Juels, Ari; **Weis, Stephen A.**

Authenticating pervasive devices with human protocols. (English) Zbl 1145.94470

Shoup, Victor (ed.), Advances in cryptology – CRYPTO 2005. 25th annual international cryptology conference, Santa Barbara, CA, USA, August 14–18, 2005. Proceedings. Berlin: Springer (ISBN 3-540-28114-2/pbk). Lecture Notes in Computer Science 3621, 293-308 (2005).

Summary: Forgery and counterfeiting are emerging as serious security risks in low-cost pervasive computing devices. These devices lack the computational, storage, power, and communication resources necessary for most cryptographic authentication schemes. Surprisingly, low-cost pervasive devices like Radio Frequency Identification (RFID) tags share similar capabilities with another weak computing device: people.

These similarities motivate the adoption of techniques from human-computer security to the pervasive computing setting. This paper analyzes a particular human-to-computer authentication protocol designed by Hopper and Blum (HB), and shows it to be practical for low-cost pervasive devices. We offer an improved, concrete proof of security for the HB protocol against passive adversaries.

This paper also offers a new, augmented version of the HB protocol, named HB^+, that is secure against active adversaries. The HB^+ protocol is a novel, symmetric authentication protocol with a simple, low-cost implementation. We prove the security of the HB^+ protocol against active adversaries based on the hardness of the Learning Parity with Noise (LPN) problem.

For the entire collection see [Zbl 1131.94006].

MSC:

94A62 Authentication, digital signatures and secret sharing

Keywords:

Authentication; HumanAut; Learning Parity with Noise (LPN); pervasive computing; RFID

Software:

DIMACS

Full Text: DOI