Simple Arithmetic for Faster, More Secure Websites

The April 8, 2011 edition of ACM TechNews:

Simple Arithmetic for Faster, More Secure Websites

AlphaGalileo (04/07/11)

Researchers from the University of Military Education and the Polytechnic Institute of Kiev have developed an approach to logins involving the concept of zero knowledge identification, which is based on a set of mathematical functions known as one-way Boolean operators. The researchers say the approach could be hundreds of thousands of times faster than conventional encryption-decryption logins and will reduce the overall computing requirements on the provider side of the system as well as make logins more secure. "The efficiency of information security algorithms is defined based on two factors: the level of security and the amount of computational resources required for the implementation of the security functions," says the University of Military Education's Nikolaos Bardis. The system give users a special function that produces an extremely large number of different results for all of its possible inputs. A set of inputs that produce a common result is selected to be the user's passwords. The advantage of the system is that an illicit user will have to try all possible password combinations before reaching the correct one. "The proposed scheme has potential use in any system where malicious users have incentives to gain illegal access and perform actions they are not entitled to," says the University of Military Education's Nikolaos Doukas.

Full article: 
http://www.alphagalileo.org/ViewItem.aspx?ItemId=100238&amp;CultureCode=en