

ADV – v3.0

ICCC 2005

Ron Bottomly

rjbotto@missi.ncsc.mil

ADV - development

Purpose

to achieve understanding of the TOE,
to be used as input to vulnerability
analysis and testing

Gaining Understanding

Decomposition of the TOE

- Interfaces to TSF
- Constituent parts of TSF
- Implementation of TSF

Analysis of Soundness

- Architecture
- Internal Structure
- Policy Model

Functional Specification: ADV_FSP

Interfaces to TSF (“TSFI”)

- All means to invoke TSF services
- Any responses to such requests

- Calls made by TSF to its environment are *not* considered TSFI



Aside: Basis of levelling

Some things are more security-interesting than others.

At lower levels of assurance, we care less about (and require less detail for) the things that are less security-critical.

3 degrees of security-relevance

SFR-enforcing – actively enforces SFR.

SFR-supporting – needed to function correctly for SFRs to be enforced, but no active role.

SFR-non-interfering – no role in SFR enforcement; can be completely removed with no security impact.

Functional Specification: ADV_FSP

Interfaces to TSF (“TSFI”)

- All means to invoke TSF services
- Any responses to such requests

- Calls made by TSF to its environment are *not* considered TSFI
- Amount of detail depends upon component level

ADV_FSP.1

SFR-enforcing TSFI:

- describe purpose and method of use
- identify all parameters

SFR-supporting TSFI:

- describe purpose and method of use
- identify all parameters

SFR-non-interfering TSFI:

- (nothing required)

ADV_FSP.2

SFR-enforcing TSFI:

- describe purpose and method of use
- identify **and describe** all parameters
- **describe SFR-enforcing operations**
- **describe direct error messages from invoking SFR-enforcing operations**

SFR-supporting TSFI:

- describe purpose and method of use
- identify **and describe** all parameters

SFR-non-interfering TSFI:

- **describe purpose and method of use**
- **identify and describe all parameters**

ADV_FSP.3

SFR-enforcing TSFI:

- describe purpose and method of use
- identify and describe all parameters
- describe SFR-enforcing operations
- describe **all** direct error messages

SFR-supporting TSFI:

- describe purpose and method of use
- identify and describe all parameters
- **summarise all operations**

SFR-non-interfering TSFI:

- describe purpose and method of use
- identify and describe all parameters
- **summarise all operations**

ADV_FSP.4

SFR-enforcing TSFI:

- describe purpose and method of use
- identify and describe all parameters
- describe **all** operations
- describe all direct error messages

SFR-supporting TSFI:

- describe purpose and method of use
- identify and describe all parameters
- **describe all** operations
- **describe all direct error messages**

SFR-non-interfering TSFI:

- describe purpose and method of use
- identify and describe all parameters
- **describe all** operations
- **describe all direct error messages**

ADV_FSP.4

All TSFI:

- describe purpose and method of use
- identify and describe all parameters
- describe all operations
- describe all direct error messages

ADV_FSP.5

All TSFI:

