
Contents

Preface	xiii
1 A security survey of middleware for the Internet of Things	1
<i>Paul Fremantle</i>	
Summary	1
1.1 Introduction	1
1.2 Approach	2
1.2.1 Cell A: confidentiality/hardware	4
1.2.2 Cell B: confidentiality/network	4
1.2.3 Cell C: confidentiality and cloud/server	6
1.2.4 Cell D: integrity and hardware/device	6
1.2.5 Cell E: integrity and network	7
1.2.6 Cell F: integrity and cloud/server	7
1.2.7 Cell G: availability and device/hardware	7
1.2.8 Cell H: availability and network	8
1.2.9 Cell I: availability and cloud/server	8
1.2.10 Cell J: authentication and device/hardware	8
1.2.11 Cell K: authentication and network	8
1.2.12 Cell L: authentication and cloud/server	9
1.2.13 Cell M: access control and device/hardware	10
1.2.14 Cell N: access control and network	10
1.2.15 Cell O: access control and cloud/server	10
1.2.16 Cell P: non-repudiation and device/hardware	11
1.2.17 Cell Q: non-repudiation and network	11
1.2.18 Cell R: non-repudiation and cloud/server	11
1.2.19 Summary of the review of security issues	11
1.3 Secure middleware for the IoT	13
1.3.1 Introduction	13
1.3.2 Review methodology	13
1.3.3 ASPIRE	15
1.3.4 UBIWARE	15
1.3.5 UBIROAD	15
1.3.6 UBISOAP	15
1.3.7 SMEPP	15
1.3.8 SOCRADES	16
1.3.9 SIRENA	16

1.3.10	WHEREX	16
1.3.11	WEBINOS	16
1.3.12	GSN	17
1.3.13	MOSDEN	17
1.3.14	Thingsonomy	17
1.3.15	OpenIoT	18
1.3.16	Diopbase	18
1.3.17	VIRTUS	18
1.3.18	Hydra/LinkSmart	18
1.3.19	EDSOA	19
1.3.20	DREMS	19
1.3.21	XMPP	20
1.3.22	Cloud-based car parking middleware	20
1.3.23	NAPS	20
1.3.24	SBIOTCM	20
1.4	Summary of IoT middleware security	20
1.4.1	Overall gaps in the middleware	21
1.5	Discussion	22
1.5.1	Contributions	22
1.5.2	Further work	22
	References	23
2	Privacy in the Internet of Things	33
	<i>Santiago Suppan and Jorge Cuéllar</i>	
	Summary	33
2.1	Introduction	33
2.2	Related work	35
2.3	The challenges and consequences of privacy breaches	35
2.4	Privacy principles and engineering for the IoT	37
2.4.1	The European Data Protection Rules	38
2.4.2	Privacy by Design	39
2.4.3	PRIPARE	40
2.5	A privacy development life cycle	41
2.5.1	Education of system developers	41
2.5.2	Phase 1 – purpose definition and data minimization	42
2.5.3	Phase 2 – threats and risks evaluation	42
2.5.4	Phase 3 – design	43
2.5.5	Phase 4 – implementation	45
2.5.6	Phase 5 – verification	45
2.5.7	Phase 6 – release of system and education of stakeholders	45
2.5.8	Phase 7 – response	46
2.6	PETs for the IoT	47
2.6.1	Privacy Dashboard	47
2.6.2	Consent management	47

2.6.3	Support of user defined policies	48
2.6.4	Privacy-enhanced authentication and authorization	49
2.6.5	Pseudonym management systems	49
2.6.6	Location privacy	49
2.6.7	PETs for constrained environments in IoT	49
2.6.8	Trust in IoT	51
2.7	Discussion	52
	Acknowledgements	52
	References	52
3	Privacy and consumer IoT: a sensemaking perspective	57
	<i>Gaurav Gupta</i>	
	Summary	57
3.1	Introduction	57
3.2	Consumer IoT and novel privacy concerns	58
3.3	IoT-induced change in information architecture of consumer devices	60
3.4	Sensemaking of information privacy and IoT	63
3.5	Integration of information privacy needs and concerns in IoT	67
3.5.1	User's privacy concerns and perceived control of information	68
3.5.2	Provider's information assertion and perceived control of information	68
3.5.3	Legislative framework and perceived control of information	69
3.5.4	Perceived control of information and intention to use	69
3.6	Discussion	70
	References	71
4	SMARTIE: a secure platform for Smart Cities and IoT	75
	<i>José L. Hernández-Ramos, Dan García Carrillo, Antonio Skarmeta, Fábio Gonçalves, Luis Cortesão, Jens-Matthias Bohli, and Martin Bauer</i>	
	Summary	75
4.1	Introduction	75
4.2	Related work	77
4.3	IoT-A Architecture Reference Model	78
4.4	SMARTIE architecture	80
4.4.1	Functional view	80
4.4.2	Application Functional Group	80
4.4.3	Management Functional Group	82
4.4.4	Service Organization Functional Group	82
4.4.5	Virtual Entity Functional Group	83
4.4.6	IoT Service Functional Group	84

