# Preface

1. **What is trusted computing?**  
   *Chris J. Mitchell*

   1.1 Introduction  
   1.2 Computer security and trusted computing  
   1.3 Trusted computing – a very brief history  
   1.4 Trusted computing – current status  
   1.5 Applications of trusted computing  
   1.6 The future of trusted computing  
   1.7 Further information  

   References

2. **Concepts of trusted computing**  
   *G. J. Proudler*

   2.1 Introduction  
   2.2 Overview  
   2.3 Trusted Computing Group  
   2.4 Trusted platforms  
   2.5 Limitations of trusted platforms  
   2.6 Using trusted computing  

   References

3. **An overview of trusted computing technology**  
   *Eimear Gallery*

   3.1 Introduction  
   3.1.1 Overview

   References
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.2</td>
<td>Purpose and scope</td>
<td>30</td>
</tr>
<tr>
<td>3.2</td>
<td>What is trusted computing?</td>
<td>31</td>
</tr>
<tr>
<td>3.2.1</td>
<td>Trust</td>
<td>31</td>
</tr>
<tr>
<td>3.2.2</td>
<td>Trusted computing functionality</td>
<td>31</td>
</tr>
<tr>
<td>3.3</td>
<td>The TCG specification set</td>
<td>33</td>
</tr>
<tr>
<td>3.3.1</td>
<td>Introduction</td>
<td>33</td>
</tr>
<tr>
<td>3.3.2</td>
<td>The TCG</td>
<td>33</td>
</tr>
<tr>
<td>3.3.3</td>
<td>The TP</td>
<td>34</td>
</tr>
<tr>
<td>3.3.4</td>
<td>Entities involved</td>
<td>37</td>
</tr>
<tr>
<td>3.3.5</td>
<td>Trusted platform components</td>
<td>38</td>
</tr>
<tr>
<td>3.3.6</td>
<td>Properties of the TPM</td>
<td>40</td>
</tr>
<tr>
<td>3.3.7</td>
<td>Initialising the TPM</td>
<td>44</td>
</tr>
<tr>
<td>3.3.8</td>
<td>Enabling, activating and taking ownership of the TPM</td>
<td>45</td>
</tr>
<tr>
<td>3.3.9</td>
<td>Platform identification and certification</td>
<td>47</td>
</tr>
<tr>
<td>3.3.10</td>
<td>Demonstrating privilege</td>
<td>51</td>
</tr>
<tr>
<td>3.3.11</td>
<td>Integrity measuring, recording and reporting</td>
<td>57</td>
</tr>
<tr>
<td>3.3.12</td>
<td>Locality</td>
<td>60</td>
</tr>
<tr>
<td>3.3.13</td>
<td>Protected storage</td>
<td>60</td>
</tr>
<tr>
<td>3.3.14</td>
<td>Transport security</td>
<td>64</td>
</tr>
<tr>
<td>3.3.15</td>
<td>Monotonic counter</td>
<td>67</td>
</tr>
<tr>
<td>3.3.16</td>
<td>Context manager</td>
<td>67</td>
</tr>
<tr>
<td>3.3.17</td>
<td>Delegation</td>
<td>68</td>
</tr>
<tr>
<td>3.3.18</td>
<td>Time-stamping</td>
<td>71</td>
</tr>
<tr>
<td>3.3.19</td>
<td>Migration mechanisms</td>
<td>72</td>
</tr>
<tr>
<td>3.3.20</td>
<td>Maintenance mechanisms</td>
<td>73</td>
</tr>
<tr>
<td>3.3.21</td>
<td>Audit</td>
<td>73</td>
</tr>
<tr>
<td>3.3.22</td>
<td>Conclusions</td>
<td>74</td>
</tr>
<tr>
<td>3.4</td>
<td>NGSCB</td>
<td>75</td>
</tr>
<tr>
<td>3.4.1</td>
<td>Introduction</td>
<td>75</td>
</tr>
<tr>
<td>3.4.2</td>
<td>The relationship between the TCG and NGSCB</td>
<td>75</td>
</tr>
<tr>
<td>3.4.3</td>
<td>The NGSCB architecture</td>
<td>76</td>
</tr>
<tr>
<td>3.4.4</td>
<td>NGSCB components</td>
<td>80</td>
</tr>
<tr>
<td>3.5</td>
<td>LaGrande</td>
<td>81</td>
</tr>
<tr>
<td>3.5.1</td>
<td>Introduction</td>
<td>81</td>
</tr>
<tr>
<td>3.5.2</td>
<td>The architecture</td>
<td>81</td>
</tr>
<tr>
<td>3.5.3</td>
<td>Hardware enhancements and extensions</td>
<td>82</td>
</tr>
<tr>
<td>3.6</td>
<td>ARM TrustZone</td>
<td>84</td>
</tr>
<tr>
<td>3.6.1</td>
<td>Introduction</td>
<td>84</td>
</tr>
<tr>
<td>3.6.2</td>
<td>Fundamental components</td>
<td>85</td>
</tr>
<tr>
<td>3.7</td>
<td>The PERSEUS system architecture</td>
<td>87</td>
</tr>
<tr>
<td>3.7.1</td>
<td>Introduction</td>
<td>87</td>
</tr>
<tr>
<td>3.7.2</td>
<td>Trusted platform functionality</td>
<td>88</td>
</tr>
<tr>
<td>3.7.3</td>
<td>The PERSEUS security kernel</td>
<td>89</td>
</tr>
<tr>
<td>3.8</td>
<td>Secure coprocessors</td>
<td>92</td>
</tr>
</tbody>
</table>
4 An overview of NGSCB
Marcus Peinado, Paul England and Yuqun Chen

