## New Supercomputer Is the World's Fastest

A 17.59-petaflops Cray Inc. supercomputer recently unveiled at the US Department of Energy's Oak Ridge National Laboratory has been recognized as the world's most powerful.

The Top500 project (www.top500.org), in which several academic and research experts list the world's fastest nondistributed supercomputer systems twice annually, ranked the Titan system in the top spot as of November 2012.

Titan's 17.59 petaflops—17.59 quadrillion ($20 \times 10^{15}$) floating-point operations per second—makes it faster than the 16-petaflops IBM Sequoia computer at the US Lawrence Livermore National Laboratory. The Top500 project rated Sequoia as the world's fastest in its June 2012 rankings.

To create Titan, Cray upgraded its Jaguar machine—once the world's most powerful—at Oak Ridge. Cray replaced Jaguar's 224,256 CPUs with 299,008 faster AMD chips and added 18,688 Nvidia GPUs, which act as CPU accelerators. This lets Titan offer nine times Jaguar's performance with just one-third more CPUs.

Running at just 2.3 petaflops, Jaguar required 7 megawatts of energy, enough to power 7,000 homes. Expanding the supercomputer without making it more energy efficient wouldn't have been practical, according to Oak Ridge. However, the new AMD chips are five times more energy efficient than Jaguar's CPUs. Thus, Titan requires only 8.2 megawatts of power, making its energy costs only a bit more than Jaguar's.

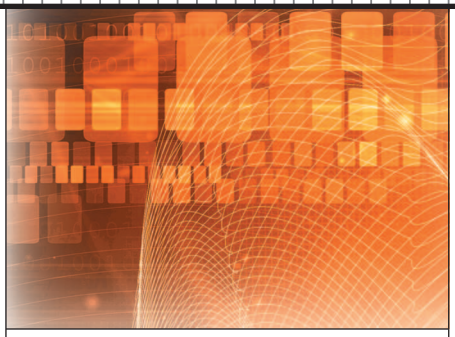
Oak Ridge plans to use Titan—which has 710 terabytes of memory—for computer simulations and other types of research in areas such as climate change, biofuels, nuclear energy, and new materials.

By 2016, the Department of Energy plans to upgrade the system so that it will perform 200 petaflops.


**Cray's new 17.59-petaflops Titan supercomputer, used at the US Oak Ridge National Laboratory, is now the world's fastest system.**

## Researchers Turn the Tables on Sophisticated Hackers

Researchers with the country of Georgia's Computer Emergency Response Team planted malware on the computers of hackers who had been placing the same malicious software on numerous governments' computers to steal important national-security documents.



The researchers even used the malware to activate an embedded camera in one of the targeted machines and take photos of one of the hackers.

Investigators say their counterstrike enabled them to electronically infiltrate the group behind the Georbot Botnet, which used sophisticated techniques to break into the systems of government ministries, legislative bodies, banks, and nongovernmental organizations in Canada, China, France, Georgia, Germany, Russia, Ukraine, and the US in 2011 and 2012.

The hackers attacked Georgian computers by exploiting software vulnerabilities and by placing malicious hyperlinks on news-related and other webpages they hoped their intended victims would visit. When someone visited these pages, their browsers automatically executed a hidden script that uploaded the TrojanDownloader:JS/SetSlice malware installation tool. The tool used known Windows vulnerabilities to secretly download a malicious executable.

Once on a machine, the malware scanned Word, PDF, Excel, text, rich-text, and PowerPoint files for keywords such as "NATO" and "CIA" to identify documents worth stealing. The hackers also compromised machines' microphones and webcams to eavesdrop on victims.

Georgia's CERT investigators began investigating the attacks with help from the US Federal Bureau of Investigation, the US Computer Emergency Readiness Team, and various Eastern European cyberemergency-response groups.


Published by the IEEE Computer Society
0018-9162/12/$31.00 © 2012 IEEE

Eventually, the researchers learned details about the malware the hackers used, as well as the way they spread and controlled it. The team then blocked the command-and-control computers the hackers used and removed the malware from compromised machines.

The investigators installed malware on one of the hackers' computers by placing on one of their own machines an infected ZIP file named "Georgian-NATO Agreement," which they figured—correctly—the attackers would try to steal. The malware activated a camera on one of the hackers' computers and took photos of him. The investigators also were able to identify information such as his home city, ISP, and email address.

The Georgian CERT team said they tracked the recent attacks to the Russian Ministry of Internal Affairs. The two countries are on bad terms and fought a brief war in 2008.

## Alliance Certifies Technology to Improve Wi-Fi Performance

The Wi-Fi Alliance, an international trade organization, has begun certifying technology designed to create direct links between mobile devices, bypassing access points (APs) and making wireless communications more efficient.

The efficiency could improve wireless activities such as media streaming, data backup, printing, and file transferring, and could extend devices' limited battery life.

The Wi-Fi Alliance has started certifying devices that comply with Tunneled Direct Link Setup (TDLS) technology, which is based on the IEEE 802.11z standard.

Typically, mobile devices communicate via an AP in a star topology. TDLS defines mechanisms that let Wi-Fi networks automatically set up a direct link between the devices while they are still connected to the AP. The technology does this by tunneling the protocol messages inside data frames.

Eliminating the AP connection makes communications more direct and bypasses AP congestion. In addition, TDLS lets devices communicate via the fastest Wi-Fi version and with the most security available, even if it's more than what the AP supports.

Devices could also measure network signal strength and decide whether a direct link would be better. The process starts when one device sends a discovery request to another via the network to determine whether it is also TDLS-compliant. If so, the target device sends a response detailing its capabilities.

