EPFL-TTO

EPFL Innovation Park J
CH-1015 Lausanne
Switzerland
+41 21 693 70 23
http://tto.epfl.ch/

Research Contact

Prof. Serge Vaudenay
+41 21 693 76 96
serge.vaudenay@epfl.ch

TTO Contact

Dr. Thomas Bourgeau
+41 21 693 33 54
thomas.bourgeau@epfl.ch

Licensing Opportunity

TTO – Technology Transfer Office

Method and device for proving his identity

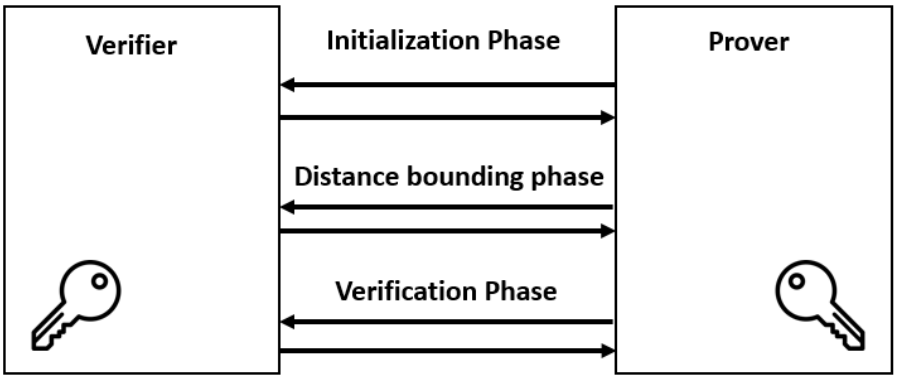

Figure 1: Robust distance-bounding method and devices allowing a user to prove his identity and proximity to a verifier.

Ref. Nr

6.1341

Keywords

Distance-bounding, authentication, relay attacks, provable security.

Intellectual Property

US Patent US9930523B2 granted

Publications

Boureanu, Ioana, et al. "Practical and Provably Secure Distance-Bounding." Journal of Computer Security,23.2, 229-257,2015.

Date

06/02/2023

Description

Distance-bounding protocols allow a verifier to both authenticate a prover and evaluate whether the latter is located in his vicinity.

These protocols are of particular interest in contactless systems, e.g., electronic payment or access control systems, which are vulnerable to distance-based frauds such as Relay attacks and, more generally, man-in-the-middle attacks.

It seems likely that nearly all wireless devices will eventually have to implement solutions to thwart these types of fraud, however existing solutions are not resistance to all popular attack-models.

Advantages

The present invention provides a robust method offering provably secure distance bounding which is more efficient, i.e., which requires less rounds and/or less data to be exchanged for offering the same reliability at a given level of noise and which may be incorporated into a variety of apparatuses i.e. smart cards, RFID devices, electronic access keys, smartphone or laptops.

Furthermore, our proposed method overcomes most of the threat models known in the literature on distance-bounding such as: Distance fraud (DF), Mafia fraud (MF), Terrorist fraud (TF) or Impersonation fraud (IF).

Applications

- Cybersecurity
- NFC-based payments
- Access control