

## Preface

---

This book provides the state-of-art account of authentication technologies which covers not only basic authentication methodologies but also emerging technologies which are yet to be deployed and adopted by industry. This book is the outcome of last 5 years extensive literature review on authentication, research, and project implementation of specific authentication technologies. Specifically, the concept of negative authentication (described in ►Chap. 3) and adaptive multi-factor authentication (►Chap. 7) are outcomes of the first author's innovative research ideas which were submitted for US patent. The salient topics of each chapter are highlighted below:

► Chapter 1 introduces the basic authentication mechanism for identifying and authorizing legitimate users to computing systems and denying the use by others. It narrates different authentication categories, which are now widely used and highlights how a combination of these categories can provide strong authentication compared to a single category of authentication factor.

► Chapter 2 discusses various biometric authentication modalities such as fingerprint, face recognition, retina, etc., and provided details on various aspects of each biometrics. Different performance metrics of biometric modalities are also covered which determines their usage under various operating conditions.

► Chapter 3 describes a complementary approach of passwords, namely, the Negative Authentication Systems (NAS), the concept of which was introduced by the first author in 2008. This chapter highlights different Negative Authentication Algorithms and represent schemes followed by design and implementation details of a prototype system.

► Chapter 4 focuses on the other complementary approaches including Honeywords, Cracking-Resistant Password Vaults using Natural Language Encoders, Bloom Filter, and Graphical Passwords.

► Chapter 5 covers Multi-factor Authentication (MFA) which provides a fail-safe feature in case of compromising any authentication factor as users are authenticated utilizing the other existing non-compromised modalities.

► Chapter 6 discusses continuous and active authentication approaches including both uni-modal and multi-modal, respectively. The chapter also covers recent research reports on using various mobile device sensors for continuous authentication.

► The last chapter (Chapter 7) discusses an adaptive multi-factor authentication (A-MFA), in particular, it shows how the adaptive selection of authentication factors can improve MFA to validate the users (at any given time) by sensing

the current operating environment (such as devices, media, and surroundings conditions) so to make the decisions unpredictable and unexploitable by hackers.

This book could not be completed without the continued support of the University of Memphis. While Prof. Dipankar Dasgupta is the lead author of the book, several research students at the Center for Information Assurance (CfIA) contributed directly and indirectly to this book project; Arunava Roy (a postdoctoral fellow) and Abhijit Nag (a doctoral student who graduated in December 2016) contributed as co-authors and helped in putting the chapters together under the guidance of Prof. Dasgupta. Authors would like to acknowledge to all whose seminal works which are referenced and cited in this book. We also acknowledge strong support of our families to complete this book project in a timely manner.

Memphis, USA

Dipankar Dasgupta  
Arunava Roy  
Abhijit Nag

Advances in User Authentication

Dasgupta, D.; Roy, A.; Nag, A.

2017, XIV, 360 p. 165 illus., 128 illus. in color.,

Hardcover

ISBN: 978-3-319-58806-3