Table des matières

Chapitre 1. Solution domotique pour SecureWSN 1
Corinna SCHMITT et Marvin WEBER

1.1. Introduction. 2
1.2. Contexte. 4
1.2.1. SecureWSN 4
1.2.2. Normes de communication 9
1.2.3. Bluetooth à basse consommation. 11
1.2.4. Le modèle Monitor-Analyze-Plan-Execute-Knowledge 13
1.2.5. Matériel et bibliothèques. 16
1.3. Décisions de conception 17
1.3.1. Exigences. 17
1.3.2. Architecture d'HAIFA 20
1.3.3. Intégration WebMaDa 32
1.4. Implémentation 34
1.4.1. Intégration CoMaDa 34
1.4.2. Passerelle ZigBee de la HAIFA 52
1.4.3. Intégration WebMaDa 60
1.4.4. Transfert des données HA sur WebMaDa 61
1.4.5. Transmission de messages HA de WebMaDa à CoMaDa 64
1.4.6. Front-end WebMaDa. 68
1.5. Évaluation de HAIFA. 69
1.5.1. Interopérabilité des actionneurs (R1) 70
1.5.2. Automatisation basée sur des règles (R2). 70
1.5.3. Interopérabilité du matériel des nœuds (R3) 72
1.5.4. Gestion de CoMaDa et WebMaDa (R4) 73
1.6. Conclusion 74
1.7. Remerciements. 75
1.8. Bibliographie. 76

Chapitre 2. Sécurité des équipements pour maison connectée : authentification, authentification mutuelle et gestion de clés 81
Robinson RAJU et Melody MOH

2.1. Introduction 81
2.2. Maison connectée : introduction et technologie 83
2.2.1. Périmètre et définition 83
2.2.2. Équipements pour maison connectée : catégories 85
2.3. Cybersécurité de la maison connectée 87
2.3.1. Menaces 87
2.3.2. Vulnérabilités 89
2.3.3. Communication de protocoles IoT 91
2.3.4. Améliorations des protocoles de communication IoT 93
2.3.5. Architectures sécurisées pour l'IoT 94
2.4. Procédés d'authentification dans les maisons connectées 98
2.4.1. Étapes de l'élaboration d'un protocole d'authentification pour l'IoT 99
2.4.2. Taxonomie des procédés d'authentification pour l'IoT 100
2.5. Authentification mutuelle et terminologie de la gestion de clés 103
2.5.1. Certificat X.509 104
2.5.2. CoAP et DTLS 106
2.5.3. TLS 1.3 108
2.5.4. Fondamentaux de la gestion de clés 109
2.6. Authentification mutuelle dans les systèmes pour maison connectée . . 111
2.6.1. Déploiement d'appareils et d'utilisateurs 112
2.6.2. Cycle d'authentification et d'autorisation d'un utilisateur 113
2.6.3. Exemples de procédés d'authentification mutuelle 114
2.7. Défis et champs de recherche à explorer 119
2.8. Conclusion 120
2.9. Bibliographie 121

Chapitre 3. Authentification avancée par PUF en télémédecine . . 131
Fayez GEBALI et Mohammad MAMUN

3.1. Introduction 132
3.2. Littérature connexe 135
3.3. Considérations relatives à la conception système 137
3.4. Fonctions physiquement non clonables (PUF) sur silicium 138

3.4.1. Authentification mutuelle et échange de clés à l'aide de PUF . . . 139
3.4.2. Extracteur flou . . . 140
3.5. Codage convolutionnel et décodage de Viterbi des mots SRAM . . . 141
3.6. Construction de PUF sur SRAM CMOS . . . 143
3.6.1. Modèle statistique de la PUF SRAM . . . 145
3.6.2. Extraction des paramètres statistiques de la cellule SRAM . . . 148
3.6.3. Obtention du contenu de la mémoire de la PUF SRAM dorée . . . 149
3.6.4. Taux d'erreur binaire (BER) . . . 150
3.6.5. Rapport signal/bruit (SNR) pour la PUF SRAM . . . 150
3.7. Algorithmes d'émission de CRP . . . 151
3.7.1. Algorithme #1 : défi unique . . . 151
3.7.2. Algorithme #2 : défi répété . . . 155
3.7.3. Algorithme #3 : défi répété avec sélection de bits . . . 156
3.8. Sécurité des dispositifs IoT basés sur PUF . . . 157
3.9. Conclusion . . . 158
3.10. Remerciements . . . 158
3.11. Bibliographie . . . 159

Chapitre 4. La sécurité des réseaux IdO dans la maison connectée . . . 163
Manju LATA et Vikas KUMAR

4.1. Introduction . . . 164
4.2. IdO et sécurité de la maison connectée . . . 167
4.3. Sécurité des réseaux IdO . . . 172
4.4. Normes et initiatives actuelles . . . 177
4.5. Conclusion . . . 180
4.6. Bibliographie . . . 180

