Status of PAKE selection process

Stanislav V. Smyshlyaev, Ph.D.
CFRG Secretary

CFRG
IETF 106, November 2019, Singapore

PAKE selection process: history

IETF 103

- 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

Results of Stages 1 & 2

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.

Results of Stages 1 & 2: nominations, questions, responses

After Stage 2 we had the candidates, the additional questions and the responses (RFC 8125 and the collected questions) for all candidates.

- Balanced:
  - SPAKE2 (nominated by Watson Ladd and Ben 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 3

Stage 3, 01.08.2019-15.08.2019

- Call for reviewers for the enumerated questions.
- Crypto Review Panel members start their security analysis.

Stage 3: Call for reviewers

There was a call for independent reviewers regarding the questions to be considered before asking the Crypto Review Panel for overall reviews:

- Is it convenient for usage within/together with TLS 1.3 Handshake?
- Is it convenient for usage within/together with IKEv2?
- Is it convenient (computational complexity, round efficiency, etc.) of the PAKE suitable for M2M/IoT?
- Other applications of PAKEs – comparative analysis for them.
- Security review.

- IPsec:
  - Yoav Nir: all 8 PAKEs
  - Valery Smyslov: all 8 PAKEs
- TLS:
  - Thyla van der Merwe, JC Jones, Martin Thomson, Kevin Jacobs: all 8 PAKEs
  - Karthik Bhargavan: 4 balanced PAKEs
  - Jonathan Hoyland: 4 augmented PAKEs
- IoT use cases:
  - David Gotrik: all 8 PAKEs
- Other:
  - Steve Thomas: 4 augmeted PAKEs
  - Kevin Lewi: 4 augmented PAKEs
  - Brian Warner: 4 balanced PAKEs
  - Bill Cox: 1 augmented PAKE
- Security proofs:
  - Bjoern Tackmann: 4 augmented PAKEs
  - Scott Fluhrer: 4 balanced PAKEs
  - Tibor Jager: 4 augmented PAKEs
  - Stanislav Smyshlyaev: 4 balanced PAKEs

Results of Stage 4

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.

At the end of Stage 4 we obtained 14 great reviews, deeply studying various aspects of PAKEs.

All of them were collected at https://github.com/cfrg/pake-selection.

Many thanks to Yaron Sheffer for organizing the PAKE selection GitHub repository!

Results of Stage 5

Stage 5, 16.09.2019-30.10.2019

- Crypto Review Panel members review all gathered materials and write overall reviews for all candidate PAKEs.

At the end of Stage 5 we obtained 4 overall reviews of the Crypto Review Panel members:

- Bjoern Tackmann
- Russ Housley
- Yaron Sheffer
- Stanislav Smyshlyaev

All of them are available at https://github.com/cfrg/pake-selection.

TL;DR's of the Crypto Review Panel reviews

1. Bjoern Tackmann: „As balanced scheme, CPACE seems best, with SPAKE2 coming in somewhat close second. As augmented scheme, I think that OPAQUE should be considered for its possible seamless integration with TLS. As a general aPAKE, I have a slight preference for the strong AuCPace variant."
2. Russ Housley: „OPAQUE"
3. Yaron Sheffer: „I think the Research Group should recommend one balanced and one augmented algorithm. [...] Of the balanced algorithms, I would recommend CPace. Of the augmented algorithms, I will follow the Mozilla report and recommend OPAQUE, which appears to be the best fit into TLS, and is also a good fit into IKEv2."
4. Stanislav Smyshlyaev: „I would recommend selecting two PAKEs (one balanced and one augmented): SPAKE2 and OPAQUE. No strong objections against: CPace, AuCPace, VTBPEKE"

Results of Stage 6

Stage 6, 01.11.2019-16.11.2019

- CFRG chairs discuss the reviews and make recommendations.

- Since the opinions of the reviewers were not unanimous and since some new questions were raised during the final stages of the first round of the PAKE selection process, we move to the Round 2 of the selection process.
- There are 4 candidates left for Round 2:
  - SPAKE2 (balanced) — nominated by Watson Ladd and Ben Kaduk
  - CPace (balanced) — nominated by Bjoern Haase
  - OPAQUE (augmented) — nominated by Hugo Krawczyk
  - AuCPace (augmented) — nominated by Björn Haase

Balanced/augmented

- There was a reasonable amount of desire in reviews to have both a balanced PAKE and an augmented PAKE.
- So the intention of Round 2 is to select one (or zero) balanced PAKE and one (or zero) augmented PAKE, allocating two categories.

