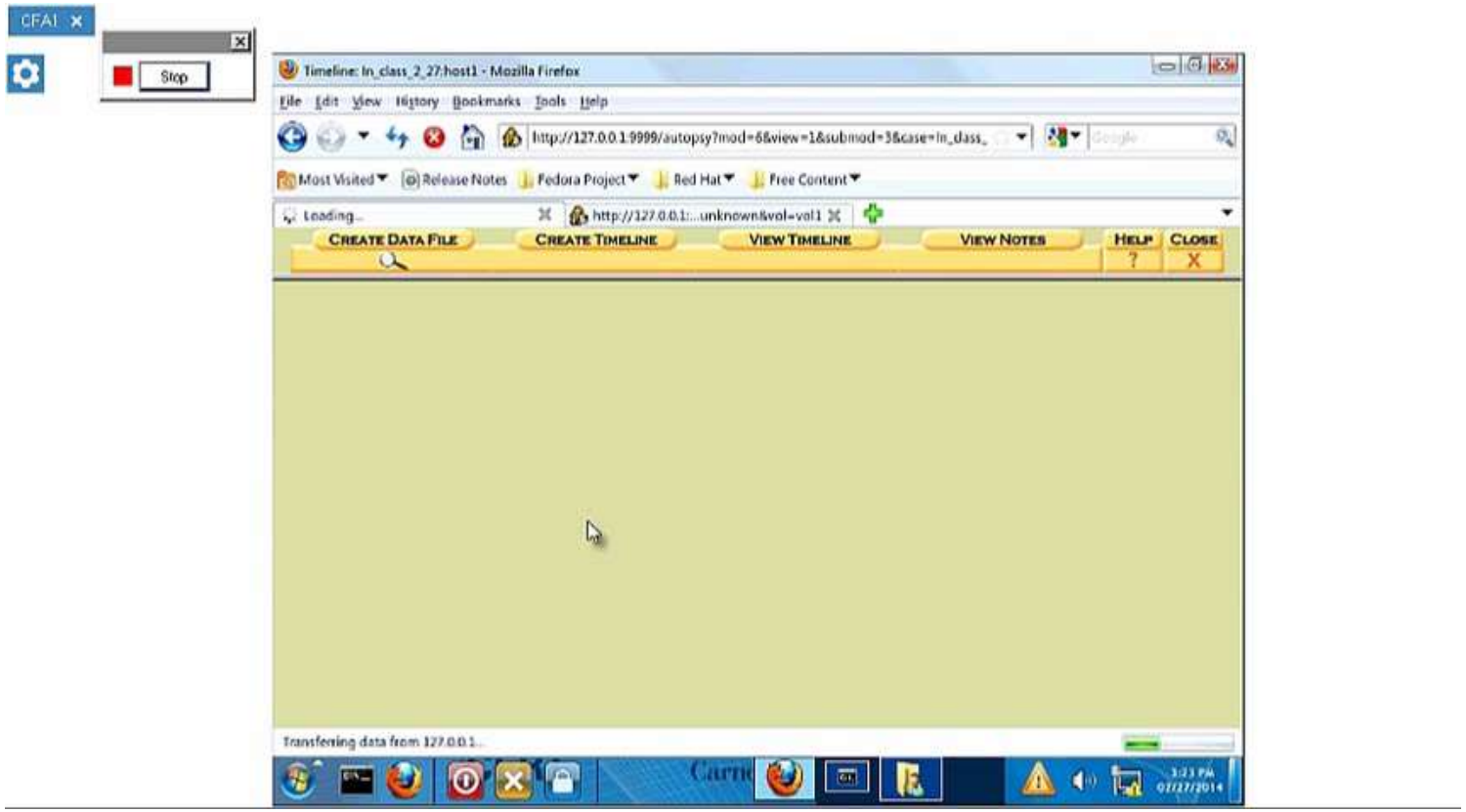
- **Classified* Documents Exfiltrated**
  - Documents In Enemy Hands
  - Source Organization Drives Imaged
  - Multiple Layers
    - APT1
    - USB
    - Personal Email

* Classified for evaluation use – not actual classified information.

Data Collection Capability

- Background Data Collection
- Restricted to Environment
- Scalable

Data Collection Capability



Multiple Sources (Increase Dataset Robustness)

- CERT Staff
- CMU Graduate Students
- DoD Personnel
  - Multiple Collections
- NCFTA Personnel

ACE-Vision

Primary Collaborator:
Professor Yaser Sheik
CMU Robotics Institute, Graphics Lab

Custom Detection System

Designed for massive parallelization

Optimized for use case:

- Maximize pre-process capability
- Minimize duplicate calculations

- Original: O(nN)
  - Infeasible for our problem set.
- Optimized: O(NlogN) time.
  - Implemented on GPU array.

Note: Our data set uses high resolution images and so n >> logN

ACE-Vision - Results

Primary Collaborator:
Professor Yaser Sheik
CMU Robotics Institute, Graphics Lab

Custom Detection System

Custom system running on octoputer hardware

- Faster-than-realtime analysis
- May allow for streaming analysis (not in scope)

ACE-Eval

Primary Collaborator:
Professor Geoffrey Gordon
CMU Machine Learning Department

Development

- Requires Categorized Data
  - Evaluator driven categorization (Training data)
  - Hybrid solution required
    - Differing KSA Complexity
      - Simple Binary Detection
      - Path Analysis
      - Hidden Markov Models
      - Frequency Analysis
    - Automated Anomaly Detection
      - Human Intervention

ACE-Eval

Primary Collaborator:
Professor Geoffrey Gordon
CMU Machine Learning Department

Development

- Data Tagging system
  - Allow subject matter experts (SME) to categorize data
- Several iterations of machine learning solutions
  - Revealed problems in dataset

ACE-Eval

Primary Collaborator:
Professor Geoffrey Gordon
CMU Machine Learning Department

Challenges

- Signal to noise ratio in data is much lower than expected
  - Need larger dataset
- Available personnel are very limited
  - Order of magnitude difference

ACE-Eval

Primary Collaborator:
Professor Geoffrey Gordon
CMU Machine Learning Department

Challenges

- Signal to noise ratio in data is much lower than expected
  - Need larger dataset
- Available personnel are very limited
  - Order of magnitude difference

Adaptation

Changing Problem

- Better standards definitions available
  - 1000/2000 Level tasks
  - Specific skills and activities isolated
- Gate-Based assessment possible
  - ML solution no longer required

Adaptation

Gate-Based Assessment

- Custom Web-app created
  - Allow capture of KSA / Level tasks
    - Nested abilities
    - Linked by Job Role
    - Reusable Templates
    - Bulk Import/Export
  - Designed for merging into evaluation pipeline

Automated Cyber-Readiness

Future Work

Future Work

Transition to CPT evaluation

- Compatible for gate-based assessment
- Part of ongoing PWP work
- Job role transition simplified with specific tasking

Future Work

Stand-Alone utility

- Vision system
  - Insider threat detection
    - Analyst Support
    - Dynamic workstation thresholding
  - User study data collection
    - Experimental tool
- User friendly template generation wizard created
  - Requires no domain specific knowledge
  - Simple screen capture will do!