Cryptology ePrint Archive: Report 2011/308

Provably Secure and Practical Onion Routing

Michael Backes, Ian Goldberg, Aniket Kate, Esfandiar Mohammadi

Abstract: The onion routing network, Tor, is undoubtedly the most widely employed technology for anony- mous web access. Although the underlying onion routing (OR) protocol's multi-pass cryptographic circuit construction appears satisfactory, a comprehensive formal analysis of its security guarantees is still lacking. Moreover, in practice the current Tor circuit construction suffers from inefficiency, which is due to the key exchange protocol that is used for circuit construction. Consequently, significant efforts have been put towards improving the efficiency of the key exchange in onion routing.

In this paper, we address both these issues. We present the first security definition for OR protocols with multi-pass circuit construction in the universal composability framework. We then show that a recently introduced efficient key exchange protocol can be used in the circuit construction such that the resulting OR protocol provably satisfies our security definition. As a result, we obtain the first provably secure and practical OR protocol with multi-pass circuit construction.

Category / Keywords: cryptographic protocols / onion routing, security proof, universal composability, one-way authenticated key exchange, 1W-AKE

Date: received 9 Jun 2011

Contact author: mohammadi at cs uni-saarland de