
Contents

Part I Introduction and Background

1	Introduction	3
2	Authorizations	9
3	An Architectural Model for Secure Authorizations	13
4	Traditional Security Objectives	27
5	Personal Data Protection Objectives	31
6	Technical Enforcement of Multilateral Security	43
7	Pseudonyms – A Technical Point of View	47
8	An Architectural Model for Pseudonymous Authorizations ..	55
9	Comparing Architectures	65
10	Audit Data Pseudonymization	77

Part II Set-based Approach

11	Requirements, Assumptions and Trust Model	91
----	---	----

VI Contents

12	Modeling Conditions for Technical Purpose Binding	97
13	Cryptographic Enforcement of Disclosure Conditions	103
14	The Mismatch Problem	109
15	Operational Pseudonymization and Pseudonym Disclosure ...	115
16	Extensions	123

Part III Application to Unix Audit Data

17	Unix Audit Data	137
18	<i>Syslog</i>	141
19	Instantiating the Set-based Approach for Syslog Audit Data .	147
20	Implementation: Pseudo/CoRe	159

Part IV Evaluation

21	APES: Anonymity and Privacy in Electronic Services	171
22	Evaluating the Design Using Basic Building Blocks	177
23	Evaluating the Performance of the Implementation	187

Part V Refinement of Misuse Scenario Models

24	Motivating Model Refinements	199
25	Models of Misuse Scenarios	203
26	Pseudonymization Based on Serial Signature-Nets	229
27	Pseudonym Linkability	233

28 Pseudonym Disclosure	247
Summary	283
A Threshold Schemes for Cryptographic Secret Sharing	285
References	287
Index	303



<http://www.springer.com/978-0-387-68254-9>

Privacy-Respecting Intrusion Detection

Flegel, U.

2007, XX, 307 p. 61 illus.,

ISBN: 978-0-387-68254-9