## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cover</td>
<td>1</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>3</td>
</tr>
<tr>
<td>Abstract</td>
<td>5</td>
</tr>
<tr>
<td>Resumen</td>
<td>7</td>
</tr>
<tr>
<td>Resum</td>
<td>9</td>
</tr>
<tr>
<td>Contents</td>
<td>14</td>
</tr>
<tr>
<td>List of Figures</td>
<td>15</td>
</tr>
<tr>
<td>List of Tables</td>
<td>17</td>
</tr>
<tr>
<td>List of Listings</td>
<td>19</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>21</td>
</tr>
<tr>
<td>1.1 Secure partitioned systems</td>
<td>21</td>
</tr>
<tr>
<td>1.1.1 Secure hypervisors</td>
<td>21</td>
</tr>
<tr>
<td>1.1.2 Validation and verification of secure hypervisors</td>
<td>22</td>
</tr>
<tr>
<td>1.1.3 Challenges on the validation of secure hypervisors</td>
<td>24</td>
</tr>
<tr>
<td>1.1.4 Terminology</td>
<td>26</td>
</tr>
<tr>
<td>1.2 Motivation and main goals</td>
<td>26</td>
</tr>
<tr>
<td>1.3 Contributions of this thesis</td>
<td>26</td>
</tr>
<tr>
<td>1.4 Outline of this thesis</td>
<td>27</td>
</tr>
<tr>
<td>1.5 Research Context</td>
<td>28</td>
</tr>
</tbody>
</table>
# 2 Secure Hypervisor Verification

## 2.1 Formal methods in secure hypervisors

- **2.1.1 Deductive verification**
- **2.1.2 Theorem provers**
- **2.1.3 Static code analysis**

## 2.2 Formal methods in safety standards

- **2.2.1 RTCA Standards**
- **2.2.2 IEC-61508 Standards**
- **2.2.3 ECSS Standards**
- **2.2.4 Common Criteria Framework**

## 2.3 Summary

---

# 3 XtratuM foundations: A formalisation approach.

## 3.1 Introduction

## 3.2 XtratuM Overview

- **3.2.1 XtratuM Architecture**

## 3.3 Trustability enforcement

- **3.3.1 Interrupt Model**
- **3.3.2 Fault Management Model**
- **3.3.3 System specification**

## 3.4 Hypervisor model

- **3.4.1 Hypervisor state variables**
- **3.4.2 General properties**
- **3.4.3 Spatial isolation properties**
- **3.4.4 Temporal isolation properties**
- **3.4.5 Hypervisor state management**
- **3.4.6 Hypervisor pre- and post-conditions**

## 3.5 Conclusion

---

# 4 Formal Validation of XtratuM Components

## 4.1 Introduction

- **4.1.1 XtratuM Hypervisor core**

## 4.2 Deductive Formal Methods

## 4.3 Proposed Approach
5 Analysing the Impact and Detection of Kernel Stack Infoleaks

5.1 Introduction

5.2 Related Work

5.2.1 Protection Mechanisms

5.2.2 Protection Techniques

5.3 Classification of Information Disclosure Vulnerabilities

5.3.1 The Anatomy Of An Infoleak

5.3.2 Targets of Infoleaks

5.3.3 Infoleaks Bug Causes

5.3.4 Infoleaks Data Sources

5.4 Analysis on the Impact of Stack Infoleaks

5.4.1 The Anatomy of An Attack

5.4.2 The Contents of the Kernel Stack

5.4.3 Infoleak Based Attacks

5.5 The Detection of Information Leak vulnerabilities

5.5.1 Infoleak Vulnerability Model

5.5.2 Semantic Patch Preparation

5.5.3 Filter and Rank of matches

5.5.4 Infoleak Code Review and Correction

5.6 Experimental Evaluation of the Detection Technique

5.6.1 Existing Infoleak Detection

5.6.2 Discovery of Vulnerabilities

5.6.3 Applications and Limitations of our Approach

5.7 Conclusions and Further Work
6 Conclusions and open research lines

6.1 Conclusions ................................................................. 75
6.2 Research Lines ............................................................ 76
6.3 Publications related to this thesis ................................. 76

Bibliography .................................................................................. 79

Acronyms ....................................................................................... 87

Glossary ....................................................................................... 89