The TDLS certification program will be available for TVs, smartphones, tablet computers, cameras, printers, PCs, projectors, and gaming devices. Companies such as Broadcom, Marvell, Ralink Technology, and Realtek Semiconductor are already participating in the program.

Wi-Fi Direct technology also lets wireless devices connect directly, but it works via a limited wireless AP embedded in the devices and requires some user intervention.

## US ISPs Adopt Plan to Curb Copyright Violations

After four years of preparation, some of the US's biggest ISPs are instituting a plan to discourage online users from violating copyrights held by content owners.

## MAN CLIMBS SKYSCRAPER STAIRWAY USING BRAIN-CONTROLLED PROSTHETIC LEG

**A Washington state man who lost his lower leg in a motorcycle accident has climbed the 2,100 stairs of one of the world's tallest buildings using a prosthetic leg he controlled with his thoughts.**

**Zac Vawter of Yelm, Washington, put the limb through its paces by climbing the 103 floors of Chicago's Willis Tower, formerly called Sears Tower and once the world's tallest building.**

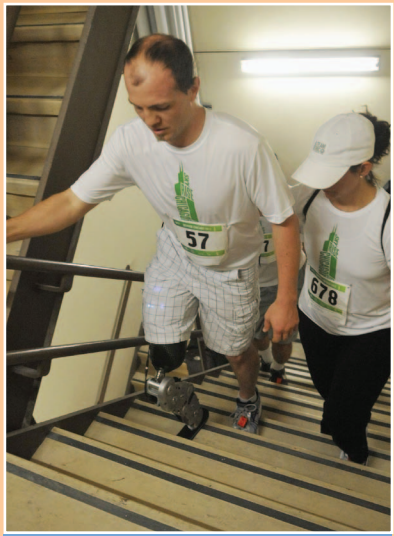
**Vawter—accompanied by 2,700 climbers from 38 states and seven countries—ascended the stairs as part of the Rehabilitation Institute of Chicago's annual SkyRise Chicago fund-raising event. He is receiving treatment at the facility.**

**The surgeon who amputated Vawter's lower leg reattached to his hamstring muscle the nerves that previously carried signals past his knee. When Vawter thinks about climbing, signals from those nerves that formerly made his lower leg move are redirected to equipment in the 10-pound prosthetic limb. The equipment then activates and coordinates the leg's two motors, belts, and chains.**

**Brain-controlled prosthetic arms have been around for several years. Recently, the Rehabilitation Institute has been focusing on leg amputees, who outnumber those who have lost arms or hands.**

**Institute officials wanted Vawter to use the leg on the Willis Tower climb so that they could test it under extreme conditions. They say researchers still must refine the prosthetic leg and don't expect to release it commercially for several years.**

**The $8 million project is funded by the US Department of Defense and includes researchers from Vanderbilt University, MIT, the University of Rhode Island, and the University of New Brunswick.**




**Zac Vawter, who lost a leg in a motorcycle accident, used a brain-controlled prosthetic limb to climb 2,100 stairs to the top of Chicago's 103-story Willis Tower.**

The Copyright Alert System, supported by movie studios and music distributors, would impose escalating mitigation measures for repeat violations.

The Center for Copyright Information—which the Motion Picture Association of America and the Recording Industry Association of America founded to work on the new system—anticipates the plan will take effect later this year. ISPs AT&T, Cablevision Systems, Comcast, Time Warner Cable, and Verizon have agreed to participate.

Until now, many ISPs simply forwarded copyright-infringement notices from content owners to subscribers. There hasn't been a common approach for effectively dealing with ongoing violations.

With the Copyright Alert System, when an ISP receives notices from a copyright holder about infringements, the provider will notify the subscribers involved that someone used their account for content theft and inform them that this is illegal and that penalties could result. Failure to comply could lead to popup notifications, educational messages, Internet-speed reductions, or redirection to a landing page until the subscribers contact their ISP.

The Copyright Alert System doesn't call for ISPs to filter content that infringing users access or to terminate their service. However, federal law requires that ISPs have a termination policy for repeat copyright violators.

Subscribers accused of infringement who pay a $35 filing fee to an arbitrator could ask for a review of their situation before an ISP imposes mitigation measures.

The Center for Copyright Information says content theft in the US annually costs $58 billion in revenue for companies, 373,000 jobs, $16 billion in employee earnings, and $2.6 billion in tax revenue for federal, state, and local governments.

## Smart Meters Are Not Always So Smart

Some smart utility meters are transmitting unencrypted information that hackers could intercept to determine, for example, if a building is occupied, according to University of South Carolina researchers. This could leave homes vulnerable to burglary or other problems.

Automatic-meter-reading devices are an early smart-meter technology found in about one-third of US homes and businesses. Some of these AMR devices automatically collect consumption, diagnostic, and other information from water, electric, and gas meters and send it via a network to a database for billing and analysis. Utility workers can also use the devices to gather information via a handheld collection wand.

The University of South Carolina team found that one type of AMR meter broadcasts information every 30 seconds, unlike those that send information only when requested by the host utility system.

Using a basic software-defined radio, an amplifier, and open source radio software, the researchers discovered that they could intercept meter signals, after learning that they could predict the various frequencies that the devices use to transmit signals.

Within a few days, after reviewing documentation on the Internet and information the meter makers publicly provide, the team determined how the devices' proprietary technologies worked.

The researchers then captured transmitted packets from 106 electric meters in the area they tested and identified the data. The information was sent in plaintext and included the device's identification number—which could help identify the metered structure's address—and its utility-usage reading. They said they could determine a household's average power usage and identify periods of time when no one is likely to be home.

Newer smart-meter technology encrypts information that is transmitted wirelessly. However, the 46 million AMR meters in the US will require considerable time to replace.



**Editor: Lee Garber, *Computer*;**
**l.garber@computer.org**