Chapitre 5. L'IdO pour une nouvelle ère de réseaux unifiés, de confiance zéro et de protection accrue de la vie privée . . . 185
Sava ZXIVANOVICH, Branislav TODOROVIC, Jean-Pierre LORRÉ, Darko TRIFUNOVIC, Adrian KOTELBA, Ramin SADRE et Axel LEGAY

5.1. Introduction . . . 186
5.2. Internet des objets . . . 188
5.3. Défis de la sécurité et de la confidentialité de l'IdO . . . 192
5.3.1. Défis de la sécurité . . . 192
5.3.2. Défis de la protection de la vie privée . . . 194

5.4. Analyse de la littérature 197
5.5. Sécurité et protection de la confidentialité avec une approche confiance zéro 201
5.6. Étude de cas : systèmes conversationnels interactifs intelligents sécurisés et privés 204
5.6.1. Caractéristiques techniques LinTO. 206
5.6.2. Cas d'utilisation 207
5.6.3. Mappage des cas d'utilisation sur l'architecture de référence . . . 208
5.7. Discussion 209
5.8. Conclusion 210
5.9. Remerciements. 210
5.10. Bibliographie 211

Chapitre 6. IdO, apprentissage profond et cybersécurité dans la maison connectée : une étude 215
Mirna ATIEH, Omar MOHAMMAD, Ali SABRA et Nehme RMAYTI

6.1. Introduction. 215
6.2. Problèmes rencontrés 217
6.3. État de l'art 219
6.3.1. IdO, vue d'ensemble 219
6.3.2. Historique 220
6.3.3. Analyse documentaire 220
6.3.4. Atouts, inconvénients et problématiques 221
6.4. Architecture IdO 224
6.4.1. Couche sensorielle 225
6.4.2. Couche réseau 225
6.4.3. Couche service 225
6.4.4. Couche application-interface 225
6.5. Sécurité de l'IdO. 226
6.5.1. Sécurité de la couche sensorielle 226
6.5.2. Sécurité de la couche réseau. 227
6.5.3. Sécurité de la couche service 227
6.5.4. Sécurité de la couche application-interface 228
6.5.5. Menaces à travers plusieurs couches. 228
6.5.6. Attaques de sécurité 229
6.5.7. Exigences de sécurité dans l'IdO 229
6.5.8. Solutions de sécurité pour l'IdO 230

6.6. Intelligence artificielle, apprentissage automatique et apprentissage profond 232
6.6.1. Intelligence artificielle 233
6.6.2. Apprentissage automatique 234
6.6.3. Apprentissage profond 236
6.6.4. Apprentissage profond contre apprentissage automatique 238
6.7. Maisons connectées 239
6.7.1. Reconnaissance d'activités humaines dans la maison connectée . . 239
6.7.2. Algorithme pour réseau de neurones pour la reconnaissance d'activités humaines. 240
6.7.3. Réseaux de neurones profonds utilisés pour la reconnaissance d'activités humaines. 243
6.8. Détection d'anomalies dans la maison connectée 245
6.8.1. Définir les anomalies 245
6.8.2. Types d'anomalies 245
6.8.3. Catégories de techniques de détection d'anomalies 246
6.8.4. Travaux de recherche pour la détection d'anomalies 246
6.9. Conclusion 249
6.10. Bibliographie 250

Chapitre 7. sTiki : un protocole d'authentification mutuelle pour les dispositifs de détection contraints 257
Corinna SCHMITT, Severin SIFFERT et Burkhard STILLER

7.1. Introduction. 258
7.2. Définitions et histoire de l'IdO 260
7.3. Problèmes de sécurité liés à l'IdO 263
7.3.1. Lignes directrices pour l'analyse de sécurité 266
7.3.2. Analyse de sécurité par modèles de menaces. 268
7.3.3. Perspective de sTiki en matière de sécurité. 270
7.4. Connaissances de base pour sTiki. 271
7.4.1. Dépendances d'application pour sTiki. 272
7.4.2. Favoriser des protocoles de sécurité économes en ressources . . . 274
7.5. Le protocole sTiki 278
7.5.1. Décisions prises en matière de conception 280
7.5.2. Implémentation des composants de sTiki 281
7.6. Évaluation de sTiki 285

7.6.1. Communication sécurisée entre agrégateur et serveur 286
7.6.2. Communication sécurisée entre collecteur et agrégateur 289
7.6.3. Coûts de communication. 291
7.6.4. Intégration dans un système existant. 292
7.6.5. Comparaison avec les approches existantes 293
7.7. Conclusion 295
7.8. Remerciements. 296
7.9. Bibliographie 296

Liste des auteurs. 301

Index 303