Cryptology ePrint Archive: Report 2011/260

Security \& Indistinguishability in the Presence of Traffic Analysis

Cristina Onete and Daniele Venturi

Abstract: Traffic analysis (TA) is a powerful tool against the security and privacy of cryptographic primitives, permitting an adversary to monitor the frequency and timing characteristics of transmissions in order to distinguish the senders or the receivers of possibly encrypted communication. Briefly, adversaries may leak implementation-specific information even for schemes that are provably secure with respect to a classical model, resulting in a breach of security and/or privacy.

In this work we introduce the notion of \emph{indistinguishability in the presence of traffic analysis}, enhancing \emph{any} classical security model such that no adversary can distinguish between two protocol runs (possibly implemented on different machines) with respect to a TA oracle (leaking information about each protocol run). This new notion models an attack where the adversary taps a single node of in- and outgoing communication and tries to relate two sessions of the same protocol, either run by two senders or for two receivers.

Our contributions are threefold: (1) We first define a framework for indistinguishability in the presence of TA, then we (2) fully relate various notions of indistinguishability, depending on the adversary's goal and the type of TA information it has. Finally we (3) show how to use our framework for the SSH protocol and for a concrete application of RFID authentication.

Category / Keywords: foundations / provable security, traffic analysis, SSH

Date: received 25 May 2011, last revised 25 May 2011

Contact author: venturi at infocom uniroma1 it