2+2 candidates

- Balanced:
  - SPAKE2
  - CPace
- Augmented:
  - OPAQUE
  - AuCPace

Plan and timeline of Round 2 (1)

Round 2, Stage 1, 21.11.2019-05.12.2019

Additional questions for all four candidates are collected from CFRG participants (and Crypto Review Panel Members). The questions can be of the following two possible types:

- Requests for clarifications for the candidate protocols or their proposed modifications (e.g., security of CPace and AuCPace without negotiation of sid, security and convenient of SPAKE2 with a hash2curve function used to obtain M and N for each pair of identifiers).
- Questions to be taken into account in addition to ones collected at Stage 1 of Round 1 (e.g., quantum annoyance, post-quantum preparedness).

The questions should be sent to crypto-panel@irtf.org.

Plan and timeline of Round 2 (2)

Round 2, Stage 2, 10.12.2019-17.12.2019

A list of new questions is published on https://github.com/cfrg/pake-selection.
The CFRG is asked if anything else should be added.

Round 2, Stage 3, 25.12.2019-10.02.2020

The authors of the candidates prepare their replies to the additional questions/requested clarifications.

Round 2, Stage 4, 12.02.2020-10.03.2020

Crypto Review Panel members prepare new overall reviews (for all 4 remaining PAKEs) taking into account both the reviews obtained on Round 1 and new information obtained during Stage 3 of Round 2.

Plan and timeline of Round 2 (3)

Round 2, Stage 5, 12.03.2020-21.03.2020

CFRG chairs discuss the reviews and make recommendations.

IETF 107 meeting

- The chairs give a review of the progress.
- If everything is clear:
  - one (or zero) balanced PAKE is selected;
  - one (or zero) augmented PAKE is selected;
  - initiate a CFRG document „Recommendations for password-based authenticated key establishment in IETF protocols“, reflecting the results and practically important recommendations.

Actions after the PAKE selection process is over

Yaron Sheffer: „Whatever protocols are selected, CFRG must make it clear that such selection is conditional on the algorithms being republished in a detailed format. CFRG must not leave this task to the IETF WGs, because that would both duplicate work and introduce a major risk of inadvertent errors that invariably manifest themselves as vulnerabilities. I would propose that each of the selected protocols be published as an RFC, containing:

- A detailed description of the protocol, to a level that can be implemented by developers who are not security experts.
- Test vectors to ensure interoperability.
- Recommendations on integrating with higher-level protocols:
  - supported identity fields and recommendations on how they should be protected, session ID and „exporter“ integration, secure capability and parameter negotiation, conditions on whether and how „optional“ protocol exchanges can be eliminated.
  - Mandated auxiliary primitives, such as hash-to-curve and memory-hard iterated hashing.“

Actions after the PAKE selection process is over

After the process is over, it looks reasonable to initiate a CFRG document „Recommendations for password-based authenticated key establishment in IETF protocols“.

- A detailed description of the PAKE(s).
- Recommendations for generation of parameters.
- Mandated auxiliary primitives.
- Test vectors.
- Guidelines for integrating into protocols:
  - on which step to negotiate PAKE parameters
  - how cross-cipher suite security should be taken into account
  - supported identity fields and recommendations on their protection
  - whether and how „optional“ protocol exchanges can be eliminated
  - required additional key confirmation steps
  - handling the counters of failed attempts of authentication
  - ...

What's now?

Round 2, Stage 1, 21.11.2019-05.12.2019

Additional questions for all four candidates are collected from CFRG participants (and Crypto Review Panel Members). The questions can be of the following two possible types:

- Requests for clarifications for the candidate protocols or their proposed modifications (e.g., security of CPace and AuCPace without negotiation of sid, security and convenient of SPAKE2 with a hash2curve function used to obtain M and N for each pair of identifiers).
- Questions to be taken into account in addition to ones collected at Stage 1 of Round 1 (e.g., quantum annoyance, post-quantum preparedness).

The questions should be sent to crypto-panel@irtf.org.

Thank you for your attention!

Questions?

- crypto-panel@irtf.org
- cfrg-chairs@ietf.org