Cryptanalysis of a Protocol from FC'10 (Poster Abstract)

Mohsen Toorani

Department of Informatics,
University of Bergen, Bergen, Norway
mohsen.toorani@ii.uib.no

Abstract. We show that the YAK protocol does not provide the key control attribute, and is vulnerable to some attacks. We also propose some improvements.

The YAK protocol [1,2] is a variant of the two-pass HMQV protocol [3], but uses zero-knowledge proofs for proving knowledge of ephemeral secret keys. It is based on public keys, certified by certificate authorities. Although the YAK protocol is claimed to be an authenticated key exchange (AKE) protocol [1,2], the authentication is just zero-knowledge verification of a random number, generated by the other party. There is no binding between entity identifiers and the session key derivation function. Any AKE protocol should provide several security attributes, and it should withstand well-known attacks [4].

There are claims for security and efficiency of the YAK protocol [1,2], but we show that it does not provide the *key control* attribute which is a requirement for key exchange protocols. We also show that the YAK protocol is vulnerable to an *unknown key-share attack* and a *key-replication attack*. The key confirmation is left optional in the YAK protocol, but it is crucial to have it in order to avoid an *impersonation attack*. In case of having the key confirmation, it is crucial to verify that public keys are of prime order. Otherwise, the protocol will be vulnerable to a *small subgroup attack*. In the YAK protocol, it is assumed that such verification is part of any zero-knowledge proof technique.

The YAK protocol is not secure in any security model that allows the above attacks. This includes the HMQV [3] and eCK [5] security models.

References

1. Hao, F.: On robust key agreement based on public key authentication. In: Sion, R. (ed.) FC 2010. LNCS, vol. 6052, pp. 383–390. Springer, Heidelberg (2010)
2. Hao, F.: On robust key agreement based on public key authentication. Secur. Commun. Netw. **7**(1), 77–87 (2014)
3. Krawczyk, H.: HMQV: a high-performance secure Diffie-Hellman protocol. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 546–566. Springer, Heidelberg (2005)
4. Toorani, M.: Cryptanalysis of a new protocol of wide use for email with perfect forward secrecy. Secur. Commun. Netw. 8(4), 694–701 (2015)
5. LaMacchia, B., Lauter, K., Mityagin, A.: Stronger security of authenticated key exchange. In: Susilo, W., Liu, J.K., Mu, Y. (ed.) ProvSec 2007. LNCS, vol. 4784, pp. 1–16. Springer, Heidelberg (2007)

R. Böhme and T. Okamoto (Eds.): FC 2015, LNCS 8975, pp. 569, 2015.
DOI: 10.1007/978-3-662-47854-7