1046-20-1006 **Gilbert Baumslag** and **Benjamin Fine*** (fine@mail.fairfield.edu), Department of Mathematics, North Benson Road, Fairfield, CT 06824, and **Douglas Troeger**. *CHALLENGE RESPONSE PASSWORD SECURITY USING COMBINATORIAL GROUP tHEORY.* Preliminary report.

With the increased use of bank cards and internet credit card transactions there is at present more than ever a need for secure password identification. For many online purchases this is being carried out by a challenged response system accompanying the password.

In this talk we present an alternative method for challenge response password verification using combinatorial group theory. The method uses the group randomizer system which is a computer program that is a subset of MAGNUS a much larger computer algebra system designed to handle algorithmic problems in combinatorial group theory.

These group theoretic techniques have several major advantages over other challenge response systems. They permit easy two-way authentication, there is an infinite and random supply of challenge questions and each password login amounts to a one-time keypad - hence strong security. We will present two relatively simple protocols. This is part of a larger project designed to store and encode information within finitely presented groups. (Received September 13, 2008)