Peiter “Mudge” Zatko
Program Manager, Information Innovation Office

If you don't like the game, hack the playbook...

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
If you don’t like the game, hack the playbook...	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

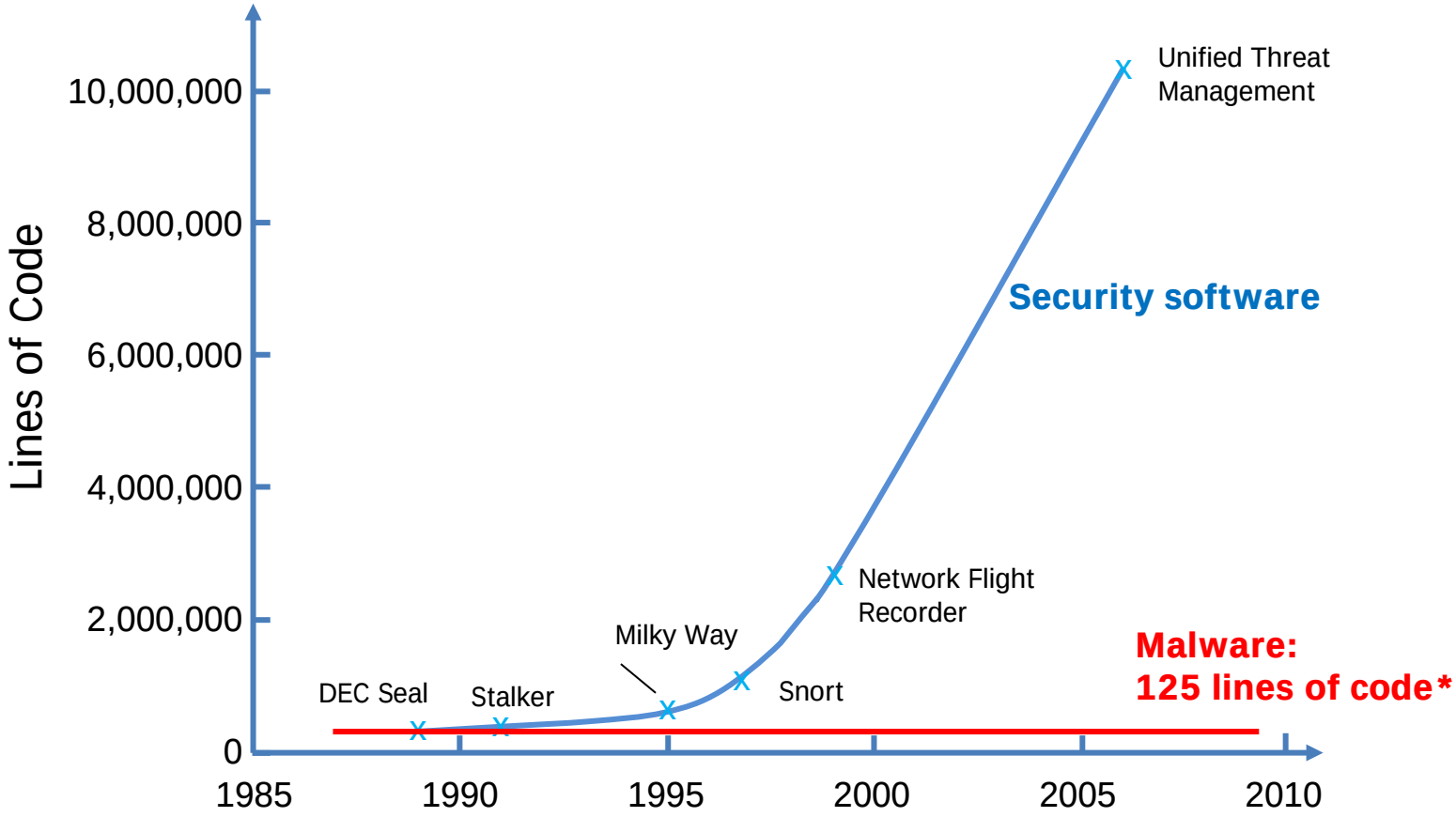
13. SUPPLEMENTARY NOTES
Presented at the Colloquium on Future Directions in Cyber Security on November 7, 2011, Arlington, VA.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**10**	

