PASSWORD AUTHENTICATED KEY EXCHANGE: FROM TWO PARTY METHODS TO GROUP SCHEMES

STEPHEN MELCZER, TARAS MYCHASKIW AND YI ZHANG

Abstract. This project investigates group password authenticated key exchange methods (GPAKEs). In particular, we detail the so-called 'fairy ring dance' method recently described by Hao et. al. [4] which allows for the extension of two party password authenticated key exchange methods (PAKEs) with explicit key confirmation to a group setting with an arbitrary number of users without increasing round complexity (the computational complexity, of course, increases with the number of users). This paper presents two new GPAKEs constructed through these means, based on the Dragonfly and PPK two party protocols, and includes timings comparing them to previous GPAKEs of Hao et. al. [4].

1. Introduction

Since their introduction in the 1990s, password-authenticated key exchange (PAKE) methods – also known as password-authenticated key agreement methods – have become popular for their ability to allow agents sharing a (typically low entropy) password to securely establish shared cryptographic keys (see Bellovin and Merritt [1] or Jablon [6] for early examples, and Hao and Ryan [3] for a more recent paper). Although they have been around for decades, most research on PAKEs has focused on key establishment between two parities. For our project, we have studied the problem of establishing Group PAKEs (GPAKEs) – that is, using a low entropy password shared between many agents to set up cryptographic keys. This has modern application with the rise of the so-called 'Internet of Things', where many consumer devices connected through a local Internet connection wish to securely communicate (such schemes would allow, for instance, secure communication between a smart television, DVD player, and cable box after their owner inputs a short shared password into each upon purchase).

The major issue in designing an efficient GPAKE is to minimize the number of rounds of communication between the agents involved, as the latency of such a protocal is determined by the slowest responder in each round. A recent pre-print of Hao et. al. [4] proposes a construction which allows for the extension of any two-party PAKE with explicit key confirmation to a multi-party PAKE without adding any extra rounds of communication. The authors continue on to give two explicit schemes following from this template: SPEKE+ (using two rounds of communication, adapted from the SPEKE [6] protocol) and J-PAKE+ (using three rounds of communication, adapted from the J-PAKE [3] protocol).

The structure of this document is as follows: Section 2 begins by giving a survey of classical two-party PAKEs – including explicit descriptions of the PAKEs which will be extended into the group setting and background information on the zero knowledge proof protocols these use. Section 3 starts with a description of theoretical methodology developed by Hao et. al. [4] to extend two-party PAKEs into a group setting. After this theoretical background, we give two explicit GPAKEs (SPEKE+ and J-PAKE+) constructed by Hao et. al. using this methodology, followed by two explicit GPAKEs which we have derived through the same means (a group variant of the IEEE 802.11-2012 standard Dragonfly protocol [5], and a variant of the PPK protocol [2]); the security of these new GPAKEs will be proven using realistic attack models. In Section 4 we test the practical efficacy of our new methods against the Java implementations of SPEKE+ and J-PAKE+ given by Hao et. al. [4]. Section 5 concludes with an overview of these results and possible directions for future work.

The main original contributions found in this project come from the two new group PAKEs we have constructed (see sub-Sections 2.4 and 2.5), including the proofs of their security and timings to compare against SPEKE+ and J-PAKE+. We have also fleshed out the security proofs of SPEKE+ and J-PAKE+, include the relevant background material on Zero Knowledge Proofs needed to explicitly specify all aspects of these protocols, and fixed some minor Java implementation errors which could cause the timings in Hao et. al. [4] to be slightly inaccurate.

2. Two Party Password-Authenticated Key Exchange (PAKE)

The genesis of password-authenticated key exchange is widely credited to the 1992 work of Bellovin and Merrit [1], whose protocol (known as Encrypted Key Exchange – or EKE, for short) came to be known as the first PAKE. All PAKEs aim for two main goals: to require their users to provide a zero knowledge proof of a short password known to both parties *a priori* (that is, before the protocol has begun) and to leverage knowledge of this password to fasciltate an authenticated key exchange. As password are assumed to be low entropy – for instance, they are often assumed to be human memorizable passwords (the literature refers to assumptions of approximately 20-30 bits of entropy) – if the passwords themselves were broadcast they would need to be protected, for instance using SSL. This would require Public Key Infrastructure, which can be expensive, hence the use of zero knowledge proofs.

Indeed, it is somewhat miraculous that PAKEs – which transform a low entropy shared secret into a much larger and more complicated shared key – exist at all. Although the EKE protocol of

2.1. **Zero-Knowledge Proof Protocols.** Info about Schnorr and XXX

2.2. **EKE.** Info about EKE

2.3. **SPEKE.** Info about SPEKE

2.4. **Dragonfly.** Info about Dragonfly

2.5. **PPK.** Info about PPK

3. Group Password-Authenticated Key Exchange (GPAKE)

Background info from paper

3.1. **SPEKE+ and J-PAKE+.** Info about SPEKE+ and J-PAKE+

3.2. **Dragonfly+.** Our extensions of Dragonfly (and others?)

3.3. **PPK+.** Our extension of PPK

4. Implementation Results

Our implementation results

5. Conclusion

The conclusion

References

[1] S. M. Bellovin and M. Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *Research in Security and Privacy, 1992. Proceedings., 1992 IEEE Computer Society Symposium on*, pages 72–84. IEEE, 1992.

[2] V. Boyko, P. MacKenzie, and S. Patel. Provably secure password-authenticated key exchange using diffie-hellman. In *LNCS 1807,Springer-Verlag, Berlin*, pages 156–171. Eurocrypt 2000, 2000.

[3] F. Hao and P. Ryan. J-PAKE: Authenticated key exchange without PKI. *Transactions on Computational Science XI, Lecture Notes in Computer Science*, 6480:192–206, 2010.

[4] F. Hao, X. Yi, L. Chen, and S. F. Shahandashti. The fairy-ring dance: Password authenticated key exchange in a group. Cryptology ePrint Archive, Report 2015/080, 2015. http://eprint.iacr.org/2015/080.

[5] D. Harkins. Dragonfly key exchange – internet research task force internet draft, 2015. http://datatracker.ietf.org/doc/draft-irtf-cfrg-dragonfly/?include_text=1.

[6] D. P. Jablon. Strong password-only authenticated key exchange. *ACM Computer Communication Review*, 26(5):5–26, 1996.