Abstract

The HMQV protocols are hashed variants of the MQV key agreement protocols. They were recently introduced by Krawczyk, who claimed that the HMQV protocols have very significant advantages over their MQV counterparts: (i) security proofs under reasonable assumptions in the (extended) Canetti-Krawczyk model for key exchange; and (ii) superior performance in some situations. In this paper we demonstrate that the HMQV protocols are insecure by presenting realistic attacks in the Canetti-Krawczyk model that recover a victims static private key. We propose HMQV-1, patched versions of the HMQV protocols that resists our attacks (but do not have any performance advantages over MQV). We also identify some fallacies in the security proofs for HMQV, critique the security model, and raise some questions about the assurances that proofs in this model can provide.