Technical Decision TD_DBMS_B_002: Session Locking Mechanism Expansion

Issue

The DBMS cPP requires per-user session limiting in FTA_MCS.1. Stakeholders have requested clarification if session limiting must be performed on a per-user basis, or if session limits can be set by other mechanisms.

Resolution

The DBMS cPP has been updated to include FTA_MCS_EXT.1 as a mandatory requirement. This SFR will allow ST authors to assign a mechanism for session limit enforcement. This update makes FTA_MCS.1 selection-based, depending on the selection within FTA_MCS_EXT.1.

The following updates apply:

- Update **Table 4: Auditable Events** in Section 6.1.1 to replace FTA_MCS.1 with FTA_MCS_EXT.1.
- Update Section 6.4.4 **Specification of Management Functions (FMT_SMF)** to include the management function "Configure the session limiting mechanism".

Example 1. FMT_SMF.1.1

The TSF shall be capable of performing the following security management functions:

- · Database configuration
- · User and role management
- Configure the session limiting mechanism

Section 6.5.1 Update

Example 2. FTA_MCS_EXT.1 Configurable Session Limiting Mechanisms

FTA_MCS_EXT.1.1 The TSF shall restrict the maximum number of concurrent sessions based on [selection: User session locking as defined by FTA_MCS.1, [assignment: mechanism(s) for session limitation enforced by the TSF]].

FTA_MCS_EXT.1.2 The TSF shall provide the capability for an authorized administrator to configure the selected enforcement mechanism(s).

Application Note 12: If "User session locking as defined by FTA_MCS.1" is selected, then the FTA MCS.1 SFR must also be included.

Section B.2 Update

Family Behaviour

This family defines requirements to place limits on the number of concurrent sessions.

Component Leveling

FTA_MCS_EXT.1
Basic limitation on
multiple concurrent
sessions

FTA_MCS_EXT.1 * management of the maximum allowed number of concurrent user sessions * management of the enforcement mechanism(s)

FTA_MCS_EXT.1 If FAU_GEN is included in the PP/ST, the following should be auditable: * Rejection of a new session based on the limitation of multiple concurrent sessions

• FIA_UID.1 Timing of identification

Appendix D: Selection-Based Requirements

As described in the introduction, baseline requirements are in the body of the cPP. Additional requirements appear here if certain selections are made.

Example 3. FTA_MCS.1 Basic limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [assignment: default number] sessions per user.

Application Note 17: CC Part 2 (para 473) allows that the default number may be defined as a management function in FMT.

Supporting Document Updates

Section 2.4: FTA_MCS_EXT.1 Configurable Session Limiting Mechanisms

TSS The evaluator shall examine the TSS and verify that it states the default number of concurrent sessions per user. If this default can be changed, the evaluator shall verify that the TSS specifies this.

Guidance Documentation The evaluator shall verify that guidance describes how to set the default number of sessions per user and, if applicable, how to change it.

Tests The evaluator shall: * Establish the maximum number of concurrent sessions and verify it is enforced. * Attempt to exceed the maximum and verify additional sessions cannot be created. * If the default number can be changed, modify it and repeat the test.