Tim Fraser

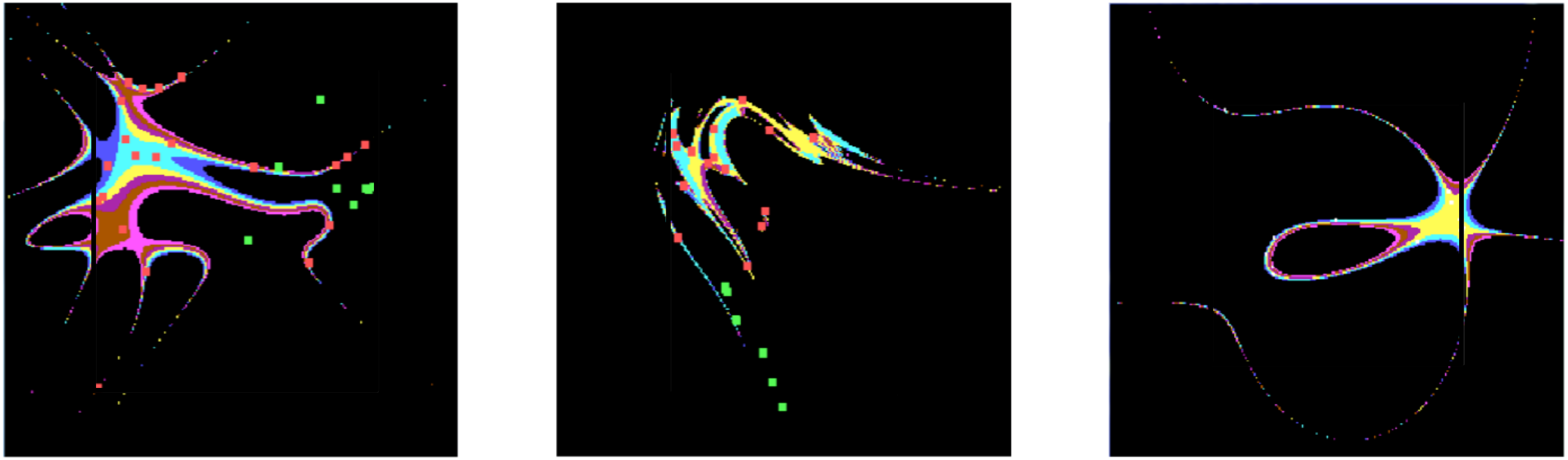
Program Manager, Information Innovation Office

Moving Anti-Malware Research Forward

DARPA Cyber Colloquium
Arlington, VA

November 7, 2011

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 SeL4 9KLOC [Klein 2009] Linux 6MLOC [Dillig 2008]
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