

**Tim Fraser**  
**Program Manager, Information Innovation Office**

---

**Moving Anti-Malware Research Forward**

DARPA Cyber Colloquium  
Arlington, VA

November 7, 2011



# Report Documentation Page

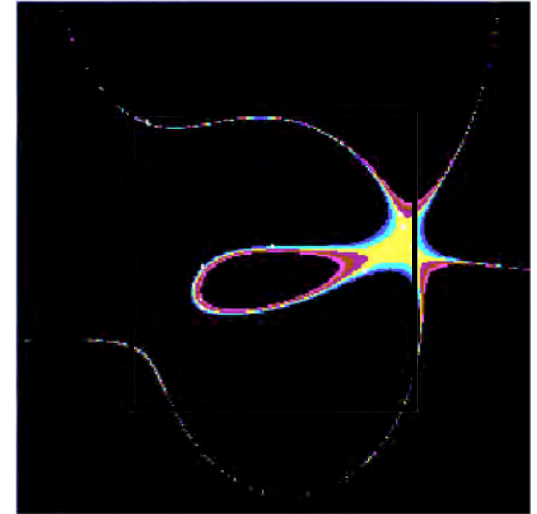
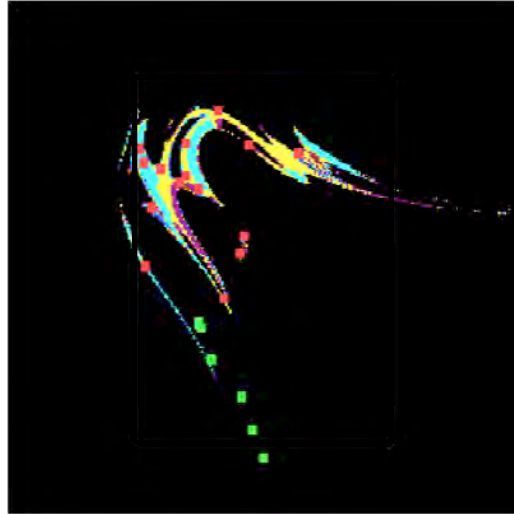
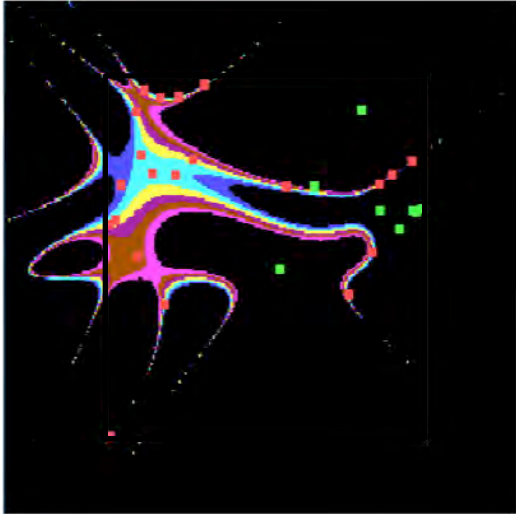
*Form Approved*  
*OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE <b>07 NOV 2011</b>		2. REPORT TYPE		3. DATES COVERED <b>00-00-2011 to 00-00-2011</b>	
4. TITLE AND SUBTITLE <b>Moving Anti-Malware Research Forward</b>				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Defense Advanced Research Projects Agency (DARPA), Information Innovation Office, 3701 North Fairfax Drive, Arlington, VA, 22203-1714</b>				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES <b>Presented at the Colloquium on Future Directions in Cyber Security on November 7, 2011, Arlington, VA.</b>					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			



# The boundary between malicious and benign is fractally complex



(Source: Sentar Inc.'s MATCH project.)

- We and our adversaries are both exploring the boundary
- Their costs are low
- Ours are high

Leveling the Playing Field with Automation



# WANTED: Breakthroughs in Deep Program Analysis

Program:	<b>Cyber Genome</b>	<b>APAC</b>
Insight:	Reuse resembles heredity	Analyses can now scale <div style="display: inline-block; border: 1px solid black; padding: 2px; margin-left: 10px;">SeL4 9KLOC [Klein 2009]</div> <div style="display: inline-block; border: 1px solid black; padding: 2px; margin-left: 10px;">Linux 6MLOC [Dillig 2008]</div>
Approach:	Extract lineage graphs	Define and demonstrate properties
Application:	Do profiling and forecasting	Certify mobile applications

Reduce Human Analysis Time – Reduce Costs



## DARPA Program Analysis Challenge

---

*A second way to participate in the APAC effort*

Open to all comers

A chance to prove your program analysis chops

Win cash

Early 2013

- DARPA provides a set of mobile applications
- Bring your own tools
- Set time limit
- Compete to label each app as malicious or benign most accurately

E-mail [ProgramAnalysisChallenge@DARPA.mil](mailto:ProgramAnalysisChallenge@DARPA.mil)