The Problem: Not Convergent

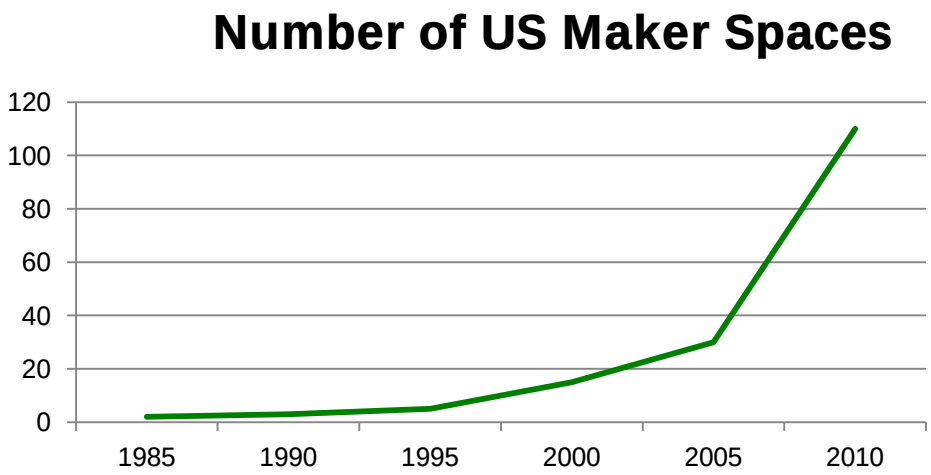


* Public sources of malware averaged over 9,000 samples (collection of exploits, worms, botnets, viruses, DoS tools)

Maker spaces and boutique security firms

- Small groups of motivated and like minded researchers have repeatedly shown significant talent and capabilities.
- Commodity high end computing, personal prototyping and fabrication capabilities, and open software tools remove barrier to entry.
- The new “home brew computer club”...
- This relationship needs to be mutually beneficial. DARPA intends to cultivate relations and become a resource.

NYC Resistor – Brooklyn, NY
Source: Make Magazine



The New Cyber Braintrust

Assembly, Helsinki, Finland May 8, 2004

Cyber Fast Track

DARPA-PA-11-52

Patient Zero

Dino Dai Zovi

Hank Leininger

Fyodor

Bruce Potter

Cyber Fast Track Themes

- Crowd
  - Many eyes on many efforts
- Fast and cheap
  - Faster than adversary lifecycle (transition while still relevant)
  - Low price point
- Diverse
  - Numerous approaches
  - Numerous efforts

The key to a good strategy is to have multiple options.

Current Cyber Fast Track Efforts

Performer	Effort	Period of Performance
Rogue Networks	Methods of Detecting Malicious Web Server Traffic	3 Months
Immunity Federal Services, LLC	Combining Expert Knowledge and Symbolic Analysis for Detection of Exploitable Bugs	7 Months
Charlie Miller	Evaluation of Near Field Communication in Mobile Smartphones	7 Months
Secure Ideas, LLC	MobiSec Live Environment Mobile Testing Framework	3 Months
Korelogic, Inc.	Hand Held Testing	2 Months
Assured Information Security, Inc.	MoRE: Measurement of Dynamic Code	4 Months
Peak Security, Inc.	TinyLANE - Mobile Hardware Endpoint Security for Individuals	9 Months
Raphael Mudge	A Language to Control and Automate Cyber Capabilities	7 Months

Cyber Fast Track So Far...

In its first 2 months:

- 31 submissions - 19 non-traditional performers
- 8 awards - 7 non-traditional performers
- Average time from submission to award is 7 days
- Average period of performance: 5 months

www.cft.usma.edu

Cyber Fast Track

PA #: DARPA-PA-11-52

CyberFastTrack@DARPA.MIL

DARPA CFT Town Hall meetings

URL: http://www.cft.usma.edu

Contact: CyberFastTrack@darpa.mil