Contents

List of Figures xi
List of Tables xiii
Preface xvii

1. INTRODUCTION 1
   1.1 Challenges of Broadcast Communication 3
   1.2 Why is Security for Broadcasts Hard? 5
      1.2.1 Broadcast Authentication 5
      1.2.2 Broadcast Signature 8
      1.2.3 Broadcast Data Integrity 9
      1.2.4 Confidential Broadcasts and Restricting Access to
           Legitimate Receivers 9
   1.3 Security Requirements for Broadcast Applications 10
   1.4 Novel Contributions 12
   1.5 Scope of this Book 13
   1.6 Book Overview 13

2. CRYPTOGRAPHIC FUNDAMENTALS 19
   2.1 Broadcast Network Requirements 19
   2.2 Cryptographic Primitives 20
      2.2.1 Symmetric and Asymmetric Cryptography 20
      2.2.2 One-Way Functions and Hash Functions 20
      2.2.3 Pseudo-Random Generator (PRG) 22
      2.2.4 Message Authentication Code (MAC) 22
      2.2.5 Pseudo-Random Function (PRF) 22
   2.3 Efficiency of Cryptographic Primitives 23
   2.4 Commitment Protocols 24
2.4.1 One-Way Chain 25
2.4.2 Merkle Hash Tree 25
2.4.3 Self-Authenticating Values 26

3. TESLA BROADCAST AUTHENTICATION 29
  3.1 Requirements for Broadcast Authentication 29
  3.2 The Basic TESLA Protocol 30
    3.2.1 Sketch of protocol 30
    3.2.2 Sender Setup 31
    3.2.3 Bootstrapping Receivers 32
    3.2.4 Broadcasting Authenticated Messages 33
    3.2.5 Authentication at Receiver 33
    3.2.6 TESLA Summary and Security Considerations 34
  3.3 TIK: TESLA with Instant Key Disclosure 35
    3.3.1 TIK Discussion 39
    3.3.2 TIK Summary and Security Considerations 40
  3.4 Time Synchronization 40
    3.4.1 Direct Time Synchronization 40
    3.4.2 Indirect Time Synchronization 43
    3.4.3 Delayed Time Synchronization 44
    3.4.4 Determining the Key Disclosure Delay 44
  3.5 Variations 45
    3.5.1 Instant Authentication 45
    3.5.2 Concurrent TESLA Instances 46
    3.5.3 Switching Key Chains 48
    3.5.4 Further Extensions 49