4.1 Introduction
4.2 Requirements
  4.2.1 Security requirements
  4.2.2 Commercial requirements
4.3 Existing approaches and problems
  4.3.1 Assurance and device support
  4.3.2 Operating system compatibility
4.4 The isolation kernel
  4.4.1 CPU
  4.4.2 Memory
  4.4.3 Devices
  4.4.4 Prototype implementation
4.5 Code authentication
  4.5.1 Execution environment and code identities
  4.5.2 Persistent protected storage
  4.5.3 Attestation
4.6 The TPM
  4.6.1 TPM support for authenticated operation – initialisation
  4.6.2 Authenticated operation in practice
4.7 System overview
4.8 Applications
  4.8.1 Enhanced smart-card applications
  4.8.2 Rights management
  4.8.3 Threat models
4.9 Related work
  4.9.1 Code authentication
4.10 Conclusions
References

5 The DAA scheme in context
Ernie Brickell, Jan Camenisch and Liqun Chen

5.1 Introduction
  5.1.1 The privacy issue in TCG technology
References
## Contents

5.1.2 What is DAA? 144  
5.1.3 A simple example of DAA use 146  
5.2 History of DAA 146  
5.2.1 The privacy-CA solution 146  
5.2.2 The DP protocol 147  
5.2.3 The GSRE scheme 149  
5.2.4 The set signature scheme 151  
5.2.5 The modified set signature scheme 152  
5.3 Related prior work 153  
5.4 The DAA scheme 155  
5.4.1 Entities 155  
5.4.2 Notation 155  
5.4.3 Security parameters 155  
5.4.4 Setup for the issuer 156  
5.4.5 Verification of the issuer’s public key 158  
5.4.6 Join protocol 159  
5.4.7 DAA-signing protocol 162  
5.4.8 Verification algorithm 165  
5.4.9 On rogue tagging 165  
5.5 Security results 166  
5.6 Options for re-issue of DAA keys 166  
5.6.1 Requirements for the re-issue of DAA keys 167  
5.6.2 Method implemented in the TPM 167  
5.6.3 Re-issue upon sale of TPM 168  
5.7 Increasing efficiency 169  
5.8 Conclusion and acknowledgements 171  
References 172

6 Single Sign-On using TCG-conformant platforms 175  
Andreas Pashalidis and Chris J. Mitchell

6.1 Introduction 175  
6.1.1 Why SSO? 176  
6.1.2 How SSO works 176  
6.1.3 Why SSO has failed 177  
6.2 Using trusted platforms for SSO 179  
6.2.1 Pseudo-SSO 179  
6.2.2 True SSO 181  
6.3 Privacy 183  
6.3.1 Privacy under TCG 1.1 185  
6.3.2 Privacy under TCG 1.2 185  
6.4 Other issues 187  
6.4.1 Cross-platform mobility 187  
6.4.2 Complexity of managing trusted states 188  
6.4.3 Costs 189
7 Secure delivery of conditional access applications to mobile receivers

