Cryptology ePrint Archive: Report 2011/101

Lightweight Anonymous Authentication with TLS and DAA for Embedded Mobile Devices

Liqun Chen and Kurt Dietrich and Hans Löhr and Ahmad-Reza Sadeghi and Christian Wachsmann and Johannes Winter

Abstract: Although anonymous authentication has been extensively studied, so far no scheme has been widely adopted in practice. A particular issue with fully anonymous authentication schemes is that users cannot easily be prevented from copying and sharing credentials.

In this paper, we propose an anonymous authentication scheme for mobile devices that prevents copying and sharing of credentials based on hardware security features. Our system is an optimized adaptation of an existing direct anonymous attestation (DAA) scheme, specifically designed for resource-constrained mobile devices. Our solution provides (i) anonymity and untraceability of mobile embedded devices against service providers, (ii) secure device authentication even against collusions of malicious service providers, and (iii) allows for revocation of authentication credentials. We present a new cryptographic scheme with a proof of security, as well as an implementation on ARM TrustZone. Moreover, we evaluate the efficiency of our approach and demonstrate its suitability for mobile devices.

Category / Keywords: cryptographic protocols / Mobile Phones, Privacy, Anonymity, ARM TrustZone

Publication Info: Full version of ISC 2010 paper.

Date: received 1 Mar 2011

Contact author: christian wachsmann at trust cased de