3.6 Denial-of-Service Protection 50
  3.6.1 DoS Attack on the Sender 51
  3.6.2 DoS Attack against the Receiver 52

4. BIBA BROADCAST AUTHENTICATION 55
  4.1 The BiBa Signature Algorithm 56
    4.1.1 The Self-Authenticating Values 57
    4.1.2 Intuition for the BiBa Signature 57
    4.1.3 Signature Generation 58
    4.1.4 Signature Verification 58
    4.1.5 Security of BiBa 59
    4.1.6 BiBa Extensions 59
    4.1.7 The BiBa Signature Scheme 61
### Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1.8</td>
<td>Security Considerations</td>
<td>62</td>
</tr>
<tr>
<td>4.2</td>
<td>The BiBa Broadcast Authentication Protocol</td>
<td>65</td>
</tr>
<tr>
<td>4.2.1</td>
<td>One-way Ball Chains</td>
<td>65</td>
</tr>
<tr>
<td>4.2.2</td>
<td>Security Condition</td>
<td>67</td>
</tr>
<tr>
<td>4.3</td>
<td>BiBa Broadcast Protocol Extensions</td>
<td>67</td>
</tr>
<tr>
<td>4.3.1</td>
<td>Extension A</td>
<td>68</td>
</tr>
<tr>
<td>4.3.2</td>
<td>Extension B</td>
<td>69</td>
</tr>
<tr>
<td>4.4</td>
<td>Practical Considerations</td>
<td>69</td>
</tr>
<tr>
<td>4.4.1</td>
<td>Selection of BiBa Parameters</td>
<td>70</td>
</tr>
<tr>
<td>4.4.2</td>
<td>BiBa Overhead</td>
<td>70</td>
</tr>
<tr>
<td>4.4.3</td>
<td>Example: Real-time stock quotes</td>
<td>70</td>
</tr>
<tr>
<td>4.4.4</td>
<td>Efficient Public-Key Distribution</td>
<td>73</td>
</tr>
<tr>
<td>4.5</td>
<td>Variations and Extensions</td>
<td>74</td>
</tr>
<tr>
<td>4.5.1</td>
<td>Randomized Verification to Prevent DoS</td>
<td>74</td>
</tr>
<tr>
<td>4.5.2</td>
<td>Multi-BiBa</td>
<td>74</td>
</tr>
<tr>
<td>4.5.3</td>
<td>The Powerball Extension</td>
<td>75</td>
</tr>
<tr>
<td>4.6</td>
<td>One-Round BiBa is as secure as Multi-Round BiBa</td>
<td>78</td>
</tr>
<tr>
<td>4.7</td>
<td>Merkle Hash Trees for Ball Authentication</td>
<td>81</td>
</tr>
<tr>
<td>5.</td>
<td>EMSS, MESS, &amp; HTSS: SIGNATURES FOR BROADCAST</td>
<td>85</td>
</tr>
<tr>
<td>5.1</td>
<td>Efficient Multicast Stream Signature (EMSS)</td>
<td>87</td>
</tr>
<tr>
<td>5.1.1</td>
<td>EMSS Summary and Security Argument</td>
<td>92</td>
</tr>
<tr>
<td>5.2</td>
<td>MESS</td>
<td>92</td>
</tr>
<tr>
<td>5.2.1</td>
<td>Analysis for Independent Packet Loss</td>
<td>94</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Correlated Packet Loss</td>
<td>98</td>
</tr>
<tr>
<td>5.3</td>
<td>Variations</td>
<td>104</td>
</tr>
<tr>
<td>5.4</td>
<td>HTSS</td>
<td>106</td>
</tr>
<tr>
<td>5.4.1</td>
<td>HTSS Summary and Security Argument</td>
<td>110</td>
</tr>
<tr>
<td>6.</td>
<td>ELK KEY DISTRIBUTION</td>
<td>111</td>
</tr>
<tr>
<td>6.1</td>
<td>Introduction</td>
<td>112</td>
</tr>
<tr>
<td>6.1.1</td>
<td>Requirements for Group Key Distribution</td>
<td>113</td>
</tr>
<tr>
<td>6.2</td>
<td>Review of the LKH Key Distribution Protocol</td>
<td>116</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Extension I: Efficient Join (LKH+)</td>
<td>118</td>
</tr>
<tr>
<td>6.2.2</td>
<td>Extension II: Efficient Leave (LKH++)</td>
<td>119</td>
</tr>
<tr>
<td>6.3</td>
<td>Review of the OFT Key Distribution Protocol</td>
<td>119</td>
</tr>
<tr>
<td>6.4</td>
<td>Reliability for Key Update Messages</td>
<td>121</td>
</tr>
<tr>
<td>6.5</td>
<td>Four Basic Techniques</td>
<td>123</td>
</tr>
</tbody>
</table>
6.5.1 Evolving Tree (ET) Protocol  
6.5.2 The Time-Structured Tree (TST) Protocol  
6.5.3 Entropy Injection Key Update (EIKU)  
6.5.4 Very-Important Bits (VIB)  

6.6 ELK: Efficient Large-Group Key Distribution  

6.7 Applications and Practical Issues  
6.7.1 Security Model  
6.7.2 System Requirements  
6.7.3 Parameters  
6.7.4 Advantages  
6.7.5 Comparison with Related Work  
6.7.6 Unicast Key Recovery Protocol  

6.8 Appendix  
6.8.1 Additional Cryptographic Primitives  
6.8.2 ET Detailed Description  
6.8.3 EIKU Detailed Description  

7. SENSOR NETWORK SECURITY  

7.1 Background  
7.1.1 Sensor Hardware  
7.1.2 Is Security on Sensors Possible?  

7.2 System Assumptions  
7.2.1 Communication Architecture  
7.2.2 Trust Requirements  
7.2.3 Design Guidelines  

7.3 Requirements for Sensor Network Security  
7.3.1 Data Confidentiality  
7.3.2 Data Authentication  
7.3.3 Data Freshness  

7.4 Additional Notation  

7.5 SNEP and $\mu$TESLA  
7.5.1 SNEP: Data Confidentiality, Authentication, and Freshness  
7.5.2 $\mu$TESLA: Authenticated Broadcast  

7.6 Implementation  
7.7 Evaluation  

7.8 Application of SNEP: Node-to-Node Key Agreement
Contents

8. RELATED WORK 175
   8.1 General Broadcast Security 175
   8.2 Broadcast Authentication 176
   8.3 Broadcast Signature 178
   8.4 Digital Signatures Based on One-way Functions without Trapdoors 179
   8.5 Small-Group Key Agreement 180
   8.6 Large-Group Key Distribution 181

9. CONCLUSION 185
   9.1 Open Problems 186

10. GLOSSARY 189

REFERENCES 193

INDEX 213