Proving Properties of Secure Systems

Roger Bishop Jones

ICL Defence Systems

ABSTRACT

This paper reviews progress on the development of formal proofs of properties of secure systems. This work has been undertaken by ICL Defence Systems in the course of design studies under contract to CESG. The paper highlights some of the benefits which have already been obtained from this activity. This document consists of the overheads for a presentation on formal proof of properties of secure systems.

1987-03-12
1. INTRODUCTION

CURRENT STATUS of WORK

SUMMARY of BENEFITS to date

PLAN for PROOF

EXPECTED FUTURE BENEFITS
2. CURRENT STATUS of WORK

first TRANSLATION COMPLETED
size 250Kb = 10*‘arithmetic‘

METHODOLOGY well ESTABLISHED
(except for schema calculus)

SUPPORTING INFRASTRUCTURE in place

PROBLEMS: Performance & Resilience
3. SUMMARY of BENEFITS to date

ERRORS revealed by TYPE CHECKING

some CONSISTENCY CHECKS

INSIGHT into Z
SEMANTICS and PROOF THEORY

experience HANDS ON with
THEOREM PROVING TOOLS

INFRASTRUCTURE for
LOW REPEAT COST
3.1. Z SEMANTICS and PROOF THEORY

Are empty types legal? e.g.:

```
INT_PAIR[p]
left, right :INT
left > right ∧ right > left
```

If not, how do we know that our schemas are legal? If so, what is the status of declarations using empty types? e.g.:

```
ip:INT_PAIR
```

Can we then assert:

```
? ip.left > ip.right ∧ ip.right > ip.left
```

?
There is a solution which provides a consistent proof theory for Z, and which translates into HOL.

We interpret schemas with non-empty bodies in the following way:

\[
\text{INT\_PAIR} = \\
\{ [\text{left, right}: \text{INT}] | \text{left} > \text{right} \land \text{right} > \text{left} \} \\
\cup \{ \mu p : [\text{left, right}: \text{INT}] | \text{left} > \text{right} \land \text{right} > \text{left} \}
\]

Inference rules relating to schema types must be qualified.

\[
(\exists x : [\text{left, right}: \text{INT}]. \text{left} > \text{right} \land \text{right} > \text{left}) \\
\forall ip : \text{INT\_PAIR}.
\quad ip.\text{left} > ip.\text{right} \land ip.\text{right} > ip.\text{left}
\]
4. PLAN for PROOF

ONCE ONLY developments

sum
partial functions
lists
labelled products
disjoint unions
schemas

SECURITY PROOF

top level, by induction over lists
lower levels not yet considered

STRATEGY

backward search
5. EXPECTED FUTURE BENEFITS

MORE of the SAME

FORMAL PROOFS of PROPERTIES!

PRACTICAL Theorem Proving EXPERIENCE

CONFIDENCE of CONSISTENCY

CONFIDENCE of SUFFICIENCY

CONFIDENCE of CORRECTNESS of DESIGN

REUSABLE ABSTRACT THEORIES of SECURITY

IMPROVED SKILLS BASE for CODE VERIFICATION
Improved UNDERSTANDING of REASONING about Z