

Contents

Editorial: Trustworthy Ubiquitous Computing	v
Part I Trust and Context in UbiComp Environments	1
1. The automatic Trust Management of self-adaptive Multi-Display Environments	3
<i>K. Bee, S. Hammer, Ch. Pratsch, and E. André</i>	
1.1 Introduction	3
1.2 Scenario	5
1.3 Trust in Ubiquitous Display Environments	6
1.4 Dimensions of Trust	7
1.5 Empirical Validation of Trust Dimensions and User Feelings	8
1.5.1 Experimental Setting	9
1.5.2 Conducting the Experiment	11
1.5.3 Results and Discussion	11
1.6 Towards an Automatic Trust Management System	12
1.6.1 Using Bayesian Networks to Model Trust	13
1.6.2 Monitoring Trust over Time	15
1.6.3 Maintaining User Trust	17
1.7 Conclusion	18
1.8 Acknowledgement	19
Bibliography	19

2. Malicious Pixels – Using QR Codes as Attack Vector 21

*P. Kieseberg, S. Schrittwieser, M. Leithner, M. Mulazzani, E. Weippl,
L. Munroe, M. Sinha*

2.1	Introduction	21
2.2	Background	22
2.2.1	QR codes	23
2.2.2	Capacity and Error correction code	24
2.3	Security of QR Codes	25
2.3.1	Threat Model	25
2.3.2	Attacking different parts	26
2.4	QR Codes as Attack Vectors	31
2.4.1	Attacking Automated Processes	31
2.4.2	Attacking Human Interaction	32
2.5	Proof-of-Concept Attack	33
2.5.1	Outline of the Attack	33
2.5.2	Practical application details	35
2.5.3	Example	36
2.6	Future research	36
2.7	Conclusion	37
	Bibliography	38

3. A Virtual Performance Stage as a Space for Children to Create and Perform Stories 39

W.A. Widjajanto, H. Schelhowe, and M. Lund

3.1	Introduction	39
3.2	Storytelling, Technology and Children	40
3.3	Methods	43
3.3.1	Wayang Performance Workshops with Children	44
3.3.2	Wayang Authoring Development	44
3.3.3	Prototype Evaluation	49
3.4	Results and Discussion	51
3.4.1	Ability to Compose a Story	51
3.4.2	Story Structure	55

3.4.3	Intercultural Aspect	56
3.4.4	Interaction between children and the authoring system	57
3.5	Conclusions	59
	Bibliography	60

Part II Methods and Concepts to Enhance and Ensure Reliability in Ubicomp Environments 63

4. Network Forensics: Detection and Mitigation of Botnet and Malicious Code via Darknet 65

R. Azrina, R. Othman, Normaziah A. Aziz, M. ZulHazmi, M. Khazin, J. Dewakunjari

4.1	Introduction	65
4.2	Background	66
4.3	Motivation and Related Works	67
4.4	Our Approach and Implementation	68
4.5	Experimental Results and Analysis	70
4.5.1	Further Analysis on Destination Port 445 Traffic	71
4.5.2	Further Analysis on ICMP traffic	72
4.5.3	Analysis of Suspected Client	73
4.6	Future Work	76
4.7	Concluding Remarks	76
	Bibliography	77

5. Trusted Log Management System 79

A. Tomono, M. Uehara, and Y. Shimada

5.1	Introduction	79
5.2	Related Techniques	81
5.2.1	ILM	81
5.2.2	Digital Forensics	81
5.2.3	Syslog and its Enhancements	82
5.2.4	Secure Logging on a PC	83
5.2.5	VLSD	83

