Project: DRA FRONT END FILTER PROJECT

Title: Report on Phase 3 Proofs

Ref: DS/FMU/FEF/048 *Issue: Revision* : *2.1* *Date:* 5 June 2016

Status: Approved *Type:* Report

Keywords:

Author:

Name	*Location*	*Signature*	*Date*
R.D. Arthan			

Authorisation for Issue:

Name	*Function*	*Signature*	*Date*
R. B. Jones	HAT Manager		

Abstract: This document is a brief report for the DRA Front End Filter project RSRE 1C/6130, it identifies the proof work carried out in phase 3.

Distribution: HAT FEF File

0 DOCUMENT CONTROL

0.1 Contents List

0.2 Document Cross References

[1] DS/FMU/FEF/039. *Proposal and Quotation for Phase 3.* R.D. Arthan, ICL Secure Systems, WIN01.

[2] DS/FMU/FEF/040. *Multi-level Formal Security Policy.* R.D. Arthan, ICL Secure Systems, WIN01.

[3] DS/FMU/FEF/042. *Multi-level Architectural Model.* R.D. Arthan, ICL Secure Systems, WIN01.

[4] DS/FMU/FEF/043. *The Labelling Property for SWORD.* R.B. Jones, ICL Secure Systems, WIN01.

[5] DS/FMU/FEF/044. *Proofs About Labelling.* R.B. Jones, ICL Secure Systems, WIN01.

[6] DS/FMU/FEF/045. *Phase 3 Theory Listings.* R.B. Jones, ICL Secure Systems, WIN01.

[7] DS/FMU/IED/WRK057. *Examples of HOL Type Definitions.* R.D. Arthan, Lemma 1 Ltd., `http://www.lemma-one.com`.

0.3 Changes History

1.1 (24 March 1994) First draft.

1.2 (24 March 1994) First draft for DRA.

Revision : *2.1* **(5 June 2016)** Final approved version.

Issue 2.2 Removed dependency on ICL logo font

0.4 Changes Forecast

None.

1 GENERAL

1.1 Scope

This document is a report on the proof work carried out under phase 3 of the FEF project. It constitutes deliverable D18 as described in the phase 3 proposal, [1].

1.2 Introduction

The background to the phase 3 technical work is discussed in the proposal, [1]. The specifications produced in phase 3 are overviewed in [1]. This document simply serves to identify the main theorems which were proved and give a pointer to the location of the proofs in the documentation structure.

2 DESCRIPTION OF THE PROOFS

The main objective behind the proof work in phase 3 was to debug the the phase 3 specifications. The proof work therefore mainly comprises consistency proofs, and proofs of various conjectures which are identified in some of the specification documents as being useful or significant.

The proofs relate to three specification documents: *Multi-level Formal Security Policy* [2]; *Multi-level Architectural Model* [3]; and *The Labelling Property for SWORD* [4]. Because of the relatively small size of the proofs in phase 3, the proof scripts relating to the three documents are collected together into a single document, *Proof About Labelling* [5], which devotes a section to each of the three specification documents. The document [6] contains listings of the theories containing both the specifications and the theorems proved, together with a listing of the theory *wrk057* which contains some supporting material borrowed from a ProofPower example document. The remaining sections of this document briefly describe the theories listed in [6].

2.1 Supporting Material

The ProofPower example document [7] is used to support the phase 3 specifications. It creates a theory, *wkr057* dealing with trees with arbitrary finite branching which are used to represent the tree-structured objects which model SSQL queries and their results. The theorems of [7] are all of a purely mathematical and somewhat technical nature. From the point of view of the FEF work, the main role of the document is to characterise a polymorphic type, $'a\ TREE$, comprising trees with arbitrary finite branching and with nodes labelled with elements of the parameter type, $'a$. This type is characterised by its constructor function, *MkTree*, which constructs a tree given the label and immediate subtrees of its root node. The mathematical properties of *MkTree* are characterised by the theorems *tree_prim_rec_thm* and *tree_induction_thm*. A deep understanding of these theorems should not be necessary for an understanding of the theorems relating to the phase 3 specifications proper.

2.2 Multi-level Security Policy

The proof scripts in [5] populate the theory *fef040* with various theorems about the generic security policy and the material on component extraction in [2]. The two main theorems are *thm_040_1* and *thm_040_2* which confirm the conjectures *conj_040_1* and *conj_040_2* identified and discused in [2]. The theory *fef040* also contains a number of general lemmas about the generic security policy and some specific lemmas required for the main theorems.

2.3 Multi-level Architectural Model

The proof scripts in [5] populate the theory *fef042* with various theorems about the architectural model of [3]. Various conjectures of interest are identified in [3] and some of these are proved.

2.4 Labelling Property

The proof scripts in [5] populate the theory *fef042* with theorems about the labelling property of [3]. These include a proof that the result labelling property is consistent, in the sense that there are systems which satisfy it. Two such witnesses to the consistency are specified and verified in [3].