A revised TSFI definition improves focus on security and reduces workload.
Introduction

- CC Terminology: TOE – TSF – Interfaces – TSFI
- Existing TSFI definitions within Common Criteria
- Revised TSFI definition
- Examples
- Conclusion
**CC Terminology: TOE (Target of Evaluation)**

TOE types:
- ICs, Smart Cards and Smart Card related Devices and Systems
- Operating systems
- Network and Network related Devices and Systems
- Etc.

**Examples:**
- Smart Card IC hardware
- Operating system
- Network related device
- Reconfigurable multiservice router
**CC Terminology: TSF (TOE Security Functionality)**

TSF: That part of the TOE that realizes the security functionality.

**Examples:**
- TOE: Operating system, TSF: Kernel, time service, etc.
- TOE: Network related device, TSF: I&A, logging service, routing management, etc.
- TOE: Smart card IC hardware, TSF: Hardware related to physical network layer, etc.
- TOE: Everything, TSF: Nothing.
**CC Terminology: Interfaces (means of interaction)**

**TOE:**

Most TOE Types:

- TSF
- ITF-1
- ITF-2
- ITF-3

Some TOE Types:

- TSF
- Embedded software (Non-TOE)
- ITF-4
- ITF-5
- Smart card IC hardware

**Examples:**

- TOE Interface
  - Operating system
  - Network related device
  - Embedded software (Non-TOE)

**Interface:**

- ITF-1: Editor (vi)
- ITF-2: Kernel debugger (KDB)
- ITF-3: Kernel API (e.g. Create new process)
- ITF-4: ISO7816 comm. interface
- ITF-5: Special Function Register (e.g. DES Key)

*Revised TSFI definition*
CC Terminology: TSFI (interface of the TSF) #1

TOE:

**Most TOE Types:**
- TSF
- ITF-2
- ITF-3

**Examples:**
- Operating system
  - ITF-2: Kernel debugger (KDB)
  - ITF-3: Kernel API (e.g. Create new process)
- Network related device
  - ITF-2: Serial Console, Management Interface

**Some TOE Types:**
- TSF
- ITF-4
- ITF-5

**Examples:**
- Embedded software (Non-TOE)
- Smart card IC hardware
  - ITF-4: ISO7816 comm. interface
  - ITF-5: Special Function Register (e.g. DES Key)
The subject of this presentation:

When are TSF interfaces to be considered TSFI?
Common Criteria TSFI definition 1

- CC Part 1 / CEM: All interfaces of the TSF => Potentially too many TSFI
  - Example:
    - TOE: some Wifi enabled ADSL router
    - Security: Secure Wifi
    - TSF: Management service kernel, IP stack
  - Lots of interfaces
    - To document
    - To evaluate
    - To test

- Security Relevant interfaces subset:
  - Security mode
  - Encryption
  - Passphrase
  - Key renewal
  - Antenna
Common Criteria TSFI definition 2

☐ CC Part 3 Annex A.2:
  Incoming interfaces of the TSF that are accessible to a potential attacker.

↓

Potentially too few TSFI

☐ Inaccessibility of the interfaces is:
  Enforced by the TOE and / or due to the Security Objectives of the operational Environment (OE).

From CC Part 3 Annex A.2:

The problems with this definition:

☐ For an SFR that does not manifest externally: Its interfaces are not thoroughly documented and therefore the SFR cannot be tested.

☐ For an SFR that involves outgoing interfaces: Its interfaces are not thoroughly documented and therefore the SFR cannot be tested.
Revised TSFI definition (NSCIB NSP#7) #1

TSF interface (TSFI):

A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF, such that:

- **Attackers can possibly access this means,**
- **And/or**
- **SFRs are traced to this means**

For the purpose of this definition:

- **An attacker is any external entity or non-TSF subject in the TOE that has not been explicitly defined as trusted in the ST**
- **An attacker can possibly access a means unless either the TSF itself, or the security objectives for the operational environment, or a combination thereof, prevents the attacker from having access.**
Revised TSFI definition (NSCIB NSP#7) #2

Splitting a means

In some cases, a developer may want to split a means into two parts, where part of the means is a TSFI, while another part of the means is not a TSFI. This allows the developer to separate the TSFI from the remainder of the means, to make his documentation burden smaller, as he only has to document the TSFI in depth, and not the entire means.

