 **Crowd Sourced Formal Verification (CSFV)**

Unreliable software places huge costs on both the military and the civilian economy. Currently, most Commercial Off-the-Shelf (COTS) software contains about one to five bugs per thousand lines of code. Formal verification of software provides the most confidence that a given piece of software is free of errors that could disrupt military and government operations. Unfortunately, traditional formal verification methods do not scale to the size of software found in modern computer systems. Formal verification also currently requires highly specialized engineers with deep knowledge of software technology and mathematical theorem-proving techniques. These constraints make current formal verification techniques expensive and time-consuming, which in turn make them impractical to apply to COTS software.

DARPA created the Crowd Sourced Formal Verification (CSFV) program to overcome these challenges. CSFV aims to investigate whether large numbers of non-experts can perform formal verification faster and more cost-effectively than conventional processes. The goal is to transform verification into a more accessible task by creating fun, intuitive games that reflect formal verification problems. Playing the games would effectively help software verification tools complete corresponding formal verification proofs.

The program envisions numerous benefits, including:

* Increased frequency and cost-effectiveness of formal verification for more types of common COTS software.
* Greatly expanded audience to participate in formal verification.
* Establishment of a permanent community of game players interested in improving software security.

**Program Manager**

Dr. Daniel Ragsdale

[daniel.ragsdale@darpa.mil](mailto:daniel.ragsdale@darpa.mil)

**\* Report a problem: john.cheng.ctr@darpa.mil**

**\* The content below has been generated by organizations which are partially funded by DARPA; the views and conclusions contained therein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of DARPA or the U.S. Government.**

**Software:**

None

**Publications:**

(Use Excel spreadsheet provided.)

[{"CSFV Team":"University of Illinois at Chicago","Title":"Witnessing Program Transformations","Link":"No link; soft copy only"},

{"CSFV Team":"University of Illinois at Chicago","Title":"A Witnessing Compiler: A Proof of Concept","Link":"No link; soft copy only"},

{"CSFV Team":"University of Washington","Title":"Verification games: Making verification fun","Link":"http://homes.cs.washington.edu/~mernst/pubs/verigames-ftfjp2012-abstract.html"},

{"CSFV Team":"University of Washington","Title":"Inference and checking of object ownership","Link":"http://homes.cs.washington.edu/~mernst/pubs/infer-ownership-ecoop2012-abstract.html"},

{"CSFV Team":"University of Washington","Title":"Reducing the barriers to writing verified specifications","Link":"http://homes.cs.washington.edu/~mernst/pubs/veriweb-oopsla2012-abstract.html"},

{"CSFV Team":"University of Washington","Title":"ReIm & ReImInfer: Checking and inference of reference immutability and method purity","Link":"http://homes.cs.washington.edu/~mernst/pubs/infer-refimmutability-oopsla2012-abstract.html"},

{"CSFV Team":"University of Washington","Title":"Rely-guarantee references for refinement types over aliased mutable data","Link":"http://homes.cs.washington.edu/~mernst/pubs/rely-guarantee-ref-pldi2013-abstract.html"},

{"CSFV Team":"University of Washington","Title":"JavaUI: Effects for controlling UI object access","Link":"http://homes.cs.washington.edu/~mernst/pubs/gui-thread-ecoop2013-abstract.html"}]