

Contents

I	Introduction and Background	1
1	Introduction	3
1.1	Scope	5
1.2	Contributions and Publications	8
1.3	Organization and Structure	9
2	Related Work on Secure Deletion	13
2.1	Introduction	13
2.2	Related Work	13
2.3	Adversarial Model	27
2.4	Analysis of Solutions	31
3	System Model and Security Goal	37
3.1	Introduction	37
3.2	System Model	37
3.3	Storage Media Models	38
3.4	Adversarial Model	41
3.5	Security Goal	42
II	Secure Deletion for Mobile Storage	49
4	Flash Memory: Background and Related Work	51
4.1	Overview	51
4.2	Flash Memory	52
4.3	Flash Secure Deletion Related Work	58
4.4	Summary.	61
5	User-Level Secure Deletion on Log-Structured File Systems	63
5.1	Introduction	63
5.2	System and Adversarial Model	64
5.3	YAFFS	64
5.4	Data Deletion in Existing Log-Structured File Systems	66
5.5	User-space Secure Deletion	70

Contents

5.6	Experimental Evaluation	75
5.7	Summary	81
6	Data Node Encrypted File System	83
6.1	Introduction	83
6.2	System and Adversarial Model	84
6.3	DNEFS's Design	84
6.4	Extensions and Optimizations	92
6.5	Summary	96
7	UBIFSec: Adding DNEFS to UBIFS	97
7.1	Introduction	97
7.2	System and Adversarial Model	97
7.3	Background	98
7.4	UBIFSec Design	100
7.5	Experimental Validation	106
7.6	Conclusions	113
III	Secure Deletion for Remote Storage	115
8	Cloud Storage: Background and Related Work	117
8.1	Introduction	117
8.2	Persistent Storage	118
8.3	Related Work	120
8.4	Summary	126
9	Secure Data Deletion from Persistent Media	129
9.1	Introduction	129
9.2	System and Adversarial Model	130
9.3	Graph Theory Background	131
9.4	Graph-Theoretic Model of Key Disclosure	133
9.5	Shadowing Graph Mutations	136
9.6	Summary	144
10	B-Tree-Based Secure Deletion	147
10.1	Introduction	147
10.2	System and Adversarial Model	148
10.3	Background	148
10.4	Securely-Deleting B-Tree Design	150

10.5 Implementation Details	155
10.6 Experimental Evaluation	158
10.7 Conclusions	162
11 Robust Key Management for Secure Data Deletion	163
11.1 Introduction	163
11.2 System and Adversarial Model	164
11.3 Distributed Keystore	167
11.4 Synchronization	171
11.5 Byzantine Robustness	177
11.6 Keystore Secure Deletion	181
11.7 Implementation Details	189
11.8 Experimental Validation	194
11.9 Conclusions	197
IV Conclusions and Future Work	199
12 Conclusion and Future Work	201
12.1 Summary of Contributions	201
12.2 Future Work	204
12.3 Concluding Remarks	207
Bibliography	207