

1. Record Nr.	UNINA9910799496503321
Autore	Smith-Creasey Max
Titolo	Continuous Biometric Authentication Systems [[electronic resource] ] : An Overview // by Max Smith-Creasey
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
ISBN	3-031-49071-1
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (127 pages)
Collana	SpringerBriefs in Computer Science, , 2191-5776
Disciplina	006.248
Soggetti	Biometric identification Pattern recognition systems Data protection - Law and legislation Biometrics Automated Pattern Recognition Privacy
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Introduction -- Traditional Authentication -- Continuous Authentication -- Biometrics for Continuous Authentication -- Considerations and Challenges -- Conclusion.
Sommario/riassunto	This book offers an overview of the field of continuous biometric authentication systems, which capture and continuously authenticate biometrics from user devices. This book first covers the traditional methods of user authentication and discusses how such techniques have become cumbersome in the world of mobile devices and short usage sessions. The concept of continuous biometric authentication systems is introduced and their construction is discussed. The different biometrics that these systems may utilise (e.g.: touchscreen-gesture interactions) are described and relevant studies surveyed. It also surveys important considerations and challenges. This book brings together a wide variety of key motivations, components and advantages of continuous biometric authentication systems. The overview is kept high level, so as not to limit the scope to any single device, biometric trait, use-case, or scenario. Therefore, the contents of this book are

applicable to devices ranging from smartphones to desktop computers, utilising biometrics ranging from face recognition to keystroke dynamics. It also provides metrics from a variety of existing systems such that users can identify the advantages and disadvantages of different approaches. This book targets researchers and lecturers working in authentication, as well as advanced-level students in computer science interested in this field. The book will also be of interest to technical professionals working in cyber security.

---