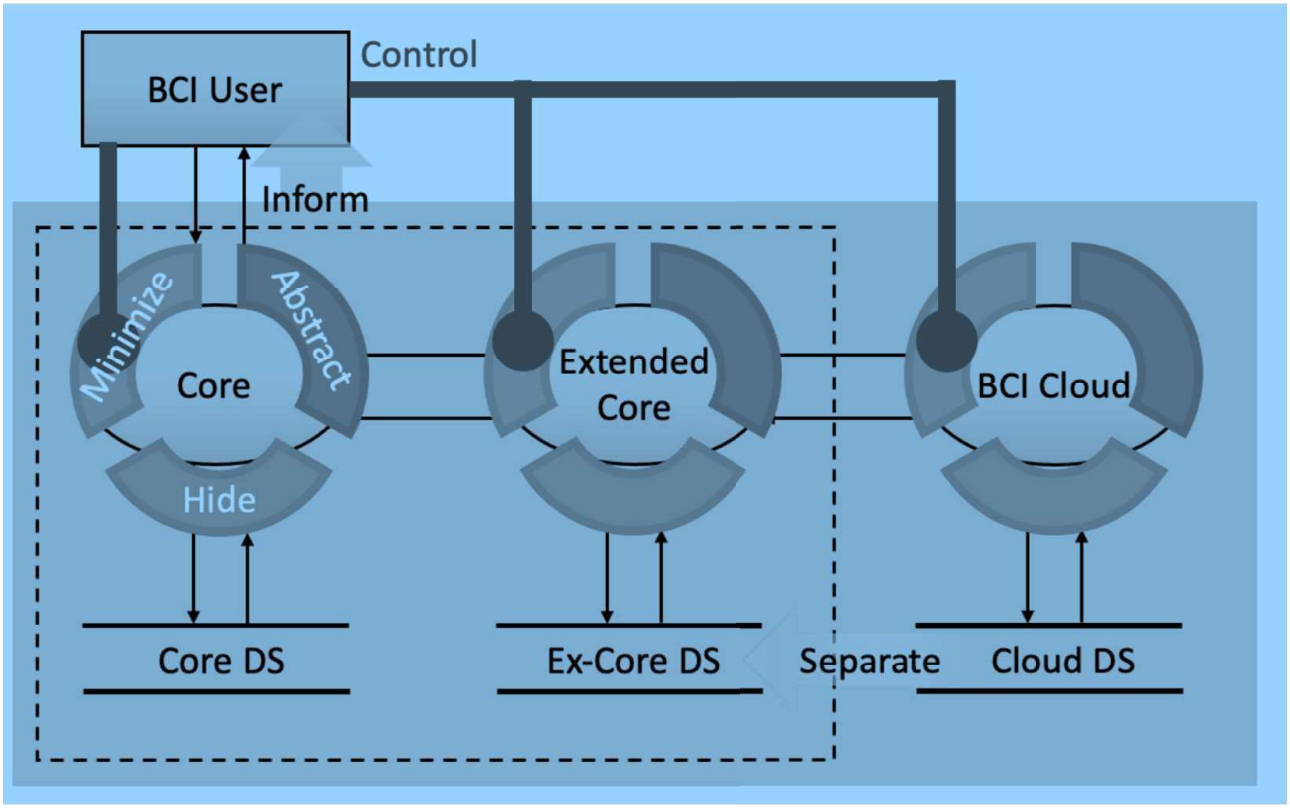
A Framework for Preserving Privacy and Cybersecurity in Brain-Computer Interfacing Applications



Maryna Kapitonova, NeuroMentum AI GmbH, Freiburg

Philipp Kellmeyer, Human-Technology Interaction Lab, Freiburg

Tonio Ball, NeuroMentum AI GmbH, Freiburg

Version 1.0 — June 30th, 2022

Abstract

Brain-Computer Interfaces (BCIs) comprise a rapidly evolving field of technology with the potential of far-reaching impact in domains ranging from medical over industrial to artistic, gaming, and military. BCIs provide technical interfaces with recording and/or stimulation functionality to connect the brain with computer systems running `"decoders"` for online analysis of the recorded brain signals. This online analysis in turn can inform various effectors such as robots, vehicles (brain-to-vehicle interfaces), brain stimulation devices, or computer games (neurogaming). Today, these emerging BCI applications are typically still at early technology readiness levels. But because BCIs create novel, technical communication channels for the human brain, they have raised privacy and security concerns. In particular, as brain data contains personal information, adversaries may utilize BCIs to compromise brain privacy. There are first empirical proofs-of-principle that such attacks are indeed possible, possibly foreshadowing a next level of privacy and cybersecurity threats targeting the brain with neurotechnological means. To mitigate such risks, a large body of countermeasures has been proposed in the literature, but a general framework is lacking which would describe how privacy and security of BCI applications can be protected by design, i.e., as an integral part already of the early BCI design process, in a systematic manner, and allowing suitable depth of analysis for different contexts such as commercial BCI product development vs. academic research and lab prototypes.

Here we propose the adoption of recent systems engineering methodologies for privacy threat modeling, risk assessment, and privacy engineering to the BCI field. These methodologies address privacy and security concerns in a more systematic and holistic way compared to previous approaches, and provide reusable patterns on how to move from principles to actions. We apply these methodologies to BCI processes and data flows and derive a generic, extensible, and actionable framework for brain-privacy-preserving cybersecurity in BCI applications. This framework is designed for flexible application to the wide range of current and future BCI applications. We also propose a range of novel privacy-by-design features for BCIs, with an emphasis on features promoting BCI transparency as a prerequisite for informational self-determination of BCI users, as well as design features for ensuring BCI user autonomy. We anticipate that our framework will contribute to the development of privacy-respecting, trustworthy BCI technologies across its various application domains.