# A massive group of Hackers from South Korea, China & the US are trying to break the LoginWall password

On April 16th 2012, LoginWall announced a global Cyber Hackathon, where the goal is to crack the unique LoginWall password. The Hackathon, which has been live online for only a few days, has already attracted hundreds of hackers from all over the world, who are trying their luck, hoping to overcome the newest challenge in the world of passwords.

The (patented) invention introduced by the LoginWall startup company constitutes a new generation in password security. It is based on a combination of the usual password characters with timing information.

Embedded time delays form an integral part of the password, and make any brute-force or other sophisticated password cracking attempts ineffective.

Password security is a well-known problem that has been around forever. A password is like a house key: you can protect your house with the best equipment, but at the end, you still need a way to enter. The same is true of passwords: no matter how many firewalls and security software programs you've added over the years, the password has always remained your point of weakness. That is, UNTIL NOW. LoginWall solves this precise problem, by creating keys that are much more unique and difficult to copy. This ensures that only the real "home owner" can enter the account.

There are a few other solutions on the market that offer relatively secure login solutions, like Tokens and fingerprint sensors, but the LoginWall advantage is that it improves the login security without using any external device. This makes LoginWall the ideal solution for all the Internet platforms available today, including smartphones, tablets and standard computers.

Netanel Raisch, LoginWall's CEO explains: "The fact that the LoginWall password uses two parameters makes it the most secure login method in the world today. While character-based passwords of any length can be tested by a brute force hacker at a blazingly fast rate using automated programs, the addition of even a single second pause between any two keys makes a brute force attack irrelevant, since it would require thousands of years to test a reasonable number of passwords that feature a time interval anywhere in the password".

The latest hacking attacks like the "Utah data breach" (http://www.computerworld.com/s/article/9225994/Utah_breach_10X_worse_than_originally_thought) happened just because standard, weak passwords were used to break into less-than-optimally-secured databases, allowing access to personal information such as usernames, passwords, email addresses and partial credit card numbers. According to LoginWall, that kind of breach simply wouldn't be possible if those sites were using the LoginWall protection and the unique LoginWall passwords.

What's wrong with today`s passwords?!

**Until today**, a password has always consisted of a combination of characters, and the advice has always been the same: *the longer the password -- the better*. Yet, a longer password is also more difficult to remember, and typing errors are frequent. A missed keystroke can cause account lockups, followed by a long and frustrating chain of actions required to restore the password and regain control of the account. More importantly, even complicated and long passwords are still vulnerable to modern brute force hacking.

In one of his interviews, Cormac Herley from Microsoft said (http://research.microsoft.com/pubs/154077/Persistence-authorcopy.pdf) - *"Passwords have proved themselves a worthy opponent: all who have attempted to* *replace them have failed. It is fair to say that little progress has been made in the last 20 years: usability has degraded significantly, while security has not improved*."

**Nowadays**, every existing password can be broken, exposing our personal information and your clients` privacy and security.

Cormac Herley from Microsoft estimates that the time spent managing complex passwords could cost U.S. businesses billions of dollars in lost productivity each year.

**Today**, according to LoginWall, it appears that a solution has been found.

**On April 23rd, after hundreds of hackers from all over the world tried to break the password, the LoginWall Hackathon came to a close. None of the hackers' attempts had succeeded.**