

Security Assessment Criteria for CORBAsecurity

David Chizmadia
National Security Agency
dmc@tycho.ncsc.mil

Agenda

- Overview
- Approaches
- Efforts

Overview

- Risk Management
- Assurance
 - What?
 - How?
- CORBAsec
 - What is there
 - What isn't there

Risk Management

GOAL: Balance cost of protection with cost of compromise

- Define and quantify cost of compromise
- Identify protection requirements
- Plan and execute protection strategy
- Verify effectiveness of protection strategy

Assurance - in what?

- Assurance == Belief
- Security assurance = belief in what?
 - CORBAsec functional conformance
 - Interfaces
 - Services
 - Penetration resistance
 - Architecture
 - Implementation

Assurance - gained how?

- Testing
 - Functional
 - Penetration
- Analysis
 - Of functions
 - Of structure
- Developer Reputation

CORBAsec - present

- Threat analysis
- Partial interface specification
- Informal advisory structural criteria
- Informal functional criteria
- Advisory analysis criteria

CORBAsec - absent

- Functional testing criteria
- Penetration testing criteria

Approaches

- Vendor assertion
- Independent functional testing
- Tiger teams
- Formal independent evaluation

Vendor Assertion

- What we have now
- Reliability varies
- Past experience (of self or others) can provide some independent validation

Independent Functional Testing

- Provides reasonable assurance in presence and expected operation of claimed functions
- Techniques well understood
- Add some cost to development/marketing,
- but, can be written off as part of quality program

Tiger Team

- Provides reasonable, but never conclusive, assurance of attack resistance
- Quality of results depends entirely on quality of team members
- Labor intensive, therefore, substantial cost to sponsor

Formal Independent Evaluation

- Provides reasonable to high assurance in both functions and attack resistance
- Requires technical evaluation criteria
- Can include functional and tiger team testing
- Requires considerable developer support
- Labor intensive so can be expensive to sponsor

Efforts

- OMG/OpenGroup Testing Program
- NSA/NIST DOCS Family of Protection Profiles

OMG/OpenGroup Testing

- Established effort
- Using same approach as OpenGroup branding program
 - Openly available tests
 - Test are executed by either the vendor or an testing independent facility
- Could be in place by end of 1997

NSA/NIST Protection Profiles

- In the planning stages
- Will attempt to do the following in the context of the Common Criteria:
 - Define common Sec req's (PPs) for ORBOS systems
 - Define ORBOS Security Reference Model (SRM)
 - Define as many PPs as needed for each component of the ORBOS SRM to compose into ORBOS PPs

Define ORBOS PPs

- Consider ORBOS's as an atomic component of operational system security architectures
- Identify a PP for each major kind of ORBOS threat environment
- ORBOS PPs become rationale for ORBOS SRM and the individual ORB and OS PPs

Define ORBOS SRM

- Modeled after OMA, but may collapse several OSs into one SRM component
- Used to allocate ORBOS system security requirements to common commercial products
- Provides context for products to identify the PPs with which they should claim compliance

Define ORBOS Component PPs

- Many to many relation between component PPs and ORBOS system PPs
- Component PPs will try to blend CC requirements with CORBAsec requirements
- May have to show how CORBAsec requirements affect other OSs
- May identify some requirements not included in CORBAsec

NSA/NIST Protection Profiles

- May attempt to define assurance oriented PPs appropriate to object oriented environments
 - Consider what vendors can tolerate
 - Consider what users want
 - Consider limitations of evaluation methodologies

NSA/NIST Protection Profiles

- Goal is for all profiles to be recognized by existing and planned evaluation schemes, i.e.:
 - US (TPEP and TTAP)
 - Canada
 - UK (UK ITSEC Scheme)
 - Germany
 - France
 - Australia

NSA/NIST Protection Profiles

- Hope/plan is to start effort by September
- Expect effort to take 24 months
 - ORBOS PPs in about 6 months
 - ORBOS SRM in about 9 months
 - ORBOS Component PPs as quickly thereafter as understanding and time permit