5.2.6	Security of the VLSD	85
5.3	Design of a Log Management System	86
5.3.1	System Overview	86
5.3.2	Collection and Management	89
5.3.3	Reference and Search	89
5.4	Guaranteeing Logs in a Network	90
5.5	New CSV	92
5.6	Evaluation	95
5.6.1	Collection of Logs	95
5.6.2	Construction of Storage for Logs	96
5.6.3	Guaranteeing the Logs	96
5.7	Conclusion	97
	Bibliography	98
6.	Reasoning of Collaborative Human Behaviour in Security-Critical	
	Work Practices: A Framework	99
	<i>G.S. Poh, N.N. Abdullah, M.R. Z'aba, and M.R. Wahiddin</i>	
6.1	Introduction	99
6.1.1	Related Works	100
6.1.2	Our Contribution	101
6.2	Security Goals	101
6.2.1	Confidentiality	102
6.2.2	Data Integrity	102
6.2.3	Authentication	102
6.2.4	Non-repudiation	102
6.2.5	Availability	102
6.3	Human Behaviour Security Framework	102
6.3.1	Model	103
6.3.2	Process	104
6.4	Modeling Tools	104
6.4.1	Work Practice Analysis	105
6.4.2	Formal model of the work practice	105
6.4.3	Simulation	105
6.4.4	Observing the simulation	105

6.5	Practical Scenario	105
6.6	Conclusion	105
	Bibliography	106

Part III Distributed Attacks Detection and Secure Access Protocol in MANET, WSN and UbiComp Environments 107

7. Mitigation of Wormhole Attack in Wireless Sensor Networks 109

A. Modirkhazeni, M. Kadhum, and T. Mantoro

7.1	Introduction	109
7.2	Wireless Sensor Network; Concepts and Applications	110
7.2.1	Applications of Wireless Sensor Networks	110
7.2.2	Sensor Device Architecture	111
7.2.3	Routing in Wireless Sensor Networks	112
7.3	Security Issues in Wireless Sensor Network	114
7.3.1	Basic Security Requirements in Wireless Sensor Network	114
7.3.2	Routing Attacks in Wireless Sensor Networks	116
7.3.3	Cryptographic Approaches in Wireless Sensor Networks	117
7.3.4	Key Management Approaches in Wireless Sensor Network	118
7.4	Wormhole Attack in Wireless Sensor Networks	121
7.4.1	Classification of Wormhole Attack	121
7.4.2	Wormhole Attack Countermeasures in Wireless Sensor Network	123
7.4.3	WSN Wormhole Attack Countermeasures; Analysis and Comparison	130
7.5	Proposed Neighbor Discovery Approach	134
7.5.1	System Assumptions	135
7.5.2	Definition	135
7.6	Simulation	138
7.7	Results	139
7.7.1	Effect of Wormhole Attack on Original Hierarchal Protocol	139
7.7.2	Effect of Wormhole Attack on the Enhanced Protocol	141
7.7.3	Mitigation of Wormhole Attack through the Enhanced Protocol	142
7.8	Conclusion and Future Works	143

Bibliography	144
8. Protocol for Secure Access in Mobile Ad-hoc Network for Emergency Services	149
<i>A. Abu Bakar, R. Ismail, A.R. Ahmad, J.-I. Abdul Manan</i>	
8.1 Introduction	149
8.2 MANET at Emergency Rescue Mission	151
8.3 Group Based Access Control (GBAC) model	152
8.3.1 Components in GBAC model	153
8.4 Delegation protocol	164
8.4.1 Delegation protocol using Proxy Signature scheme	165
8.5 Conclusions	170
Bibliography	171

Part IV Access Control and Mobile Payment in Trustworthy UbiComp Environment **175**

9. A Lightweight Graph-Based Pattern Recognition Scheme in Mobile Ad Hoc Networks	177
<i>R.A. Raja Mahmood, A.H. Muhamad Amin, A. Amir, A.I. Khan</i>	
9.1 Introduction	177
9.2 MANETs Security Threats	178
9.2.1 Attacks in MANETs	179
9.2.2 Wormhole Attack	180
9.2.3 Black hole or Packet Drop or Sequence Number Attack	181
9.2.4 Routing Disruption Attack	182
9.2.5 Flooding or Resource Consumption Attack	182
9.2.6 Dropping Routing Traffic Attack	182
9.3 Intrusion Detection System in MANETs	183
9.3.1 Intrusion Detection System Architectures	184
9.3.2 Intrusion Detection Decision Making	184
9.3.3 Existing Intrusion Detection System Solutions	185
9.3.4 Intrusion Detection Schemes	186