4.4.7	Security Functional Group	86
4.4.8	Communication Functional Group	88
4.4.9	Architecture configurations	89
4.5	SMARTIE scenarios for IoT-enabled smart cities	92
4.5.1	Smart energy management	92
4.5.2	Public transport scenario	93
4.5.3	Traffic management scenario	94
4.5.4	City information centre scenario	94
4.6	Discussion	95
	Acknowledgements	95
	References	96
5	Model-based security engineering for the Internet of Things	99
	<i>Ricardo Neisse, Gary Steri, Igor Nai Fovino, Gianmarco Baldini, and Lodewijk van Hoesel</i>	
	Summary	99
5.1	Introduction	99
5.2	Related work	101
5.3	IoT framework	103
5.4	Methodology for security engineering in IoT	104
5.4.1	Structure and behavior models	105
5.4.2	Data and identities	108
5.4.3	Business roles	109
5.4.4	Context information and situations	110
5.4.5	Risk analysis	110
5.4.6	Trust relationships	111
5.4.7	Security policy rules	113
5.5	Smart business case study: Cold Chain Monitoring	117
5.5.1	Overview and motivation	117
5.5.2	Hardware components	118
5.5.3	IoT framework components	120
5.5.4	Information sharing and data confidentiality	122
5.6	Security engineering for smart business case study	122
5.7	Discussion	126
	References	126
6	Federated Identity and Access Management in IoT systems	131
	<i>Paul Fremantle</i>	
	Summary	131
6.1	Introduction	131
6.1.1	Security and privacy in IoT	131
6.1.2	Motivation for Federated Identity and Access Management in IoT	132

6.1.3	Web API Management	133
6.1.4	Research questions and contributions	133
6.1.5	Outline of the chapter	134
6.2	Related work	134
6.2.1	IoT security	134
6.2.2	Web API Management	135
6.3	FIAM for IoT	136
6.3.1	OAuth	136
6.3.2	MQTT	137
6.3.3	FIOT implementation	138
6.3.4	Results of the FIOT system	144
6.3.5	Conclusions of the first phase	147
6.4	Further exploration of FIAM and IoT, especially with regard to API Management	148
6.4.1	IGNITE – an API gateway for IoT protocols	149
6.5	Results	150
6.6	Discussion	153
6.6.1	Further research topics	153
	References	154
7	On the security of the MQTT protocol	159
	<i>Benjamin Aziz</i>	
	Summary	159
7.1	Introduction	159
7.1.1	The MQTT protocol	160
7.1.2	Chapter contributions	161
7.1.3	Chapter structure	162
7.2	Related work	162
7.3	TPi: a timed process algebra	163
7.4	A model of the MQTT protocol	164
7.4.1	The subscribers	165
7.4.2	The passive attacker	166
7.5	Analysis of the protocol	166
7.5.1	QoS = 0 protocol	166
7.5.2	QoS = 1 protocol	167
7.5.3	QoS = 2 protocol	169
7.6	Client/server timed input failures	171
7.6.1	The case of QoS = 0	172
7.6.2	The case of QoS = 1	172
7.6.3	The case of QoS = 2	173
7.7	Discussion	174
	References	175

8 Securing communications among severely constrained, wireless embedded devices 179

Alexandros Fragkiadakis, George Oikonomou, Henrich C. Pöhls, Elias Z. Tragos, and Marcin Wójcik

Summary	179
8.1 Introduction	179
8.2 Related work	181
8.3 Secure communications for the IoT	182
8.4 Digital investigations for the IoT	185
8.5 CS encryption	188
8.5.1 Computational secrecy of CS	189
8.5.2 Information theoretic secrecy of CS	189
8.6 Digital signatures	191
8.6.1 Goals of integrity protection and origin authentication	192
8.6.2 Technical challenges and solutions for integrity and origin authentication in the IoT	193
8.6.3 Summary: end-to-end integrity and authenticity based on ECC	196
8.7 Datagram Transport Layer Security	196
8.7.1 DTLS protocol for IoT	197
8.7.2 Summary	199
8.8 Discussion	199
References	200

9 Lightweight cryptographic identity solutions for the Internet of Things 207

Chongyan Gu, Neil Hanley, and Máire O'Neill

Summary	207
9.1 Introduction	207
9.2 Related work	209
9.2.1 Weak PUFs	210
9.2.2 Strong PUFs	210
9.2.3 Evaluation metrics	211
9.2.4 Attack scenarios	212
9.2.5 Protocol level options	213
9.2.6 Error correction	214
9.3 Evaluation of an identity-based PUF for IoT applications	214
9.3.1 FPGA-based PUF identifier	214
9.4 Discussion	223
References	224

10 A reputation model for the Internet of Things	229
<i>Benjamin Aziz, Paul Fremantle, and Alvaro Arenas</i>	
Summary	229
10.1 Introduction	229
10.2 Overview of the concept of reputation	230
10.3 MQTT	232
10.4 A reputation model for MQTT	232
10.4.1 Monitoring events	232
10.4.2 Reputation models	234
10.5 A reputation system architecture for MQTT	239
10.6 Simulation of the model	240
10.6.1 Results	240
10.6.2 Reputation results	241
10.7 Related work	241
10.8 Discussion	242
References	243
Index	247