Status of PAKE selection process

Stanislav V. Smyshlyaev, Ph.D.
CFRG Secretary

CFRG
IETF 105, July 2019, Montreal
After receiving several PAKE proposals and seeing documents complete, the chairs want to announce PAKE selection process. The aim is to select one or more ("zero or more") PAKEs to recommend to the wider IETF community.

Submissions to satisfy RFC 8125, Requirements for PAKE Schemes.

Both balanced (both sides store the same representation of password) and augmented (one side maintains a transform of the password and the other maintains the raw password) PAKEs are considered.

Better to select one without a variety of options.

Involving Crypto Review Panel to come up with recommendations.

Support of the process at the CFRG session ("and please do it soon") and later at the TLS and IPSECME sessions.
Plan and timeline (1)

Stage 1, 01.06.2019-30.06.2019
- Call for candidate protocols.
- Discussing the list of questions to be asked.

Stage 2, 01.07.2019-19.07.2019
- The designers of the protocols prepare papers with responses for:
  - all positions of RFC 8125;
  - additional questions selected at Stage 1.
## Plan and timeline (2)

<table>
<thead>
<tr>
<th>Stage 3, 01.08.2019-15.08.2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call for reviewers for the enumerated questions.</td>
</tr>
<tr>
<td>Crypto Review Panel members start the process of verification of security proofs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stage 4, 16.08.2019-15.09.2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>The reviewers prepare their analysis.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stage 5, 16.09.2019-30.10.2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>Crypto Review Panel members review all gathered materials, prepare the final list of verified answers, write overall reviews for all candidate PAKEs.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Stage 6, 01.11.2019-16.11.2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFRG chairs discuss the reviews and make recommendations.</td>
</tr>
</tbody>
</table>
Plan and timeline (3)

IETF 106 meeting

- The chairs give a review of the progress.
- If everything is clear:
  - zero (or more) PAKEs are selected;
  - initiate a CFRG document „Recommendations for password-based authenticated key establishment in IETF protocols“, reflecting the results and practically important recommendations;
  - documents on usage of the selected PAKEs in TLS/IPsec/etc. can be developed.
Results of Stage 1: nominations

We’ve obtained the following nominations:

- **Balanced:**
  - SPAKE2 (nominated by Watson Ladd and Benjamin Kaduk)
  - J-PAKE (nominated by Feng Hao)
  - SPEKE (nominated by Dan Harkins)
  - CPace (nominated by Björn Haase)

- **Augmented:**
  - OPAQUE (nominated by Hugo Krawczyk)
  - AuCPace (nominated by Björn Haase)
  - VTBPEKE (nominated by Guilin Wang)
  - BSPAKE (nominated by Steve Thomas)
Results of Stage 1: additional questions

The following list of questions was formed.

- How does it meet the “SHOULD” requirements of RFC 8125?
- Does it meet „crypto agility“ requirements, not fixing any particular primitives and/or parameters?
- What setting is the PAKE suitable for? Applications?
  - “Peer communication” or “client-server”?
  - Which use-cases is the protocol recommended for?
  - Can two communicating parties initiate the key exchange process?
  - Is it suitable to be considered as a standalone (i.e., without integration into any existing cryptographic protocol) scheme?
  - Can it be integrated into IKEv2? TLS Handshake?
- Performance assessment.
  - “Round efficiency” of the PAKE?
  - How many operations of each type (scalar multiplications, inversions in finite fields, hash calculations etc.) are made by each side?
Results of Stage 1: additional questions

- Is there a publicly available security proof? If yes,
  - Known problems with the proof?
  - Is the considered security model relevant for all applications that PAKE is intended for?
  - Sufficient level of security for common values of password lengths?
- Security assessment.
  - Does its security depend on nontrivial implementation properties?
  - Precomputation security (for augmented PAKEs)?
  - If the PAKE relies on the assumption of a trusted setup: the security implications (and mitigation measures) if the discrete logarithm relationship becomes known.
- Which recommendations for secure usage can be given?
  - Explicit key confirmation performed or must be performed externally? Optional or mandatory?
  - Recommendations on using iterated hashing (e.g., with Scrypt)?
  - Recommendations to avoid a user enumeration attack?
Results of Stage 2

On Stage 2, the authors had to provide:

- a. responses for the positions of RFC 8125 regarding their PAKEs;
  - R1: balanced/augmented.
  - R2: security proof.
  - R3: recommendations for protection in hostile environments.
  - R4: for ECC: mappings to be used.
  - R5: optimization goals.
  - R6: comments on special application scenarios.
  - R7: privacy considerations.
  - R8: status with respect to patents.

- b. their own opinions on the questions collected at Stage 1.
Current status

Results of Stage 2: received responses

We’ve obtained the complete lists of responses for all of the nominations:

- **Balanced:**
  - SPAKE2 (Watson Ladd)
  - J-PAKE (Feng Hao)
  - SPEKE (Dan Harkins)
  - CPace (Björn Haase)

- **Augmented:**
  - OPAQUE (Hugo Krawczyk)
  - AuCPace (Björn Haase)
  - VTBPEKE (Guilin Wang)
  - BSPAKE (Steve Thomas)
What’s next?

