Trusted Computing Exemplar (TCX)

Project Objective
Provide a working example showing how trusted computing systems and components can be constructed to meet high assurance evaluation criteria. Reference implementation consists of a high assurance Least Privilege Separation Kernel (LPSK) and a hosted trusted application. Project artifacts are openly disseminated as they are produced.

Integrated Activities
Rapid High Assurance Development Framework
  Life Cycle Management, Engineering Process
  Semantic-programming-based documentation system
Develop Reference Implementation
  Least Privilege Separation Kernel - EAL7
  High Assurance Network Authentication Appliance
Evaluate Components for High Assurance
Disseminate Results via Open Methodology

Least Privilege Separation Kernel
  • Simple, Compact, Structured to be Evaluatable at EAL7
    Static Security and Resource Configuration
  • Flow Control
    Process and Data Domain Separation
  • Access Control Policy
    Static Process/Resource Access Bindings
  • Basic Kernel Services
    Static Scheduling
    Memory-based IPC, Simple Synchronization Primitives
    Device Management
  • Current Status
    Functionality and Security Requirement Analysis
    Demonstrated Least Privilege Separation Model using
    Formal Development Methodology Tool Set

Operational Payoff/Transition Targets
Evaluable Reference Implementation
Components with a priori Assurance Against System Subversion
High Assurance Development Framework Transfer to Next Generation
  New Experts in Security Development
  High Assurance Knowledge and Capabilities

This work has been supported by a number of sponsors, most recently the Office of Naval research.

Contact Information
C. E. Irvine
irvine@nps.edu
831-656-2461

Department of Computer Science
Graduate School of Operations and Information Sciences
Center for Information Systems Security Studies and Research

www.nps.edu
www.cISR.nps.edu