Drew Dean
Program Manager, Information Innovation Office

PROCEED and Crowd-sourced Formal Verification

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
PROCEED and Crowd-sourced Formal Verification	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)**	**9**	

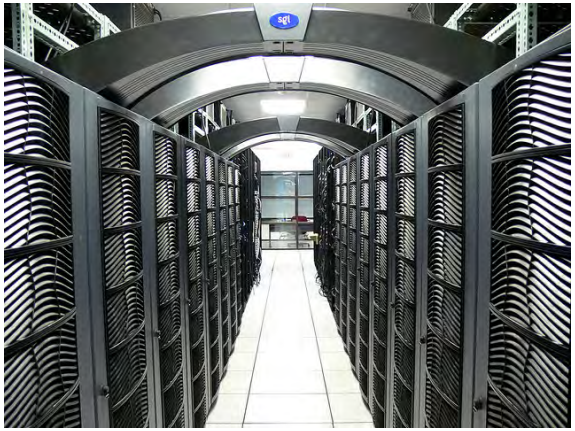
Do you trust the cloud?

Source: Library of Congress/Flickr

Secure communications…

Source: General Services Administration

Secure storage…

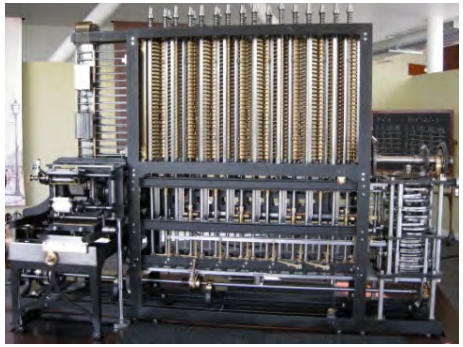


Source: Christopher Bowns/Flickr

Secure computation?

PROgramming Computation on EncyrptEd Data (PROCEED)

