Noise Test Vector Format

Alex Wied (alex@centromere.net)
Rhys Weatherley (rhys.weatherley@gmail.com)

Revision 1, 2017-11-21, unofficial/unstable

Contents

1. Introduction

The purpose of this document is to specify the format and semantics of test vectors for Noise.

2. Overview

Test vectors are represented as JSON but with an extra set of restrictions. The rationale for this is:

- Some embedded systems may not have JSON tools available.
- It is more human readable.

More details about the rationale can be found on the mailing list[1].

3. Format

Vectors are valid JSON and must be formatted exactly as follows:

```
{
"vectors": [
{
"name": "<free form description of handshake>",
"protocol_name": "<any valid handshake pattern name>",
"fail": false|true,
"fallback": false|true,
"fallback_pattern": "<any valid handshake pattern name>",
"init_prologue": "hex string",
"init_psks": ["hex string", ...]
"init_static": "hex string",
"init_ephemeral": "hex string",
"init_remote_static": "hex string",
"resp_prologue": "hex string",
"resp_psks": ["hex string", ...]
"resp_static": "hex string",
"resp_ephemeral": "hex string",
"resp_remote_static": "hex string",
"handshake_hash": "hex string",
"messages": [
{
"payload": "hex string",
"ciphertext": "hex string"
}, ...
]
}, ...
]
}
```

4. Semantics

The following keys are optional:

- `name`
- `fail`
- `init_*` and `resp_*` (*except* the prologues)
- `handshake_hash`
- `fallback` (used for testing Noise Pipes, described below, defaults to `false`)
- `fallback_pattern`

Optional keys may be `null` or omitted entirely. The `fail` key, if omitted, defaults to false The name key, if omitted, defaults to protocol_name. The init_psks and resp_psks keys default to an empty list if omitted. All other keys are mandatory.

PSKs are applied to the handshake in the same order specified in the vector.

The handshake_hash key specifies the expected handshake hash value for both parties at the end of a successful handshake. If fail is true and the failure occurs before the handshake is complete, then the handshake_hash value must be ignored.

The messages array describes a conversation alternating between the initiator and responder, starting with the initiator. No distinction is made between when the handshake begins and when it is complete. For example, if a handshake pattern has three messages in it, the responder will send the first non-handshake Noise message. For one-way patterns the messages simply flow from the initiator to the responder.

4.1. Noise Pipes

There are three main scenarios to test for Noise Pipes: XX for a "full handshake", IK with a successful response for an "abbreviated handshake", and IK followed by XXfallback for a "fallback handshake".

The "full handshake" and successful "abbreviated handshake" cases are tested in the same way as before because they are normal XX and IK handshake patterns.

The "fallback handshake" case requires some special handling by the test runner to deal with the transition from IK to XXfallback. This special handling is indicated in the test case by setting fallback to true. The pattern for the test case must be set to IK and init_remote_static must be a different public key than the one corresponding to resp_static, to trigger the fallback (they would normally correspond for a successful IK handshake).

The first message in the messages array is the initial IK handshake message from initiator to responder. The responder fails on this message and triggers fallback. The roles are reversed and the handshake restarts with the pattern set to XXfallback. The init_remote_static value is ignored when the handshake restarts and the init_* and resp_* fields are reversed in meaning.

The initiator's semi-ephemeral public key is carried across from IK to XXfallback. This value does not explicitly appear in the test case as an init_* or resp_* field. It is assumed that the implementation will extract the value from the first IK handshake message and pass it to the XXfallback session.

The second message in the messages array is the initial XXfallback handshake message from the former responder (now the initiator) back to the former initiator (now the responder).

The remaining messages proceed as per a normal handshake followed by data transfer.

If the fallback pattern name is not `XXfallback`, then the `fallback_pattern` key can be provided to specify an alternative pattern:

```
"fallback": true
"fallback_pattern": "XXfallback+hfs"
```

5. Example

Note: Long lines in the example below have been wrapped.

```
{
"vectors": [
{
"protocol_name": "Noise_NN_25519_AESGCM_BLAKE2b",
"init_prologue": "4a6f686e2047616c74",
"init_ephemeral": "893e28b9dc6ca8d611ab664754b8ceb7bac5117349a4439a6b0569da977c464a",
"resp_prologue": "4a6f686e2047616c74",
"resp_ephemeral": "bbdb4cdbd309f1a1f2e1456967fe288cadd6f712d65dc7b7793d5e63da6b375b",
"handshake_hash": "67b154b6ecdb34fcb837863430a4705c46c1af6e4fbcf1c7f69b324e5b841aed
                   395246bb28fc184b94198ab33dfb9d3967c13c507879431a33d0d952dd1c7eea",
"messages": [
{
"payload": "4c756477696720766f6e204d69736573",
"ciphertext": "ca35def5ae56cec33dc2036731ab14896bc4c75dbb07a61f
               879f8e3afa4c79444c756477696720766f6e204d69736573"
},
{
"payload": "4d757272617920526f746862617264",
"ciphertext": "95ebc60d2b1fa672c1f46a8aa265ef51bfe38e7ccb39ec5be34069f14480884
               30b4b427c7ab9fac9f434513fa08726db51b1b447074227725c16a35f6b37c4"
},
{
"payload": "462e20412e20486179656b",
"ciphertext": "9d37117df3063b2dd15b76ab8feb70d1a863ed48809447faffba69"
},
{
"payload": "4361726c204d656e676572",
"ciphertext": "0637f52a8c2a4fc85335e3e54ff6f354c640a748db72134abc544a"
},
{
"payload": "4a65616e2d426170746973746520536179",
"ciphertext": "6d2a593b40932c40c700d71f5e4223e0ee4401e8682bc1e9c756523f34b2354fcb"
},
{
"payload": "457567656e2042f6686d20766f6e2042617765726b",
"ciphertext": "a5c747fe5132b92fc0819925ea2e2cf6ce10f
               d2c52fa8d25a4480c71fcd0d508a8c57adf54"
}
]
}
]
}
```

6. IPR

This document is hereby placed in the public domain.

7. References

[1] T. Perrin, “Test vector format.” 2017. https://moderncrypto.org/mail-archive/noise/2016/000505.html