Foreword

Conventional security systems check the identity of an individual only once at the entry point (i.e. login) before granting them access to protected resources. This is not enough in high-security environments where access to sensitive resources needs to be constantly monitored to ensure that the authorized user is always the one using the resources. Conventional systems permit session hijacking, in which an attacker takes control of a post-authenticated session and performs unauthorized activities. Continuous authentication (CA) systems arose to prevent such occurrences, and represent a new generation of security systems that require the user to re-authenticate themselves repeatedly (and as frequently as desired) for continued access to sensitive resources.

The idea of continuous authentication emerged in the early 2000s, in part due to heightened security concerns brought about after Sept. 11. Interest in this technology has been increasing since then, both in academia and industry. Continuous authentication may be applied in various environments where high-security is needed. Although most of the systems proposed in the literature have targeted the protection of computing environments, other proposals make the case for safeguarding the aircraft cockpit against unauthorized control, or for ensuring driver identity while he/she is operating the vehicle.

Many different types of technologies (e.g. RFID, tokens) may be used to achieve continuous authentication, but systems based on biometrics have emerged as the most popular. Biometrics are ideal for continuous authentication because they cannot be misplaced (unlike tokens), forgotten (unlike passwords), and are difficult to forge by an imposter. This is especially true when multiple biometrics are used.

Although much has been written about continuous authentication in the past decade, this book on “Continuous Authentication using Biometrics,” edited by Dr. Issa Traoré and Dr. Ahmed A. Ahmed, is the first effort at bringing together several representative pieces of work on this important topic. This book is a significant undertaking because it contributes to raising the awareness of the research and industry communities about this emerging area. The book involves 11 double-blinded peer-reviewed chapters contributed by 23 different researchers from around the globe spanning various aspects of continuous authentication. The contributors are among the leading experts in the field, and they cover topics ranging from authentication metrics and fundamental concepts, to practical applications using various types of biometrics (e.g. keystroke, mouse, iris scan, cognitive biometrics, palmprint), to different architectures (e.g. uni-modal and multi-modal).
Researchers and students in academia, as well as security professionals in industry and government will no doubt find this book helpful in advancing the security landscape. The depth of knowledge brought in by the contributors to this endeavour ensures that this book will serve as a professional reference, and provide a comprehensive and insightful view of this emerging field. I congratulate all the authors, as well as the editors, for marking an important milestone in the development of continuous authentication.

Terence Sim  
School of Computing National University of Singapore, Singapore

Terence Sim received the PhD degree in Electrical and Computer Engineering from Carnegie Mellon University in 2002, the MS degree in Computer Science from Stanford University in 1991 and the BS degree in Computer Science and Engineering from the Massachusetts Institute of Technology in 1990. He is an Assistant Professor at the School of Computing, National University of Singapore. His research interests are in biometrics, face recognition, computer vision, computational photography, and music processing. He also serves as Vice Chairman of the Biometrics Technical Committee, Singapore, and as Vice President of the Pattern Recognition and Machine Intelligence Society, Singapore. He has contributed several influential papers in continuous biometrics authentication.