Information Innovation Office (I2O):
Information: a force multiplier

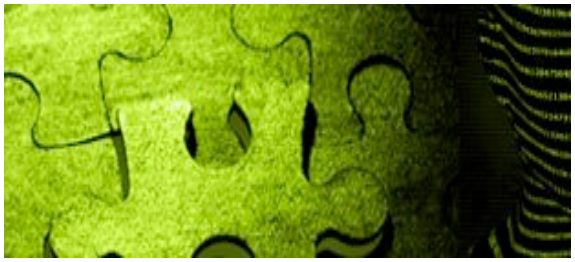
Dan Kaufman

Briefing prepared for Computing Research Association
February 28, 2011

I2O: Mission and Thrusts

Mission: Ensure U.S. technological superiority in all areas where information can be a force multiplier and provide a decisive military advantage.

Thrust Areas



Understand

Empower

Connect

- Intelligence, surveillance, and reconnaissance (ISR) exploitation
- Cyber
- Language, education and training
- Social networking and social sciences

Insight: next generation ISR exploitation system

Adaptive exploitation and resource management tools
Unified all-source ISR workstation

- Increase number of participants
- Lower cost of entry

- Test multiple operational concepts

- Evaluation under realistic conditions
- Support service transition

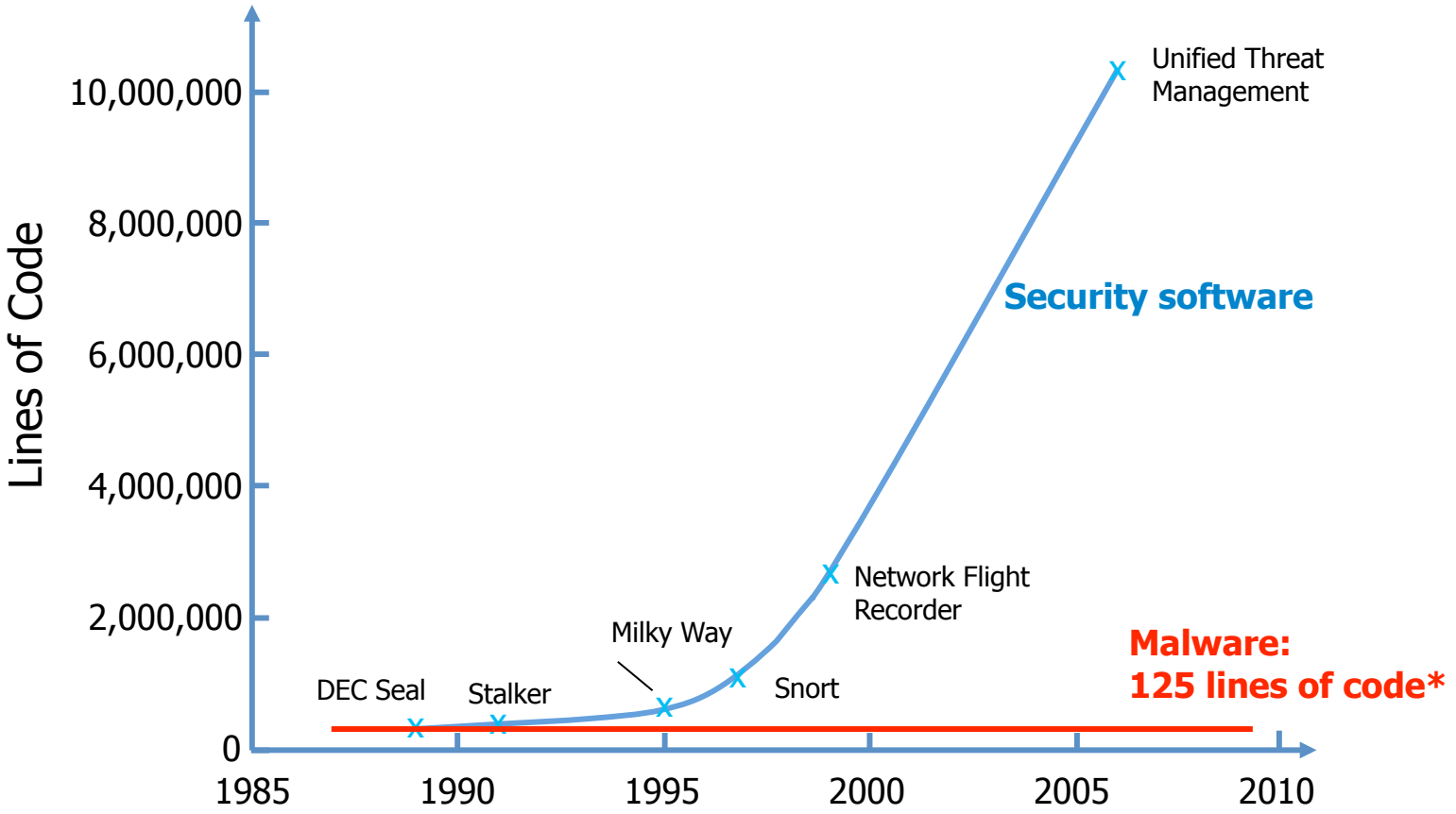
Real test bed
- Collected data
- Processed data
- Variable resolution