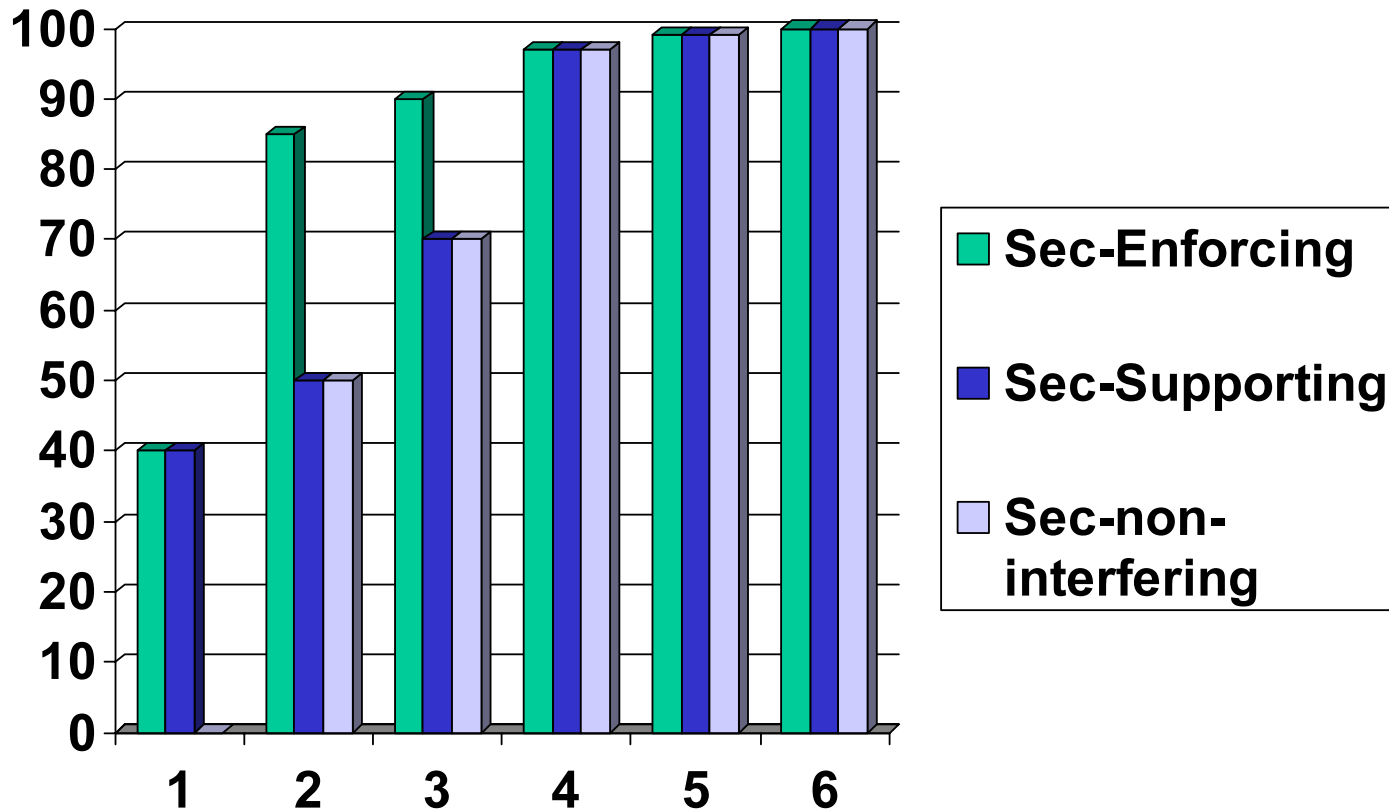
- describe purpose and method of use
- identify and describe all parameters
- describe all operations
- describe all direct error messages
- describe and provide rationale for all indirect error messages
- use semi-formal style