Goal: practical computation on encrypted data without decrypting



Source: Catherine Helzerman /Fickr

Babbage Difference Engine

150 years

1832 - 1982

7 Orders of Magnitude

Source: Flylogic Engineering LLC; Corbis

Intel 80286

2010 - 2015

5 years

Source: Corbis

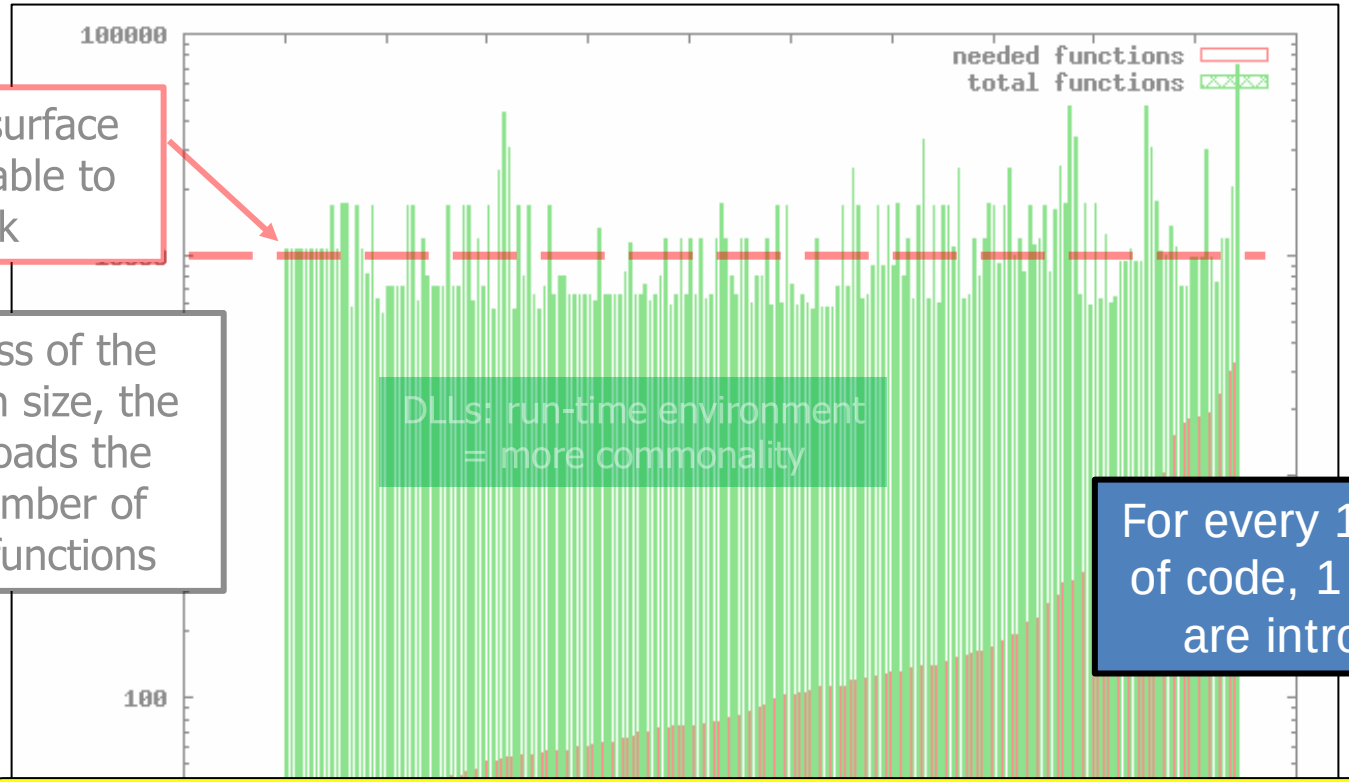
Encrypted NAND Gate

Potential Applications

- Email content-filtering guard between networks with different classification levels
- Privacy-preserving cloud-based voice over IP service
- Secure cloud-based mapping service that cannot determine your location, route, or destination

Crowd Sourced Formal Verification (CSFV)

The Problem



Constant surface area available to attack

Regardless of the application size, the system loads the same number of support functions

DLLs: run-time environment = more commonality

For every 1,000 lines of code, 1 to 5 bugs are introduced.

Are there fundamental scientific reasons that prevent us from doing better?
No: *"There are no intrinsic laws of nature in cyber-security as there are in…physics, chemistry, or biology."*
[JASON Report on Science of Cyber-Security, 2010]

Formal Verification

- Formal verification can obtain 0.1 - 0.5 bugs per KLOC, however:
  - Extremely expensive: software development costs increase by 2x to 100x
    - seL4 microkernel formal verification took 11 person-years
  - Fundamental formal verification problems resist automation
    - Computationally undecidable: Heuristics have improved, but remain incomplete

Source: Corbis

CSFV

Source: morgueFile

The Concept: Crowd Sourced Formal Verification

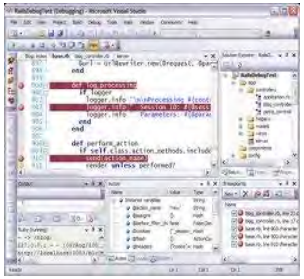
"Game-ify" Geeky Formal Verification

Applies game solutions to the original formal verification problem

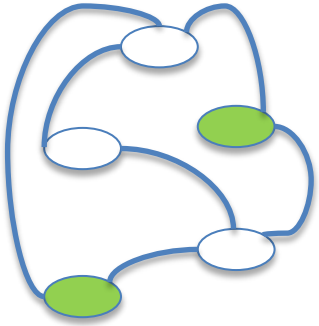
Exploits a large user base requiring no formal verification expertise