Virtual environment
- Simulated sensor data
- Augmented real world

Physical test bed
- National Training Center

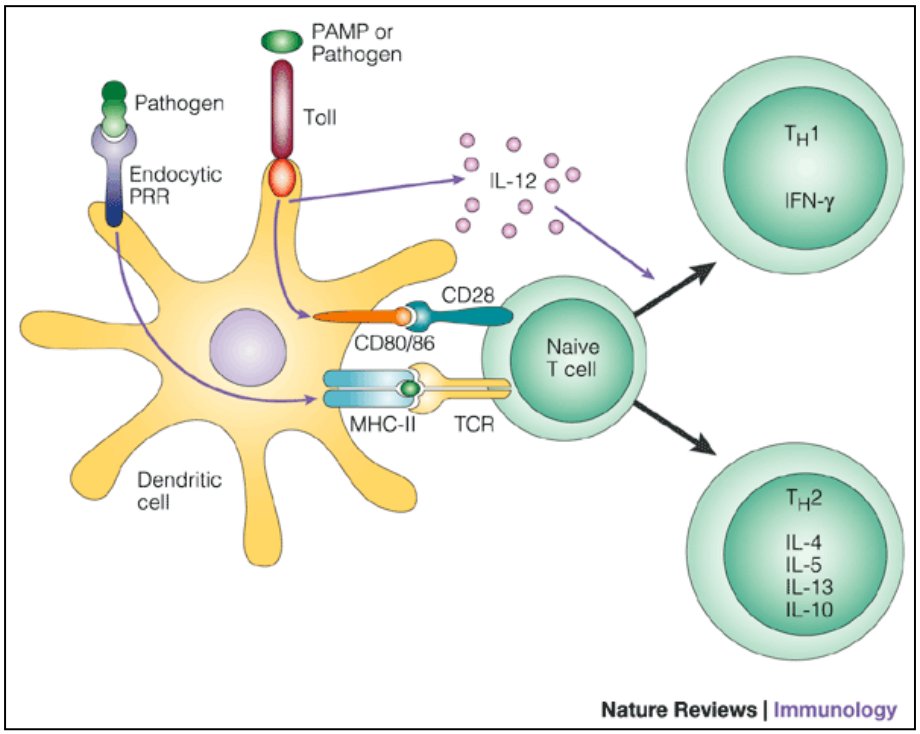
Theater

Cyber: We are divergent with the threat…



* Malware lines of code averaged over 9,000 samples

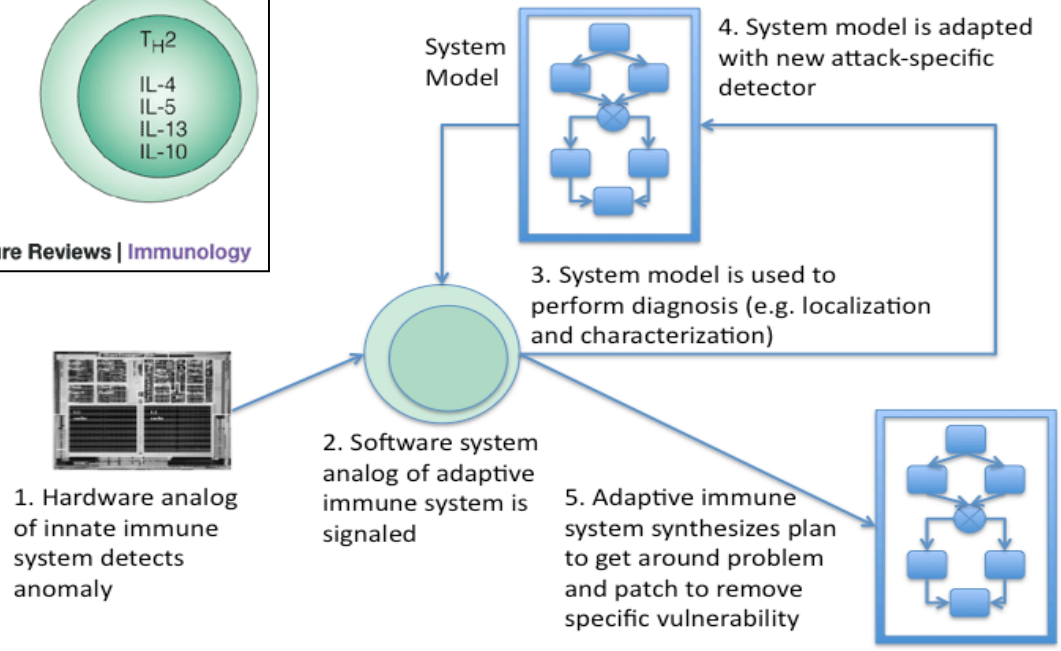
Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH)



- Preventing common attacks.
- Adapting in response to unanticipated attacks.
- Create diversity so attacker has to deal with heterogeneity.

New architectures guided by biology that eliminate common technical vulnerabilities

- Diagnoses root causes of vulnerabilities and builds situational assessment.
- Learns from previous attacks and gets better at self-protection.
- Increases and refreshes system diversity.



