Comments on “Cryptanalysis of a robust key agreement based on public key authentication"

Feng Hao
Department of Computer Science
University of Warwick

September 2019

Introduction. YAK is a public-key authenticated key exchange protocol, which was initially presented at FC’10 as a short paper [Hao10]. A full paper was later published in a journal [Hao14]. The specification of the YAK protocol is the same in both papers. In [Too16], the author claims that YAK is subject to several attacks and security weaknesses. However, the claims are not fairly and accurately presented. I will respond to each of the claims below.

1. Key control

The author claims that YAK is subject to a key control attack: if Bob chose the ephemeral private key b = -a where a is his long-term private key, the session key will be fixed at K=H(1). First of all, it is worth noting that joint key control is listed as a property that “may be desirable”, but not a mandatory requirement for key agreement protocols (see Chapter 12, Handbook of applied cryptography, Menezes et al, 1996). The “attack” scenario above assumes a legitimate user actively sabotaging the security of its own session. Of course, the security of the session cannot be guaranteed. Furthermore, contrary to what the author states, similar key control “attacks” could also happen to other protocols: for example, in HMQV, when receiving $X=g^x$ from Alice (along with Alice’s identity A and her public key certificate), Bob can register a static public key with the private key $b = -ye^{-1}$ (where y is Bob’s empehermal private key for the ephemeral public key $Y=g^y$ and e = H(Y, A); see [Hao14] for more details on notations). This will fix the session key to H(1) as well. This “attack” assumes Bob can do real-time registration of the static key, which follows the same as described in Kaliski’s unknown key-sharing attack on MQV [Kal01]. However, this shouldn’t be considered a valid attack. It is not meaningful to protect security when the legitimate user actively sabotages its own session.

2. Unknown key-share attack

The author presents an unknown key-share attack on YAK and states that this attack can be prevented by including the user identity in the Schnorr zero-knowledge proof. Unfortunately, the author has missed the fact that the user identity is defined as a mandatory input to the hash function of the Schnorr ZKP; see Section III.A [Hao14].

3. Key-replication attack

The author assumes a simulated model in which an adversary lets the two parties use the same ephemeral keys in two sessions and derive the same session key. This simulated attack is entirely artificial and cannot work in any practical setting.

4. Impersonation attack

The author describes a so-called impersonation attack: "*The adversary generates a random number and generates proofs for his knowledge of the random number. As the authentication at the other party is just knowledge proofs of the random number, the adversary will be verified and authenticated. Of course, the adversary cannot generate a session key, but there is no further step for the key confirmation*." In any authenticated key exchange (AKE) protocol, there is always key confirmation, which can be either "implicit" or "explicit" (see Chapter 11 "key agreement schemes" from *Cryptography, Theory and Practice*, 3rd edition, Stinson, 2005). The author equates "implicit key confirmation" with "no key confirmation", which is a misunderstanding of how a key agreement protocol works.

5. Small subgroup attack

The author claims that YAK is subject to a small subgroup attack and states this attack can be prevented by checking the order of the public key. Unfortunately, the author has missed the fact that validating the order of the public key is a mandatory check in YAK (Section III.A, [Hao14]), which is also reflected in the computational cost analysis (Section VI, [Hao14]).

6. Perfect forward secrecy

The author assumes an adversary who knows not only the long-term private key of the communicating party, but also the ephemeral key, and claims that this attacker is able to compute the session key, hence breaking the forward secrecy. Clearly, the same attacker can trivially break all AKE protocols, which makes this so-called "attack" not meaningful. I suggest reviewing the "extreme adversary principle" stated in [Hao14].

Conclusion. I hope this document can help interested readers to understand more about YAK and the general subject of public-key authenticated key exchange.

References

[Too16] Toorani, M. (2016). Cryptanalysis of a robust key agreement based on public key authentication. Security and Communication Networks, 9(1), 19-26.

[Hao10] Hao, F. (2010). On robust key agreement based on public key authentication. In International Conference on Financial Cryptography and Data Security (pp. 383-390). Springer, Berlin, Heidelberg.

[Hao14] Hao, F. (2014). On robust key agreement based on public key authentication. Security and Communication Networks, 7(1), 77-87.

[Kal01] Kaliski Jr, B. S. (2001). An unknown key-share attack on the MQV key agreement protocol. ACM Transactions on Information and System Security (TISSEC), 4(3), 275-288.