Automated Cyber-Readiness Evaluation (ACE)

Rotem Guttman
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

Evaluating Mission-Readiness for Cyber Operators at Scale

- Scalable
- Objective
- Reliable
- Valid

68 Cyber Protection Teams (Defend DoD Networks)
DoD Challenge Problem

Evaluating Mission-Readiness for Cyber Operators at Scale

- Scalable
- Objective
- Reliable
- Valid

27 Combat Mission Teams
(Support Combatant Commands)
DoD Challenge Problem

Evaluating Mission-Readiness for Cyber Operators at Scale

- Scalable
- Objective
- Reliable
- Valid

+25 Support Teams
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

- **ACE-Capture**
  - Video

- **ACE-Vision**
  - Text

- **Simulated Training Environment**

- **ACE-Eval**
  - ACE Skill Report
Role Choice

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
**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: $O(N\log N)$ time.
  - Implemented on GPU array.

Note: Our data set uses high resolution images and so $n \gg \log N$
ACE-Vision - Results

Custom Detection System
Custom system running on octoputer hardware
• Faster-than-realtime analysis
• May allow for streaming analysis
  (not in scope)

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

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

Development

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

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

Primary Collaborator:
Professor Geoffrey Gordon
CMU Machine Learning Department
ACE-Eval

Challenges

• Signal to noise ratio in data is much lower than expected
  - Need larger dataset

• Available personnel are very limited
  - Order of magnitude difference

Primary Collaborator:
Professor Geoffrey Gordon
CMU Machine Learning Department
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
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!