ADV_FSP.6

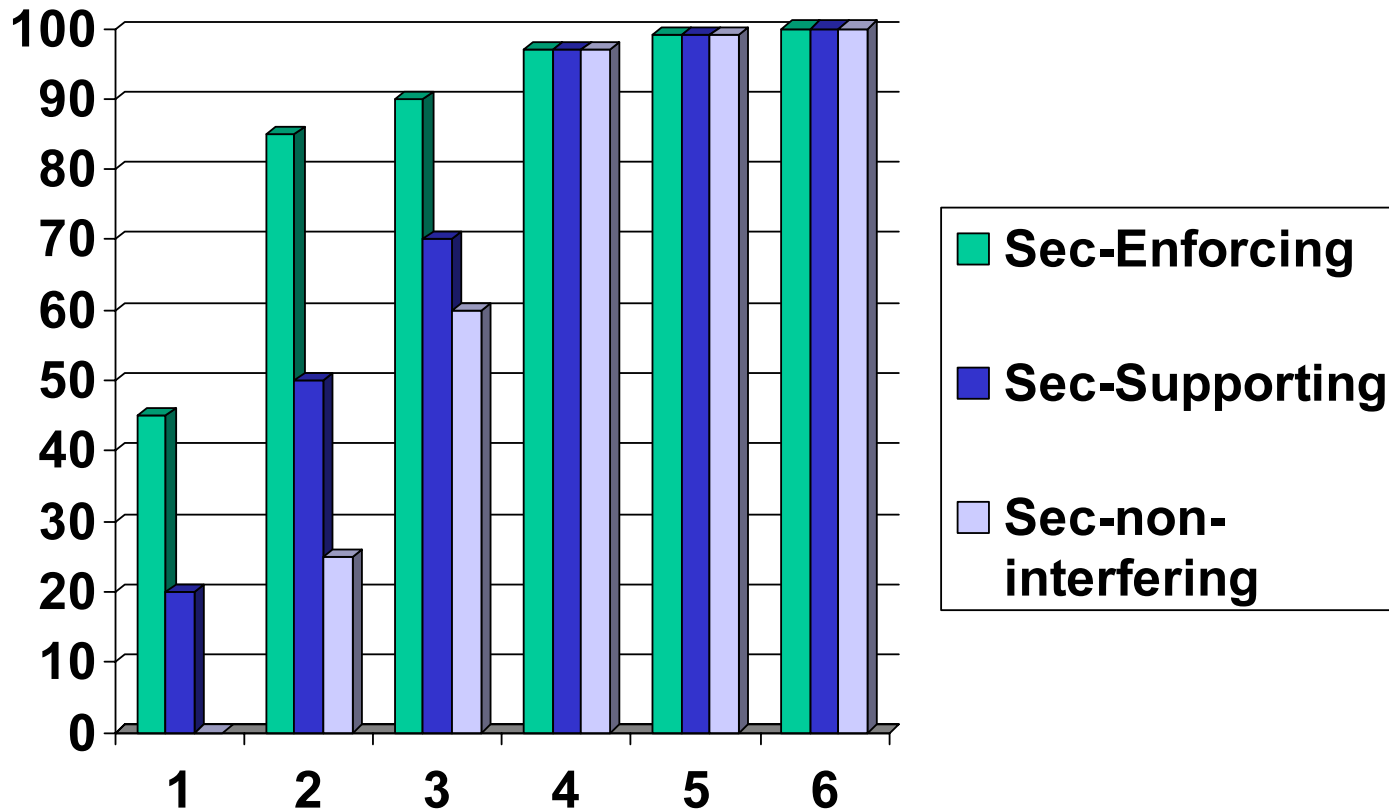
All TSFI:

- describe purpose and method of use
- identify and describe all parameters
- describe all operations
- describe all direct error messages
- describe and provide rationale for all indirect error messages
- describe and provide rationale for **any remaining** error messages
- use **formal** style

Required detail (by FSP component)



Relative information



TOE Description: ADV_TDS

FSP - what the TSF does; TDS - how the TSF does it

Parts of the TSF

- Links the interfaces of the functional specification to the implementation

TSF Module – at same conceptual level as implementation

TSF Component – modules or components

- Complexity of the TSF determines how many levels of abstraction are appropriate

Automobile Description

Ignition - starter, battery

Drive Train - engine, transmission, axles,
wheels, brakes

Exhaust - muffler

Electrical

- starter, battery

Structure

Safety

Comfort/Convenience

ADV_TDS.1

Describe TOE in terms of components

Identify all components in the TSF

Identify them as:

- *SFR-enforcing*
- *SFR-supporting*

or

- *SFR-non-interfering*

ADV_TDS.1

Describe TOE in terms of components

Identify all TSF components

SFR-enforcing components:

- describe SFR-enforcing behaviour in general
- describe interactions with other components

SFR-supporting components:

