Using a Sparse Merkle Tree in Balloon

Computer science bachelor's degree project proposal

Tobias Pulls[1]

Karlstad University, Dept. of Mathematics and Computer Science, Sweden
tobias.pulls@kau.se

1 Background

Balloon is a forward-secure append-only persistent authenticated data structure that is designed for an initially trusted *author* that generates events to be stored in a data structure (the Balloon) kept by an untrusted *server*, and *clients* that query this server for events intended for them based on keys and snapshots [2]. Balloon is the composition of two authenticated data structures: a hash treap and a history tree. The hash treap acts like an authenticated index of all data stored in the history tree. A *sparse Merkle tree* is a different type of authenticated data structure that could replace the hash treap in Balloon [1,2].

2 Expected Outcome

A successful project is expected to define and evaluate how to securely use a sparse Merkle tree instead of a hash treap in Balloon. Once defined, the modified Balloon should be compared with the original. The comparison should at least be analytical in terms of complexity and relevant design decisions, and if time permits also experimentally by proof-of-concept implementation.

3 Description of Work

This project involves data structures, applied cryptography, and computer security. Interested student(s) are expected to show proficiency in at least one of the relevant areas. No special equipment is required for the project. Tobias Pulls is the client and supervisor of the project.

References

1. Ben Laurie and Emilia Kasper. Revocation transparency. *Google Research, September*, 2012.
2. Tobias Pulls and Roel Peeters. Balloon: A forward-secure append-only persistent authenticated data structure. In Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, *ESORICS 2015*, volume 9327 of *Lecture Notes in Computer Science*, pages 622–641. Springer, 2015.