Code

Model



Verified Code

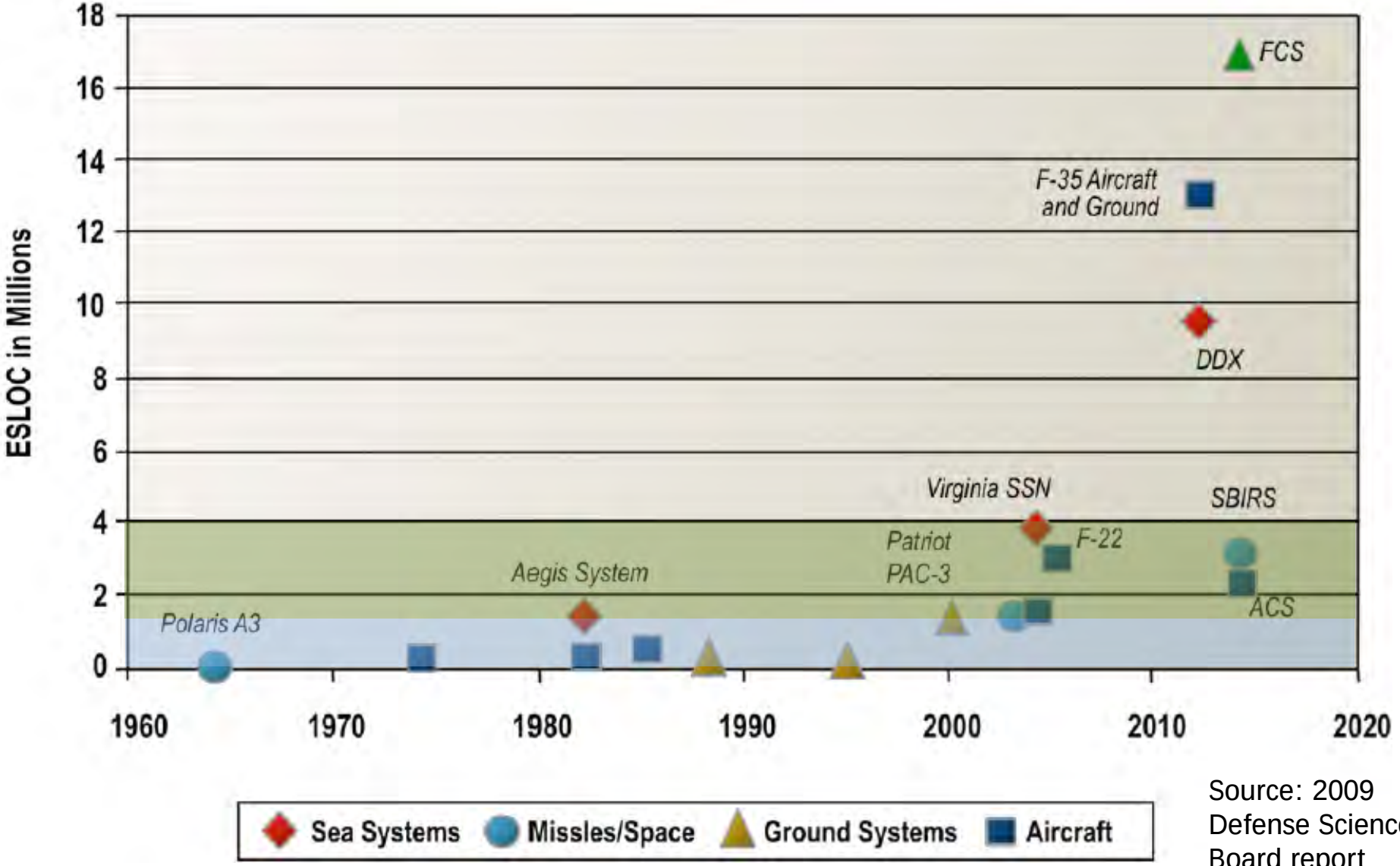


Verified Model

Source: University of Washington

CSFV New Capabilities

Scalability to DoD Software Systems



ESLOC = Executable Source Lines Of Code

Source: 2009 Defense Science Board report

Contact Information

Watch for Special Notice SN 12-17 to be released on FedBizOpps (fbo.gov)

Drew Dean

Drew.Dean@darpa.mil