Automated Cyber-Readiness Evaluation (ACE)
Rotem Guttman

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213
Core DoD Challenge Problem

Evaluating Mission-Readiness for Cyber Operators

- Scalable
- Objective
- Reliable
- Valid

US cyberspace force to expand further - Pentagon chief

US Defense Secretary Chuck Hagel said Friday the cyberspace force at US Cyber Command will grow to more than 6,000 by the year 2016.
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 → Simulated Training Environment

Video → ACE-Vision

Text → ACE-Eval

ACE-Eval → ACE Skill Report
Role Choice

Forensic Analyst

- 2 Hours
- Existing DoD Standard
- Self-Contained

Joint Cyberspace Training & Certification Standards (JCT&CS)
Scenario Development

Scenario I & II Details

• Missing Person
  • Foul Play Suspected

• Classified* Documents Exfiltrated
  • Computer Drive Image
  • Multiple Layers of Story
    • APT1
    • USB
    • Personal Email

*Fabricated Documents
(Not actual classified data)
Data Collection Capability

- Background Data Collection
- Restricted to Environment
- Scalable
Data Collection

Multiple Sources (Increase Dataset Robustness)

• CERT Staff
• CMU Graduate Students
• DoD Personnel
• Multiple Collections
• NCFTA Personnel
ACE-Vision

Custom Detection System
Designed for massive parallelization
Optimized for use case:
• Maximize pre-process capability
• Minimize duplicate calculations

• Original: $O(nN)$
  • Infeasable for our problem set.
• Optimized: $O(N\log N)$ time.
  • Implemented on GPU array.

Note: Our data set uses high resolution images and so $n >> \log N$
Creating Timeline using all dates (Time Zone:)

Timeline saved to /home/examiner/Autopsy/In_class_2_27/host1/output/all.txt

Entry added to host config file

Calculating MD5 Value

MD5 Value: BC9CCC0A1248EF458523D8890182DB64

(Note: It is easier to view the timeline in a text editor than here)
Vision Module

- Status: In-Progress
Vision Module

• Status: In-Progress
• Collaboration: Professor Yaser Sheik of the CMU Robotics Institute – Graphics Lab.

Creating Timeline using all dates (Time Zone: )
Timeline saved to /home/examiner/Autopsy/In_class_2_27/host1/output/all.txt
Entry added to host config file
Calculating MD5 Value

MD5 Value: BC9CC8A1248EF45852308890182DB64

NOTE: It is easier to view the timeline in a text editor than here)
### ACE Vision Output

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>148</td>
<td>0:50:52 Focused on Shell2 Window</td>
<td>GUI</td>
</tr>
<tr>
<td>149</td>
<td>0:51:00 Focused on Shell4 Window</td>
<td>GUI</td>
</tr>
<tr>
<td>150</td>
<td>0:51:13 sudo autopsy</td>
<td>Shell4</td>
</tr>
<tr>
<td>151</td>
<td>0:51:17 Shell Link Menu opened</td>
<td>Shell4</td>
</tr>
<tr>
<td>152</td>
<td>0:51:18 &quot;Open Link&quot; clicked</td>
<td>Shell4</td>
</tr>
<tr>
<td>153</td>
<td>0:51:22 Focused on Mozilla Firefox Window - <a href="http://localhost:9999/autopsy">http://localhost:9999/autopsy</a></td>
<td>GUI</td>
</tr>
<tr>
<td>154</td>
<td>0:51:24 Firefox &quot;File&quot; Menu opened</td>
<td>Firefox</td>
</tr>
<tr>
<td>155</td>
<td>0:51:26 &quot;Work Offline&quot; menu option clicked</td>
<td>Firefox</td>
</tr>
<tr>
<td>156</td>
<td>0:51:27 &quot;Try Again&quot; button clicked</td>
<td>Firefox</td>
</tr>
<tr>
<td>157</td>
<td>0:51:30 &quot;New Case&quot; button clicked</td>
<td>Autopsy</td>
</tr>
<tr>
<td>158</td>
<td>0:51:34 Case name: &quot;Silver&quot;</td>
<td>Autopsy</td>
</tr>
<tr>
<td>159</td>
<td>0:51:41 Case description: &quot;Missing Persons - Saul Silver&quot;</td>
<td>Autopsy</td>
</tr>
<tr>
<td>160</td>
<td>0:51:44 Case Investigator A: &quot;Rotem Guttman&quot;</td>
<td>Autopsy</td>
</tr>
<tr>
<td>161</td>
<td>0:51:50 Case Investigator B: &quot;Josh Hammerstein&quot;</td>
<td>Autopsy</td>
</tr>
<tr>
<td>162</td>
<td>0:51:51 &quot;New Case&quot; button clicked</td>
<td>Autopsy</td>
</tr>
<tr>
<td>163</td>
<td>0:51:52 &quot;Add Host&quot; button clicked</td>
<td>Autopsy</td>
</tr>
<tr>
<td>164</td>
<td>0:51:59 gedit switched to investigator_notes</td>
<td>Gedit</td>
</tr>
<tr>
<td>165</td>
<td>0:52:02 gedit switched to string_search1.txt</td>
<td>Gedit</td>
</tr>
<tr>
<td>166</td>
<td>0:52:06 gedit &quot;Find&quot; window opened</td>
<td>Gedit</td>
</tr>
<tr>
<td>167</td>
<td>0:52:07 gedit &quot;Find&quot; button clicked - search for: &quot;hostname&quot;</td>
<td>Gedit</td>
</tr>
<tr>
<td>168</td>
<td>0:52:09 gedit switched to string_search1.txt</td>
<td>Gedit</td>
</tr>
<tr>
<td>169</td>
<td>0:52:18 Focused on Mozilla Firefox Window - <a href="http://localhost:9999/autopsy?mod=0&amp;view=7&amp;case=Silver&amp;x=83&amp;y=6">http://localhost:9999/autopsy?mod=0&amp;view=7&amp;case=Silver&amp;x=83&amp;y=6</a></td>
<td>GUI</td>
</tr>
<tr>
<td>170</td>
<td>0:52:21 Host Name: &quot;saul-n3erunyuq5&quot;</td>
<td>Autopsy</td>
</tr>
<tr>
<td>171</td>
<td>0:52:39 Host Description: &quot;Saul Silver's Computer&quot;</td>
<td>Autopsy</td>
</tr>
</tbody>
</table>

*Confidence measures associated with each row omitted.*
Visualization: Synchronized Data
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 Skill Report

ACE SKILL REPORT

Mission Ready:
- Properly mounted evidence drive(s)
- Properly Analyzed Registry
- Properly Analyzed Logs
- Displayed Knowledge of data carving techniques
- Performed MAC timeline analysis

Not Mission Ready:
- Determined exploitation vector
- Performed Tier 1,2,3 Malware Analysis

Output of Evaluation System
- Determines mission-readiness
- Isolates deficiencies
- Recommends additional training
- Automated remediation plans
Future Work

• High Transition Potential
  • Compatible with existing work
  • CPT integration
  • Additional job roles

• FY16 Plans
  • Evaluation of analyst to DoD partner’s satisfaction
  • Identification of additional roles
  • Integration of ACE capabilities with AC3 processes

• Post FY16
  • Integration with PWP work
  • Role expansion
  • Squad level evaluation