PHYS.ORG

Password-cracking feats at blistering speed shown in Oslo

December 11 2012, by Nancy Owano

(Phys.org)—Remember when the running advice for password setup was to avoid using your name backwards? My how we have smelled the coffee. A new rig-and-burn presentation for an audience of academics and security professionals at the Passwords^12 Conference in Oslo, Norway, earlier this month, demonstrated that password-cracking is an easy game with crippling amounts of password theft capable of happening at crippling speed.

Researcher Jeremi Gosney, the founder and CEO of Stricture Consulting Group, was the thinker behind the hardware and software setup that could make 350 billion guesses per second. The result was that eight-character passwords could fall in hours; some passwords could be had in minutes. The deployment that was capable of 350 billion guesses per second was a five-server computer cluster with 25 AMD Radeon graphics cards and virtualization software. The password-penetrating design was able to unleash unexpected speed, ripping through Windows passcodes. *Security Ledger* runs a detailed account of the rig's specs and results. According to reports, his approach was enough to brute force eight-character passwords containing upper- and lower-case letters, digits, and symbols, in just hours.

The brute forcing algorithms went to work at speeds that are remarkable. He showed that with the right improved software and powerful hardware, such attacks are quite feasible. His setup is only relevant toward offline attacks, where the thief has already retrieved a password database or file. The cluster that he used would not be relevant to online attacks against a live system. His scenario applies to exploits involving collections of leaked or stolen passwords.

Gosney's success, however, in ripping through eight character passwords will only make security professionals that much more aware of what they already know, that older algorithms and shorter length passwords are vulnerable to attacks. System breaches leading to substantial password leaks have been part of news headlines for some time. Gosney said in an email to *Ars Technica* that "We can attack hashes approximately four times faster than we could previously." Gosney has been working on clustering approaches for the last four or five years.

The GPU cluster in his recent presentation uses a cluster platform to let each card function as if on a single desktop plus ocl-Hashcat Plus.

The general rule for computer users is to think about long and strong passwords, between 13 and 20 characters, if possible. If worried about choosing words that are too "common," users can turn to password management tools, which are designed to help a user create passwords that are less vulnerable.

More information: passwords12.at.ifi.uio.no/Jere … _HPC_Passwords12.pdf
securityledger.com/new-25-gpu- … asswords-in-seconds/
www.overclockersclub.com/news/33354/

Citation: Password-cracking feats at blistering speed shown in Oslo (2012, December 11) retrieved 29 April 2024 from
https://phys.org/news/2012-12-password-cracking-feats-blistering-shown-oslo.html