Tom Berson
PARC Computer Science Lab
berson@parc.com

Background

I am interested in the uses and abuses of secrets. This interest has led me for more than thirty years through the byways of computer security and cryptography. In 1977 I earned a Ph.D. at the University of London with a thesis on dynamic recognition of hand-written characters based on a kinetic model of the human arm and fingers. It worked.

Preliminary Ideas about Human Interactive Proof

1. We are interested in exploiting differences between computer ability and human ability. But the problem is asymmetric: we want to exploit things which humans can do, but which computers can not do. Is the complementary problem, IPC (Interactive Proof of being a Computer), of any interest?

2. Computer security people have dealt with "Identification and Authentication" (I&A) issues for a long time. The general wisdom in that field is that authentication is based on one or more of three "factors":

> Something you know (*e.g.* a password) *N.B. computers now know everything*
> Something you have (*e.g.* a badge)
> Something you are (*e.g.* a fingerprint)

Are we proposing a new authentication factor

> Something you can do (*e.g.* recognize beauty)?

The intuition is that this do-ability wants to be at an upper level in some hierarchy.

3. One attractive aspect of HIP is that it might turn any of the notorious AI failures (I'm assuming you agree that AI has failed once or twice to fulfill its promises) into a raging success story. This would be sweet lemonade indeed.

4. It may be useful to formalize the proof setting and the experiments so that we can have some precision in description, analysis, and comparison. What I have in mind is something like what cryptographers have done to formalize interactive proofs. In particular, we need to bound the prover's ability (*e.g.* it cannot be a computer assisted by a human).

5. Still in the formal vein, does HIP => Turing? What other reductions can be established and proven (or disproven)?