For an example:
Refer to sheets ‘Examples – Network related devices’ 2 & 3 later in the presentation
Revised TSFI definition (NSCIB NSP#7) #3

- Compared to Common – Why does the revised TSFI definition work?
  - Criteria definitions
    - CC Part 1 / CEM – The irrelevant interfaces are eliminated as TSFI
    - CC Part 3 Annex A.2 – The required interfaces are included as TSFI
Impact of the revised TSFI definition

Assuming there are less TSFI due to the revised TSFI definition:

Advantages:

☐ Saves time:

<table>
<thead>
<tr>
<th>CC Family / Class</th>
<th>Developer</th>
<th>Impact Evaluator</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADV_FSP</td>
<td>Much less detail required for Non-TSFI interface documentation</td>
<td>Reduced evaluation load due to smaller evidence</td>
</tr>
<tr>
<td>ATE</td>
<td>Less TSFIs to test</td>
<td>Reduced evaluation load due to smaller evidence</td>
</tr>
</tbody>
</table>

☐ The evaluator can focus on security because of the absence of irrelevant TSFI

Disadvantages (The definition has been used multiple times in evaluations):

☐ None
Examples

The approach of NSCIB NSP#7 has been used multiple times but:
- I could only find a few fit for this presentation.
- Brightsight – Developer NDAs did not allow me to provide details.

As a substitute the next slides provide
- A fictitious example
- Anonymized example
- Some real examples

Thanks to ZTE 中兴 who allowed me to show details of one of their TOEs
Examples – Operating System

Examples of interfaces that are no longer TSFI:

☐ None
Examples – Network related devices #1

Examples of interfaces that are no longer TSFI:

- Serial Console
  - Not a TSFI because not accessible to potential attacker and not related to claimed security functionality.

Note: This type of devices is always located in a secure area
Examples – Network related devices #2

Example of split interfaces some of which that are no longer TSFI:

- Management console:
  - Functionality is provided by the Management service that is part of TSF.
  - Consists of console commands of which only a small subset are security relevant.
  - Not accessible to a potential attacker due to it being encapsulated in a secure tunnel (ssh).

TSFI:
- Security related management console commands (5%)

Non-TSFI:
- Non-security related management console commands (95%)

TSFI:
- Secured channel
Examples – Network related devices #3

Example of split interfaces some of which that are no longer TSFI:

- Simple Network Management Protocol v3 (SNMPv3)
  - SNMP is provided by SNMP service that is part of the TSF.
  - The actual SNMP data (payload) itself is not accessible to a potential attacker due to it being encapsulated in a secure tunnel (ssh)
  - The actual SNMP data (payload) itself is not security relevant

Non-TSFI: Secure tunnel

TSFI:
Examples – Smart card IC hardware

Examples of interfaces that are no longer TSFI:

☐ Some of the Special Function Registers (Those towards building blocks such as a Timer, Modular Arithmetic Accelerator, etc.)

- Normal approach for smart card: everything is TSF
- The Special Function Registers are accessible ONLY to the (Non-TOE) Smart Card embedded software and therefore not to a potential attacker.
- The TOE protects the Smart Card Embedded Software (and its assets).
Conclusion

☐ NSCIB NSP#7 works: The Revised TSFI definition has successfully been used multiple times.

☐ The savings depend upon the TOE, ranging from zero (e.g. Operating System) to considerable (e.g. Network related devices) effort

☐ The revised TSFI definition leads to limited effort spend on security irrelevant interfaces. Therefore the focus shifts to the security relevant interfaces.
Contact information

Brightsight BV
Delftechpark 1
2628 XJ Delft
The Netherlands

We are looking for people that want to perform CC evaluations under BSI, IPA, NITES, NSCIB, SCCS or SERTIT

Peter van Swieten
+ 31 15 269 2500
swieten@brightsight.com
www.brightsgight.com