Security and privacy are often studied by focusing on how (rather than why) attacks are perpetrated. However, in practice, the attacker is motivated by various incentives and his success often depends on his (limited) capabilities, and on users’ defensive strategies. Moreover, due to their inherent interconnected nature, users often face mutual security and privacy risks. In many cases, the selfish behavior of users with misaligned incentives results in inefficient outcomes for all stakeholders. Game theory has demonstrated to be very powerful for modeling and analyzing the interplay between rational agents with (possibly) conflicting interests. Consequently, it is a key tool for studying attacker-defender interactions in security and privacy environments. It is also very relevant for analyzing the strategic behaviors of interconnected agents in networked systems [2].

At the Laboratory for Communications and Applications 1 (EPFL), we have applied game theory in order to analyze several privacy and security problems. We have analyzed individuals' decisions about how to manage and secure their genomic data [1]. In the context of location privacy, we have modeled and analyzed the best strategies of mobile users against a strategic adversary [4,6], the outcomes resulting from non-cooperative behavior [10], and incentives to foster collaboration in location privacy-preserving mechanisms [5]. In addition, we have studied the interactions between various stakeholders in online advertising [3,7,8] and we have designed optimal protocols for revoking users in ephemeral networks [9,11].

Contact:

Alexandra-Mihaela Olteanu  alexandramihaela.olteanu@epfl.ch
Prof. Jean-Pierre Hubaux  jean-pierre.hubaux@epfl.ch