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

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
07 NOV 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Moving Anti-Malware Research Forward	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) **Defense Advanced Research Projects Agency (DARPA),Information Innovation Office,3701 North Fairfax Drive,Arlington,VA,22203-1714**	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
Approved for public release; distribution unlimited

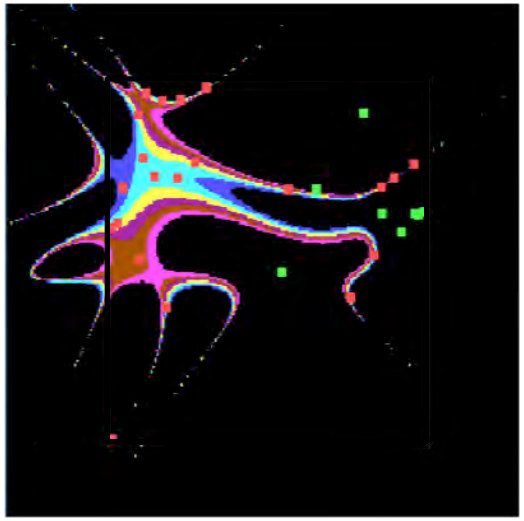
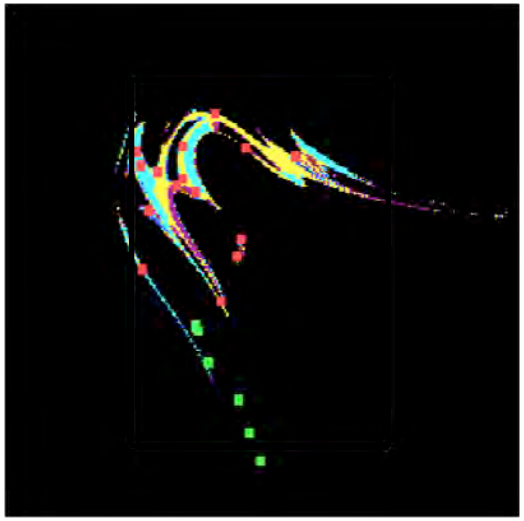
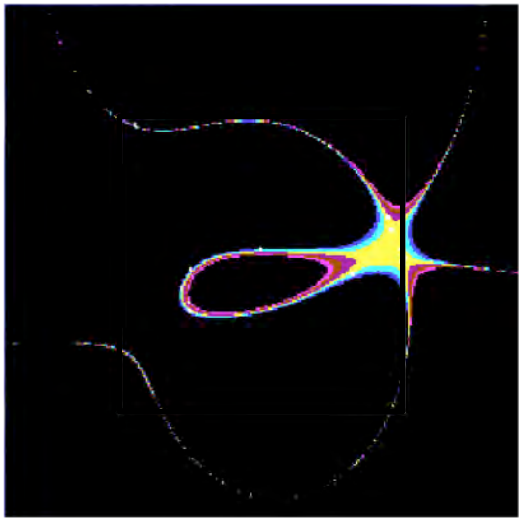
13. SUPPLEMENTARY NOTES
Presented at the Colloquium on Future Directions in Cyber Security on November 7, 2011, Arlington, VA.

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. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**4**	

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:	**Cyber Genome**	**APAC**
Insight:	Reuse resembles heredity	Analyses can now scale
Approach:	Extract lineage graphs	Define and demonstrate properties
Application:	Do profiling and forecasting	Certify mobile applications

SeL4 9KLOC [Klein 2009]

Linux 6MLOC [Dillig 2008]

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