Cyber Genome

Provides an alternative to signature-based malware detection schemes that are trivial to defeat through small variations in malware signatures.

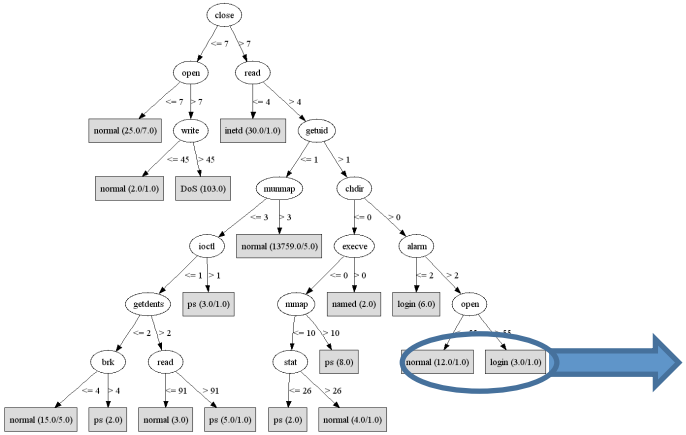
Leverage Bio-Inspired constructs to create the cyber equivalent of fingerprints and DNA

- Autonomously map digital artifacts to identify the cyber genetics and heredity.
- Determine the provenance of the malware.

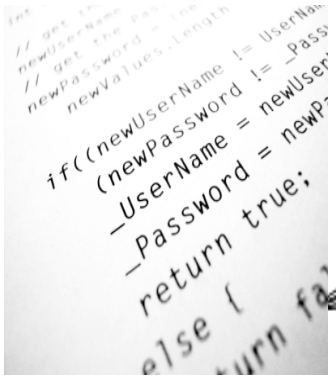
Currently, a change to a single bit or letter in a large file changes the signature of that file.

- Anti-virus technologies can only scan for known signatures and limited heuristics.

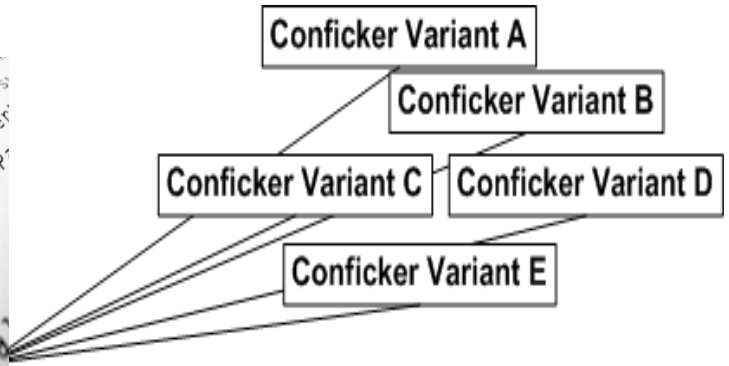
Cyber Genome will derive core "Cyber DNA" to defend against malware variants instead of signatures.



