

# Contents

<b>Chapter 1. Home Automation Solutions for SecureWSN</b> . . . . .	1
Corinna SCHMITT and Marvin WEBER	
1.1. Introduction . . . . .	2
1.2. Background. . . . .	4
1.2.1. SecureWSN . . . . .	4
1.2.2. Communication standards . . . . .	8
1.2.3. The monitor-analyse-plan-execute-knowledge model . . . . .	12
1.2.4. Hardware and libraries . . . . .	14
1.3. Design decisions . . . . .	15
1.3.1. Requirements . . . . .	16
1.3.2. HAIFA architecture. . . . .	18
1.3.3. WebMaDa integration . . . . .	29
1.4. Implementation . . . . .	30
1.4.1. CoMaDa integration . . . . .	30
1.4.2. HAIFA's ZigBee Gateway. . . . .	48
1.4.3. WebMaDa integration . . . . .	55
1.4.4. Uploading HA data to WebMaDa . . . . .	56
1.4.5. Sending HA messages from WebMaDa to CoMaDa . . . . .	59
1.4.6. WebMaDa's frontend. . . . .	62
1.5. Evaluation of HAIFA . . . . .	64
1.5.1. Actuator interoperability (R1) . . . . .	65
1.5.2. Rule-based automation (R2) . . . . .	65
1.5.3. Node hardware interoperability (R3) . . . . .	68
1.5.4. CoMaDa and WebMaDa management (R4) . . . . .	68
1.6. Summary and conclusions . . . . .	68
1.7. Acknowledgements . . . . .	69
1.8. References . . . . .	70

<b>Chapter 2. Smart Home Device Security: A Survey of Smart Home Authentication Methods with a Focus on Mutual Authentication and Key Management Practices</b> . . . . .	75
Robinson RAJU and Melody MOH	
2.1. Introduction . . . . .	75
2.2. Smart home – introduction and technologies . . . . .	77
2.2.1. Smart home – introduction . . . . .	77
2.2.2. Smart home devices – categories . . . . .	79
2.3. Smart home security. . . . .	80
2.3.1. Threats . . . . .	81
2.3.2. Vulnerabilities. . . . .	82
2.3.3. IoT communication protocols . . . . .	84
2.3.4. Enhancements to IoT communication protocols . . . . .	86
2.3.5. IoT security architectures . . . . .	87
2.4. Smart home authentication mechanisms. . . . .	91
2.4.1. Stages of defining an authentication protocol for IoT . . . . .	92
2.4.2. Taxonomy of authentication schemes for IoT . . . . .	93
2.5. A primer on mutual authentication and key management terminologies . . . . .	96
2.5.1. X.509 certificate . . . . .	97
2.5.2. CoAP and DTLS . . . . .	99
2.5.3. TLS 1.3 . . . . .	101
2.5.4. Key management fundamentals . . . . .	102
2.6. Mutual authentication in smart home systems. . . . .	104
2.6.1. Device and user onboarding . . . . .	105
2.6.2. Flow of user authentication and authorization . . . . .	106
2.6.3. Examples of mutual authentication schemes . . . . .	107
2.7. Challenges and open research issues . . . . .	112
2.8. Conclusion . . . . .	113
2.9. References . . . . .	114
<b>Chapter 3. SRAM Physically Unclonable Functions for Smart Home IoT Telehealth Environments</b> . . . . .	125
Fayez GEBALI and Mohammad MAMUN	
3.1. Introduction . . . . .	126
3.2. Related literature. . . . .	129
3.3. System design considerations. . . . .	130
3.4. Silicon physically unclonable functions (PUF) . . . . .	131
3.4.1. Mutual authentication and key exchange using PUF . . . . .	132
3.4.2. Fuzzy extractor . . . . .	133
3.5. Convolutional encoding and Viterbi decoding the SRAM words . . . . .	133
3.6. CMOS SRAM PUF construction. . . . .	136

