# Automated Cyber-Readiness Evaluation (ACE) Rotem Guttman

Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213





Software Engineering Institute

**Carnegie Mellon University** 

Distribution Statement A Approved for Public Release; Distribution is Unlimited

#### Copyright 2015 Carnegie Mellon University

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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution except as restricted below.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon<sup>®</sup> and CERT<sup>®</sup> are registered marks of Carnegie Mellon University.

DM-0002758

### **Core DoD Challenge Problem**



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. Evaluating Mission-Readiness for Cyber Operators

- Scalable
- Objective
- Reliable
- Valid

SEI Research Review 2015 October 7–8, 2015 © 2015 Carnegie Mellon University Distribution Statement A: Approved for Public

Release; Distribution is Unlimited

#### 3

Software Engineering Institute Carnegie Mellon University

# **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
  - <u>Verifiably</u> asses mission-readiness based on actions taken
- Benefits
  - Automated Analysis
  - Specific deficiencies isolated
  - Automated remediation plans
  - Recording available for future review

### **ACE Architecture Overview**





SEI Research Review 2015 October 7–8, 2015

© 2015 Carnegie Mellon University Distribution Statement A: Approved for Public Release; Distribution is Unlimited

### **Role Choice**





#### **Forensic Analyst**

- 2 Hours
- Existing DoD Standard
- Self-Contained

Joint Cyberspace Training & Certification Standards (JCT&CS)

### **Scenario Development**



\*Fabricated Documents (Not actual classified data)

#### Scenario I & II Details

- Missing Person
  - Foul Play Suspected

### Classified\* Documents Exfiltrated

- Computer Drive Image
- Multiple Layers of Story
  - APT1
  - USB
  - Personal Email



7

SEI Research Review 2015

Software Engineering Institute Carnegie Mellon University

### **Data Collection Capability**





- Background Data Collection
- Restricted to Environment
- Scalable

SEI Research Review 2015 October 7–8, 2015

© 2015 Carnegie Mellon University Distribution Statement A: Approved for Public Release; Distribution is Unlimited

### **Data Collection**





### 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)
  - Infeasable for our problem set.
- Optimized: O(NlogN) time.
  - Implemented on GPU array.

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

Timeline: In_class_2_27:host1 - Mozilla Fire	ox			0	O X
Eile Edit View History Bookmarks Iool	u <u>H</u> elp				
😋 🜍 🔻 🍫 😳 🏠 🏚 http:	//127.0.0.1.9999/autopsy?	mod=6&view=1&submod=5&ca	ase=in_dass_ 🔹 🔻	📲 🗸 Geogle	94
📸 Most Visited 🔻 🙆 Release Notes 🕕 Fed	ora Project 🔻 🔒 Red Hat	🔻 📙 Free Content 🔻			
Timeline: In_class_2_27:host1	<b>\$</b>				*
CREATE DATA FILE CRE	ATE TIMELINE	VIEW TIMELINE	View Notes	HELP (	X
Creating Timeline using all dates (Time Zo	one: )				
Timeline saved to /home/examiner/Auto	psy/In_class_2_27/ho	ost1/output/all.txt			
Entry added to host config file					
Calculating MDS Value					
MD5 Value: BC9CCC8A1248EF458523D889	01820864				
OK (NOTE: It is easier to view the timeline in	a text editor than here)	)			

Done









Timeline: In_class_2	27:host1 - Mozilla Firefox		
Eile Edit View High			
0 0 • 47		teople	9
🔞 Most Visited 🔻 🙆			
🏠 Timeline: In_class_2			-
CREATE DATA		?	X
Creating Timeline us			
Timeline saved to /h			
Entry added to host			
Calculating MD5 Valu			
MD5 Value: BC9CCC6			
OK D			
(NOTE: It is easier to			
Done			
🕑 🔤 後			1:24 PA

