PhonOID Protocol Class #81

Manuel Blum

ABSTRACT:

A PhonOID is a challenge-response authentication protocol for use over a phone. A good protocol has a number of properties including:

1) resistance to any chosen-challenge attack by a computationally powerful but bounded adversary who makes fewer than a dozen chosen-challenges.

2) ease of use: a human can quickly and easily authenticate himself to either a human or computer challenger.

I will describe my protocol class #81, and show that an average person (me) can use it to respond quickly and easily to challenges. Finally, through cajolery and hints, I will encourage the audience to mount a chosen challenge attack that breaks my particular instance of the general protocol.

A protocol from class #81 is the kind of protocol that one can learn in 4th and 5th grade. Once learned, it should stand one in good stead for the rest of one's life, not only for challenge-response authentication but also wherever one needs random-looking passwords.

This talk should/will be given immediately after Rachel Rue's talk. The latter shows the relative ease with which one can learn a random access random function from the 26 characters to the 10 digits. Such a function is essential for the protocol.