Security for an auxiliary human memory

Jukka A. Koskinen
Tampere University of Technology
P.O.Box 553
FIN-33101 Tampere
Finland
Tel. +358–3–365 3918
Email: jak@cs.tut.fi

29 April 2000

Keyword: Anonymity.

This work in progress has been motivated by the current trends towards portable and even wearable computers and their continuous connectivity to the internet. One plausible consequence of such development is that personal human memory will be augmented far beyond the current use of calendars, notebooks etc. This is likely to involve so large amounts of data that have to be available for such a long time, that networked services will be needed and an essential part of the user's memory resides outside his security perimeter.

At this stage we rely on very abstract notions of the user's interface and the communication service, and likewise assume that the large memory storage can be organized in an efficient way, which supports also content based retrieval. In the poster we describe the security issues in a situation where a user accesses his personal information by communicating with an external memory server, using the operations store, search, fetch and optionally erase. We start from the rather obvious fact that anything that must remain private must always be encrypted when it is not totally controlled by the user. We sketch protocols to carry out the basic operations, whereby we apply
– blindly signed tickets by the server to authorize storage and to provide part of the anonymity for the user;
– a group of users sharing the same memory area to protect the encryption of their data and to provide the rest of anonymity;
– a signature by the server as a storage receipt, to provide accountability;
– an additional hash value in the storage receipt. This is provided by the user and its preimage will be needed to authorize erasure.