Malware Decision Tree



Extracted "Cyber DNA"



Protection against entire families of malware

PROgramming Computation on EncryptEd Data (PROCEED)

Vision: To perform arbitrary computations on encrypted data without decryption, preserving confidentiality *even on untrustworthy computational infrastructure.*

What if all computation could be done on encrypted data?

- System hardware and software provenance concerns reduced
- Data provenance and availability remain concerns

- Program Overview/Approach
  - The problem of computing on encrypted data was posed as an open question in 1978
  - Secure multi-party computation (SMC) solutions were invented in the 1980s, but efficiency remains a problem today
  - The first (theoretical) fully homomorphic encryption (FHE) scheme was invented in 2009
  - PROCEED is searching for efficient implementations of SMC or FHE approaches that can be implemented on modern computing hardware

Encrypted computing in the cloud as privately as in your data center

GALE Broadcast Monitoring System*
Arabic example

3 Automatic **translation** of Arabic transcript

2 Automatic **transcription** of Arabic speech

1 Real-time streaming video (~5 min delay)

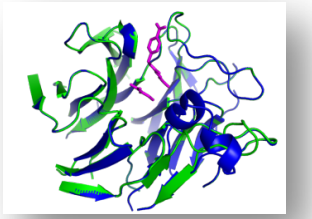
Sample Fielded Arabic Translation

* A BBN application developed & deployed by TSWG

Effective learning and problem solving are critical to DoD

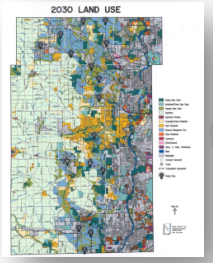
- Many complex problems critical to DoD difficult to solve by conventional means

Drug design

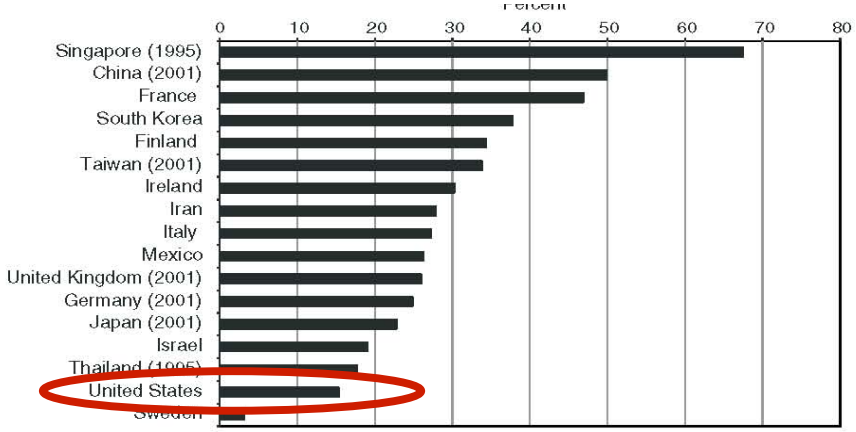


Packing problems

Strategy discovery



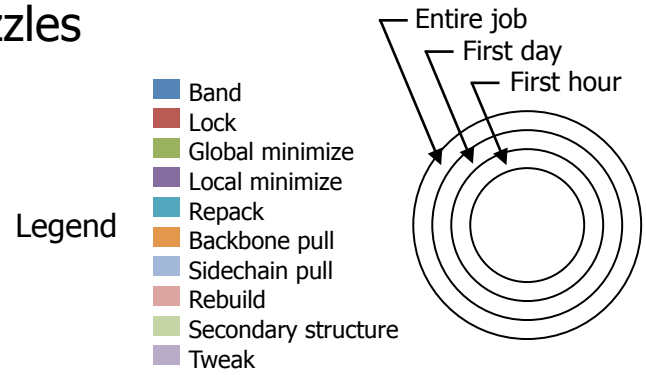
- DoD is facing a shortage of top quality U.S. engineers and scientist

