The power of graphics processing units may threaten the world's password security system

August 9 2010, by Rick Robinson

It's been called revolutionary - technology that lends supercomputer-level power to any desktop. What's more, this new capability comes in the form of a readily available piece of hardware, a graphics processing unit (GPU) costing only a few hundred dollars.

Georgia Tech researchers are investigating whether this new calculating power might change the security landscape worldwide. They're concerned that these desktop marvels might soon compromise a critical part of the world's cyber-security infrastructure - password protection.

"We've been using a commonly available graphics processor to test the integrity of typical passwords of the kind in use here at Georgia Tech and many other places," said Richard Boyd, a senior research scientist at the Georgia Tech Research Institute (GTRI). "Right now we can confidently say that a seven-character password is hopelessly inadequate - and as GPU power continues to go up every year, the threat will increase."

Designed to handle the ever-growing demands of computer games, today's top GPUs can process information at the rate of nearly two teraflops (a teraflop is a trillion floating-point operations per second). To put that in perspective, in the year 2000 the world's fastest supercomputer, a cluster of linked machines costing $110 million, operated at slightly more than seven teraflops.

Graphics processing units are so fast because they're designed as parallel computers. In parallel computing, a given problem is divided among multiple processing units, called cores, and these multiple cores tackle different parts of the problem simultaneously.

Until recently, multi-core graphics processors - which are made by either Nvidia Corp. or by AMD's ATI unit - were hard to use for anything except producing graphics for a monitor. To solve a non-graphics problem on a GPU, users had to couch their problems in graphical terms, a difficult task.

But that changed in February 2007, when Nvidia released an important new software-development kit. These new tools allow users to directly program a GPU using the popular C programming language.

"Once Nvidia did that, interest in GPUs really started taking off," Boyd explained. "If you can write a C program, you can program a GPU now."

This new capability puts power into many hands, he says. And it could threaten the world's ubiquitous password-protection model because it enables a low-cost password-breaking technique that engineers call "brute forcing."

In brute forcing, attackers use a fast GPU (or even a group of linked GPUs) - combined with the right software program - to break down passwords that are blocking them from a computer or a network. The intruders' high-speed technique basically involves trying every possible password until they find the right one.

For many common passwords, that doesn't take long, said Joshua L. Davis, a GTRI research scientist involved in this project. For one thing, attackers know that many people use passwords comprised of easy-to-remember lowercase letters. Code-breakers typically work on those

combinations first.

“Length is a major factor in protecting against brute forcing a password,” Davis explained. “A computer keyboard contains 95 characters, and every time you add another character, your protection goes up exponentially, by 95 times.”

Complexity also adds security, he says. Adding numbers, symbols and uppercase characters significantly increases the time needed to decipher a password.

Davis believes the best password is an entire sentence, preferably one that includes numbers or symbols. That’s because a sentence is both long and complex, and yet easy to remember. He says any password shorter than 12 characters could be vulnerable - if not now, soon.

Would-be password crackers have other advantages, says Carl Mastrangelo, an undergraduate student in the Georgia Tech College of Computing who is working on the password research. A computer stores user passwords in an encrypted “hash” within the operating system. Attackers who locate a password hash can besiege it by building a rainbow table, which is essentially a database of all previous attempts to compromise that password hash.

“Generating a rainbow table takes a long time,” Mastrangelo explained. “But if an attacker wants to crack many passwords quickly, once he’s built a rainbow table it might then only take about 10 minutes per password rather than several days.”

Software programs designed to break passwords are freely available on the Internet, Boyd says. Such programs, combined with the availability of GPUs, mean it’s only a matter of time before the password threat will be immediate.

Boyd hopes his password work will increase awareness of the GPU's potential for harm as well as benefit. One result of this research, he says, could be GPU-based workstations that would offer rapid assessments of a given password's real-world security strength.

Source: Georgia Institute of Technology