- describe why it is not SFR-enforcing

SFR-non-interfering components:

- describe why it is not SFR-enforcing

ADV_TDS.2

Describe TOE in terms of components

Identify all TSF components

SFR-enforcing components:

- describe SFR-enforcing behaviour **in detail**
- **describe non-SFR-enforcing behaviour in general**
- describe interactions with other components

SFR-supporting components:

- **describe behaviour in general**
- **describe interactions with other components**

SFR-non-interfering components:

- describe why it is not SFR-enforcing
- **describe interactions with other components**

ADV_TDS.3

Describe TOE in terms of components

Describe TSF in terms of modules

Identify and describe all TSF components

Describe all interactions between components

Map components to modules

SFR-enforcing modules:

- describe data areas common with other modules
- describe purpose, and interfaces
- describe algorithm

SFR-supporting modules:

- describe purpose and interactions with other modules

SFR-non-interfering modules:

- describe purpose and interactions with other modules

ADV_TDS.4

Describe TOE in terms of components

Describe TSF in terms of modules

Identify and describe all TSF components

Describe all interactions between components

Map components to modules

SFR-enforcing **and SFR-supporting** modules:

- describe data areas common with other modules
- describe purpose, and interfaces
- describe algorithm

SFR-non-interfering modules:

- describe purpose and interactions with other modules

ADV_TDS.5

Describe TOE in terms of components

Describe TSF in terms of modules

Identify and describe all TSF components

Describe all interactions between components

Map components to modules

For all modules:

- describe data areas common with other modules
- describe purpose, and interfaces
- describe algorithm

ADV_TDS.6

Describe TOE in terms of components

Describe TSF in terms of modules

Identify and describe all TSF components

Describe all interactions between components

Map components to modules

For all modules:

- describe data areas common with other modules
- describe purpose, and interfaces
- describe algorithm

Provide formal high-level description

TSF Implementation Representation: ADV_IMP

Human-understandable version of the implementation

- Source code
- Hardware schematics

ADV_IMP.1

Full representation *available*, though not delivered.

Implementation details only; no design decisions remaining

In a form used by developers

Map to subset of TDS.

ADV_IMP.2

Full representation *available*, though not delivered.

Implementation details only; no design decisions remaining

In a form used by developers

Map to subset of TDS.

Transform representation to implementation

Gaining Understanding: Analysis of Soundness

- Architecture
- Internal Structure
- Policy Model

Architectural Design: ADV_ARC

How does the design of the TSF ensure that its security cannot be defeated?

- TSF cannot be circumvented
- TSF cannot be changed

Architectural Design: ADV_ARC

How does the design of the TSF ensure that its security cannot be circumvented?

Examples:

Interrupts use hardware traps to TSF processing

Firewall is only point in common to both internal and external networks



Architectural Design: ADV_ARC

How does the design of the TSF ensure that its security cannot be changed?

Examples:

Hardware privilege levels separate user code from TSF code; sandboxes

Firewall with no means of directly-connecting, installing, running code

TSF Internals: ADV_INT

How does the structure of the TSF lend itself to being analysed?

- Complexity of the TSF determines how much analysis is appropriate
- Hardware is usually more straightforward
- Emphasis is usually on software portions

TSF Software Internals

View TSF as *modules*; examine:

Code Cohesion – all the code contributes to a unified purpose

Data Cohesion – all collocated data definitions are strongly related

Coupling – modules directly communicate as black boxes; few global variables

Complexity – data paths through TOE

Duplicate code or data – unnecessarily adds confusion by replicating work

Extraneous code or data – never used

TSF Security Policy Model: ADV_SPM

How does the behavior of the TSF ensure that security is always maintained?

Mathematically-precise proof:

- if initial state is secure and
- if all assumptions hold,
- then all future states will be secure.



Contact

CC v3.0 available at:

<http://www.commoncriteriaportal.org>

Ron Bottomly
rjbotto@missi.ncsc.mil