Stage 3, 01.08.2019-15.08.2019
- Call for reviewers for the enumerated questions.
- Crypto Review Panel members start their security analysis.

Stage 4, 16.08.2019-15.09.2019
- The reviewers who volunteered at Stage 3 prepare their analysis.
- Crypto Review Panel members prepare their security reviews.

Stage 5, 16.09.2019-30.10.2019
- Crypto Review Panel members review all gathered materials and write overall reviews for all candidate PAKEs.

Stage 6, 01.11.2019-16.11.2019
- CFRG chairs discuss the reviews and make recommendations.
Call for reviewers

The questions which should be considered by independent reviewers before asking the Crypto Review Panel for overall reviews:

- Is it convenient for usage within/together with TLS 1.3 Handshake (taking into account all discussions about possible additional extensions, slides by Björn Haase, etc.)?
- Is it convenient for usage within/together with IKEv2?
- Is the computational complexity of the PAKE suitable for M2M/IoT (i.e., with corresponding limitations of hardware)?
- Is the “Round efficiency” of the PAKE OK for a protocol for M2M/IoT?
- Is it convenient for integration in existing protocols in M2M/IoT?
- Privacy considerations (e.g., recommendations to prevent user enumeration).
Call for reviewers

The questions which should be considered by independent reviewers before asking the Crypto Review Panel for overall reviews:

- Is it convenient for usage within/together with TLS 1.3 Handshake (taking into account all discussions about possible additional extensions, slides by Björn Haase, etc.)?
- Is it convenient for usage within/together with IKEv2?
- Is the computational complexity of the PAKE suitable for M2M/IoT (i.e., with corresponding limitations of hardware)?
- Is the “Round efficiency” of the PAKE OK for a protocol for M2M/IoT?
- Is it convenient for integration in existing protocols in M2M/IoT?
- Privacy considerations (e.g., recommendations to prevent user enumeration).
Call for reviewers

The questions which should be considered by independent reviewers before asking the Crypto Review Panel for overall reviews:

- Is it convenient for usage within/together with TLS 1.3 Handshake (taking into account all discussions about possible additional extensions, slides by Björn Haase, etc.)?
- Is it convenient for usage within/together with IKEv2?
- Is the computational complexity of the PAKE suitable for M2M/IoT (i.e., with corresponding limitations of hardware)?
- Is the “Round efficiency” of the PAKE OK for a protocol for M2M/IoT?
- Is it convenient for integration in existing protocols in M2M/IoT?
- Privacy considerations (e.g., recommendations to prevent user enumeration).
Thank you for your attention!

Questions?

Volunteers for preparing independent reviews?

cfrg-chairs@ietf.org
Backup slides
What's next?

- **R1:** A PAKE scheme MUST clearly state its features regarding balanced/augmented versions.
- **R2:** A PAKE scheme SHOULD come with a security proof and clearly state its assumptions and models.
- **R3:** The authors SHOULD show how to protect an implementation of their PAKE scheme in hostile environments, particularly, how to implement their scheme in constant time to prevent timing attacks.
- **R4:** In case the PAKE scheme is intended to be used with ECC, the authors SHOULD discuss their requirements for a potential mapping or define a mapping to be used with the scheme.
- **R5:** A PAKE scheme MAY discuss its design choice with regard to performance, i.e., its optimization goals.
- **R6:** The authors of a scheme MAY discuss variations of their scheme that allow the use in special application scenarios. In particular, techniques that allow agreeing on a long-term (public) key are encouraged.
- **R7:** A scheme MAY discuss special ideas and solutions on privacy protection of its users.
- **R8:** The authors of an MUFTE scheme MAY declare the status of their patent.
Further steps after we select one (or more)

- Selection for usage in IETF protocols is not the same as selection of one PAKE for usage “by itself”.
- Recommendations for usage in protocols should be given (e.g., key confirmation, handling the counters of failed attempts of authentication, handling errors, etc.).
- If we create a new CFRG document (RFC on one or more PAKEs with additional blessing(s) from CFRG? “Recommendations for usage of PAKEs in IETF protocols”?), the recommendations should be given there.
- Recommendations for generation of parameters should be given: e.g., SPAKE, SESPAKE and PKEX need that the discrete logarithms of the public role-specific elements are unknown, and determining them is computationally infeasible.
What’s next?

Possible usage of PAKEs: TLS, IPsec, messengers, IoT etc.
One PAKE for all applications? Or distinct sets of requirements?

Examples

1. An augmented (and secure against attacks involving precomputations) PAKE is good for client-server protocols — but may be redundant for one-to-one communications (messengers? Wi-Fi DPP?).

2. Explicit key confirmation stage may be good for usage a PAKE „by itself“, but may be redundant for usage in IKEv2 and TLS Handshake.
“Usage of PAKE with TLS 1.3”, draft-barnes-tls-pake-04

For usage with TLS 1.3 PAKE must be:

- Possible to execute in one round-trip, with the client speaking first.
- The Finished MAC must provide sufficient key confirmation for the protocol, taking into account the contents of the handshake messages.
- Providing forward secrecy.

Examples: SPAKE+, SPEKE, DragonFly, OPAQUE, SRP.

- For key establishment in messengers?
- For M2M/IoT?
- ...