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

4.1.8 Security Considerations 62

4.2 The BiBa Broadcast Authentication Protocol 65

4.2.1 One-way Ball Chains 65

4.2.2 Security Condition 67

4.3 BiBa Broadcast Protocol Extensions 67

4.3.1 Extension A 68

4.3.2 Extension B 69

4.4 Practical Considerations 69

4.4.1 Selection of BiBa Parameters 70

4.4.2 BiBa Overhead 70

4.4.3 Example: Real-time stock quotes 70

4.4.4 Efficient Public-Key Distribution 73

4.5 Variations and Extensions 74

4.5.1 Randomized Verification to Prevent DoS 74

4.5.2 Multi-BiBa 74

4.5.3 The Powerball Extension 75

4.6 One-Round BiBa is as secure as Multi-Round BiBa 78

4.7 Merkle Hash Trees for Ball Authentication 81

5. EMSS, MESS, & HTSS: SIGNATURES FOR BROADCAST 85

5.1 Efficient Multicast Stream Signature (EMSS) 87

5.1.1 EMSS Summary and Security Argument 92

5.2 MESS 92

5.2.1 Analysis for Independent Packet Loss 94

5.2.2 Correlated Packet Loss 98

5.3 Variations 104

5.4 HTSS 106

5.4.1 HTSS Summary and Security Argument 110

6. ELK KEY DISTRIBUTION 111

6.1 Introduction 112

6.1.1 Requirements for Group Key Distribution 113

6.2 Review of the LKH Key Distribution Protocol 116

6.2.1 Extension I: Efficient Join (LKH+) 118

6.2.2 Extension II: Efficient Leave (LKH++) 119

6.3 Review of the OFT Key Distribution Protocol 119

6.4 Reliability for Key Update Messages 121

6.5 Four Basic Techniques 123

6.5.1 Evolving Tree (ET) Protocol 123
6.5.2 The Time-Structured Tree (TST) Protocol 125
6.5.3 Entropy Injection Key Update (EIKU) 125
6.5.4 Very-Important Bits (VIB) 128

6.6 ELK: Efficient Large-Group Key Distribution 130

6.7 Applications and Practical Issues 133
6.7.1 Security Model 133
6.7.2 System Requirements 134
6.7.3 Parameters 134
6.7.4 Advantages 135
6.7.5 Comparison with Related Work 136
6.7.6 Unicast Key Recovery Protocol 137

6.8 Appendix 138
6.8.1 Additional Cryptographic Primitives 138
6.8.2 ET Detailed Description 138
6.8.3 EIKU Detailed Description 140

7. SENSOR NETWORK SECURITY 149

7.1 Background 151
7.1.1 Sensor Hardware 151
7.1.2 Is Security on Sensors Possible? 152

7.2 System Assumptions 153
7.2.1 Communication Architecture 153
7.2.2 Trust Requirements 154
7.2.3 Design Guidelines 155

7.3 Requirements for Sensor Network Security 155
7.3.1 Data Confidentiality 155
7.3.2 Data Authentication 155
7.3.3 Data Freshness 156

7.4 Additional Notation 156

7.5 SNEP and μTESLA 157
7.5.1 SNEP: Data Confidentiality, Authentication, and Freshness 157
7.5.2 μTESLA: Authenticated Broadcast 161

7.6 Implementation 165

7.7 Evaluation 168

7.8 Application of SNEP: Node-to-Node Key Agreement 172

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