Secure Protocols for Serverless Remote Product Authentication

Abdourhamane Idrissa, Alain Aubert,
Thierry Fournel, Viktor Fischer

Laboratoire Hubert Curien
CNRS, UMR5516
Universite de Lyon, F-42023, Saint-Etienne, France

Abstract

Industrial companies lose large sums of money because of counterfeits and they need to efficiently protect their trademarks. Most of them implement their own anti-counterfeiting policy to deal with the menace. A number of technologies, such as holograms, smart cards, biometric markers and inks, can be employed to protect and authenticate genuine products. Instead of using markers and additional identification means, one of the recent methods use a PUF-like authentication method based on image processing. However, in order to authenticate the object (e.g. a trademark product), the method needs direct access to the database system containing the object's "fingerprint" . The paper presents a new secure method to remotely authenticate the object without communication with the database server. In this method, an autonomous and secure embedded system called authentifier authenticates the product by extracting its morphometric fingerprint and comparing it with a signed original morphometric fingerprint printed on the object. However, we show that in order to secure the protocol, the authentication hardware needs to be authenticated, too. For this reason, we propose security protocols that allow to authenticate the verifier and to remotely check its integrity. The proposed security protocols are shown to be sure using formal methods of security protocol evaluation.