Verified Time Balancing of Security Protocols
A Case Study

Student Name: Donovan Crichton
Student Number: u6881864

A description of the ZRTP Protocol

Syntax

0.0.1 p

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

0.0.2 v

v represents the 4-character long string containing the version of the ZRTP protocol.

0.0.3 cid

cid represents the client identificationn string which identifies the vendor and release of the ZRTP software.

0.0.4 (

$h3$) $h3$ represents the following:
$h0$ representing a 256-bit random nonce.
$h1$ representing a hash of $h0$ with SHA-256.
$h2$ representing a hash of $h1$ with SHA-256.
$h3$ representing a hash of $h2$ with SHA-256.

0.0.5 (

zid) test

0.1 Messages

0.1.1 Hello

Alice says hello to Bob.

$alice_0(p, v, cid, h3, zid, flags, hashAlgs, cipherAlgs, authTags, keyAgreements, SAStypes, mac)$