Hopper, Nicholas J.; **Blum, Manuel**

Secure human identification protocols. (English) Zbl 1062.94549

Boyd, Colin (ed.), Advances in cryptology - ASIACRYPT 2001. 7th international conference on the theory and application of cryptology and information security, Gold Coast, Australia, December 9–13, 2001. Proceedings. Berlin: Springer (ISBN 3-540-42987-5). Lect. Notes Comput. Sci. 2248, 52-66 (2001).

Summary: One interesting and important challenge for the cryptologic community is that of providing secure authentication and identification for unassisted humans. There are a range of protocols for secure identification which require various forms of trusted hardware or software, aimed at protecting privacy and financial assets. But how do we verify our identity, securely, when we don't have or don't trust our smart card, palmtop, or laptop?

In this paper, we provide definitions of what we believe to be reasonable goals for secure human identification. We demonstrate that existing solutions do not meet these reasonable definitions. Finally, we provide solutions which demonstrate the feasibility of the security conditions attached to our definitions, but which are impractical for use by humans.

For the entire collection see [Zbl 0977.00048].

MSC:

94A60 Cryptography
94A62 Authentication, digital signatures and secret sharing

Full Text: Link