

Verified Time Balancing of Security Protocols

A Case Study

Student Name: Donovan Crichton
Student Number: u6881864

1 The Message Preamble

All ZRTP Messages are prefixed by a preamble, message length and message type.

- Let pr represent the message preamble $0x505a$ followed by a 16-bit message length in 32-bit words, followed by the message type 2-word block string (e.g. “hello”).

2 The Hello Messages

- Let v represent the 4-character long string containing the version of the ZRTP protocol.
- Let c represent the client identification string which identifies the vendor and release of the ZRTP software.
- Let $h3$ represent the following:
 - Let $h0$ represent a 256-bit random nonce.
 - Let $h1$ represent a hash of $h0$ with SHA-256.
 - Let $h2$ represent a hash of $h1$ with SHA-256.
 - Let $h3$ represent a hash of $h2$ with SHA-256.
- Let z represent the 96-bit long unique identifier for the ZRTP endpoint. This is a random number generated at installation time to act as a key when looking up shared secrets in a local cache.
- Let fs represent a 4-bit long sequence of flags. The leading bit is 0, the second represents a signature-capable flag, the third a MiTM flag to identify that this message was sent from a PBX. The fourth and final bit represents a passive flag which is only used on devices that send hello, but will never send commit messages.
- Let hc represent the number (count) of hashing algorithms.

- Let cc represent the number of cipher algorithms.
- Let ac represent the number of auth tag types.
- Let kc represent the number of key agreement types.
- Let sc represent the number of SAS types.
- Let hs represent the ordered set of hashing algorithms.
- Let cs represent the set of cipher algorithms.
- Let as represent the set of SRTP auth tag types.
- Let ks represent the set of key agreement types.
- Let ss represents the set of short authentication string types.
- Let m represents the machine authentication code that finishes the ZRTP message.

Alice says Hello to Bob

$alice_0(pr, v, c, h3, z, fs, hc, cc, ac, kc, sc, hs, cs, as, ks, ss, m)$

Bob receives Alice's Hello

$bob_0(pr_{a0}, v_{a0}, c_{a0}, h3_{a0}, z_{a0}, fs_{a0}, hc_{a0}, cc_{a0}, ac_{a0}, kc_{a0}, sc_{a0}, hs_{a0}, cs_{a0}, as_{a0}, ks_{a0}, ss_{a0}, m_{a0})$

Bob acknowledges Alice's hello via HelloAck

$bob_1(pr)$

Alice receives Bob's HelloAck

$alice_1(pr_{b1})$

Bob says Hello to Alice

$bob_2(pr, v, c, h3, z, fs, hc, cc, ac, kc, sc, hs, cs, as, ks, ss, m)$

Alice receives Bob's Hello

$alice_2(pr_{b2}, v_{b2}, c_{b2}, h3_{b2}, z_{b2}, fs_{b2}, hc_{a0}, cc_{b2}, ac_{b2}, kc_{b2}, sc_{b2}, hs_{b2}, cs_{b2}, as_{b2}, ks_{b2}, ss_{b2}, m_{b2})$

Alice acknowledges Bob's Hello via HelloAck

$alice_3(pr)$

Bob receives Alice's HelloAck

$bob_3(pr_{a3})$

The Commit Message

- Let ha represent the negotiated hash algorithm.
- Let ca represent the negotiated cipher algorithm.
- Let at represent the negotiated auth-tag type.
- Let kt represent the negotiated key-agreement type.
- Let st represent the negotiated short authentication string type.
- Let hvi represent the initiators hash value where:
 - Let svi represent a random number.
 - Let g represent the base.
 - Let p represent the prime modulus.
 - svi , g , and p are all functions of kt such that:
 - Let $pvi = mod(g^{svi}, p)$.
 - Let $||$ denote bitwise concatenation.
 - Let $dh2i$ represent the initiators DH Part 2 Message.
 - Let $hellor$ represent the responders Hello Message.
 - $hvi = ha(dh2i||hellor)$