9.4	Distributed Hierarchical Graph Neuron	188
9.4.1	Graph Neuron Theory	188
9.4.2	Hierarchical Graph Neuron	190
9.4.3	Distributed Hierarchical Graph Neuron	192
9.5	Three-Stage Cooperative Intrusion Detection System using DHGN	194
9.5.1	Three-Stage Attack Recognition Process	195
9.5.2	Challenges in Implementing DHGN in DDoS Detection	197
9.6	Experiments	198
9.6.1	Test1: Distorted images of distinct characters I, A, F and X	199
9.6.2	Test2: Distorted images of low-percentage similar characters S, F and J	199
9.6.3	Test3: Distorted images of high-percentage similar characters I, T and Z	200
9.7	Result and Discussion	200
9.7.1	Classification Accuracy of Distinct Patterns	200
9.7.2	Classification Accuracy of Low Similarity Patterns	201
9.7.3	Classification Accuracy of High Similarity Patterns	201
9.7.4	Summary	202
9.8	Conclusion	203
	Bibliography	204
10.	Security Framework for Mobile Banking	207
	<i>D. Weerasinghe, V. Rakocevic, and M. Rajarajan</i>	
10.1	Introduction	207
10.2	Mobile Banking	208
10.3	Architecture	211
10.4	Security Protocol Design	213
10.4.1	Registration	215
10.4.2	Authentication	216
10.4.3	Authorization	217
10.5	Security Tokens and Data Key generation	218
10.5.1	Security Token Design	219
10.5.2	Data Key generation	221
10.5.3	Execution Challenge Response generation	221

10.6	Conclusion & Discussions	222
	Bibliography	224
11.	Anonymous, Secure and Fair Micropayment System to Access Location-Based Services	227
	<i>Isern-Deyà, Payeras-Capellà, Mut-Puigserver and Ferrer-Gomila</i>	
11.1	Introduction	227
11.2	Micropayment Schemes Overview	228
11.3	Related Work	229
11.4	Location-Based Services	230
	11.4.1 Payment Methods to Access LBS	231
11.5	LBS Access Protocol Description	232
	11.5.1 Initial Considerations	233
	11.5.2 Bank Account Setup	234
	11.5.3 Services List	234
	11.5.4 Withdrawal	235
	11.5.5 Transfer	236
	11.5.6 Deposit	240
	11.5.7 Refund	241
11.6	Informal Analysis of Properties	241
	11.6.1 Analysis of Security Properties	241
	11.6.2 Analysis of Efficiency	244
11.7	Conclusions	245
	Bibliography	246
12.	Privacy Preserving with A Purpose-based Privacy Data Graph	249
	<i>Y. Tian, B. Song, and E.-N. Huh</i>	
12.1	Introduction	249
12.2	Background	251
	12.2.1 Privacy Principles & Policies	251
	12.2.2 RBAC	252
	12.2.3 User Privacy Preference	253
	12.2.4 Purpose	254

12.3	Proposed System	254
12.3.1	Basic Concepts	255
12.3.2	System Design Phase	257
12.3.3	Role Level Design Phase	258
12.3.4	Transforming Phase	258
12.3.5	Personal Level Design Phase	260
12.4	Algorithms and Pseudo Code	260
12.4.1	Detection algorithm in role specification	261
12.4.2	Privacy Preference Conversion Algorithm	263
12.5	Comparison	263
12.5.1	Storage Space	263
12.5.2	Variety of Personal Privacy Policy	264
12.6	Conclusion	265
	Bibliography	265



<http://www.springer.com/978-94-91216-70-1>

Trustworthy Ubiquitous Computing

Khalil, I.; Mantoro, T. (Eds.)

2012, XX, 268 p., Hardcover

ISBN: 978-94-91216-70-1

A product of Atlantis Press