Cryptology ePrint Archive: Report 2011/658

Anonymous attestation with user-controlled linkability

D. Bernhard and G. Fuchsbauer and E. Ghadafi and N.P. Smart and B. Warinschi

Abstract: This paper is motivated by the observation that existing security models for Direct Anonymous Attestation (DAA) have problems to the extent that insecure protocols may be deemed secure when analysed under these models. This is particularly disturbing as DAA is one of the few complex cryptographic protocols resulting from recent theoretical advances actually deployed in real life. Moreover, standardisation bodies are currently looking into designing the next generation of such protocols.

Our first contribution is to identify issues in existing models for DAA and explain how these errors allow for proving security of insecure protocols. These issues are exhibited in all deployed and proposed DAA protocols (although they can often be easily fixed).

Our second contribution is a new security model for a class of "pre-DAA scheme", i.e., DAA schemes where the computation on the user side takes place entirely on the trusted platform. Our model captures more accurately than any previous model the security properties demanded from DAA by the Trusted Computing Group (TCG), the group that maintains the DAA standard. Extending the model from pre-DAA to full DAA is only a matter of refining the trust models on the parties involved.

Finally, we present a generic construction of a DAA protocol from new building blocks tailored for anonymous attestation. Some of them are new variations on established ideas, and may be of independent interest. We give instantiations for these building blocks that yield a DAA scheme more efficient than the one currently deployed, and as efficient as the one about to be standardised by the TCG which has no valid security proof.

Category / Keywords: Cryptographic protocols / DAA, group signatures, security models.

Date: received 5 Dec 2011, last revised 21 Mar 2012

Contact author: nigel at cs bris ac uk