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

Feng Hao
Newcastle University, UK

ISO/IEC WG2 meeting
Hong Kong, 8 Apr 2014

Background on PAKE

Private and authenticated channel?

Enter code: 432

10–bit

No Public Key Infrastructure

Enter code: 432

10–bit

To establish a high-entropy session key from a low-entropy secret without any trusted third party

Brief review of PAKE

- EKE (1992)
  - Using the password as a symmetric encryption key
- SPEKE (1996)
  - Hiding the password in the generator
- SRP-6 (1998)
  - A variant of EKE
- J-PAKE (2008)
  - Hiding the password in the exponent

Current status in ISO/IEC

- Three PAKE protocols in ISO/IEC 11770-4
  - SPEKE (balanced PAKE)
  - SRP-6, AMP (augmented PAKE)
- Our proposal
  - Add another balanced PAKE: J-PAKE
  - Will compare J-PAKE with SPEKE

1. Patent

- SPEKE is patented (until 2017)
- J-PAKE is not patented
  - It follows a completely different design approach
  - Essence of the solution comes from the juggling technique invented in 2006 to solve the Dining Cryptographers' Problem (Hao-Zielinski, SPW'06)

2. Security proofs

- Original SPEKE paper has no security proofs
- In an unpublished manuscript (IACR 2001/057)
  - SPEKE is proved secure under the DIADH assumption in the random oracle model with a relaxed security definition
- J-PAKE is proved secure under the DDH assumption in the random oracle model with a strict security definition

3. Implementation in DL setting

- SPEKE usually requires to use a safe prime
  - However, this limits the choice of groups
  - Also, not efficient due to long exponent

- J-PAKE has no such restriction
  - Flexible to implement in groups with short exponents (e.g., DSA-group)

4. Implementation in EC setting

- SPEKE requires an extra function to hash passwords onto random points on curve
  - That is the i2p function in ISO/IEC
  - However, implementing i2p is non-trivial

- J-PAKE requires no such hashing
  - Flexible to implement in any EC setting (e.g., ECDSA-group)

5. Adoption in the real-world

- Included into open source libraries
  - OpenSSL (2008), NSS (2010), Bouncycastle (2013)
- Real-world application
  - Firefox sync (since 2010)

Summary of Rationale

1. J-PAKE is not patented, while SPEKE is;
2. J-PAKE has theoretical advantages than SPEKE in terms of security proofs;
3. J-PAKE has practical advantages in terms of implementation in both DL and EC settings;
4. J-PAKE has already been used in practice by millions of users in the past three years.

More information about J-PAKE

- Initial publication of J-PAKE at SPW'08
  - Also available at http://grouper.ieee.org/groups/1363/Research/contributions/hao-ryan-2008.pdf
- Full discussion track records since 2008
  - Cambridge Security Research blog http://www.lightbluetouchpaper.org/2008/05/29/j-pake/
- To date, no attacks have been found

Thank you