3.6.1. SRAM PUF statistical model . . . . .	138
3.6.2. Extracting the SRAM cell statistical parameters . . . . .	141
3.6.3. Obtaining the golden SRAM PUF memory content . . . . .	142
3.6.4. Bit error rate (BER) . . . . .	142
3.6.5. Signal-to-noise ratio (SNR) for SRAM PUF . . . . .	143
3.7. Algorithms for issuing CRP. . . . .	144
3.7.1. Algorithm #1: single-challenge . . . . .	144
3.7.2. Algorithm #2: repeated challenge . . . . .	147
3.7.3. Algorithm #3: repeated challenge with bit selection . . . . .	148
3.8. Security of PUF-based IoT devices . . . . .	150
3.9. Conclusions . . . . .	151
3.10. Acknowledgements . . . . .	151
3.11. References . . . . .	151
<b>Chapter 4. IoT Network Security in Smart Homes . . . . .</b>	<b>155</b>
Manju LATA and Vikas KUMAR	
4.1. Introduction . . . . .	156
4.2. IoT and smart home security . . . . .	159
4.3. IoT network security. . . . .	164
4.4. Prevailing standards and initiatives . . . . .	169
4.5. Conclusion . . . . .	172
4.6. References . . . . .	172
<b>Chapter 5. IoT in a New Age of Unified and Zero-Trust Networks and Increased Privacy Protection. . . . .</b>	<b>177</b>
Sava ZXIVANOVICH, Branislav TODOROVIC, Jean Pierre LORRÉ, Darko TRIFUNOVIC, Adrian KOTELBA, Ramin SADRE and Axel LEGAY	
5.1. Introduction . . . . .	178
5.2. Internet of Things . . . . .	179
5.3. IoT security and privacy challenges . . . . .	182
5.3.1. Security challenges . . . . .	183
5.3.2. Privacy challenges . . . . .	184
5.4. Literature review. . . . .	187
5.5. Security and privacy protection with a zero-trust approach . . . . .	190
5.6. Case study: secure and private interactive intelligent conversational . . . . .	193
5.6.1. LinTO technical characteristics . . . . .	194
5.6.2. Use case . . . . .	195
5.6.3. Use case mapping on the reference architecture . . . . .	197
5.7. Discussion . . . . .	197
5.8. Conclusion . . . . .	198
5.9. Acknowledgements . . . . .	199
5.10. References . . . . .	199

---

<b>Chapter 6. IOT, Deep Learning and Cybersecurity in Smart Homes: A Survey</b> . . . . .	203
Mirna ATIEH, Omar MOHAMMAD, Ali SABRA and Nehme RMAYTI	
6.1. Introduction . . . . .	203
6.2. Problems encountered . . . . .	205
6.3. State of the art . . . . .	207
6.3.1. IoT overview . . . . .	207
6.3.2. History . . . . .	208
6.3.3. Literature review . . . . .	208
6.3.4. Advantages, disadvantages and challenges . . . . .	209
6.4. IoT architecture . . . . .	212
6.4.1. Sensing layer . . . . .	213
6.4.2. Network layer . . . . .	213
6.4.3. Service layer . . . . .	213
6.4.4. Application–interface layer . . . . .	213
6.5. IoT security . . . . .	214
6.5.1. Security in the sensing layer . . . . .	214
6.5.2. Security in the network layer . . . . .	215
6.5.3. Security in the service layer . . . . .	215
6.5.4. Security in the application–interface layer . . . . .	216
6.5.5. Cross-layer threats . . . . .	216
6.5.6. Security attacks . . . . .	216
6.5.7. Security requirements in IOT . . . . .	218
6.5.8. Security solutions for IOT . . . . .	219
6.6. Artificial intelligence, machine learning and deep learning . . . . .	221
6.6.1. Artificial intelligence . . . . .	222
6.6.2. Machine learning . . . . .	222
6.6.3. Deep learning . . . . .	224
6.6.4. Deep learning vs. machine learning . . . . .	225
6.7. Smart homes . . . . .	227
6.7.1. Human activity recognition in smart homes . . . . .	227
6.7.2. Neural network algorithm for human activity recognition . . . . .	228
6.7.3. Deep neural networks used in human activity recognition . . . . .	230
6.8. Anomaly detection in smart homes . . . . .	233
6.8.1. What are anomalies? . . . . .	233
6.8.2. Types of anomaly . . . . .	233
6.8.3. Categories of anomaly detection techniques . . . . .	233
6.8.4. Related work of anomaly detection in smart homes . . . . .	234
6.9. Conclusion . . . . .	237
6.10. References . . . . .	238

---

<b>Chapter 7. sTiki: A Mutual Authentication Protocol for Constrained Sensor Devices</b> . . . . .	245
Corinna SCHMITT, Severin STIFFERT and Burkhard STILLER	
7.1. Introduction . . . . .	246
7.2. Definitions and history of IoT . . . . .	248
7.3. IoT-related security concerns . . . . .	251
7.3.1. Security analysis guidelines . . . . .	253
7.3.2. Security analysis by threat models . . . . .	255
7.3.3. sTiki’s security expectations . . . . .	256
7.4. Background knowledge for sTiki. . . . .	258
7.4.1. Application dependencies for sTiki . . . . .	258
7.4.2. Inspiring resource-efficient security protocols . . . . .	260
7.5. The sTiki protocol . . . . .	264
7.5.1. Design decisions taken . . . . .	266
7.5.2. Implementation of sTiki’s components . . . . .	267
7.6. sTiki’s evaluation . . . . .	270
7.6.1. Secured communication between aggregator and server . . . . .	271
7.6.2. Secured communication between collector and aggregator . . . . .	275
7.6.3. Communication costs . . . . .	276
7.6.4. Integration into an existing system . . . . .	277
7.6.5. Comparison to existing approaches . . . . .	278
7.7. Summary and conclusions . . . . .	279
7.8. Acknowledgements . . . . .	280
7.9. References . . . . .	281
<b>List of Authors</b> . . . . .	287
<b>Index</b> . . . . .	289