2011-03

Trusted Computing Exemplar Project

Irvine, Cynthia E.; Levin, Timothy E.Nguyen, Thuy D.; Dinolt, George W.; Center for Information Systems Security Studies and Research (CISR)

Trusted Computing Exemplar Project

Cynthia E. Irvine, Timothy E. Levin, Thuy Nguyen, George W. Dinolt
Center for Information Systems Security Studies and Research (CISR)
Naval Postgraduate School

The science and discipline of trusted computing has been neglected for well over a decade. We lack the availability of high assurance trusted systems, developers who can create these systems, as well as public domain worked examples upon which new projects could be modeled. To address this need, CISR has initiated a *Trusted Computing Exemplar Project*, which will provide an openly distributed ***worked example*** of how high assurance trusted computing components can be built. In this project, we have undertaken four related activities:

1. Creation of a prototype framework for rapid high assurance system development
2. Development of a reference-implementation trusted computing component
3. Evaluation of the component for high assurance, and
4. Open dissemination of deliverables related to the first three activities

A prototype *high assurance development framework* will be created first, and then used to produce a reference implementation *trusted computing component,* the Embedded MicroKernel Prototype. High assurance methodologies and techniques will be applied during the entire lifecycle. A third-party *evaluation* of the component will be initiated during development. The documentation, source code, development framework and other deliverables will be made *openly available* as they are produced.

The prototype framework for rapid high assurance development will provide a set of interoperable tools and define a set of efficient, repeatable procedures for constructing trusted computing systems and components, which will support the "open source" dissemination of project deliverables

We will develop a high assurance, embedded micro-kernel, and trusted application, as a reference implementation exemplar for trusted computing. The primary security function of the Embedded MicroKernel will be to enforce process and data-domain separation, while providing primitive operating system services sufficient to support simple applications. The kernel will have a static runtime resource configuration and its security policy regarding access to resources will be based on static process/resource access bindings, which are subject to offline configuration. We anticipate that the kernel will support a small, configurable number of processes, data objects, and I/O devices. Application processes will be statically scheduled, with each process being given a predetermined amount of time, set by the configuration.

The demonstration system will be a network *trusted path extension* device for communicating security critical information with a remote secure server. This device will connect a specifically configured COTS workstation, through a local area network, to a secure server. The device provides trusted path authentication and negotiation services for users to establish trusted sessions with the server. Once logged on through the trusted path extension, user sessions at the workstation may interact with the secure server using the negotiated security parameters. Trusted Path Extension functions will be implemented as trusted application programs of the Embedded MicroKernel, which will be hosted on a *handheld* style hardware platform.

Using the development framework describe above, the outputs of the Trusted Computing Exemplar Project, such as source code, project plans, and evaluation evidence, will be made available to the public, providing previously unavailable examples of "how-to" for high assurance trusted computing.