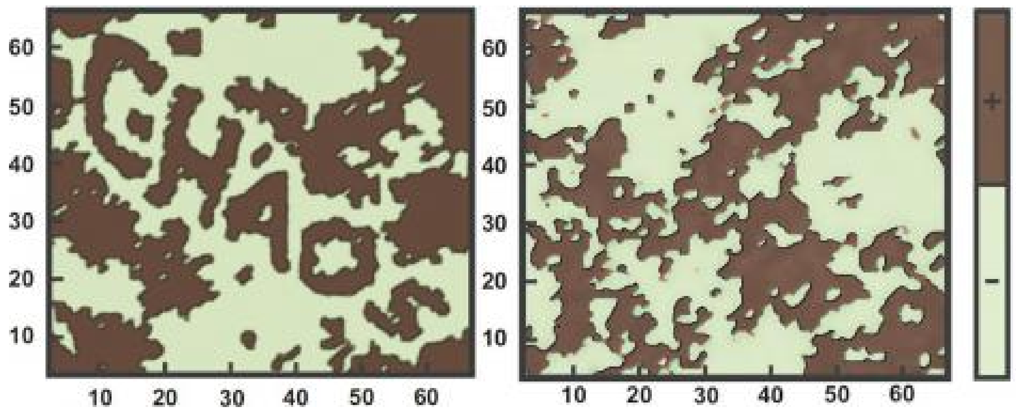
PHYS.ORG

Strong protection for weak passwords

April 19 2011



Indecipherable for computers: The Captcha with the password is very grainy, as it is generated in a physical system close to a critical change of state (left). In a chaotic process, it is made completely unreadable. The process can be reversed with an easily remembered password, however. © Sergej Flach / MPI for the Physics of Complex Systems

(PhysOrg.com) -- The combination of simple codes and Captchas, which are even more encrypted using a chaotic process, produces effective password protection.

The passwords of the future could become more secure and, at the same time, simpler to use. Researchers at the Max Planck Institute for the Physics of Complex Systems in Dresden have been inspired by the physics of critical phenomena in their attempts to significantly improve password protection. The researchers split a password into two sections. With the first, easy to memorize section they encrypt a Captcha – an image that computer programs per se have difficulty in deciphering. The researchers also make it more difficult for computers, whose task it is to automatically crack passwords, to read the passwords without authorization. They use images of a simulated physical system, which they additionally make unrecognizable with a chaotic process. These p-Captchas enable the Dresden physicists to achieve a high level of password protection, even though the user need only remember a weak password.

Computers sometimes use brute force. Hacking programs use so-called brute-force attacks to try out all possible character combinations to guess passwords. CAPTCHAs (Completely Automated Public Turing test to tell Computers and Humans Apart) are therefore intended as an additional safeguard the input of which originates from a human being and not from a machine. They pose a task for the user which is simple enough for any human, yet very difficult for a program. Users must enter a distorted text which is displayed on the screen, for example. Captchas are increasingly being bypassed, however. Personal data of members of the "SchulerVZ" social network for school pupils have already been stolen in this way.

Researchers at the Max Planck Institute for the Physics of Complex Systems in Dresden have now developed a new type of password protection that is based on a combination of characters and a Captcha. They also use mathematical methods from the physics of critical phenomena to protect the Captcha from being accessed by computers. “We thus make the password protection both more effective and simpler,” says Konstantin Kladko, who had the idea for this interdisciplinary approach during his time at the Dresden Max Planck Institute; he is currently a researcher at Axioma Research in Palo Alto/USA.

The Dresden-based researchers initially combine password and Captcha in a completely novel way. The Captcha is no longer generated anew each time in order to distinguish the human user from a computer on a case-by-case basis. Rather, the physicists use the codeword in the image, which can only be deciphered by humans as the real password, which provides access to a social network or an online bank account, for example. The researchers additionally encrypt this password using a combination of characters.

However, that’s not all: the Captcha is a snapshot of a dynamic, chaotic Hamiltonian system in two dimensions. For the sake of simplicity, his image can be imagined as a grey-scale pixel matrix, where every pixel represents an oscillator. The oscillators are coupled in a network. Every oscillator oscillates between two states and is affected by the neighbouring oscillators as it does so, thus resulting in the grey scales.

Chaotic development makes password unreadable

The physicists then leave the system to develop chaotically for a period of time. The grey-scale matrix changes the colour of its pixels. The result is an image that no longer contains a recognizable word. The researchers subsequently encrypt this image with the combination of characters and save the result. “We therefore talk of a password-protected Captcha or p-Captcha,” says Sergej Flach, who teamed up with Tetyana Laptyeva to achieve the decisive research results at the Max Planck Institute for the Physics of Complex Systems. Since the chaotic evolution of the initial image is deterministic, i.e. reversible, the whole procedure can be reversed using the combination of characters, so that the user can again read the password hidden in the Captcha.

“The character combination we use to encrypt the password in the Captcha can be very easy to remember,” explains Konstantin Kladko. “We thus take account of the fact that most people only want to, or can only, remember simple passwords.” The fact that the passwords are correspondingly weak is now no longer important, because the real protection comes from the encrypted password in the Captcha.

On the one hand, the password hidden in the Captcha is too long for computers to be able to guess it using a brute-force attack in a reasonable length of time. On the other, the physicists use a critical system to generate the password image. This system is close to a phase transition: with a phase transition, the system changes from one physical state to another, from the paramagnetic to the ferromagnetic state, for example. Close to the transition, regions repeatedly form which temporarily have already completed the transition. “The resulting image is always very grainy. Therefore, a computer cannot distinguish it from the original it is searching for,” explains Sergej Flach.

“Although the study has just been submitted to a specialist journal and is only available online in an archive, it has already provoked a large number of responses in the community - and not only in Hacker News,” says Sergej Flach. “I was very impressed by the depth of some comments in certain forums - in Slashdot, for example.” The specialists are obviously impressed by the ingenuity of the approach, which means passwords could be very difficult to crack in the future. Moreover, the method is easy and quick to implement in conventional computer systems. “An expansion to several p-Captcha levels is obvious,” says Sergej Flach. Hoiwever, this requires increased computing power to reverse the chaotic development in a reasonable time: “We therefore want to investigate various Hamiltonian and non-Hamiltonian systems in the future to see whether they provide faster and even more effective protection.”

More information: Tetyana V. Laptyeva, Sergej Flach, Konstantin Kladko, The weak password problem: chaos, criticality, and encrypted p-CAPTCHAs, arXiv:1103.6219v1, 31. März 2011.
arxiv.org/abs/1103.6219

Provided by Max-Planck-Gesellschaft

Citation: Strong protection for weak passwords (2011, April 19) retrieved 27 April 2024 from https://phys.org/news/2011-04-strong-weak-passwords.html