- Preface p. xi
- Introduction p. xiii
- Contributors p. xv
- 1 Building on Rock Rather Than Sand M Hogg and S M Bouch and M F G Smeaton p. 1
- 1.1 Introduction to iTrust and the eBusiness Environment p. 1
- 1.2 Benefits of an Integrated Approach? p. 3
- 1.3 Architecture p. 3
- 1.4 Architecture Overview p. 4
- 1.5 Authentication and Authorisation p. 7
- 1.6 Implementing the Architecture p. 11
- 1.7 Summary p. 20
- 2 XML and Security A Selkirk p. 21
- 2.1 Introduction p. 21
- 2.2 A Brief History of XML p. 21
- 2.3 An XML Primer p. 23
- 2.4 The Benefits of XML p. 25
- 2.5 XML Technologies p. 25
- 2.6 XML Digital Signatures p. 31
- 2.7 Problems with XML Signature p. 40
- 2.8 Uses for XML Signature p. 40
- 2.9 XML Encryption p. 41
- 2.10 Summary p. 43
- 3 Using XML Security Mechanisms A Selkirk p. 45
- 3.1 Introduction p. 45
- 3.2 Web Services p. 45
- 3.3 Web Service Protocols p. 47
- 3.4 Public Key Infrastructure in a Web Service Environment p. 49
- 3.5 New Security Problems p. 54
- 3.6 XML Security Services p. 55
- 3.7 XML Key Management Specification p. 57
- 3.8 Security Assertion Markup Language p. 59
- 3.9 XML Access Control p. 59
- 3.10 Summary p. 61
- 4 Security Modelling Language M R C Sims p. 63
- 4.1 Introduction p. 63
- 4.2 Why Model a System's Security? p. 63
- 4.3 Scope of the SecML p. 64
- 4.4 Overview of the Modelling Approach p. 65
- 4.5 Building a Model p. 65
- 4.6 Summary p. 69
- Appendix A Element Classes p. 70
- Appendix B Element Class Diagrams p. 85
- Appendix C SecML Element Names p. 89
- Appendix D Example SecML Diagrams p. 92

- 5 Public Key Infrastructures--the Next Generation K P Bosworth and N Tedeschi p. 95
- 5.1 Introduction p. 95
- 5.2 A Brief History of Public Key Infrastructures p. 96
- 5.3 The Main Problem with a PKI is ... p. 105
- 5.4 Other PKI Problems p. 106
- 5.5 Current Solutions to Globalisation p. 112
- 5.6 Certificate Validation p. 115
- 5.7 Better Solutions for the Future p. 117
- 5.8 Summary p. 119
- 6 An Overview of Identifier-Based Public Key Cryptography I Levy p. 121
- 6.1 Introduction p. 121
- 6.2 Traditional PKC versus Identifier-Based PKC p. 122
- 6.3 The Cocks IDPKC Method p. 123
- 6.4 Key Semantics p. 127
- 6.5 An Example Usage Scenario p. 130
- 6.6 Summary p. 131
- 7 Secure Digital Archiving of High-Value Data T Wright p. 133
- 7.1 Introduction p. 133
- 7.2 Technology p. 134
- 7.3 Secure Digital Archiving p. 140
- 7.4 Summary p. 144
- 8 Wireless Security C W Blanchard p. 147
- 8.1 Introduction p. 147
- 8.2 Security Mechanisms in 3G for the CS and PS Domain p. 148
- 8.3 Security Mechanisms in 3G for the IM Domain p. 155
- 8.4 Is There a Role for PKI in 3G? p. 159
- 8.5 Summary p. 161
- 9 Adapting Public Key Infrastructures to the Mobile Environment N T Trask and S A Jaweed p. 163
- 9.1 Introduction p. 163
- 9.2 WAP Overview p. 163
- 9.3 WAP Security p. 165
- 9.4 The Reality of Implementing a WAP PKI p. 169
- 9.5 Summary p. 169
- 10 TETRA Security D W Parkinson p. 171
- 10.1 Introduction p. 171
- 10.2 Terminology and Environment p. 172
- 10.3 The Need for Security p. 172
- 10.4 The TETRA Security Model p. 173
- 10.5 Direct Mode Operation p. 177
- 10.6 Cryptography p. 178
- 10.7 End-to-End Encryption p. 180
- 10.8 TETRA Security in Practice p. 183
- 10.9 Beyond the Standard p. 184

- 10.10 Summary p. 185
- 11 Firewalls--Evolve or Die D J Gooch and S D Hubbard and M W Moore and J Hill p. 187
- 11.1 Introduction p. 187
- 11.2 The Traditional Security Solution--Firewalls p. 188
- 11.3 The Changing Business Model and Role of the Firewall p. 189
- 11.4 Protocol Tunnelling p. 190
- 11.5 IPsec p. 192
- 11.6 IPsec VPNs p. 194
- 11.7 Extending Security to the Desktop p. 195
- 11.8 Firewall and VPN Policy Management p. 196
- 11.9 The Future p. 200
- 11.10 Summary p. 201
- 12 The Ignite Managed Firewall and VPN Service G Shorrock and C Awdry p. 203
- 12.1 Introduction p. 203
- 12.2 The Ignite Managed Firewall Service p. 204
- 12.3 Summary p. 214
- 13 Information Assurance C J Colwill and M C Todd and G P Fielder and C Natanson p. 215
- 13.1 Introduction p. 215
- 13.2 A Brave New World--New Ways of Doing Business p. 215
- 13.3 Evolving Threats and Risks p. 216
- 13.4 Information Warfare p. 218
- 13.5 Established Security and Risk Management Processes p. 218
- 13.6 What is Different About the Information Assurance Focus? p. 219
- 13.7 IA Threat and Risk Analysis p. 221
- 13.8 Using the IA Protagonist Model p. 222
- 13.9 Detecting and Reacting to Attack p. 226
- 13.10 Benefits to Customers p. 226
- 13.11 Future Development p. 227
- 14 Biometrics--Real Identities for a Virtual World M Rejman-Greene p. 229
- 14.1 Introduction p. 229
- 14.2 Using Biometric Systems p. 231
- 14.3 Performance and Testing Issues p. 234
- 14.4 Security of Biometric Devices and Systems p. 236
- 14.5 Legal and Acceptability Issues p. 237
- 14.6 Standardisation Activities--Evidence of a Maturing Technology p. 238
- 14.7 The Future of Biometric Methods of Authentication p. 238
- 15 Transforming the 'Weakest Link'--a Human-Computer Interaction Approach to Usable and Effective Security M A Sasse and S Brostoff and D Weirich p. 243
- 15.1 Introduction p. 243
- 15.2 Technology p. 245
- 15.3 User p. 248
- 15.4 Goals and Tasks p. 255
- 15.5 Context p. 256
- 15.6 Summary p. 258

- 16 Security Management Standard--ISO 17799/BS7799 M J Kenning p. 263
- 16.1 Introduction p. 263
- 16.2 The Standard p. 264
- 16.3 Case Study--Certification of the SETT p. 265
- 16.4 Technical Implications p. 267
- 16.5 Commercial Advantage p. 269
- 16.6 Summary p. 271
- Acronyms p. 273
- Index p. 281