Rationale for Inclusion of J-PAKE in ISO/IEC 11770-4

Feng Hao
School of Computing Science
Newcastle University, UK
feng.hao@ncl.ac.uk

16 Feb, 2014

1 ISO/IEC 11770-4

ISO/IEC 11770-4:2006 (incorporating corrigendum September 2009) specifies "mechanisms based on weak secrets" according to the following three categories:

1. Balanced password-authenticated key agreement;
2. Augmented password-authenticated key agreement;
3. Password-authenticated key retrieval.

Currently in ISO/IEC 11770-4, the first category includes SPEKE (both the DL and EC settings). The second category includes SRP-6 (the DL setting only) and AMP (both the DL and EC settings). The third category includes PKRS-1 (both the DL and EC settings).

2 Proposal and rationale

This document proposes to include J-PAKE (both the DL and EC settings) into the first category in ISO/IEC 11770-4. Reasons for supporting the inclusion of an additional balanced password-authenticated key agreement protocol, alongside of the existing SPEKE protocol, are the following.

1. J-PAKE is not encumbered by patents while SPEKE is.
2. J-PAKE has been proved secure under the Decisional Diffie-Hellman (DDH) assumption in the random oracle model [2]. The original SPEKE paper has no security proofs. However, in an IACR ePrint manuscript [3], it has been reported that SPEKE can be proved secure under a new Decision Inverted-Additive Diffie-Hellman (DIADH) assumption in the random oracle model. In terms of proofs, J-PAKE has two theoretical advantages

over SPEKE. First, the DDH assumption is more standard than the DI-ADH assumption, and has been more widely studied. Second, the J-PAKE proofs [2] strictly limit an on-line attacker to guess exactly one password in one impersonation attempt, which is the best possible scenario against on-line dictionary attacks. By contrast, the SPEKE proofs [3] allow an on-line attacker to guess multiple passwords in one impersonation attempt using the SPEKE protocol.

3. J-PAKE is more flexible than SPEKE in the implementation in the DL setting. For security reasons, SPEKE is normally implemented in a prime field $GF(p)$ where p is limited to a "safe" prime. J-PAKE has no such restrictions. Without any change to the protocol, J-PAKE generically works in any multiplicative groups that are suitable for cryptography (including the DSA-like group).

4. J-PAKE is more suitable than SPEKE for an EC implementation. Unlike SPEKE, J-PAKE does not require any extra hashing-to-curve primitive, i.e., I2P function in ISO/IEC 11770-4. (Implementing an I2P function securely and efficiently without leaking side-channel timing information about the password secret is a non-trivial task.) Without any change to the protocol, J-PAKE generically works in any EC groups that are suitable for cryptography (including the ECDSA-like group).

5. J-PAKE has been included into a number of open source libraries, including OpenSSL, Mozilla Network Security Services (NSS) and Bouncy castle (version 1.48 and onwards).

6. Since 2010, J-PAKE has been integrated into the Firefox browser (version 4 and onwards) to implement the secure sync service. Over the past three years, it has been used by millions of Firefox users to securely synchronize the user profile data between different computers.

3 More background on J-PAKE

The J-PAKE protocol was initially presented at SPW'08 [1]. It was then submitted to IEEE P1363.2 and published on the official IEEE standards website as one of the IEEE P1363 research contributions [4]. (However, in 2008, IEEE P1362.2 had reached the maximum allowed 8 years for a standardization project and hence could no longer accept new PAKE protocols into the P1363.2 draft.) A journal version of the J-PAKE paper was published by *Springer Transactions on Computational Science* in 2010 [2].

Since the first presentation of J-PAKE at SPW'08, a blog [5] was written on the Cambridge Research Blog to invite public scrutiny on the protocol and its security proofs. To date, no attacks has been found. The full track records of discussions and comments on J-PAKE over the past 6 years are publicly visible at the Cambridge Research Blog [5], which also includes links to Java prototype implementations of J-PAKE in both the DL and EC settings.

References

[1] Feng Hao, Peter Ryan, "Password Authenticated Key Exchange by Juggling," Proceedings of the 16th Workshop on Security Protocols (SPW'08), Cambridge, UK, LNCS 6615, pp. 172-179, 2008. Available at: `http://grouper.ieee.org/groups/1363/Research/contributions/hao-ryan-2008.pdf`.

[2] Feng Hao, Peter Ryan, "J-PAKE: Authenticated Key Exchange Without PKI," *Springer Transactions on Computational Science XI*, LNCS 6480, pp. 192-206, 2010. Available at: `http://eprint.iacr.org/2010/190.pdf`

[3] Philip MacKenzie, "On the Security of the SPEKE Password-Authenticated Key Exchange Protocol," Cryptology ePrint Archive: Report 2001/057. Available at: `http://eprint.iacr.org/2001/057`.

[4] J-PAKE listed as one of the IEEE P1363 Research Contributions. Available at `http://grouper.ieee.org/groups/1363/Research/Schemes.html#HR08`

[5] Light Blue Touchpaper Blog on J-PAKE. Available at `http://www.lightbluetouchpaper.org/2008/05/29/j-pake/`