Abstract

In general service providing systems, user authentication is required for different purposes such as billing, restricting unauthorized access, etc. A good solution is to use pseudonyms as temporary identities. On the other hand, it may also be required to have a backdoor in pseudonym systems for identity revealing that can be used by law enforcement agencies for legal reasons. Such pseudonym providing systems rely on one or more trusted third parties. The threat models of the existing schemes do not assume existence of collusion among these trusted parties, however, collusion among them can severely breach privacy such that pseudonyms can be linked to real identities in an unauthorized way. In this paper, we propose a novel pseudonym providing and management system. Our system is privacy-preserving and guarantees a level of anonymity for a particular number of system users. Besides, trust is distributed among all system entities instead of centralizing it into a single trusted third party. More importantly, our system is highly resistant to collusions among the trusted entities. Our system also has the ability to reveal user identity in case of a request by law enforcement. To maximize the privacy of the users, our design requires the collaboration among all trusted entities for identity revealing. We perform analytical and simulation based performance evaluation in order to analyze the anonymity level and resistance against collusion attacks. Our results show that CoRPPS provides high level of anonymity with strong resistance against collusion attacks