

Contents

1 Introduction and Motivations	1
1.1 Context and Research Motivations	1
1.2 Problem Statement and Research Outcomes	4
1.3 Thesis Outline	6
References	7

Part I Cyber-security

2 Digital Identity	11
2.1 Introduction	11
2.2 Identity: Yesterday and Today	12
2.3 Identity Perspectives: Multiple Facets of the Identity	13
2.4 Digital Identity: Definitions, Basics and Nomenclature	15
2.5 Digital Identity, Security and Trust	18
2.6 Digital Identity: Major Issues and Complexities	19
2.6.1 Mutation from One YOU to Multiple YOUs	19
2.6.2 Origins of Fragmented Identity	25
2.6.3 Digital Identity and Digital Memories	27
2.6.4 Digital Identity in Social Networks	29
2.6.5 Digital Identity, Context-Awareness, and Ubiquity	31
2.6.6 Frauds, Misuse, Fake Profile and Crimes of Identity	31
2.6.7 Digital Identity Aggregation Drivers and Issues	32
2.6.8 Digital Identity Aggregation for Security Use Cases	33
2.6.9 Economy of Digital Identity Aggregation: Digital Gold Mine	35
2.6.10 Technical Issues of Digital Identity Aggregation	38
2.6.11 Digital Identity Aggregation Systems and Algorithms	40
2.6.12 Digital Native's Perception of Identity	43
2.6.13 Issues and Concerns Associated with Handling the Digital Afterlife	44

- 2.6.14 Digital Identity, Online Reputation and Metadata 45
- 2.6.15 Digital Identity Issue with Cyborg Enhancement 46
- 2.6.16 Digital Identity in Big Data Era 46
- References 50
- 3 Digital Identity Management 57**
 - 3.1 Digital Identity Management: Basics 57
 - 3.2 Taxonomy of Digital Identity Management Definitions 58
 - 3.2.1 DigIdM Security System and Technical Definition-Focus . . . 58
 - 3.2.2 DigIdM Security Management Definition-Focus 59
 - 3.2.3 DigIdM User-Supremacy Definition-Focus 61
 - 3.3 From Vertical into Horizontal Management 61
 - 3.4 Digital Identity Management Technical Models 62
 - 3.4.1 DigIdM Centralization: Meta-directory Technical Model . . . 64
 - 3.4.2 DigIdM Centralization: Virtual-Directory Technical Model . . . 65
 - 3.4.3 DigIdM Federation Technical Model 66
 - 3.4.4 Comparing DigIdM Technical Models 69
 - 3.4.5 XRI and Social Web Technical Approach 71
 - 3.5 User-Centricity DigIdM Technical Models 74
 - 3.6 Making Less Visible Persistent Digital Identity 77
 - 3.6.1 Un-forgotten Digital Identity and Un-forgiven
Digital Society 77
 - 3.6.2 Digital Identity Persistence and Loss of Control 77
 - 3.6.3 Digital Identity Hiding and User Control 78
 - 3.6.4 Digital Renaissance of Metadata 79
 - 3.6.5 Metadata and Digital Identity Expiration Dates 80
 - 3.6.6 DigIdMeta and MetaEngine Tool 81
 - 3.6.7 Expiration Date Within Content-Centric Network 87
 - References 92
- 4 Privacy and Digital Identity 97**
 - 4.1 Privacy: Preliminaries 98
 - 4.2 Digital Identity Management and Privacy 100
 - 4.3 Digital Identity and Privacy Issues 101
 - 4.3.1 Digital Identity Attributes Disclosure 102
 - 4.3.2 Digital Identity Attributes Processing and Analysis 102
 - 4.3.3 Digital Identity Persistence and Visibility 103
 - 4.3.4 Loosely Coupled Collaborative IS, Digital Identity
and Privacy 105
 - 4.4 Privacy Policies 105
 - 4.4.1 Global Privacy Policies 106
 - 4.4.2 Domestic Privacy Policies 109
 - 4.4.3 Business-Specific Privacy Policies 113
 - 4.5 Digital Identity-Related Privacy Requirements 114
 - 4.5.1 Purpose Specification of Attributes Collection 114
 - 4.5.2 Consent for Attributes Usage/Release 115

- 4.5.3 Limited Usage of Attributes 115
- 4.5.4 Limited Retention of Attributes 115
- 4.5.5 Accuracy of Stored Attributes 115
- 4.5.6 Openness 116
- 4.5.7 Authentication and Enrollment Needs 116
- 4.5.8 Choice and Terms of the Contract 116
- 4.5.9 Secondary Use 116
- 4.5.10 Compliance. 117
- 4.5.11 Project-Specific Privacy Requirements 117
- References. 117

Part II Interoperability Through Service-Orientation

- 5 DigIdeRP Framework. 123**
 - 5.1 Privacy Implementations: Current Landscape 123
 - 5.2 Service-Oriented Architecture 124
 - 5.3 High-Level View Description of DigIdeRP Framework 126
 - 5.4 OMG Service-Oriented Modeling Language. 131
 - 5.5 Detailed View of SoaML-Based DigIdeRP Framework 133
 - 5.6 Service Design Approaches 135
 - 5.7 Business Process-Based Portray: DigIdeRP Processes 136
 - 5.8 Business Architecture. 138
 - 5.9 Service Identification and Specification. 139
 - 5.10 Service Consumption Roadmap. 143
 - 5.11 Component-Based Architecture 145
 - 5.12 Deployment Specification 146
 - References. 147
- 6 SOA-Artifacts-Level: Implementation of Privacy-as-a-Set-of-Services 149**
 - 6.1 SoaML Design Toolkit. 149
 - 6.2 SOA Artifacts Related to the Service Provider Participant 149
 - 6.3 SOA Artifacts Related to the Identity Provider Participant 150
 - 6.4 SOA Artifacts Related to the Subject Participant. 150
 - 6.5 SOA Artifacts Code Generation. 154
 - Reference. 162

Part III Conclusion and Outlook

- 7 Conclusion and Outlook 165**
 - 7.1 Main Contributions and Summary Conclusions 165
 - 7.2 Research Limits and Future Work 171

- 7.2.1 DigIdeRP Framework Limits and Opportunities
of Evolution 171
- 7.2.2 Service Design and Architecture Metrics. 172
- 7.2.3 PaaS System Deployment in Service-
Oriented Environments. 172
- 7.2.4 “Forgetting” Persistent Digital Identity and
Brain Informatics 173
- 7.2.5 Digital Identity and Privacy in Content-Centric
Internetworking 174
- 7.2.6 Digital Identity Management in Data Superabundant Era. . . 174
- References. 175
- About the Author. 177**



<http://www.springer.com/978-3-319-08230-1>

Architecting User-Centric Privacy-as-a-Set-of-Services
Digital Identity-Related Privacy Framework

Ben Ayed, G.

2014, XIX, 177 p. 47 illus., 4 illus. in color., Hardcover

ISBN: 978-3-319-08230-1