2011-04

Trusted Computing Exemplar (TCX) Project (archived)

Irvine, Cynthia; Levin, Tim; Nguyen, Thuy

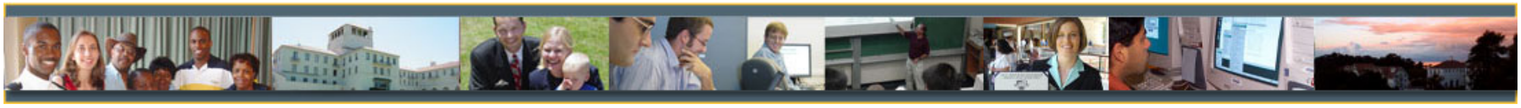
Monterey, California, Naval Postgraduate School

https://hdl.handle.net/10945/35288

NAVAL POSTGRADUATE SCHOOL
CENTER FOR INFORMATION SYSTEMS SECURITY STUDIES AND RESEARCH

Search Site

Centers of Academic Excellence
IA Education & Research



Research: Projects: TCX

TCX
small but complete

Trusted Computing Exemplar (TCX) Project
The purpose of the Trusted Computing Exemplar (TCX) project is to provide a working example that shows how trusted computing systems and components can be constructed.

The project will develop a high assurance, Least Privilege Separation Kernel (LPSK) with a hosted trusted application as a reference implementation for trusted computing.

Because the product as well as the process will be showpieces for trusted computing development, high assurance methodologies and techniques will be applied during the entire lifecycle. The goal is to produce a very small, portable component that will provide users with correct security operation and an a priori assurance against system subversion.

It is our expectation that the open availability of the TCX results will enhance the capability to develop highly secure software in both commercial and open-source sectors. In particular, the high assurance development framework can be reused or adapted to support the development of secure systems that are more complex than the TCX demonstration system. The relevance of the TCX project is exemplified further by the surge of recent interest in high assurance systems, separation kernels, and evaluation profiles.

Methodology
The project will first create a prototype high assurance development framework. This project will then use this framework to produce a reference implementation trusted computing component, the LPSK. A third party will initiate an evaluation of the component during its development (e.g., once the high-level design documentation is written). The project will make the documentation, source code, development framework and other deliverables openly available as they are produced.

Project Status
The TCX project was initially conceptualized in late 2002 and project work was started in mid 2003. The feasibility of the effort was studied and it was determined that the static nature of the system, the simplicity of the policy to be enforced, as well as the considerable previous experience in high assurance development of our team made the project feasible within the timeframe envisioned. Since then, significant progress has been made in the following areas: threats and requirements analysis, formal model, life cycle management and development environment.

As a proof of concept, the TCX project will build and evaluate a Trusted Path Extension (TPE) device, hosted by the LPSK. The purpose of this device is to provide an unforgeable trusted path with which network clients can securely interact with security-enabled remote servers and will integrate protocols and client/server security mechanisms developed in the MYSEA project. The evaluation portion of this project will encompass the definition of a high assurance Common Criteria protection profile for network access devices, production of the evaluation evidence, as well as support for the government evaluation team in its evaluation activities.

Thesis Advisors

- Cynthia Irvine, CISR
- Tim Levin, CISR
- Thuy Nguyen, CISR

Research Team

- Cynthia Irvine, CISR
- Tim Levin, CISR
- Thuy Nguyen, CISR
- Paul Clark, CISR
- David Shifflett
- Jean Khosalim
- Charles Prince
- Buddy Vernon
- Phil Hopfner
- John Clark

Students

- Douglas R. Kane

Sponsors

- Office of Naval Research (ONR)
- National Reconnaissance Office (NRO)

Publications

Levin, T. E., Irvine, C. E., and Nguyen, T. D., "An Analysis of Three Kernel-based Multilevel Security Architectures", NPS Technical Report NPS-CS-06-001, August

2006. (PDF)

Nguyen, T. D., Levin, T. E., and Irvine, C. E., "TCX Project: High Assurance for Secure Embedded Systems", 11th IEEE Real-Time and Embedded Technology and Applications Symposium Work-In-Progress Session, San Francisco, CA, March 2005. (PDF)

Levin, T. E., Irvine C. E., and Nguyen T. D., "A Least Privilege Model for Static Separation Kernels", NPS-CS-05-003, Naval Postgraduate School, October 2004 (PDF)

Irvine C. E., Levin, T. E., and Nguyen T. D., "Trusted Computing Exemplar 2004 Developments", NPS-CS-05-001, Naval Postgraduate School, October 2004 (PDF)

Irvine, C. E., Levin, T. E., Nguyen, T. D., and Dinolt, G. W., "The Trusted Computing Exemplar Project", Proceedings of the 2004 IEEE Systems, Man and Cybernetics Information Assurance Workshop, West Point, NY, June 2004, pp. 109-115. (PDF)

Irvine, C. E., Levin, T. E., Nguyen, T. D., Shifflett, D. J., Khosalim, J., Clark, P. C., Wong, A., Afinidad, F., Bibighaus, D., and Sears, J., "Overview of a High Assurance Architecture for Distributed Multilevel Security", Proceedings of the 2004 IEEE Systems, Man and Cybernetics Information Assurance Workshop, West Point, NY, June 2004. (PDF)

"U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness", Information Assurance Directorate, National Security Agency, June 2007. (Offsite PDF)

Irvine, C. E., Levin, T. E. and Dinolt, G. W., "A National Trusted Computing Strategy", NPS-CS-02-003, Naval Postgraduate School, May 2002 (PDF)

Trusted Computing Exemplar Project (Executive Summary)
Trusted Computing Exemplar Project (White Paper)
Trusted Computing Exemplar Project (Quad Chart)
TCX Poster 2007 (PDF)
TCX Poster 2007 (PPT)

Related Projects

- MYSEA - Monterey Security Architecture
- SecureCore
- Security Domain Model

Offsite Links

- Common Criteria
- NIAP Common Criteria Evaluation and Validation Scheme

Key Words
operating system, COTS, medium robustness, multilevel, mandatory access control, MAC, discretionary access control, DAC, labels, integrity, cryptography, mandatory integrity control, MIC, cryptography

This page was last modified: April 2011

Home / Webmaster / Privacy Policy / FOIA / Sitemap / NPS