

[Home](#) > [Events](#) >



DEsigning a Secure Systems Engineering Competition

DESSEC: DEsigning a Secure Systems Engineering Competition
A Workshop

April 6 - 8, 2010
at the Washington Duke Inn in Durham, North Carolina

Call for Proposals and Participation

PROPOSAL SUBMISSION EXTENDED TO DECEMBER 22, 2009

(This CFPP is also available in [text](#) and [PDF](#) formats)

If we want to have a cyber infrastructure that can both resist attacks and be safely extended with new technology, we have to learn how to build it. In effect, we are asking for practical, composable security, at scale. One way to teach ourselves this lesson might be to conduct a series of competitive development efforts that encourage diverse means of realizing some specified system with some specified security properties.

Today there are few worked examples of systems of significant scale that

1. Have a sound assurance argument for system trustworthiness
2. Are easy to use and easy to manage, and
3. Can be extended to incorporate new functions without completely redoing the assurance argument.

Our goal is to generate worked examples of such systems through competitive developments and evaluations. In the process of generating such examples, we also intend to identify the most effective techniques for doing so, to educate students in the methodologies for developing such systems, to involve industry so that the technology can be applied in future developments, and to involve government laboratories for evaluation purposes.

Individual technologies exist that address issues of sound system design, correct implementation, verification and test, and extensibility. Only rarely are they brought together to address an entire system. Where the need for high confidence of safe and correct operation has demanded this kind of engineering for a core set of functions, for example in nuclear reactor core cooling systems, aircraft flight control systems, and systems with stringent security requirements, these methods have been used. But they have often required extraordinary resources, and the required certification processes have often slowed the incorporation of new technology in those systems. People learn by doing, and by example. By funding competitive developments employing alternative approaches and evaluating the results fairly, we may learn, teach, and advance.

But there are many questions to be answered before such a competition can be initiated:

- What is to be built?
- How will its functions and dependability requirements be specified?
- What tools and techniques will be used in construction?
- How will the results be measured and evaluated, including the assurance argument, extensibility, usability, manageability?
- Can proprietary methods or tools be included?

This workshop is intended to develop answers to these questions. If the workshop succeeds, the results will be available for use in actual competitive developments. Participants must understand, however, that (a) the workshop may not succeed, and (b) even if it does, the organizers cannot guarantee that any competition developed at the workshop will receive funding.

Proposals

To be considered for invitation to the workshop, we ask that you submit a prototype definition of a competition. Workshop participants will be invited based upon how their competition proposal addresses the details below, whether or not their specific proposal is selected for study at the workshop. Participants will also be chosen based upon the need for a balanced set of expertise needed to achieve the workshop goals.

Composable secure systems are needed in many different contexts or domains. For example, one would hope that the systems designed to control the distribution of energy (electric power, oil, gas) would have this property, so that the addition of a new device or function to the network would not cause a sudden increase in risk. One might also wish for a small, mobile, flexible communication and information storage device that supports the addition of new functions without endangering the operation of existing ones. Vehicles with autonomous or hybrid human-computer control systems, such as automobiles or aircraft, provide another domain of great interest. Large scale information technology systems that support real time communication and coordination such as rail or air traffic control systems that may interact with many vehicles provide yet another example. Any of these examples would be good topics for a competition proposal.

Proposals should include all of the following details, preferably within one page, or two pages at most. A complete specification is not the goal. Rather, a clear, concise description addressing all these points will suffice.

- a brief description of the system to be built (title and description)
- a method to be used to specify it,
- a definition of the security to be provided,
- the threat environment in which the system is expected to operate,
- a method for evaluating what is built against the specification,
- a description of how the extensibility challenge will be posed,
- a list of potential supporting tools and resources that could be made available to competitors, and
- an estimate of the level of effort (number of person years) that might be required to produce an entry.

Workshop Organization

The workshop will be convened over a period of three days. Some advance preparation will be required of participants to assure the workshop time is spent effectively, so that a report can be delivered at the end of the workshop week. No “homework” will be required after the meeting. Three parallel teams will develop different answers to the questions of what will be built, how it will be specified, and how it will be evaluated. The first day will be devoted to the questions of what will be built and how it will be extended. At the end of the day each team will present its proposal to the group as a whole. The second day will be devoted to the questions of specification and evaluation, again with a joint session at the end of the day. The third day will be devoted to identifying tools that might be used by competitors and constructing a strawman model of an entry to the competition. Results will be briefed at the end of the third day. A support team will collect the results and prepare the workshop report.

The workshop will be led by the workshop chair in cooperation with chairs for each of the three tracks. Prior to the receipt of the prototype competition definitions, the workshop chair will form a committee to review and evaluate the submissions provided. This review process will help identify the domains to be addressed at the workshop and will guide the recruitment of track chairs.

Sample submission

The idea is not to specify a competition in detail but to give enough information to provide a skeleton that might be fleshed out during the workshop. The following example necessarily addresses a particular domain, but we are interested in submissions from a wide range of areas, for example SCADA systems, sensor systems, communication systems (e.g., cellphone), control systems (e.g., automotive).

Title:

Privacy Enforcing Card Operating System (PECOS)

Proposal:

Develop a smart card operating system and application environment that supports designation of input data as private in different categories (eg – private health data, private financial data, private legal data, private personal data) and applies controls on application access to data on that basis. A trusted path for the designation of private data and the authorization of its release must be supported with a suitable user interface.

Specification method:

External interfaces will be specified for the competition using natural language. Competitors may choose their own specification languages for development purposes. Similarly, assurance arguments may be expressed using techniques chosen by the competitors.

Security to be provided:

System must never expose data designated as private except in response to requests approved via trusted path.

Threat environment:

Attacks permitted via external signal inputs only (i.e. software attacks). Any input or input sequence is permitted. Hardware tampering and external monitoring of on-card signals is excluded – we are not trying to test the physical infrastructure but the strength and extensibility of the software base.

Evaluation method:

- 1) Automated testing of submitted solution
- 2) Review of assurance argument by selected members from other projects
- 3) Review of usability by selected members from other projects
- 4) Red teaming by members of other project teams.

Extensibility challenge:

Specification of a new application requiring access to one or more types of private data will be provided to competitors following initial submission and evaluation. The new function and the assurance argument for the extended system (including the new function) must be implemented within 7 days. The system will then be re-evaluated as before.

Supporting tools:

Sun Java toolkits, JCRE, MULTOS, open source development and analysis tools.

Estimated level of effort required to complete an entry:

Five person years (assumes use of open source MULTOS as basis)

Submission Procedure

Please submit your proposed competition as a .pdf, .doc, or .ps document via the Openconf system at <http://www.thei3p.org/openconf> no later than December 22nd, 2009. Questions may be addressed to: the.i3p@dartmouth.edu.

Notification Procedure

Invitations will be distributed by the organizing committee at the I3P not later than February 22nd, 2010.

Organizers

The Institute for Information Infrastructure Protection (the I3P) is organizing this workshop with support from the National Science Foundation under Award Number 0927921, which includes support from the Central Intelligence Agency, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. Any opinions, findings, and conclusions or recommendations expressed in this material do not necessarily reflect the views of the National Science Foundation, the CIA, the I3P, or Dartmouth College.



The Institute for Information Infrastructure Protection (I3P) is a consortium of leading national cyber security institutions, including academic research centers, government laboratories and non-profit organizations. For more info visit www.thei3p.org

Last Updated: 11/30/09