Armoring Password Based Protocol Using Zero-knowledge with Secret Coin Tossing

DaeHun Nyang
Information Security Technology
Division, ETRI, Korea
e-mail: nyang@etri.re.kr

Abstract — **We present a systematic way to gracefully adopt a protocol for password authentication and key-exchange protocol into the ZKIP system.**

I. Introduction

We suggest a systematic way to design secure password-based authentication protocols, which is the password verifier model. The method makes use of zero-knowledge interactive proof(ZKIP), which has been known not to be useful for the protection of passwords. For the proper usage of ZKIP, we introduce a specialized form of ZKIP, which has a secret coin-tossing stage.

II. Is ZKIP Incompatible with Password?

The most naive way to adopt ZKIP-based identification scheme into a password-based authentication protocol is using the password verifier model and setting the password as a prover's secret in the ZKIP setting. Here, the verifier is derived from the password using some oneway(trapdoor) function. In the traditional ZKIP setting, password verifier is the counterpart of a public key, of which exposure does not leak any sensitive information of secret. Although the password verifier is masked by the question during the protocol, the question is known to an eavesdropper and the masked password verifier will be a reference for the guessing attack. Consequently, the protocol is, as it is, vulnerable to guessing attack.

III. ZKIP-based Password Authentication

The weakness referred in section II can be overcome by using the notion of the "secret question". The main reason that the guessing attack is mountable is the exposure of the masked password verifier. Thus, guessing attack will not be mountable against the protocol if the masking value, or the question number is not obtainable to the eavesdropper.

However, note that the information sent to a fraudulent Server from a User may be misused for the guessing attack. Thus, User must certify that the corresponding Server knows the password verifier. To achieve this, we use the simpler form of the EKE[1]. $H()$ is a oneway hash function and $h()$ is another oneway hash function, but it returns only k bits, where k is selected considering the trade-off of the speed and the security. $OWF()$ and $f()$ are a ZKIP-specific oneway (trapdoor) function and a deterministic function that merely expands a password into a large-sized value, respectively.

- System setup:
  Verifier for user's password is $V = OWF(f(P))$ and kept securely in server's storage.
- Authentication:

1. Perform the simplified EKE for the proof of Server's knowledge of V.
   (a) User sends $ID_{User}, X = V(g^x \bmod p)$ with a test number $A = OWF(r)$, where $V(x)(V^{-1}(x))$ is symmetric encryption(decryption) of x with the key V.
   (b) Server selects $y \in_R Z_p^*$ and sends (K', Y) to User. $K \equiv [V^{-1}(X)]^y \bmod p, Y = V(g^y \bmod p), K' = H(K, X, Y, ID_{User})$, where K will be used to generate a shared session key, Y is for key-exchange, and K' is for checking the validity of K.
   (c) User computes $K \equiv [V^{-1}(Y)]^x \bmod p$ and checks $H(K, X, Y, ID_{User}) = K'$. If User will be sure that Server knows V.
2. If User succeeds in the simplified EKE, she gets a key K. Otherwise, aborts.
3. User computes a witness number B using c, r and her knowledge of password and sends it to server. c, the question number must be computed by $c = h(K, A, X)$, where $|c|$, the size of c determines the security level.
4. Server verifies user's response(the witness number) with A, V, c. If matches, Server authenticates her.
5. After the completion of the protocol, a shared key is now $SK = H(K, X, Y, ID_{User}, A, B)$.

Note that A, the test number is sent in the simplified EKE stage. Thus, it is not possible to predict c when she decides her test number A. Also, there is a trade-off between performance and security because of $|c|$. If $|c|$ is large, the security level is high but more computations are needed.

IV. Conclusion

We extend availability of ZKIP into the password-based authentication protocol area. The idea presented here is a framework and can be applied to many existing/upcoming ZKIP-based identification scheme such as [2, 3, 4]. More efficient protocol instead of the simplified EKE can be designed and replaced. Resulting protocol enjoys not only all the features of underlying ZKIP, but also the convenience of password.

References

[1] S. Bellovin and M. Merrit, "Encrypted key exchange: password based protocols secure against dictionary attacks," *IEEE Comp. Society Symp. on Research in Security and Privacy*, pp.72–84, 1992.

[2] U. Feige, A. Fiat and A. Shamir, "Zero-knowledge proofs of identity," *Journal of Cryptology*, vol. 1, No. 2, pp. 77–94, 1988.

[3] L.C. Guillou and J.J. Quisquater, "Protocol fitted to security microprocessor minimizing both transmission and memory," *Advances in Cryptology : Proceedings of EuroCrypt 88,LNCS*, Springer-Verlag, pp. 123–128, 1988.

[4] C.P. Schnorr, "Efficient Identification and Signatures for Smart cards," *Advances in Cryptology : Proceedings of Crypto 89, LNCS*, Springer-Verlag, pp. 239–251, 1989.

0-7803-7123-2/01/$10.00 ©2001 IEEE