Authentication services used many times a day. If there is no user authentication, then it would be impossible to use email accounts, discussion boards, e-banking or even electronic communication. On the other hand, it releases a lot of personal information during every authentication process. User login can be linked to used services and assets by service providers. The frequency of usage and therefore the map of our behavior on the Internet can be created to make more focused advertisement, to track us or even to steal our electronic identity. The purpose of this paper is to state the requirements and provide the initial design for an anonymous authentication scheme which prevents the leakage of private information. The new scheme, to be widely acceptable, must be beneficial for both users and service providers, who implement the authentication systems. Therefore the new authentication system must provide a feature for revealing dishonest users. These users can be eventually deanonymized and charged for damages. This paper provides such a responsibility-protecting feature in this new scheme.
References


Index Terms

Computer Science Security

Keywords

Anonymity, Privacy, Authentication, Efficiency, Responsibility