Bob prepares a DH Part 2 Message

$bob_4(pr, h1, rs1i, rs2i, asi, psi, pvi, m)$

Bob sends a Commit to Alice

$bob_5(pr, h2, z, ha, ca, at, kt, st, hvi, m)$

Alice receives Bob's Commit

$alice_4(pr_{b5}, h2_{b5}, z_{b5}, ha_{b5}, ca_{b5}, at_{b5}, kt_{b5}, st_{b5}, hvi_{b5}, m_{b5})$

The DH Part 1 Message

- Let $rstr$ represent a message denoting “Responder”.
- Let $s1r$ represent the responders first shared secret if it exists, or null otherwise.
- Let $s2r$ represent the responders second shared secret if it exists, or null otherwise.
- Let $rs1r = m(s1r, rstr)$ represent the non-invertible hash of the responders first retained shared secret.
- Let $rs2r = m(s2r, rstr)$ represent the non-invertible hash of the responders second retained shared secret.
- Let $auxr$ represent the responders auxiliary shared secret.
- Let $rh3$ represent the responder H3 value.
- Let $asr = m(auxr, rh3)$ represent the non-invertible hash of the responders auxiliary shared secret.
- Let $pbxr$ represent the responders pbx shared secret.
- Let $psr = m(pbx, rstr)$ represent the non-invertible hash of the responders pbx shared secret.
- Let pvr represent the responders hash value where:
 - Let svr represent a random number.
 - Let g represent the base.
 - Let p represent the prime modulus.
 - svr , g , and p are all functions of kt such that:
 - Let $pvr = \text{mod}(g^{svr}, p)$.

Alice sends DH Part 1 to Bob

$$alice_5 = (pr, h1, rs1r, rs2r, asr, psr, pvr, m)$$

Bob receives Alice’s DH Part 1

$$bob_6 = (pr_{a5}, h1_{a5}, rs1r_{a5}, rs2r_{a5}, asr_{a5}, psr_{a5}, pvr_{a5}, m_{a5})$$

Bob checks Alice’s DH Part 1 and calculates DH Result

- if $pvr_{a5} = p_{b5}$ or $pvr_{a5} = p_{b5} - 1$ then terminate protocol. Otherwise continue:
- Let $dhr = \text{mod}(pvr_{a5}^{svi_{b5}}, p)$ represent the DH result.

The DH Part 2 Message

- Let $istr$ represent a message denoting “Initiator”.
- Let $s1$ represent the initiators first shared secret if it exists or null otherwise.
- Let $s2$ represent the initiators second shared secret if it exists or null otherwise.
- Let $rs1i = m(s1, istr)$ represent the non-invertible hash of the initiators first retained shared secret.
- Let $rs2i = m(s2, istr)$ represent the non-invertible hash of the initiators second retained shared secret.
- Let $auxi$ represent the auxiliary shared secret.
- Let $ih3$ represent the initiators H3 value.
- Let $asi = m(auxi, ih3)$ represent the non-invertible hash of the initiators auxiliary shared secret.
- Let $pbxi$ represent the pbx shared secret.
- Let $psi = m(pbx, istr)$ represent the non-invertible hash of the initiators pbx shared secret.

2.1 Bob sends DH Part 2 to Alice

$$bob_7 = bob_4$$

2.1.1 Alice receives Bob’s DH Part 2

$$alice_6(pr_{b7}, h1_{b7}, rs1i_{b7}, rs2i_{b7}, asi_{b7}, psi_{b7}, pvi_{b7}, m_{b7})$$

Alice checks Bob’s DH Part 2 and calculates DH Result

- if $pvi_{b7} = p_{a5}$ or $pvr_{b7} = p_{a5} - 1$ then terminate protocol. Otherwise continue:
- if $hash(bob_7 || alice_0) \neq hvi_{b5}$ then terminate protocol. Otherwise continue:
- Let $dhr = mod(pvr_{b7}^{svi_{a5}}, p)$ represent the DH result.