

Contents

- 1 The Big Picture 1**
- 2 The Benefits of Understanding Passwords 5**
 - 2.1 Why We Need to Understand Passwords 5
 - 2.2 People Make Passwords 6
 - 2.3 Building a Parser 7
 - 2.4 Building a Model 11
 - 2.5 Scoring Passwords 13
 - 2.6 Identifying Similarity 20
- 3 Your Password is Your New PIN 25**
 - 3.1 PINs and Friction 25
 - 3.2 How to Derive PINs from Passwords 26
 - 3.3 Analysis of Passwords and Derived PINs 30
 - 3.4 Security Analysis 33
 - 3.5 How do people select their PINs? 35
- 4 Like Passwords – But Faster, Easier and More Secure 37**
 - 4.1 Auto-Correction and Auto-Completion 37
 - 4.2 Related Work 40
 - 4.3 Your Credential is A Story 42
 - 4.4 Extended Feature Set 44
 - 4.5 Recall Rates 46
 - 4.6 Security Analysis 48
 - 4.7 Entry Speed 54
- 5 Improved Visual Preference Authentication 57**
 - 5.1 Preference-Based Authentication 57
 - 5.2 Related Work 59
 - 5.3 Approach 60
 - 5.4 Solution 62

5.5	Experiment	66
5.6	Analysis	67
6	How to Kill Spoofing	73
6.1	The Principles of Spoofing – and Spoof Killer	73
6.2	Related Work	75
6.3	Understanding Conditioning	75
6.4	App Implementation	77
6.5	Experimental Evaluation	80
6.6	User Reactions	89
7	Can Biometrics Replace Passwords?	91
7.1	Why We Need Biomterics	91
7.2	A Brief Overview of Fingerprinting	93
7.3	Some Concerns to be Addressed	94
7.4	A Possible Architecture	95
7.5	Processes	97
8	Legacy Servers: Teaching Old Dogs New Tricks	101
8.1	About Legacy Systems and Authentication	101
8.2	Translating To and From Cookies	103
8.3	Translating Between Fastwords and Passwords	104
Index	107
References	109



<http://www.springer.com/978-1-4614-4877-8>

Mobile Authentication
Problems and Solutions
Jakobsson, M.
2013, XIV, 113 p., Softcover
ISBN: 978-1-4614-4877-8