Drew Dean
Program Manager, Information Innovation Office

PROCEED and Crowd-sourced Formal Verification

DARPA Cyber Colloquium
Arlington, VA
November 7, 2011
Report Documentation Page

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE
07 NOV 2011

2. REPORT TYPE

3. DATES COVERED
00-00-2011 to 00-00-2011

4. TITLE AND SUBTITLE
PROCEED and Crowd-sourced Formal Verification

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHOR(S)

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:

a. REPORT
unclassified

b. ABSTRACT
unclassified

c. THIS PAGE
unclassified

17. LIMITATION OF ABSTRACT
Same as Report (SAR)

18. NUMBER OF PAGES
9

19a. NAME OF RESPONSIBLE PERSON

Standard Form 298 (Rev. 8-98)  Prescribed by ANSI Std Z39-18
Do you trust the cloud?

Secure communications…

Secure storage…

Secure computation?

Approved for Public Release, Distribution Unlimited.
**Goal:** practical computation on encrypted data without decrypting

**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
DARPA’s Newest Cyber Program

Crowd Sourced Formal Verification (CSFV)
The Problem

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]

Constant surface area available to attack

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

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

Source: University of Washington

CSFV New Capabilities
Scalability to DoD Software Systems

ESLOC = Executable Source Lines Of Code

Source: 2009 Defense Science Board report

Approved for Public Release, Distribution Unlimited.
Contact Information

Watch for Special Notice SN 12-17 to be released on FedBizOpps (fbo.gov)
Drew Dean
Drew.Dean@darpa.mil