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 appears satisfactory, a comprehensive analysis of its security guarantees is still lacking. This has also resulted in a sig- nificant gap between research work on OR protocols and existing OR anonymity analyses. In this work, we address both issues with onion routing by defining a provably secure OR protocol, which is practical for deployment in the next generation Tor network.

We start off by presenting a security definition (an ideal functionality) for the OR methodology in the universal composability (UC) framework. We then determine the exact security properties required for OR cryptographic primitives (onion construction and processing algorithms, and a key exchange protocol) to achieve a provably secure OR protocol. We show that the currently deployed onion algorithms with slightly strengthened integrity properties can be used in a provably secure OR construction. In the process, we identify the concept of predictably malleable symmetric encryptions, which might be of independent interest. On the other hand, we find the currently deployed key exchange protocol to be inefficient and difficult to analyze and instead show that a recent, significantly more efficient, key exchange protocol can be used in a provably secure OR construction.

In addition, our definition greatly simplifies the process of analyzing OR anonymity metrics. We define and prove forward secrecy for the OR protocol, and realize our (white-box) OR definition from an OR black-box model assumed in a recent anonymity analysis. This realization not only makes the analysis formally applicable to the OR protocol but also identifies the exact adversary and network assumptions made by the black box model.

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

Date: received 9 Jun 2011, last revised 20 Mar 2012

Contact author: mohammadi at cs uni-saarland de