Timeline: In_class_2_27:host1 - Mozilla Firefox			00 8
Eile Edit View History Bookmarks Tools Help			
③ ● ▼ 47 ◎ ▲ http://127.0.0	1.9999/autopsy?mod=6&view=1⊂	omod=5&case=In_dass_ 🔿 👻 🔀 🕇 Geogle	9,
📸 Most Visited 🔻 🙆 Release Notes 🕕 Fedora Proje	ct 🔻 📙 Red Hat 👻 📙 Free Content		
🚯 Timeline: In_class_2_27:host1 👘			-
CREATE DATA FILE CREATE TIN		E VIEW NOTES HE	CLOSE X
Timeline saved to /home/examiner/Autopsy/In Entry added to host config file Calculating MDS Value MDS Value: BC9CCC0A1240EF450523D8890182D80 OK (NOTE: It is easier to view the timeline in a text e	_class_2_27/host1/output/all.1	txt	

٩

**61** 

12

**I** 

A + T 02/27/2014

Carne

Done



# **ACE Vision Output**



	А	В	С
148	0:50:52	Focused on Shell2 Window	GUI
149	0:51:00	Focused on Shell4 Window	GUI
150	0:51:13	sudo autopsy	Shell4
151	0:51:17	Shell Link Menu opened	Shell4
152	0:51:18	"Open Link" clicked	Shell4
153	0:51:22	Focused on Mozilla Firefox Window - http://localhost:9999/autopsy	GUI
154	0:51:24	Firefox "File" Menu opened.	Firefox
155	0:51:26	"Work Offline" menu option clicked	Firefox
156	0:51:27	"Try Again" button clicked.	Firefox
157	0:51:30	"New Case" button clicked	Autopsy
158	0:51:34	Case name: "Silver"	Autopsy
159	0:51:41	Case description: "Missing Persons - Saul Silver"	Autopsy
160	0:51:44	Case Investigator A: "Rotem Guttman"	Autopsy
161	0:51:50	Case Investigator B: "Josh Hammerstein"	Autopsy
162	0:51:51	"New Case" button clicked	Autopsy
163	0:51:52	"Add Host" button clicked	Autopsy
164	0:51:59	gedit switched to investigator_notes	Gedit
165	0:52:02	gedit switched to string_search1.txt	Gedit
166	0:52:06	gedit "Find" window opened	Gedit
167	0:52:07	gedit "Find" button clicked - search for: "hostname"	Gedit
168	0:52:09	gedit switched to string_search1.txt	Gedit
169	0:52:18	Focused on Mozilla Firefox Window - http://localhost:9999/autopsy?mod=0&view=7&case=Silver&x=83&y=6	GUI
170	0:52:21	Host Name: "saul-n3eruqnyq5"	Autopsy
171	0:52:39	Host Description: "Saul Silver's Computer"	Autopsy

\*Confidence measures associated with each row omitted.

Software Engineering Institute | Carnegie Mellon University

SEI Research Review 2015 October 7–8, 2015 © 2015 Carnegie Mellon University Distribution Statement A: Approved for Public Release; Distribution is Unlimited