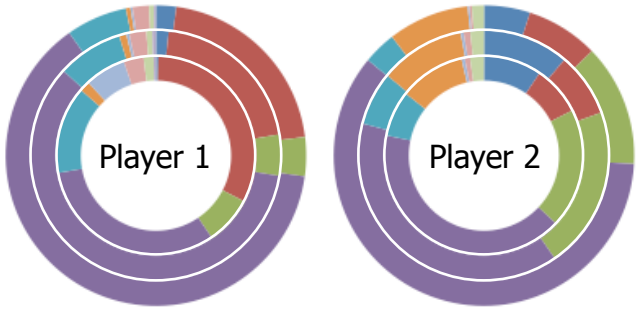


From 4th to grade to 10th grade, U.S. student performance in math/science drops from 8th/11th to 21st/25th relative to other countries.

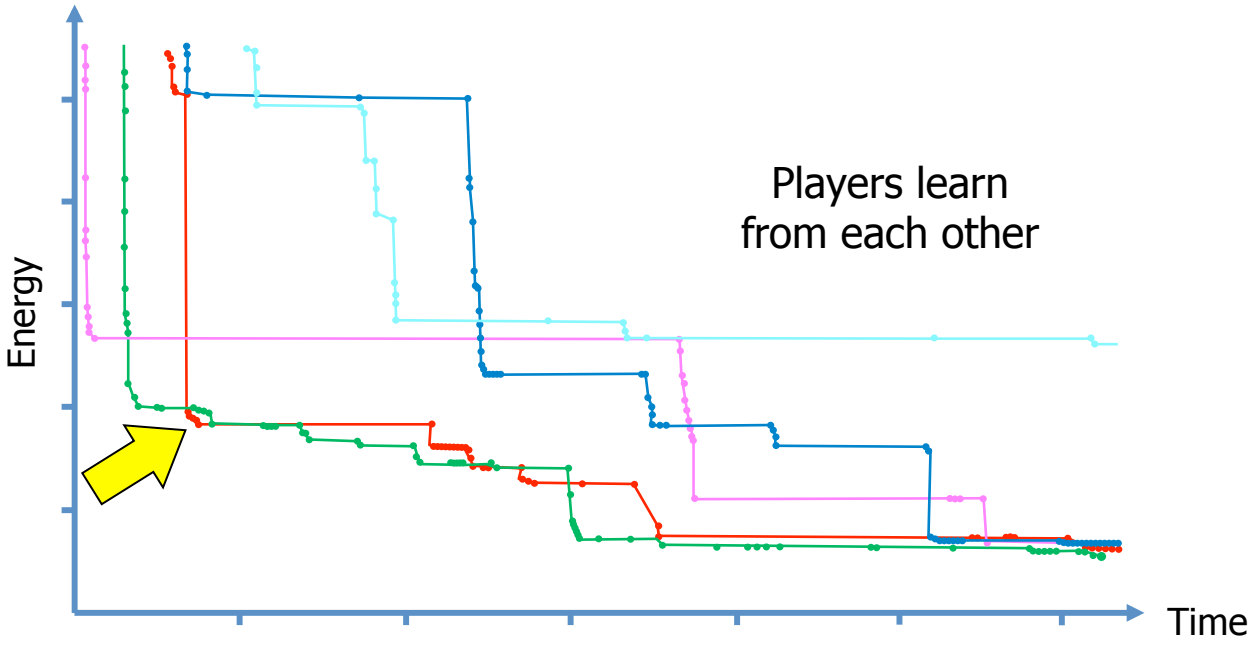
Social networking for complex tasks… Foldit

Puzzles





Players learn successful strategies



Social networking: DARPA Red Balloon challenge

Purpose: Research mobilization, self-organization potential of social networks & crowd sourcing.

Challenge: Locate 10 large, red weather balloons at undisclosed locations across the United States on Saturday, December 5, 2009.

Result: All 10 balloons located in 8 hours 52 minutes

- Winner = MIT Red Balloon Challenge Team (recursive scheme)
- 4,368 total registrants
- Widespread news coverage

  NY Times, *WSJ, Washington Post*, CNN, MSNBC, ABC, etc.

Balloon Locations/ Time First Submitted

Balloons Went Up at 10:00 EST