Eimear Gallery and Allan Tomlinson

7.1 Introduction
7.1.1 Motivation
7.1.2 Purpose and scope

7.2 CA systems
7.2.1 DVB standards
7.2.2 Simulcrypt
7.2.3 Common interface
7.2.4 Limitations of existing mechanisms
7.2.5 Modifications required for mobile receivers

7.3 Security requirements
7.3.1 Security threats
7.3.2 Security services and mechanisms

7.4 Protocols for secure application download using trusted computing technologies
7.4.1 Model
7.4.2 Notation
7.4.3 Assumptions
7.4.4 Initiation of the protocols
7.4.5 Public key protocol
7.4.6 Analysis of the public key protocol
7.4.7 Secret key protocol
7.4.8 Analysis of the secret key protocol
7.4.9 Concluding remarks

7.5 Mapping the protocols to trusted computing architectures
7.5.1 Building the protocols using TCG specifications
7.5.2 Building the protocols on NGSCB
7.5.3 Implementing trusted download using PERSEUS

7.6 Protocols for secure application download using alternative architectures
7.6.1 Model
7.6.2 Assumptions
7.6.3 Initiation of the protocols
7.6.4 Alternative protocol

7.7 Mapping the alternative protocol to specific hardware architectures
7.7.1 The XOM architecture
7.7.2 Application of XOM to trusted download
## Contents

7.7.3 Analysis of XOM trusted download  
7.7.4 The AEGIS architecture  
7.7.5 Application of AEGIS to trusted download  
7.7.6 Analysis of AEGIS trusted download  

7.8 Conclusions  
Acknowledgement  
References

### 8 Enhancing user privacy using trusted computing

*Anand S. Gajparia and Chris J. Mitchell*

8.1 Introduction  
8.2 Trusted computing  
8.3 The PI model  
8.4 Scenarios  
8.4.1 Registration scenario  
8.4.2 Location-based service scenario  
8.4.3 Medical records  
8.5 TCG mechanisms  
8.5.1 TPM identities  
8.5.2 TCG measuring, reporting and storing processes  
8.5.3 Sealing data  
8.6 Protecting PI using trusted computing  
8.6.1 Overview  
8.6.2 Using trusting computing with PI  
8.6.3 Constraints, LIPA and LI tokens  
8.7 Concluding remarks  
References

### 9 Certificate management using distributed trusted third parties

*Alexander W. Dent and Geraint Price*

9.1 Introduction  
9.1.1 Secure execution environments  
9.2 Distributed TTPs  
9.2.1 Advantages and disadvantages  
9.3 Distributed CAs  
9.3.1 The CA-applet concept  
9.3.2 CA-applet functionality  
9.3.3 Potential problems with CA-applets  
9.4 Applications  
9.4.1 Personal CAs  
9.4.2 Ad hoc networks  
9.4.3 Distributed registration/certificate data preparation  
9.4.4 Short-lived certificates  
9.4.5 Lightweight PKI

---

8 Enhancing user privacy using trusted computing  
239

9 Certificate management using distributed trusted third parties  
251
10 Securing peer-to-peer networks using trusted computing
Shane Balfe, Amit D. Lakhani and Kenneth G. Paterson

10.1 Introduction
10.2 Overview of security issues for P2P networks
10.3 Overview of trusted computing
10.4 P2P pseudonymous authentication using trusted computing
10.5 Securing P2P networks using trusted computing
10.6 Two approaches to securing P2P networks using trusted computing
10.7 Issues and open problems
10.8 Conclusions
Acknowledgements
References

11 The future of trusted computing: an outlook
Klaus Kursawe

11.1 Applications
11.2 Infrastructure
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3</td>
<td>Trusted operating systems</td>
<td>300</td>
</tr>
<tr>
<td>11.3.1</td>
<td>Hardening existing operating systems</td>
<td>301</td>
</tr>
<tr>
<td>11.3.2</td>
<td>Secure operating systems</td>
<td>301</td>
</tr>
<tr>
<td>11.4</td>
<td>Pervasive TC</td>
<td>302</td>
</tr>
<tr>
<td>11.4.1</td>
<td>PCs and servers</td>
<td>302</td>
</tr>
<tr>
<td>11.4.2</td>
<td>Embedded trust</td>
<td>303</td>
</tr>
</tbody>
</table>

References

Index 305