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

Mohsen Toorani

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

Abstract. We show that the YAK protocol is vulnerable to several attacks including the impersonation, unknown key-share, key-replication, and small subgroup 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 [4], and it should withstand well-known attacks. There are claims for security and efficiency of the YAK protocol [1, 2], but we show that the main description of the YAK protocol is vulnerable to the following attacks:

1. Impersonation attack
2. Unknown key-share attack
3. Key-replication attack
4. Small subgroup attack

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: Proceedings of the 14th International Conference on Financial Cryptography and Data Security (FC'10), LNCS 6052. (2010) 383–390
2. Hao, F.: On robust key agreement based on public key authentication. Security and Communication Networks **7**(1) (2014) 77–87
3. Krawczyk, H.: HMQV: A high-performance secure Diffie-Hellman protocol. In: Advances in Cryptology–CRYPTO'05, Springer (2005) 546–566
4. Toorani, M.: Cryptanalysis of a new protocol of wide use for email with perfect forward secrecy. Security and Communication Networks (2014)
5. LaMacchia, B., Lauter, K., Mityagin, A.: Stronger security of authenticated key exchange. In: Provable Security, Springer (2007) 1–16