### **Visualization: Synchronized Data**

Software Explorering Institute | Carmyle Million Calencely

Chat with Admin Team

٥

Admin Team

Stop

ple pit yew jearch jook III ( Copen • Save Car "uning searchine X The read tany indications of gambling Car tany indications of interest funcent Vega led Jones hossible location of interest ings Creek Cemetery up in C hossible username: subsilversurfer prama.tambelli Hillized apps: Skype (check bissible email address: mont.vega94/gmail.com subsilversurfer/phail.com bissible conversation log: 154272366 What6ipos;s going	naminer@fil4-fores-2011-01-086- Edt Yew Search Jerminal Tab niner@fil4-fores-2011-01-086- aniner@fil4-fores-2011-01-1386 case core.2010 Desktop Dat miner@fil4-fores-2011-01-1386 aniner@fil4-fores-2011-01-1386	a Belp 31 caaminer@h14-foren-2011-01-0385- -]\$ 15 cuments Downloads Pictures temp -]5 echo "granu.taxbells" > case/ -]5 grep -1 -7 Case/Sirty words5.	X Valatit dirty vor tat 5 das	examiner@ft14-foren-2011-01-380 - ity sp.ed cs3.fs1 e/strikg_search5.ts1	N N N
Corn Corn Throng searching of gambling Tany indications of gambling Tany indications of gambling Tansent Wega Ted Jones Nossible location of interest Lings Creek Cemetery up in 1 Ressible username: Hulsilversurfer prama.tambelli Rtilized apps: Skype (check Possible email address: mont.vega94/gmail.com Hulsilversurfer[gmail.com Hulsilversurfer[gmail.com Hulsilversurfer[gmail.com	Edt Vew Search Jerninal Taj niner@fc14-foren-2011-01-1366 - 2011rer@fc14+foren-2011-01-1386 case core.2010 Desktop Der imiter@fc14-foren-2011-01-1388	BHD M examiner@Al4-foren-2011-01-0386 - -j\$ is cuments Downloads Pictures temp -j\$ echo "gramu.tambelli" > case/ -j\$ grep -1 -f case/CIrty_words5.	X Velatil difty_vor tat > cas	examiner@fc14-foren-2011-01-386 - ity sp.ed cs3.ts1 e/string_Search5.tst	м -
"thing searchine of gambling for any indications of gambling for any indication of interest fincent Wega Ted Jones "Tossible location of interest Lings Greek Genetery up in G	niner@fc14-foren-2011-01-1365 esse core.2010 Desktop Des miner@fc14-foren-2011-01-1305 miner@fc14-foren-2011-01-1305	<pre>34 csaminer@ht14-foren-2011-01-038s - -]\$ L5 cuments Downloads Pictures temp -]\$ echo "gram.tambells" &gt; case/ -]\$ grep -1 -f Case/Cirty words5.</pre>	X Vələttil dirly vor tət > cəs	examiner@ft14-foren-2011-01-380 - ity sp.6d c55.ta1 e/string_sear085.ta1	× .
Any indications of gambling of Any indications of gambling of Assible persons of interest Find Jones Possible location of interest Lings Creek Cemetery up in P Possible username: subsileersurfer prama.tambelli Itilized apps: Skype (check Possible email address: rent.vegs4040paall.com coulsilversurfer0paall.com coulsilversurfer0paall.com coulsilversurfer0paall.com	aniter@fc14-fores-2011-01-1386 case core.2010 Desktop De aniter@fc14-fores-2011-01-1386 aniter@fc14-fores-2011-01-1386	-j\$ is cuments Downloads Pictures temp -j\$ echo "gramu.tambelli" > case/ -j\$ grep -i -f case/dirty_words5.	Vslatit dirty vor txt > cas	ity sp.dd ds5.tal e/string_search5.tal	
154272366 WhatGaposis going					
137146900 bey Saul 137149050 1 donkapos;t mess aroun 131199446 D(["gn", 'Saul Silver'] 131424052 #saulsilversurfer/Sgrav 13142644 Saul, no dice on Philly 1423796199 #saulsilversurfer/Sgrav 1423796454 grama.tambelli saulsi 1423796454 grama.tambelli saulsi 1423796454 grama.tambelli saulsi 1423796459 saulsilversurfer 1423796414 #saulsilversurfer/Sgr	nd Saul, I know you&aposjre an ma.tambell1;7e9eb883ae02Dc5a y ama.tambell1;6r3fr4dr24cB3e26J lversurfergrama.tambell1 sauls ama.tambell1;7e9eb883ae820c5aJ	ound ilversurfergrama.tambelli saulsilv	ersurferG	irama Tambelli į Yo G-man, this :	
			Plain fext *	Tab Width: # * Ln 19, Col 1	26
		carneg as a l	the states		10144



### 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**

ACI	E SKILL REPORT
Mission	n Ready:
•	Properly mounted evidence drive(s)
•	Properly Analyzed Registry
•	Properly Analyzed Logs
•	Displayed Knowledge of data carving techniques
•	Performed MAC timeline analysis
Not Mis	ssion Ready:
•	Determined exploitation vector
•	Performed Tier 1,2,3 Malware Analysis

R

PAGE 1 OF 3 317 WORDS

Output of Evaluation
System

- Determines missionreadiness
- 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