The Zero-Trust Verification Protocol

by Ryan James Brooks & $REDACTED

Protocol

A verifier (holding knowledge) and a prover (holding secrets about that knowledge) must meet in a public setting. Both parties are to be provided with the same list of assertions and challenge questions in order to perform this simulation.

1. The verifier will make an assertion about a secret the prover holds.
2. The prover must decide if the assertion is TRUE or FALSE.
3. The prover must flip a coin for each assertion:
    1. If the assertion is TRUE:
        1. HEADS: 1 is truth.
        2. TAILS: 2 is truth.
    2. If the assertion is FALSE:
        1. HEADS: 2 is truth.
        2. TAILS: 1 is truth.
4. The prover must announce her truth number (1 or 2).
5. The verifier will ask the prover a question.
6. The verifier will flip his coin.
7. The verifier will ask the prover to follow his own coin flip:
    1. If the assertion is TRUE:
        1. HEADS: Choose truth.
        2. TAILS: Choose lie.
    2. If the assertion is FALSE
        1. HEADS: Choose lie.
        2. TAILS: Choose truth.
8. The prover will announce her answer.
9. Repeat steps 5-8 until all questions relating to the original assertion have been asked.

The protocol protects secrets in the following ways:

- If both parties agree that an assertion is TRUE or FALSE, both party's results will MATCH.
- If either party is in disagreement of the assertion, results will MISMATCH. This indicates that one of the two parties are being dishonest, or are mistaken.
- Because results are generated by coin flip, the verifier learns nothing after execution of this protocol. He only learns that the assertion was TRUE or FALSE.
- The verifier's coin flips will be generated by a well-known random number generator (Dyno bot) in a publicly-visible location (a Discord server), such that no-one can claim that results were predetermined and shared with both parties before execution of the protocol.
- The prover will generate a "secret" to hold for each assertion (her private coin flip). So long as she keeps this a secret, the verifier will be unable to convince the world of his assertions.

Simulator

This protocol is able simulate the same interaction independently prior to interaction with the prover. He must provide the results to a trusted third-party before speaking with the prover.

This simulator is able to 'fool' every verifier into believing that the statement is true (even if it's false), while producing a transcript that's indistinguishable from the output of a real prover. Because this protocol uses a coin flip to determine the answer to all questions, the generated output will be exactly the same for all verifiers (50% distribution of heads/tails).

To perform a simulation, the process is simple:

Follow the exact protocol above, with just a verifier, alone, answering questions on behalf of the prover in question.

Example

This example demonstrates a single question relating to a single assertion. As you can see, the prover's choices may only be determined by coin flip. As such, the only thing she could ever possibly disclose is the truth of the assertion itself – and only then to the verifier, who would be unable to convince anyone of his claims.

ASSERTION: Toehider is your favorite band. (true)
Prover's coin: HEADS (1 is truth)

QUESTION: What is your favorite Toehider song?
Verifier's coin: HEADS (choose truth)

1: "How Do Ghosts Work?" (correct choice)
2: "Who Knows What That Daemon Saw?"