CYGNACOM
SOLUTIONS

Reference Monitor Concept in the CC
ICCC 2005 Theme C2-03

Kris Rogers
CygnaCom Solutions
September 29, 2005

CYGNACOM SOLUTIONS

Introduction

- Principles of the Reference Monitor Concept
- Anderson Report 1972
- TCSEC 1985
- CC V2.1 1999
- CC V3 2005

CYGNACOM SOLUTIONS

Anderson Report 1972

- First introduced reference monitor concept
- Implementation of the reference monitor concept is defined as a "reference validation mechanism."
- 3 principles

3 Reference Monitor Principles

1. The reference validation mechanism must be **tamper proof.**
   - **"Tamperproofness"**
2. The reference validation mechanism must **always be invoked**.
   - **"Always invoked"**
3. The reference validation mechanism must be **small enough to be subject to analysis** and tests to assure that it is correct.
   - **"Small enough to be analyzed"**

CYGNACOM SOLUTIONS

TCSEC Introduction

- Trusted Computer Security Evaluation Criteria (TCSEC)
- Also known as the Orange Book
- Used for IT security evaluations in the U.S. before the Common Criteria.
- 6 hierarchical classes of requirements
  - Lowest to highest: C1, C2, B1, B2, B3, and A1.

CYGNACOM SOLUTIONS

Reference Monitor in the TCSEC

- Reference monitor concept is incorporated into the **system architecture requirements**
- System architecture requirements are **assurance requirements.**

CYGNACOM SOLUTIONS

TCSEC "Tamperproofness"

- C1: "The TCB shall maintain a domain for its own execution that protects it from external interference or tampering."
- B1: "The TCB shall maintain process isolation through the provision of distinct address spaces under its control."

CYGNACOM SOLUTIONS

TCSEC "Always Invoked"

- C2: "The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements."

CYGNACOM SOLUTIONS

TCSEC "Small enough to be analyzed"

- B2: Modularity
- B3: Layering and minimization
- Full reference monitor not required until B3

CYGNACOM SOLUTIONS

TCSEC B2 System Architecture

- The TCB shall be internally **structured into well-defined largely independent modules.**
- It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not.
- The TCB modules shall be designed such that the **principle of least privilege** is enforced.
- Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writeable).
- The user interface to the TCB shall be completely defined and all elements of the TCB identified.

CYGNACOM SOLUTIONS

TCSEC B3 System Architecture

- The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with **precisely defined semantics.**
- This mechanism shall play a central role in enforcing the internal structuring of the TCB and the system.
- The TCB shall incorporate significant use of **layering, abstraction and data hiding**.
- Significant system engineering shall be directed toward **minimizing the complexity** of the TCB and **excluding from the TCB modules that are not protection-critical.**

CYGNACOM SOLUTIONS

Common Criteria Version 2

- Tamperproofness
- Always invoked
- Small enough to be analyzed

CYGNACOM SOLUTIONS

CC V2 "Tamperproofness"

- FPT_SEP Domain separation
- FPT_SEP.1 TSF domain separation
- FPT_SEP.2 SFP domain separation
  - SFP is
- FPT_SEP.3 Complete reference monitor

CYGNACOM SOLUTIONS

CC V2 "Always invoked"

- FPT_RVM Reference mediation.
- FPT_RVM.1 Non-bypassability of the TSP
- FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

CYGNACOM SOLUTIONS

CC V2 "Small enough to be analyzed"

- ADV_INT family
- Addressed under CC V3

CC V2 Problems

- FPT_SEP and FPT_RVM were defined as security functional requirements (SFRs)
- Protection of the TSF and Non-bypassability depend on the overall design of the TOE
- Overall design is not addressed by the existing CC V2 security assurance requirements (SARs).
- Also, SFRs are not required at any evaluation assurance level (EAL).

CYGNACOM SOLUTIONS

Common Criteria Version 3

- "Tamperproofness" and "Non-bypassability"
  - ADV_ARC: Architectural design
    - Self-protection
    - Domain isolation
    - Non-bypassability
- "Small enough to be analyzed"
  - ADV_INT TSF Internals

CYGNACOM SOLUTIONS

CC V3 ADV_ARC.1 Architectural Design with domain separation and non-bypassability

- ADV_ARC.1.1D The developer shall provide the architectural design of the TSF.
- ADV_ARC.1.1C The descriptive information contained in the architectural design shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.
- ADV_ARC.1.2C The architectural design shall describe the security domains maintained by the TSF consistently with the SFRs.
- ADV_ARC.1.3C The architectural design shall describe how the TSF initialisation process is secure.
- ADV_ARC.1.4C The architectural design shall demonstrate that the TSF protects itself from interference and tampering.
- ADV_ARC.1.5C The architectural design shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

CC V3 ADV_INT

- INT.1 Partial modular decomposition
- INT.2 Full modular composition
- INT.3 Reduction of complexity through layering
- INT.4 Minimisation of complexity

CYGNACOM SOLUTIONS

Future Work / Issues

- ADV_ARC family needs to be integrated with ACO class
- Current draft is missing guidance for trusted applications running on top of an OS when the OS is not part of the TSF
- No levels for ADV_ARC family
- Vague guidance in Appendix A and CEM may result in weakest possible interpretation becoming universally accepted
  - I.e., requirement is addressed by hand waving

CYGNACOM SOLUTIONS

Trusted Application Issues

- Current draft of CC v3 is missing guidance for applications running on top of an OS when the OS is not part of the TSF
- Applications should be required to protect their own data structures, code, and interfaces, but cannot be expected to protect themselves from the underlying OS
- Is it OK for Protection of the TSF to be partially or wholly provided by the IT environment?

References

- Anderson, James P. Computer Security Technology Planning Study, ESD-TR-73-51, Vol. II, ESD/AFSC, Hanscom AFB, Bedford, MA, October 1972
- Department of Defense Trusted Computer Security Evaluation Criteria, DOD 5200.28-STD, December 1985.
- Common Criteria Version 2.2, January 2004
- Common Criteria Version V3.0 Rev 2, July 2005

CYGNACOM SOLUTIONS

Contact Information:

- Kristina C. Rogers
- Security Evaluation Laboratory Director
- CygnaCom Solutions
- 749 Santa Rosita
- Solana Beach, CA 92075
- Tel: 858-509-0180
- Fax: 703-848-0985
- Email: krogers@cygnacom.com